

¿LA ALTA GERENCIA “GASTA” EN PLANES DE CONTINUIDAD Y CONTINGENCIA?

Por **Alberto Ramírez Ayón**, CISM, CISA

En la triada de seguridad de la información existen los siguientes conceptos: Confidencialidad, Integridad y Disponibilidad. La Disponibilidad puede entenderse como el concepto de asegurar que la información (incluyendo los sistemas) puedan ser accedidos cuando se requiera.

¿Por qué son importantes los planes de continuidad y contingencia? ¿Será para justificar la inversión de tecnología, recursos materiales o humanos? ¿Acaso para pasar sólo las auditorías internas y externas?

En el transcurso de la historia hemos visto como desastres naturales, errores humanos, actos de terrorismo, accidentes, etcétera, han ocasionado que empresas y bancos pierdan información vital para su negocio. Hoy en día cualquier corporación o firma requiere -de manera imperativa- contar con una estrategia que le permita recuperarse de una situación imprevista, para poder garantizar la continuidad de los servicios y productos a sus clientes y accionistas. Las corporaciones deben contar con mecanismos que le provean elasticidad para regresar al punto o posición original. En la actualidad contamos con un seguro para los autos; sin embargo, esperamos nunca tener que usarlo. Bueno, pues de ese mismo modo hay que ver una infraestructura que permita continuar brindando los servicios mínimos e indispensables. Algunos sectores tienen mayor regulación para que las empresas cuenten con planes, tales como el sector financiero, el cual está sometido a auditorías de varias entidades externas.

Para verificar el cumplimiento y efectividad de los procesos de “recuperación ante de desastres”. Se auditan los planes y las pruebas que se realicen para corroborar que dichos planes permitirán la operación.

Los tiempos han cambiado y actualmente encontramos estándares, políticas, manuales, procedimientos, mejores prácticas internacionales, marcos de referencia. Pero muchas veces, las áreas que gestionan estos esfuerzos, se ven detenidas ya que, en ocasiones, la alta gerencia y dirección no encuentra el beneficio real de destinar recursos o tener una infraestructura para una “contingencia”. Y es ahí, donde se deben mostrar los riesgos de NO contar con ésta. Dependerá del giro, tamaño, número de personas, presupuesto, diversos factores, incluso geográficos, sociales y de otras índoles en cada caso. A los ojos de algunos, todo este “rollo” es un gasto mas no una inversión.

¿Se han puesto a pensar en el impacto financiero, de imagen, social o legal que podría acarrear el no contar con una estrategia ante un desastre? No sólo basta con tener respaldos de las bases de datos y sistemas. ¿Estamos guardando suficiente historial de transacciones u operaciones? No es suficiente contar con un servidor alterno ¿Sino saber si cuenta con los mismos niveles de seguridad que el de producción? No es solamente que algunas personas tengan laptops o equipos móviles, sino entender el impacto si el sistema que soporta dicho dis-

positivos no está disponible. Cualquier esfuerzo tecnológico se puede ver mermado si la estrategia no es parte del negocio. En otras palabras, que ésta tenga el soporte y compromiso de la alta gerencia para asegurar la DISPONIBILIDAD.

SÓLO PUEDES ESPERAR LO INESPERADO

Es importante realizar un análisis de impacto al negocio, el cual identifique y cuantifique -de forma cuantitativa y cualitativa- el impacto en caso de una potencial pérdida o interrupción a los procesos de una organización. Priorizar los procesos críticos que coadyuvan a cumplir con las metas y se alinean a la misión de cualquier entidad. Clasificar los procesos y los tiempos máximos tolerables para estar con una interrupción.

Hay que evaluar cuáles son las amenazas que pueden explotar vulnerabilidades dentro de la organización, así como su probabilidad de ocurrencia. Alguna vez escuché una frase en inglés: *Expect the unexpected*, la cual refleja una realidad que debemos entender. Los planes deben contemplar desde la estrategia de alto nivel de negocio, hasta los procedimientos técnicos sobre telecomunicaciones, bases de datos, y en general la infraestructura tecnológica. Un árbol de llamadas de las personas claves en el proceso; procedimientos claros para la declaración de contingencia. El personal debe saber qué es lo que tiene que hacer. Si hay un sitio alterno, deben saber dónde está, cómo llegar, quiénes irán y qué es lo que deberán hacer. Opciones hay muchas. Habrá que evaluar de acuerdo a diferentes factores, incluyendo el presupuesto, la solución que se requiere.

Sin lugar a duda, uno de los principales factores de éxito de cualquier iniciativa de este tipo, es contar con el compromiso de la alta gerencia y dirección; ergo, hay que comenzar por exponerles cuáles son los beneficios de contar con un plan de continuidad de negocios (BCP por sus siglas en inglés). La alta gerencia y dirección NO decidirán los aspectos técnicos de la solución o del mismo plan, pero sí serán patrocinadores y promotores de cualquier iniciativa relacionada. Al final, ellos también aprueban cualquier presupuesto.

Quizá la percepción de la gente cambie el día que una manifestación bloquee el acceso a sus oficinas, un error humano borre tablas de las bases de datos, una fuga de agua moje equipos de cómputo con aplicaciones críticas, o que un corte de energía afecte las oficinas principales y el centro de cómputo. Ya ni siquiera mencionaré cosas más dramáticas porque esos ejemplos son sólo cuentos que pasan en las películas ¿no es cierto?... No. No fue sarcasmo. Sólo que a veces la realidad supera la ficción y debemos estar preparados.

Y como siempre cito en mi blog: *Always Mind the Information Security Gap!* •