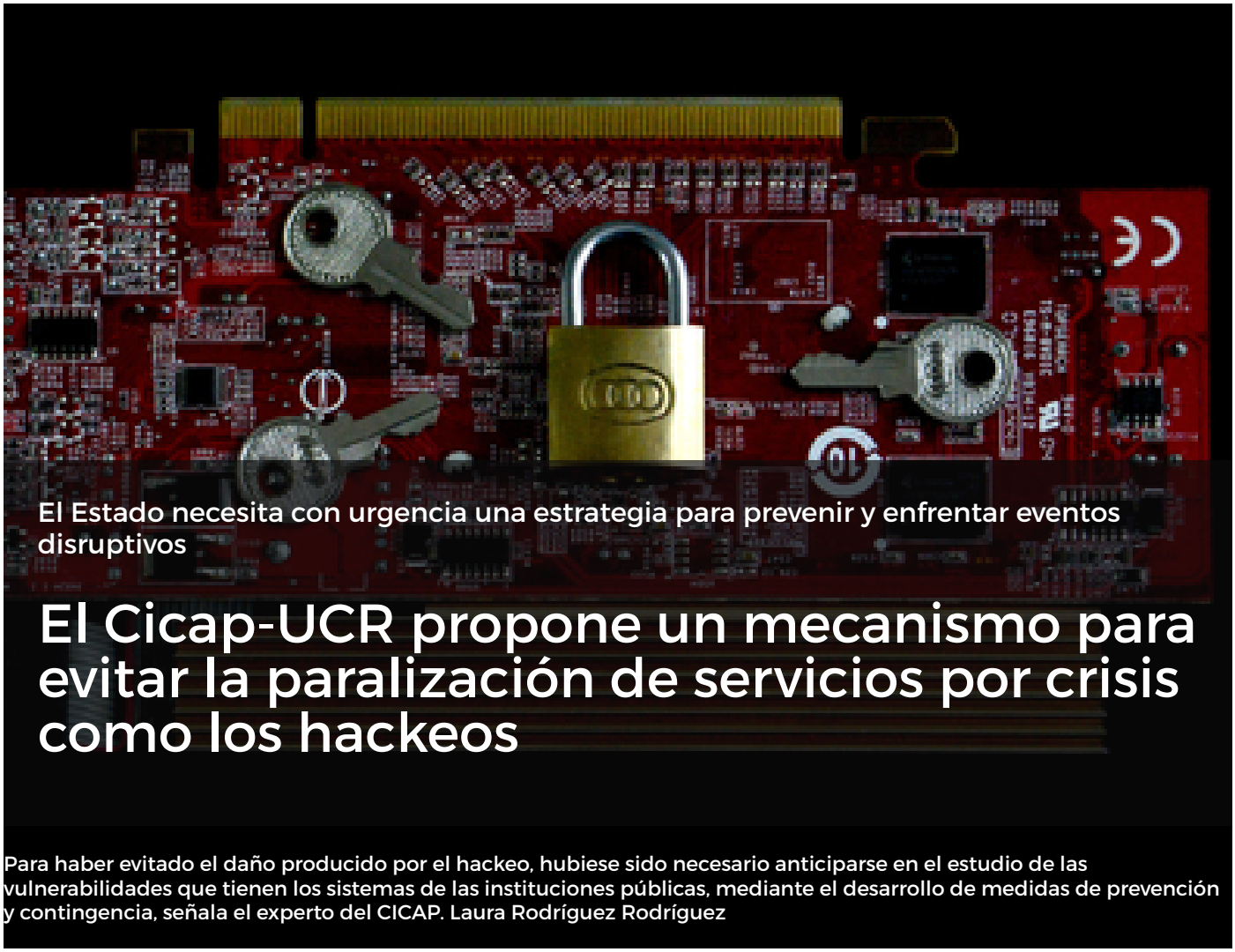
UNIVERSIDAD DE COSTA RICA



El Estado necesita con urgencia una estrategia para prevenir y enfrentar eventos disruptivos

El Cicap-UCR propone un mecanismo para evitar la paralización de servicios por crisis como los hackeos

Para haber evitado el daño producido por el hackeo, hubiese sido necesario anticiparse en el estudio de las vulnerabilidades que tienen los sistemas de las instituciones públicas, mediante el desarrollo de medidas de prevención y contingencia, señala el experto del CICAP. Laura Rodríguez Rodríguez

La norma INTE/ ISO 22301 “Sistema de Gestión de Modelo de Continuidad de Negocios” da pautas para garantizar el funcionamiento de una organización ante situaciones críticas

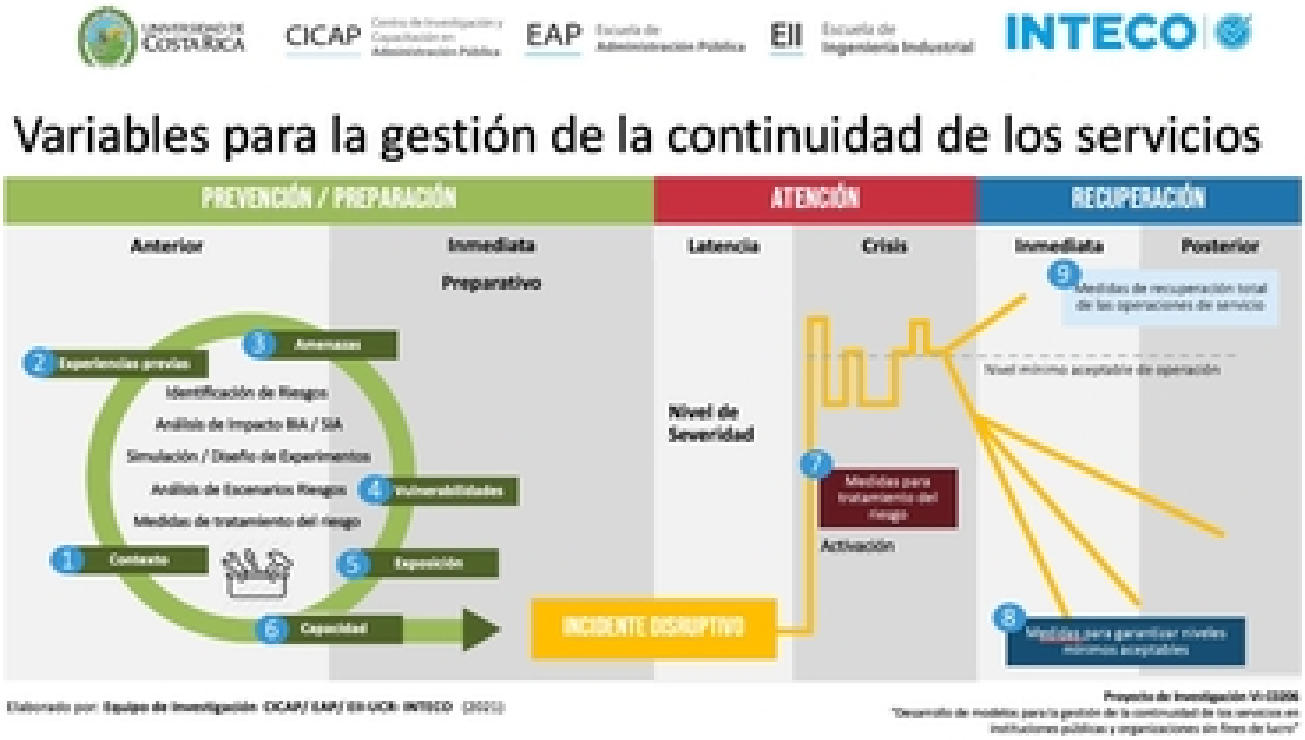
23 JUN 2022 Economía

Hoy es el hackeo de los sistemas en instituciones estatales. Antes fue la pandemia. Mañana puede ser un terremoto, un huracán, otra pandemia, una huelga, una crisis política, un bloqueo o cualquier evento humano o natural de esos que acostumbramos a ver en el país. Son muchos los factores en este “**contexto multiamenaza**” que pueden dañar el funcionamiento del Estado, dejándolo inoperante y prácticamente congelado, al punto de volver a utilizar procedimientos dignos del siglo XX: con papel y lapicero...

Esto, a menos claro, que se tomen las **previsiones necesarias** para reducir o eliminar el impacto de eventualidades o fenómenos como los descritos. Porque tampoco se trata de inventar el agua caliente. De hecho, el modelo de gestión existe desde hace varios años y hasta cuenta con una norma internacional de calidad INTE/ ISO 22301: “Sistema de Gestión de Modelo de Continuidad de Negocios”.

Esta norma ya ha sido aplicada por empresas de clase mundial y a raíz de sucesos de escala global, como el atentado terrorista a las Torres Gemelas en Estados Unidos en 2001, que afectó el comercio y el transporte aéreo significativamente. En Costa Rica, sobre todo a raíz de la aparición de la pandemia hace más de dos años, ya se planteó la necesidad de generar un esquema similar adaptado a instituciones estatales.

En la Universidad de Costa Rica (UCR), desde el año 2018, el Centro de investigación en y Capacitación en Administración Pública (CICAP) comenzó a analizar este tema para su aplicación en el Estado. Y ya en el 2020, en conjunto con la Escuela de Administración Pública, la Escuela de Ingeniería Industrial y el Instituto de Normas Técnicas de Costa Rica (INTECO), se estudiaron **métodos, normas y buenas prácticas** para que las organizaciones estatales tuvieran modelos de continuidad para los distintos servicios, a fin de **fortalecer los servicios públicos** que requiere la población.



Actualmente, estas instancias desarrollan un proyecto de investigación inscrito en la Vicerrectoría de Investigación para ampliar su incidencia en las instituciones públicas. La propuesta consta de tres fases: la primera es de **prevención**, la segunda se enfoca en el **momento disruptivo** y la tercera es de **recuperación**.

El investigador del CICAP, Rodolfo Romero, explica que la prevención es el paso más importante de los tres y es aquí donde se debe realizar una **mayor y mejor inversión de tiempo y recursos**. Una buena identificación de las amenazas externas, de las vulnerabilidades del sistema y de las capacidades de respuesta puede minimizar o eliminar la afectación producto de un hackeo, o de cualquier otro evento de gran escala.

Rodolfo Romero, investigador del CICAP: medidas preventivas en el modelo de continuidad de servicios

Romero fue claro en advertir que la **mala preparación en la ciberseguridad de algunas instituciones estatales debió preverse y evitarse**, sobre todo en una institución clave para la salud de la población como la Caja Costarricense de Seguro Social. Enfatizó que si se tiene la percepción de que, tarde o temprano, un evento como el hackeo va a ocurrir, es necesario anticiparse en el estudio de las vulnerabilidades que tienen los sistemas de las instituciones públicas, por medio de un análisis robusto para desarrollar medidas de prevención y contingencia pertinentes en cada institución.

Una solución propuesta por este experto es haber recurrido a sistemas de respaldo redundantes para que la información no se perdiera ante el robo y encriptación de datos que causaron las bandas cibercriminales. El investigador del CICAP subraya en que, **por cada dólar** que el país hubiese invertido en seguridad digital, **se hubiera ahorrado entre cuatro y cinco veces más de esa suma**, que será el costo de la recuperación de estos ataques.

En el ojo del huracán

La siguiente etapa por considerar es el **lapso durante el cual ocurre la crisis**. Como se mencionó al inicio, la parte de prevención será fundamental para que esta segunda sea más llevadera. Esto generará menos presión sobre las medidas de mitigación o contingencia, y además creará un **efecto psicológico de fortaleza** y confianza en el engranaje institucional.

Para Romero, la **colaboración entre el sector público y el privado** es vital para disminuir el impacto de estas disrupciones en los servicios que se brindan a la población y las funciones del Estado.

Rodolfo Romero, investigador del CICAP: medidas a tomar durante el momento disruptivo

Finalmente, está la **fase de recuperación**. Y en esta también influye la etapa de preparación ante la crisis. El investigador del CICAP afirmó que si se conocen de antemano los procesos críticos y cuáles pueden ser los niveles mínimos de operación funcional de cada institución, será más rápido y simple volver a una normalidad óptima.

Además, Romero explicó que, tras un evento disruptivo, **se debe extraer qué es lo más importante de reactivar** para darle prioridad a este proceso, sin que esto signifique resolver todos los problemas ocasionados por el fenómeno sufrido al mismo tiempo.

Dentro de esta última etapa, el experto recordó que la **evaluación de cómo actuó el modelo de continuidad** en la institución es también fundamental para tener claridad sobre por qué y cómo ocurrió la crisis. Además, se debe establecer si la medidas planeadas para atenuar los impactos respondieron según los objetivos trazados.

Rodolfo Romero, investigador del CICAP: recuperación y evaluación claves en continuidad de servicios

En todo caso, y como ocurre en las diversas áreas de la vida, cometer errores también es válido para **entender en qué se falló** y cómo la organización debe **reaccionar mejor** ante la siguiente situación disruptiva.

En el caso de la UCR, la Sede de Occidente ya cuenta con un modelo diseñado que considera todas estas posibilidades. Esta **estrategia fue generada por un grupo de estudiantes** de la Escuela de Ingeniería Industrial, vinculado a esta investigación.

Integrantes del proyecto de investigación "Desarrollo de modelos para la gestión de la continuidad de los servicios en instituciones públicas y organizaciones sin fines de lucro"

Por el CICAP y EAP:

Catalina Artavia Pereira

Catalina Esquivel Rodríguez

Álvaro Montero Sánchez

Rodolfo Romero Redondo

Estudiantes de la EII:

Lisa Campos Pérez

Jorge Esquivel Arias

Daniela Varela Rojas

Marcela Piñeiro Retana

Por INTECO:

Alexandra Rodríguez Venegas

Felipe Calvo Villalobos

Pablo Mora Vargas
Periodista, Oficina de Divulgación e Información
pablo.moravargas@ucr.ac.cr

Etiquetas: eventos disruptivos, crisis, modelo de continuidad, hackeo, hackers, pandemia.