COVID-19

Medidas que los CISOs pueden adoptar para mantener el negocio en funcionamiento.

Abril 2020

kpmg.com.ar

La preocupación en torno al alcance y el impacto de los desafíos que plantea el COVID-19 han llevado a las entidades a evaluar qué medidas deben adoptar para mantener el negocio. El Director de Seguridad de la Información (CISO) cumple un rol esencial a la hora de garantizar que la organización funcione, a medida que se implementan medidas para contener la pandemia.

¿La Entidad puede funcionar de manera efectiva mediante el trabajo remoto?

Distintas medidas del Gobierno Nacional y regulaciones emitidas en distintas jurisdicciones han dispuesto el distanciamiento social para contener la propagación del virus y el aislamiento preventivo, requiriendo trabajo remoto, siempre que sea posible.

El CISO debe garantizar que los empleados de la entidad puedan trabajar de manera remota con la confianza de que podrán cumplir sus tareas fuera de la oficina. Alcanzar esta flexibilidad puede implicar que deba replantearse decisiones respecto a los derechos de acceso y los riesgos.

¿Es posible escalar los canales digitales para lidiar con la demanda?

El aislamiento obligatorio, las restricciones a los viajes, incluso dentro del país, y la propagación del virus, generan nuevos patrones de demanda y aumentan el tráfico en los canales digitales.

— ¿Aumenta el número de clientes que desean realizar operaciones a través de canales digitales? ¿Puede escalar estos sistemas y servicios para responder al aumento en la demanda?

— En el caso de los centros de atención a clientes que permanezcan cerrados, ¿los clientes pueden interactuar con la entidad a través de otros canales?

— ¿Existe la opción de permitir que el personal de los centros de atención trabaje de manera remota o de transferir su carga de trabajo a otra ubicación?

¿Depende de personal clave de TI?

Puede ocurrir que algunos empleados se infecten, no puedan viajar o deban cumplir con compromisos de cuidado familiar. Es de esperar que exista un alto nivel de ausentismo:

— ¿Se ha asegurado de que los miembros clave del equipo estén cumpliendo con el distanciamiento social?

— ¿Puede dividir el personal en equipos A/B o que trabajen en turnos?

— ¿Qué ocurriría si el personal clave de TI (incluidos los contratistas) no puede viajar o se encuentra infectado con el virus? ¿Depende de un pequeño número de personas clave?

— ¿Cómo podría reducir esa dependencia? Por ejemplo, ¿puede garantizar que existan procedimientos de emergencia para que otros administradores puedan acceder a los sistemas críticos?

¿Está preparado para lidiar con los riesgos de amenazas internas en un contexto de trabajo remoto?

Es posible que su capacidad de control disminuya y que los empleados puedan sentirse descontentos. Las organizaciones deben ajustar la estrategia para proteger sus activos del uso inapropiado, sea intencional o no.

— ¿Ha determinado las áreas de riesgo inaceptable, que en ningún caso deberían llevarse a cabo en un contexto de trabajo remoto? Comience a adoptar medidas para la continuidad de estas actividades.

— ¿Es posible identificar controles que puedan flexibilizarse, por ejemplo, autorizar el acceso a soluciones de colaboración, permitir las impresiones remotas y el envío de correos a direcciones personales? ¿Puede supervisar los cambios en la infraestructura y en la política?

— El uso de tecnología paralela (shadow IT) se volverá inevitable. ¿Ha reiterado las prácticas recomendadas para reducir el riesgo, especialmente en las áreas que involucran información sensible? ¿Comprende cuáles son los requisitos contractuales y el impacto de las normas recientes en materia de privacidad?

— Algunos controles serán eludidos, de manera intencional o no. ¿Está listo para enfocar sus tácticas de detección en identificar situaciones intencionales/maliciosas?

— ¿Está preparado para realizar una recolección de datos remota manteniendo el distanciamiento social? ¿La política "trae tu propio dispositivo" ("BYOD") admite la investigación del equipo del empleado?

¿Qué ocurriría en caso de interrupción de los servicios de un centro de datos?

Los centros de datos también pueden verse afectados por el virus. Es posible que, ante un caso positivo, sea necesario evacuar el edificio y realizar una limpieza profunda. Además, la interrupción del transporte puede impedir el acceso y el personal del centro de datos podría verse imposibilitado de trabajar.

— En caso de que uno de los centros de datos deba evacuarse, ¿cuenta con planes para la recuperación ante desastres para lidiar con la interrupción de las tareas? ¿Estos planes fueron probados?

— ¿Depende de personas clave (incluido el apoyo de los contratistas) para operar el centro de datos? ¿De qué manera puede gestionar esa dependencia?

¿Puede escalar sus capacidades en la nube?

Es posible que existan nuevas demandas de servicios basados en la nube, que requieran escalar la capacidad de procesamiento disponible, lo que podría implicar costos adicionales. La demanda de otros servicios podría verse reducida.

— ¿Está preparado para supervisar la demanda de los servicios de computación en la nube y gestionar la asignación de los recursos de manera efectiva?

— ¿Ha adoptado medidas para responder a los costos adicionales que podrían surgir como consecuencia de escalar o brindar otros servicios basados en la nube?

¿Cuáles son los proveedores de los que depende?

Sus proveedores y socios de alianzas se encontrarán bajo presión, y es posible que sus operaciones también se vean interrumpidas.

— ¿Quiénes son sus proveedores críticos y cómo se las arreglaría si ellos no pudieran operar, incluso si sus proveedores clave debieran interrumpir los servicios?

— ¿Qué medidas podría adoptar actualmente para disminuir esa dependencia, por ejemplo, utilizar los recursos dentro de su equipo?

— ¿Ha conversado sobre las implicancias con los principales proveedores? ¿Cuenta con puntos de contacto adecuados con esos proveedores?

— ¿Ha identificado qué proveedores de TI pueden atravesar presiones financieras y cuál sería su estrategia de abastecimiento alternativa, en caso de que ellos no puedan prestar servicios?

¿Qué ocurriría si se presenta un incidente cibernético?

Los grupos criminales organizados aprovechan el miedo que genera el COVID-19 para llevar a cabo campañas de spear-phishing altamente dirigidas y crean sitios web falsos, lo que aumenta el riesgo de un incidente de ciberseguridad.

— ¿Ha explicado a los empleados dónde obtener información sobre la pandemia de COVID-19 y la respuesta de la Firma frente al virus?

— ¿Ha advertido al personal sobre el mayor riesgo de ataques de phishing que utilizan el COVID-19 como pretexto?

— ¿Necesita modificar su enfoque hacia las operaciones de seguridad durante la pandemia, por ejemplo, mediante la adopción de medidas para monitorear los incidentes de seguridad?

¿Qué ocurriría si se presenta un incidente cibernético o de TI?

Mientras el COVID-19 ocupa las noticias, debería estar atento a la posibilidad de que ocurra una falla de TI debido a los cambios en la demanda de infraestructura o un ciberataque oportunista.

— ¿Podría abordar el incidente en forma remota? ¿Cuenta con las instalaciones de conferencia necesarias y acceso a sitios/procesos y guías para la gestión de incidentes?

— ¿Depende de personas claves para responder al incidente? En caso afirmativo, ¿de qué manera podría reducir esa dependencia?¿Confía en que sus copias de resguardo están actualizadas y en que, en el peor escenario, podrá recuperar los datos y sistemas corporativos clave?

¿Está utilizando sus recursos de manera eficiente?

Deberá poder operar con un número limitado de empleados. Por eso, es necesario que identifique claramente cuáles son las tareas en las que el equipo debe enfocarse.

— ¿Ha establecido prioridades en las tareas del equipo? ¿Hay tareas que puede postergar para liberar personal para la planificación de contingencias y el establecimiento de prioridades?

— ¿Le resulta posible acceder a fondos de emergencia, en caso de que deba adquirir equipos rápidamente o contar con apoyo adicional de contratistas/especialistas?

— Si usted se ve obligado a reducir el gasto discrecional a fin de mantener el efectivo, ¿tiene claro cuáles son los gastos que debe proteger y dónde generar ahorro?

¿Lidera con el ejemplo?

Más allá de estas consideraciones en torno a la organización, usted continúa siendo parte de la alta gerencia, y el equipo buscará su apoyo y liderazgo.

— ¿Se ha asegurado de que su equipo esté implementando prácticas sensatas en materia de higiene y distanciamiento social, entre ellas, la posibilidad de ofrecer trabajo remoto y flexible para adaptarse a las necesidades cambiantes?

— ¿Los datos de contacto de todo el equipo están actualizados? ¿Saben a quién contactar en caso de emergencia?

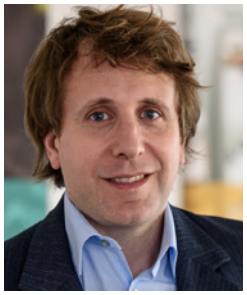
— ¿Da el ejemplo de las conductas que espera de su equipo? ¿Qué ocurriría si usted se encontrara imposibilitado para trabajar? ¿Quién lo reemplazaría?

El COVID-19 genera incertidumbre y preocupación. Los CISO's, en colaboración con sus colegas, pueden jugar un rol fundamental mediante la adopción de un enfoque racional y metodológico para abordar la continuidad del negocio y, así, permitir que las organizaciones mantengan sus operaciones en este contexto de desafíos, a la vez que protegen la seguridad y la salud de las personas.

Contactos

Walter Risi

Socio IT Advisory en Risk Consulting



Nicolás Manavella

Socio IT Advisory en Risk Consulting

kpmg.com/socialmedia

Diseñado por el equipo de Servicios Creativos - Marketing y Comunicaciones Externas - Argentina.