Deloitte.

COVID-19: CIBERSEGURIDAD Y LA FUERZA DE TRABAJO REMOTO

CÓMO LAS VULNERABILIDADES CIBERNÉTICAS Y LAS EFICIENCIAS OPERATIVAS ESTÁN CAMBIANDO LA "PRÓXIMA NORMALIDAD"

Lo que ha hecho que la irrupción de COVID-19 sea tan profunda es que pocas organizaciones, si es que las hay, tuvieron en cuenta una pandemia global en su planificación de continuidad comercial. Y, a diferencia de los eventos típicos en los que se basan la mayoría de los planes de continuidad del negocio (ataques cibernéticos, desastres naturales, interrupciones de la cadena de suministro, etc.), la crisis COVID-19 no tendrá un final limpio, donde todo volverá a la normalidad. COVID-19 ya está causando cambios profundos y permanentes en las estrategias en torno a las personas, los procesos y las tecnologías, y lo que significa ser una organización altamente resistente. **En pocas palabras, el día en que todos necesitan poder trabajar desde cualquier lugar está sobre nosotros.**

LA PRÓXIMA NORMALIDAD

Casi de la noche a la mañana, las empresas de todo el mundo se encontraron en situaciones de cierre donde los trabajadores tenían que refugiarse y trabajar desde casa. Esto ha creado factores estresantes de ciberseguridad en múltiples dimensiones, que incluyen:

- **La explosión de BYOD "Traiga su propio dispositivo"**
  Muchos trabajadores no tienen computadoras portátiles entregadas por la compañía para uso doméstico. Esto significa que están accediendo a redes y sistemas corporativos en dispositivos que pueden tener vulnerabilidades o ya están comprometidos. Del mismo modo, los trabajadores dependen en gran medida de las herramientas de colaboración y conferencia web para hacer su trabajo, que puede verse comprometido por ciber-delincuentes (los titulares recientes sobre "Zoom-bombardeo" son el ejemplo más destacado, pero no el único). Todo esto ha aumentado significativamente la complejidad de la seguridad debido a la expansión repentina de la superficie de ataque de las organizaciones.

- **El entorno informático doméstico**
  Las empresas no tienen control sobre el entorno informático doméstico de sus colaboradores. Los problemas que surgieron en estos entornos durante la crisis de COVID-19 van desde colaboradores más jóvenes que expresan dificultades para trabajar en pequeños departamentos con compañeros de cuarto que también están trabajando, hasta trabajadores cuyo ancho de banda es insuficiente para ofrecer un rendimiento aceptable para videoconferencias. Y, dado que todo, desde televisores hasta tostadoras, puede estar conectados a Internet, tenemos un típico entorno doméstico que está especialmente preparado para las vulnerabilidades de Internet de las cosas (IoT). Para un verdadero futuro "trabajo desde cualquier lugar", los equipos de seguridad, y TI en general, necesitan desarrollar programas y protocolos que permitan a los trabajadores remotos realizar sus trabajos sin introducir riesgos excesivos o comprometer la productividad en la organización.

SIN EL CONOCIMIENTO DE TI

+1,000

Dispositivos personales inseguros se conectan a redes empresariales todos los días en el 30% de las empresas estadounidenses, británicas y alemanas.

- **Acceso seguro remoto:** la mayoría de las empresas simplemente no estaban preparadas para un mundo donde todos los trabajadores debían tener acceso remoto seguro a redes y sistemas. Para las organizaciones que dependen de sistemas legado, esto es especialmente problemático porque son propensos a problemas de rendimiento, escalabilidad y disponibilidad. Este problema fue ilustrado por los problemas que muchas oficinas estatales de desempleo tuvieron con el procesamiento de un diluvio de reclamos, debido al uso de sistemas heredados basados en COBOL, algunos de los cuales tienen varias décadas de antigüedad. Si se va a pedir a las personas que trabajen desde su hogar en los dispositivos que elijan, también estas personas deben comprender las políticas exigidas de higiene y seguridad corporativas. Los equipos de seguridad deben adoptar un modelo de "confianza cero" donde implementen una sólida gestión de identidad y acceso, pudiendo detectar y responder fácilmente a comportamientos anómalos.

- **La amenaza interna:** el clima laboral y económico continuará contribuyendo a un mayor volumen de amenazas internas. El liderazgo debe considerar cómo está equipada la empresa para perseguir un programa de monitoreo de amenazas internas basado en el riesgo. Voluntaria o involuntariamente, la mayoría de los incidentes cibernéticos son causados por un colaborador de la organización afectada.

- **Procesos "ad hoc" inseguros:** los procesos comerciales que se diseñaron para un entorno de oficina seguro ahora se ejecutan en varios entornos domiciliarios y potencialmente inseguros. Por ejemplo, antes de COVID-19, ningún banco tendría procesadores de hipotecas que aprobaran préstamos de sus casas. Pero bajo la "nueva normalidad" en la que ahora vivimos, los bancos no tienen más remedio que adaptarse a este nuevo proceso ad hoc (a menos que dejen de prestar el servicio). A corto plazo, esto significa que los equipos de seguridad deben apresurarse para integrar la seguridad y el cumplimiento en este nuevo proceso, lo cual no es trivial: deben autenticar las identidades, garantizar el acceso seguro de la documentación de respaldo y volver a los sistemas gubernamentales, todo desde un dispositivo no emitido por la compañía. No hay un libro de tácticas para hacer esto, porque nunca se ha hecho antes.

En el futuro, las empresas de todo tipo deberán evaluar sus procesos en la oficina y seguir los pasos necesarios para permitir una migración segura a un entorno de trabajo remoto.

Las empresas ahora se están preparando para el mundo post COVID, donde la habilitación remota de los colaboradores y la productividad son regulares e integrales a sus planes. A medida que las organizaciones consideran cómo institucionalizar algunos de los procesos y funciones que implementaron rápidamente en los primeros meses de 2020, la ciberseguridad debería ser un actor destacado en todos los esfuerzos. Cuando se hace correctamente, con la intención de permitir la productividad mientras se asegura lo que más le importa a una organización, la seguridad cibernética se integra en las discusiones ejecutivas estratégicas y en el diseño a través de la implementación, para que la "nueva normalidad" no se convierta en la próxima fuente de un riesgo cibernético.

Disponibilidad
Garantizar la capacidad adecuada para conexiones remotas para realizar roles críticos.

Gestión de Vulnerabilidades
Instale actualizaciones de software regularmente para asegurarse de que los parches estén actualizados.

Gestión de Acceso
Asegúrese que se utilizan dispositivos y protocolos autorizados para el acceso remoto.

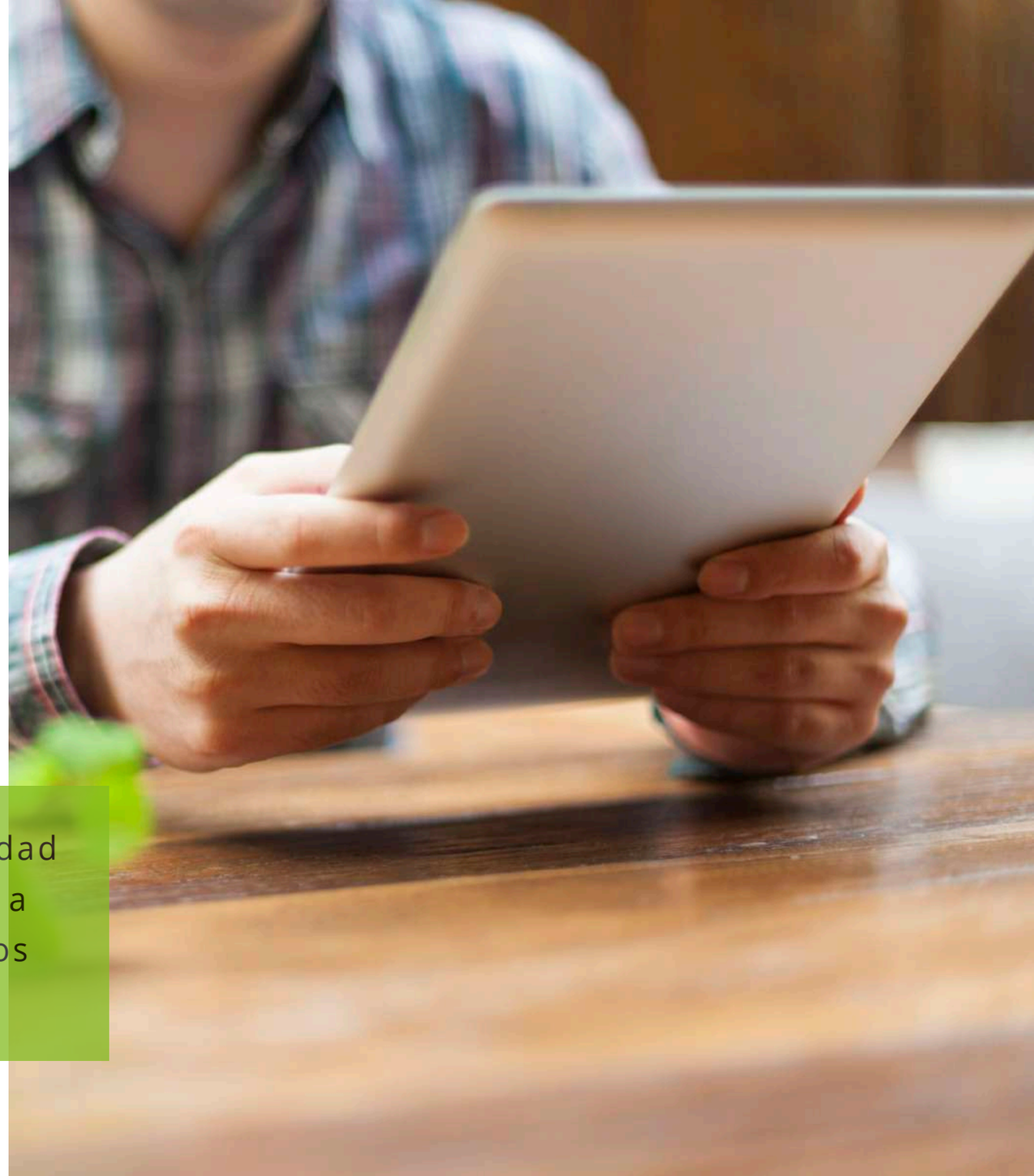
Políticas de seguridad
Actualizar y recordar a todos los colaboradores las políticas de seguridad.

COVID-19 LA RECUPERACIÓN SERÁ LA “NUEVA NORMALIDAD”

La recuperación de la crisis de COVID-19 no será un “encendido del interruptor” limpio. Será un proceso gradual de personas que regresen al trabajo y a una vida “normal” de poblaciones específicas, geográficas (incluso dentro del mismo país), grupos de edad, segmentos de negocios, etc. Los países adoptarán diferentes enfoques para que todos vuelvan al trabajo, de vuelta a sus economías. Dado que esta recuperación será el primer compromiso, habrá errores y es probable que también haya recaídas de infecciones que causen la restitución de las ordenanzas para quedarse en casa (ya hemos visto que esto sucede en algunos países asiáticos, y sin duda lo veremos en otras partes en los próximos meses).

En este entorno, no existe una única “nueva normalidad”. Por el contrario, habrá una serie de “próximos normales”. El estado de la sociedad modulará constantemente hasta el momento que haya disponibilidad global de una vacuna, que, desde abril del 2020, los profesionales de la salud predijeron que falta al menos un año.

Corresponderá a las organizaciones de ciberseguridad adoptar nuevos niveles de agilidad para adecuarse a este entorno de modulación, lo que plantea desafíos considerables.



PROSPERANDO EN EL FUTURO

Antes del brote de COVID-19, las empresas dedicaban la mayor parte de su gasto en tecnología y seguridad a la generación de ingresos y la eficiencia operativa. Esto es lógico, ya que esas, son generalmente las principales prioridades de una organización. Sin embargo, el mundo posterior a COVID puede ver una nueva distribución de recursos hacia la resiliencia empresarial centrada en la seguridad para mayores capacidades de trabajo remoto en el futuro.

LAS ORGANIZACIONES PUEDEN:

01. Asegurarse de que los equipos de TI desarrollen e implementen políticas y pautas de seguridad corporativas para traer su propio dispositivo (BYOD) y requieran que el software de seguridad corporativo esté instalado en los dispositivos de los colaboradores antes de que dichos dispositivos puedan usarse para conectarse.

02. Revisar y establecer reglas corporativas de firewall para acceso remoto, análisis de comportamiento de usuarios y entidades (UEBA) y monitoreo de integridad de archivos, para implementar de manera efectiva para los colaboradores que ejercen sus funciones de manera remota.

03. Restringir los dispositivos personales no aprobados en su red corporativa y limitar el acceso del dispositivo personal a solo los servicios corporativos requeridos en la nube que son necesarios para las operaciones comerciales críticas.

Esto generará un renovado interés en tecnologías que permitan un acceso remoto seguro y mejoren la productividad, incluyendo:

- **Infraestructura de escritorio virtual (VDI) y escritorio como servicio (DaaS).** Esto mitigará los problemas en torno a las personas que usan dispositivos no aprobados para acceder a los activos informáticos empresariales al permitir que los equipos de seguridad y TI administren de forma centralizada los escritorios de los usuarios, dándoles un control mucho mayor que el que es posible con los escritorios tradicionales. VDI ha existido desde principios de la década de 2000, pero tardó en establecerse debido a problemas de complejidad y rendimiento. Hoy, sin embargo, con VDI basado en la nube y ofertas de escritorio como servicio, esos problemas se han mitigado en gran medida, lo que hace que VDI sea una solución poderosa para el futuro del trabajo desde cualquier lugar.

- **La gestión de identidad y acceso (IAM)** también ha tenido problemas de adopción como resultado del costo y la complejidad. Al igual que VDI, la aparición de soluciones IAM basadas en la nube ha reducido drásticamente la complejidad técnica, lo que hace que sea práctico para los equipos de seguridad implementar soluciones en toda la empresa. Las organizaciones también pueden buscar proveedores de identidad para habilitar y administrar esta capacidad, en muchos casos, con un mayor rendimiento de la solución y un menor costo general para la organización. IAM es fundamental para adoptar una arquitectura de “confianza cero”, que será requerida por la mayoría de las organizaciones que buscan gestionar adecuadamente el riesgo con una fuerza de trabajo remota a gran escala.

- **La migración a la nube aumentará su velocidad.** como resultado de la pandemia de COVID-19. Las empresas que dependen de sistemas heredados están experimentando problemas de rendimiento, escalabilidad y disponibilidad con su infraestructura local. Esto acelerará la migración de estos sistemas a la nube, o un entorno de nube híbrida, con el equipo de seguridad cibernética como un componente fundamental del proceso para garantizar que todas las consideraciones, beneficios y riesgos cibernéticos se están sopesando e implementando.

A las organizaciones nativas de la nube les fue bien durante la interrupción de COVID-19. Ya habían adoptado completamente las modernas tecnologías de nube, identidad y acceso remoto, por lo que pasar a un modelo de fuerza de trabajo 100% remota fue un paso relativamente pequeño. Las organizaciones que más luchan son las que han pospuesto la necesidad de madurar su postura cibernética en toda la empresa.

EL FUTURO DE LAS PERSONAS, LOS PROCESOS Y LA TECNOLOGÍA.

El rendimiento empresarial es impulsado por personas, procesos y tecnología. Los tres deben abordarse para ejecutar de manera efectiva la transformación digital requerida para permitir un mundo donde las fuerzas de trabajo remotas son la norma frente a la excepción.

Cómo y dónde trabajamos será uno de los cambios más pronunciados de la pandemia de COVID-19, ya que muchas empresas experimentan los beneficios de ahorro de costos y productividad de una fuerza de trabajo remota. La mayor confianza que esto requiere entre colaboradores y empleadores será un resultado positivo de esta experiencia, y la flexibilidad se convertirá en la nueva norma, tanto desde la perspectiva del empleador como del colaborador. Los primeros comentarios de todo el mundo muestran que esto les sienta bastante bien a los colaboradores más jóvenes, que tienden a valorar mucho la flexibilidad y el equilibrio entre la vida laboral y personal. COVID-19 en realidad está acelerando la presencia de un sistema de valores en la corriente principal del negocio.

Desde una perspectiva y postura cibernética y la seguridad higiénica de las organizaciones pueden mejorar naturalmente como resultado de la pandemia. Es probable que las funciones de seguridad centrales como parches, gestión de vulnerabilidades y programas de conciencia cibernética sean mejor atendidos y mantenidos. La oportunidad se presenta al tomar lecciones aprendidas de lo que se necesitaba, así como creada por necesidad, y transformarlos en la próxima generación de seguridad y capacidades.

PERSONAS

Las personas deben ser “confiables pero verificadas” para realizar sus tareas en un entorno hogareño adecuado sin supervisión directa, y al mismo tiempo cumplir con las políticas de seguridad higiénica adecuadas.

PROCESO

Cualquier proceso que requiera interacción física debe evaluarse y, siempre que sea posible, digitalizarse para permitir la ejecución segura del proceso en un entorno de trabajo remoto.

TECNOLOGÍA

El acceso seguro, los escritorios virtuales, la administración remota de dispositivos, los sistemas y aplicaciones a escala de la nube serán críticos para permitir la transición fluida de la oficina a los entornos domésticos.

CONTÁCTANOS

Nicolás Corrado
Socio Lider Cyber
Risk Advisory
nicorrado@deloitte.com

Valetin Soulages
Socio Cyber
Risk Advisory
vsoulages@deloitte.com

Para más información sobre nuestros servicios escribanos a:
cyberchile@deloitte.com

Deloitte.

www.deloitte.cl

Las partes aceptan que COVID 19 constuye Fuerza Mayor, conforme los términos del artículo 45 del Codigo Civil. Asimismo, Las partes reconocen los riesgos que implica la propagación de la COVID-19 y las repercusiones potenciales asociadas con la prestación de los Servicios. El personal de las partes cumplirá con las restricciones o las condiciones que impongan sus res pectivas organizaciones en las prácticas laborales a medida que la amenaza de la COVID-19 continúe. Las partes intentarán seguir cumpliendo con sus obligaciones respectivas conforme a los plazos y el método establecido en la presente, pero aceptan que puede requerirse la adopción de prácticas laborales alternativas y la puesta en marcha de salvaguardas durante este periodo, tales como el trabajo a distancia, las restricciones de viaje relacionadas con destinos particulares y la cuarentena de algunas personas. Dichas prácticas y salvaguardas laborales pueden afectar o impedir la ejecución de diversas actividades, por ejemplo, talleres u otras reuniones en persona. Las partes trabajarán conjuntamente y de buena fe a fin acordar los eventuales cambios necesarios para atenuar los efectos negativos de la COVID-19 sobre los servicios, incluido el cronograma, el enfoque, los métodos y las prácticas laborales en la prestación de los mismos, y todos los costos asociados adicionales. En todo caso, Deloitte no será responsable de cualquier incumplimiento o retraso en la ejecución de sus obligaciones ocasionados o exacerbados por la propagación de la COVID-19 y sus efectos asociados.