trendTIC

Fecha: 30/10/2024 Audiencia: 0 Sección: CIENCIA Y TECNOLOGIA
Vpe: $0 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $0 Difusión: 0
Vpe portada: $0 Ocupación: 92,85%

ChileCompra tras ciberataque del 2023: como un incidente grave genera un giro virtuoso y mayor estrategia en ciberseguridad

"Esto no nos puede estar pasando", fue seguramente un pensamiento generalizado en el war room de ChileCompra aquel 12 de septiembre de 2023, día en que la entidad a cargo de todas las adquisiciones públicas del Estado de Chile sufriera un ciberataque, dejando sin operaciones la plataforma de ChileCompra durante 8 días, cuatro de ellos hábiles, con un potencial impacto a 1.000 organismos del Estado y a más de 120.000 proveedores. ¿El culpable? Un ransomware que afectó a IFX Networks, de origen colombiano, quien era el proveedor tecnológico de la plataforma en ese entonces. Los aprendizajes han sido múltiples y muy satisfactorios tras el incidente. Sin embargo, desde aquel 12 de septiembre, nada ha vuelto a ser lo mismo para los encargados de ciberseguridad en ChileCompra.

A partir de la fecha del incidente, ChileCompra ha analizado y generado una serie de materiales, estrategias y valiosos aprendizajes para aumentar la capacidad y efectividad de respuesta ante ataques de ciberseguridad. Para contextualizar el relato, debemos mencionar que tras verificar que las bases de datos no estuvieran infectadas, el día 19 de septiembre 2023 ChileCompra habilitó la plataforma en línea alojada en su sitio de contingencia y el 20 de octubre de 2023 la plataforma ya contaba con una operación normal, dando total seguridad a sus usuarios de que la data estaba 100% segura.

Interesantes es el estudio que realizó la Universidad de Chile con el Instituto de Sistemas Complejos de Ingeniería, con el profesor Marcelo Olivares, donde se concluyó que los montos transados durante la caída se recuperaron en su totalidad a la semana siguiente. Efectivamente hubo un estrés en ese momento porque no se podía comprar, pero en las semanas siguientes existió la recuperación y no hubo pérdidas (Ver recuadro).

Paolo Jeldres
Jefe de Seguridad de la Información y Ciberseguridad
ChileCompra

Desde ChileCompra complementan que contaban con un Plan de Recuperación de Desastres (DRP, por sus siglas en inglés) acotado, lo que permitió recuperar un respaldo de los datos de compras públicas y levantar, tras ocho días de caída, una plataforma en un sitio de contingencia con otro proveedor, el que contaba con los principales módulos utilizados por los usuarios compradores y proveedores. Hoy en día, y tras haber sufrido el peor incidente en su historia, ChileCompra entiende que el DRP es un componente de algo mucho más crucial: el Plan de Continuidad del Negocio (BCP, por sus siglas en inglés).

"Si bien teníamos un DRP donde podíamos migrar toda nuestra operación a otro site, cuando nos migramos, la capacidad del segundo site no era adecuada para la operación que tenía que soportar dentro de Mercado Público", explica Paolo Jeldres, Jefe de Seguridad de la Información y Ciberseguridad en ChileCompra.

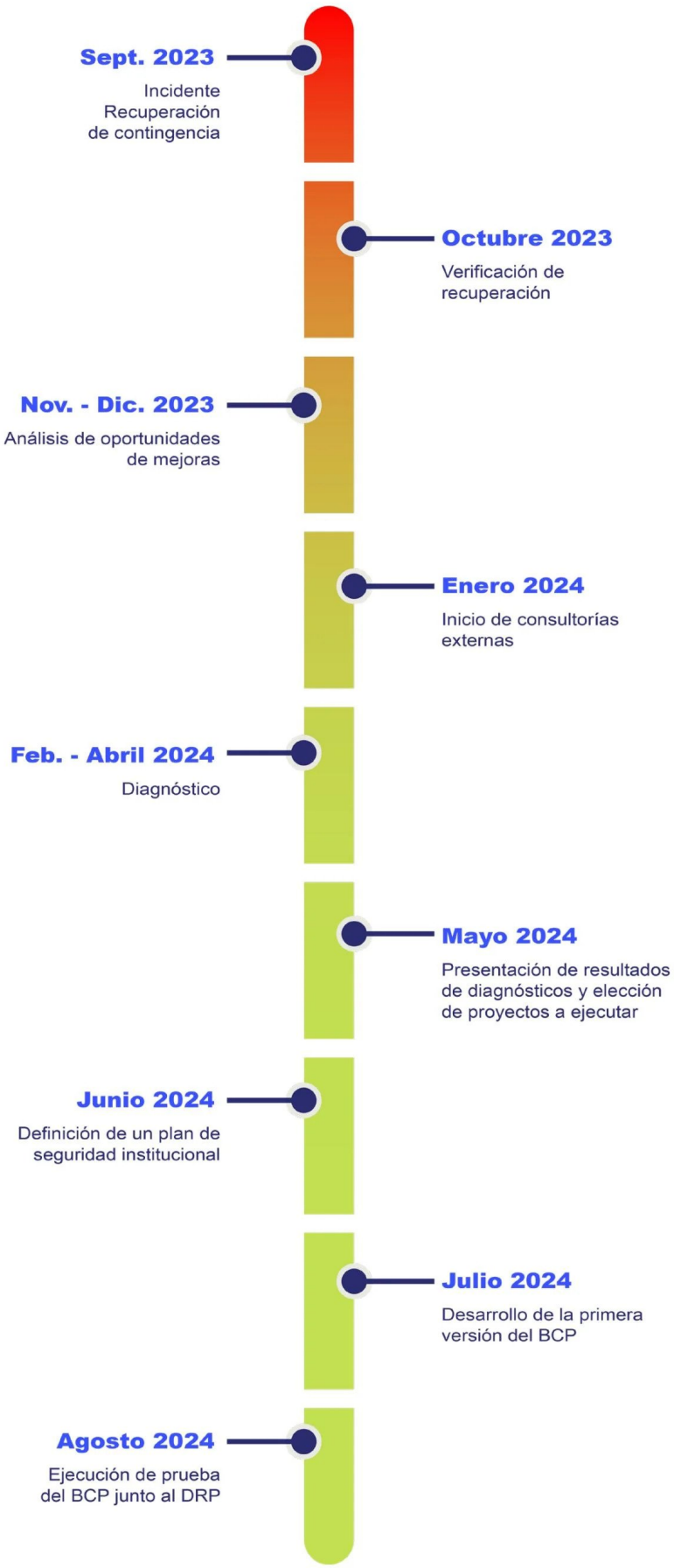
Más allá del BCP:

La importancia de las personas, la resiliencia y la colaboración interinstitucional

"Cuando uno se ve enfrentado a un incidente de esta magnitud se genera una suerte de impresión y como de paralización. Además, el incidente crece más y más, entonces todos los que participan del war room quedan algo pasmados en algún momento, pero comienzan a reaccionar cuando asimilan la situación y hay que tomar acciones", dice el experto de ChileCompra. "Es allí donde comienzan a aparecer los talentos naturales de las personas; algunos lo enfrentan desde el lado del liderazgo para coordinar acciones y otros son aquellos que tienen conocimientos duros del negocio y son ellos quienes comienzan a operar los planes de contingencia. El documento del BCP no funcionó, pero las personas sí"

Jeldres enfatiza que en ChileCompra hay gente que posee mucha experiencia con un acabado conocimiento de los procesos del negocio, tanto de compradores como de proveedores, lo que se enlaza a su vez con mensajes comunicacionales hacia el resto del equipo, que en definitiva fue lo que se hizo, "donde se generó una sincronización perfecta entre el área de negocios y comunicaciones, lo que decantó en que se fuera comunicando a los usuarios de Mercado Público", señala el ejecutivo.

Sin embargo, y a pesar de la calidad de los colaboradores, Jeldres indica que es clave establecer paso a paso un plan de continuidad operacional. "Si bien, efectivamente existieron esos planes de contingencia, estos estaban más en la cabeza de las personas, lo que nos lleva a pensar que dependemos mucho de la experiencia que tienen las personas que allí trabajan. Sin embar-



go, creo que para evitar contratiempos y estrés incluso, es importante que esto esté documentado y allí es super relevante que el BCP esté documentado".

Otra de las lecciones más valiosas fue la importancia de la coordinación y colaboración entre los diferentes servicios públicos. "En este caso tuvimos el apoyo de los directores de tecnología del Servicio de Impuestos Internos y DIPRES; por lo tanto, esta colaboración entre pares es una lección que también es útil para el resto. También tuvimos el apoyo del equipo de respuesta ante incidentes del Ministerio del Interior-CSIRT, que es clave", dice Paolo Jeldres.

Jeldres enfatiza que es necesario adoptar un enfoque proactivo en temas de ciberseguridad, el cual esté presente del principio en todos los proyectos que requieren la digitalización de procesos de negocios. Esto no puede ser una revisión al final del término del proyecto. "Lo importante es garantizar la continuidad de las operaciones, al menos de los procesos críticos, lo que se realiza a través de un plan de continuidad del negocio que se pruebe constantemente", señala.

BCP en 1 mes y diez días: ¿cómo lo hicieron?

Las mejoras para todo el sector público en temas de ciberseguridad resultan imperiosas. La ciberseguridad no es necesariamente un problema de tecnología, sino que de establecer procesos.

"En las primeras reuniones con los encargados, nunca se habló del documento del BCP, pero no porque no exista, es porque es un documento que no se prueba y no se actualiza, queda rápidamente obsoleto. Todo surgió a partir de las cabezas de las personas que estuvieron en ese momento reunidas. Hay que tener una guía, una ruta que oriente, para no aumentar el estrés del equipo. Se realizó un diagnóstico de todo el equipo posterior al incidente, donde surgieron 18 oportunidades de mejora en ciberseguridad, es decir, 18 iniciativas o proyectos", detalla el ejecutivo.

La clave es clara: la continuidad del negocio y las operaciones críticas. Desarrollar un plan de continuidad de negocios (BCP) que considere el levantamiento de las necesidades de resiliencia de los procesos de la institución, además de un plan de recuperación de desastres (DRP). "Tuvimos que armar un Plan de Seguridad Institucional, que tiene Controles de Seguridad, Concientización y

un Plan de Continuidad del Negocio

Primero que todo Jeldres detalla el paso a paso que tuvieron que realizar, donde destaca las medidas inmediatas que se tomaron: la creación del Comité Técnico, conformado por el Jefe de división de tecnologías, Jefe departamento de operaciones, Ingenieros DevOps que se requieran, Jefe de seguridad de la información y ciberseguridad (encargado del comité), Ingenieros de ciberseguridad que se requieran, Proveedores, Otros profesionales de Chile Compra. Y la conformación del Centro de Comando, conformado por los jefes de la Institución

"Luego generamos un Generamos un Producto Mínimo Viable (MVP, por sus siglas en inglés), el cual se probó el 10 de agosto, donde los alcance y objetivos del plan BCP fueron los procesos de negocio críticos que apalanca la plataforma, tales como orden de compra, licitaciones, convenio marco, compra ágil trato directo, entre otros. Mantener la operatividad de los procesos de negocios críticos, así como comunicar de manera efectiva con todas las partes interesadas, también es clave", explica Paolo.

ESTUDIO UNIVERSIDAD DE CHILE

El estudio "Asesoría experta e investigación vinculada a la caída de Mercado Público: Cuantificación de los impactos y lecciones aprendidas", indica que el ataque no afectó la competitividad y la participación de proveedores en los procesos de compra efectuados por los organismos del Estado en 2023. Esto debido a que las entidades públicas transaron en las semanas posteriores (entre 20 de septiembre y 31 de octubre) al ciberataque más de 150 mil millones de pesos, sin un efecto negativo en la competitividad y la participación de proveedores en los procesos, dado que se efectuó una mayor transacción de montos a través de licitaciones públicas.

Asistentes al taller de ciberseguridad: "un año del ciberataque, lecciones aprendidas y mejoras en la plataforma de Mercado Público". Organizado por la Dirección ChileCompra y el CSIRT de Gobierno.

Si pudiéramos entregar recomendaciones para crear una primera versión de un BCP, debemos mencionar: contar con el apoyo de la alta dirección de la institución, mantener la simplicidad del documento (un paso a paso para poder operar), definir los procesos de negocio críticos, establecer fechas límites cercanas e involucrar a todas las áreas claves.

Tecnológicamente hablando: ¿cómo opera hoy el BCP y DRP?

"Convengamos que el DRP es un componente del BCP. El DRP que proyectamos en el mediano plazo estará en la nube. Actualmente tenemos dos site (nubes privadas), y queremos que uno de ellos sea la nube de Google y allí alojar la mayor parte de nuestro sistema y lo que apalanca Mercado Público, pero que nos permita no generar tantos costos, porque actualmente nuestro site de contingencia debemos tenerlo con la misma capacidad que tiene el site primario para que pueda responder por completo a una contingencia como la del año pasado", señala Jeldres.

En este caso la nube entrega elasticidad, porque permite tener una capacidad que está dormida, pero cuando surge una contingencia y el site primario, por ejemplo, desaparece, automáticamente se activa este secundario que está en la nube; gracias a su elasticidad, da el ancho para que todas las operaciones de Mercado Público sigan respondiendo de la misma manera como lo hacían en el primario.

"Es allí donde comienzan a aparecer los talentos naturales de las personas; algunos lo enfrentan desde el lado del liderazgo para coordinar acciones y otros son aquellos que tienen conocimientos duros del negocio y son ellos quienes comienzan a operar los planes de contingencia. El documento del BCP no funcionó, pero las personas sí"

"En este desafío estamos con nuestro DRP, el cual esperamos probar de aquí a fin de año. Hicimos ya una prueba del BCP en paralelo con el DRP. Nuestra estrategia es probar el DRP de manera modular, donde todas las semanas estamos haciendo determinadas pruebas, tanto de bases de datos, servidores virtuales y también a nivel de redes. Todos estos testeos los estamos probando con la lógica actual del DRP, la que probamos el 10 de agosto de este año, todo lo que tiene que ver con Google en la nube, estamos probando básicamente conexiones y tratar de establecer eso de manera robusta y sólida para poder llegar ojalá a fin de año a realizar una prueba general desde la nube", detalla el ejecutivo.

A modo de recomendación, Paolo Jeldres es enfático y muy conciso: "No basta con tener un documento de BCP, sino que es crucial concientizar a todos los actores, probarlo regularmente y perfeccionarlo continuamente para adaptarlo a diversos escenarios", Finaliza.