INFORME DE HLB SOBRE SEGURIDAD CIBERNÉTICA DE 2020

NAVEGANDO POR EL PANORAMA DEL RIESGO CIBERNÉTICO EN LA ERA DEL TRABAJO REMOTO

HLB THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

CONTENIDO

La pandemia del COVID-19 obligó a muchas organizaciones de todo el mundo a adoptar procesos digitales y de trabajo remoto a una velocidad récord. Al hacerlo, los CTO y la gestión de TI enfrentaron mayores vulnerabilidades que permitieron que se produjeran ataques cibernéticos y violaciones de datos.

Bruscamente las organizaciones pasaron de entornos de oficina controlados a diversos lugares de trabajo desde el hogar. Continuar con las actividades comerciales mientras se aseguraban múltiples entornos virtuales, resultó ser todo un desafío. Pero el trabajo remoto llegó para quedarse, por lo que las empresas deberán adaptarse y superar los obstáculos de seguridad.

En el marco del Mes de la Concientización sobre Seguridad Cibernética de 2020, encuestamos a 76 profesionales de TI con relación a su percepción de la seguridad de la información y la protección de datos en el complejo entorno digital actual. Asimismo comentamos con los expertos en ciberseguridad de HLB sobre el panorama actual de riesgo cibernético, las lecciones aprendidas del confinamiento y el camino que deben seguir los CTO para protegerse contra delitos informáticos en la era del trabajo remoto.

LOS PROFESIONALES DE TI REPORTAN CAMBIOS EN LA CIBERSEGURIDAD

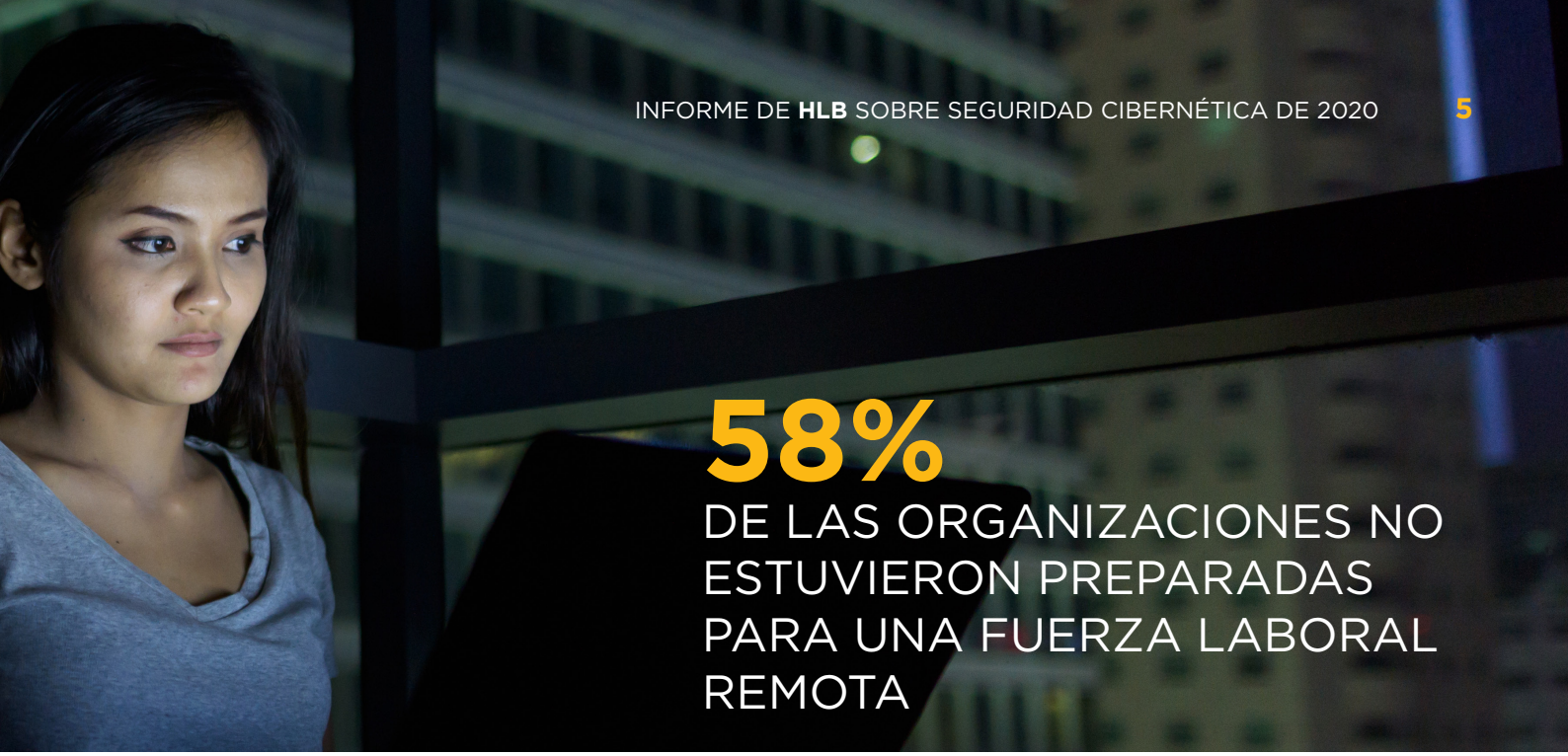
En todo el mundo, las compañías cambiaron los equipos para trabajar a distancia, con el fin de reducir las interrupciones en las actividades comerciales cuando los gobiernos anunciaron medidas de confinamiento para evitar una mayor propagación del coronavirus. Si bien la continuidad de las actividades era la preocupación más inmediata y apremiante, los cambios también debían reflejar los desafíos inesperados de ciberseguridad de la fuerza laboral virtual.

Los resultados de nuestra encuesta de HLB y el análisis de expertos revelaron que, a medida que pasaba el tiempo, las empresas se adaptaron al trabajo remoto y vieron un aumento en las amenazas cibernéticas, lo que llevó a cambios en las estrategias y el protocolo de seguridad cibernética para el 88% de los encuestados. El Director de Innovación de HLB, Abu Bakkar, junto con el Líder de Asesoría Global, Jim Bourke y los socios de HLB Digital, Carlos Morales y Gustavo Adolfo, comparten sus experiencias junto con las respuestas de los profesionales de TI.

LOS MAYORES DESAFÍOS PARA HACER SEGURAS LAS OFICINAS EN CASA

Desde proteger los dispositivos personales hasta dar acceso a las redes privadas virtuales (VPN), los CTO tuvieron que luchar para poner en funcionamiento las fuerzas de trabajo remoto. Inicialmente, las dificultades más importantes se originaron en las configuraciones individuales del hogar, como por ejemplo:

Acceso a WiFi de uso doméstico. Con el WiFi doméstico, todo está completamente abierto y los trabajadores utilizan diferentes tipos de infraestructuras, lo que dificulta la estandarización. Bourke comenta que las organizaciones pasaron de tener sólo un par de oficinas que asegurar, a tener tantas configuraciones diferentes para rastrear como empleados tiene la empresa, cuando pasaron al trabajo remoto desde casa, creando un obstáculo enorme.



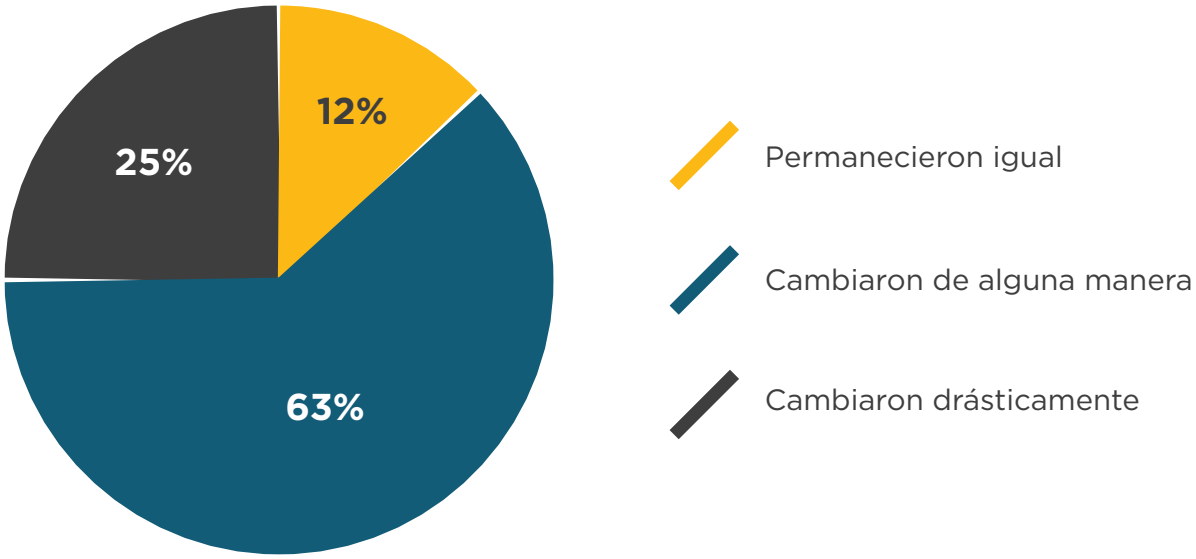
58%
DE LAS ORGANIZACIONES NO ESTUVIERON PREPARADAS PARA UNA FUERZA LABORAL REMOTA

Acceso a las VPN. Las redes privadas virtuales proporcionan conexiones seguras. Sin embargo, pocas empresas ofrecen acceso a todos los empleados. Adolfo reconoce que las compañías usaban VPN, pero no estaban disponibles para todos los empleados. Por ejemplo, en algunos casos, solo el personal de TI y las personas que necesitaban trabajar de forma remota con regularidad tenían acceso a las VPN. Este fue un desafío que tuvieron que superar.

Desempeño. Las videoconferencias de banda ancha de alta velocidad y diversas tecnologías de voz ejercen presión sobre las redes domésticas. Mientras que algunos países sufren de esto más que otros, las diferencias en la infraestructura regional pueden afectar el desempeño del trabajo remoto. Si bien los edificios de oficinas pueden solucionar estos problemas, es más difícil cuando todo su personal se encuentra a distancia.

Figura 1: Estrategias de ciberseguridad cambiaron como respuesta al COVID-19

Pregunta: Desde el inicio de la pandemia, dirías que las estrategias de ciberseguridad y protocolos en tu organización han...



LOS CTO y CEO IDENTIFICAN Y ESTABLECEN PRIORIDADES PARA LAS PREOCUPACIONES URGENTES

Ante cualquier crisis, los CEO y CTO deben actuar con rapidez. Sin embargo, durante la pandemia, también se requirió de una inmensa flexibilidad. Según Bourke, "la principal preocupación, desde el primer día, fue el acceso a los datos para garantizar la continuidad de las actividades comerciales".

No sorprende que del primer asunto que deben ocuparse los equipos de TI fuera implementar rápidamente soluciones para respaldar la disponibilidad de datos para la fuerza laboral remota y mantener las operaciones de la manera más fluida posible. Pero, a medida que pasaba el tiempo, las empresas encontraron formas de mejorar el acceso a los datos, lo que cambió su enfoque hacia la ciberseguridad y la confidencialidad de los datos.

Y ahora, aunque cuatro de cada cinco encuestados dicen que se sienten cómodos con su nivel de seguridad, también mencionan que su principal prioridad es realizar una evaluación interna de riesgos. Esto sugiere que confían en la capacidad de su empresa para identificar y abordar problemas. Aun así, también reconocen que el trabajo remoto ha alterado las evaluaciones iniciales de riesgo y es vital reevaluarlo.

MANTENER LA CONTINUIDAD DE LAS ACTIVIDADES COMERCIALES

Pocas compañías pueden prepararse completamente para que los sitios globales enfrenten desafíos similares, como estar en confinamiento o no tener empleados en oficinas. Bourke dice: "La mayoría de las empresas perdieron esa continuidad. Pudieron hacer la mayoría de las cosas, pero no pudieron hacer todo. Y ahora no quieren volver a estar en esa posición".
Una vez que las organizaciones cambiaron a equipos virtuales, los CEO expresaron su preocupación por la eficiencia del personal. Estos problemas de confianza llevaron a muchos a preguntarse: "¿Pueden nuestros empleados ser productivos fuera de la oficina?" Al principio de la pandemia, Morales recibió múltiples solicitudes de clientes de soluciones de información sobre sistemas de

monitoreo de empleados o servicios de monitoreo.

ADAPTARSE AL TRABAJO REMOTO

Incluso para las compañías con personal a distancia, tener de repente a decenas, cientos o miles de empleados trabajando desde casa crea una perturbación. Morales indica: "Lo que hemos visto es que muchas empresas están descubriendo cómo hacer que el trabajo desde el hogar tenga disponible tecnología. La mayoría de las organizaciones tenían servidores locales en la oficina y las soluciones de las VPN no eran tan sólidas como deberían ser". El resultado fue un cambio rápido a soluciones SaaS como Microsoft Office 365 o Google Drive para compartir información.

Un aspecto positivo que ha surgido del rápido cambio a trabajo a distancia es que el proceso de adopción digital dentro de las 7 organizaciones contempladas en el INFORME DE HLB SOBRE SEGURIDAD CIBERNÉTICA DE 2020 se ha acelerado. Los que antes se mostraban escépticos respecto de las plataformas de colaboración y las videollamadas para interactuar con otros, ahora no tenían más remedio que adoptar estas tecnologías. Muchos las han encontrado mucho más fáciles de usar y eficientes de lo que pensaban y han cambiado su percepción respecto a ellas. La mentalidad inicial del CEO de preocuparse por la eficiencia se resolvió, ya que los trabajadores a distancia demostraron eficiencia.

ABORDAR LOS RIESGOS CIBERNÉTICOS EXTERNOS

Con una cuarta parte de los encuestados diciendo que han tenido que realizar cambios drásticos en sus estrategias y protocolos de ciberseguridad, muchas empresas buscaron formas de transferir sus objetivos de seguridad cibernética organizacional a los hogares de los empleados. Después de todo, el aislamiento del trabajo remoto hace que las compañías sean más vulnerables a los ciberataques.

"Muchas organizaciones estaban preparadas para la ciberseguridad. Pero para lo que no estaban preparadas era para los problemas de seguridad informática en un entorno de trabajo remoto. Los responsables de la toma de decisiones no anticiparon que toda su fuerza laboral estaría trabajando de manera virtual. Así que ahora su mentalidad cambió nuevamente para preguntarse cómo podemos proteger nuestra información confidencial y privada a la que todos nuestros empleados necesitan tener acceso mientras trabajan desde casa".

JIM BOURKE
LÍDER ASESOR GLOBAL

AUMENTAN LOS CIBERATAQUES EN 2020

Desde amenazas a la seguridad móvil hasta acceso no autorizado a archivos, los recientes ciberataques exponen un problema cada vez mayor. Estos ataques en línea pueden afectar múltiples redes y computadoras. Deshabilita programas y roba datos. Los ciberataques también pueden utilizar las computadoras de sus trabajadores a distancia para lanzar ataques adicionales.

Los riesgos cibernéticos incluyen daños a la reputación, pérdidas financieras e interrupción a las operaciones comerciales. Las amenazas son generalizadas y nuestra encuesta encontró lo siguiente:

- El 53% de los encuestados estaban al tanto de actividades y/o ataques cibernéticos inusuales desde el comienzo de la pandemia;
- 12% reportó que su compañía había sido atacada;
- Sin embargo, el 35% restante respondió que no había notado ninguna diferencia. Desafortunadamente, sin reevaluar el riesgo cibernético y ajustar los protocolos, es posible que muchas empresas aún no se den cuenta de las amenazas y vulnerabilidades existentes en la nube informática. Bourke comenta: "¡Saber que el 65% de las organizaciones han estado o pueden haber estado expuestas durante este período es atemorizante! Y del 35% que no notó una diferencia, ¿cuántos de ellos pudieron haber pasado por alto una posible violación de datos?"

AISLAMIENTO DE LA FUERZA LABORAL Y ATAQUES DE PHISHING

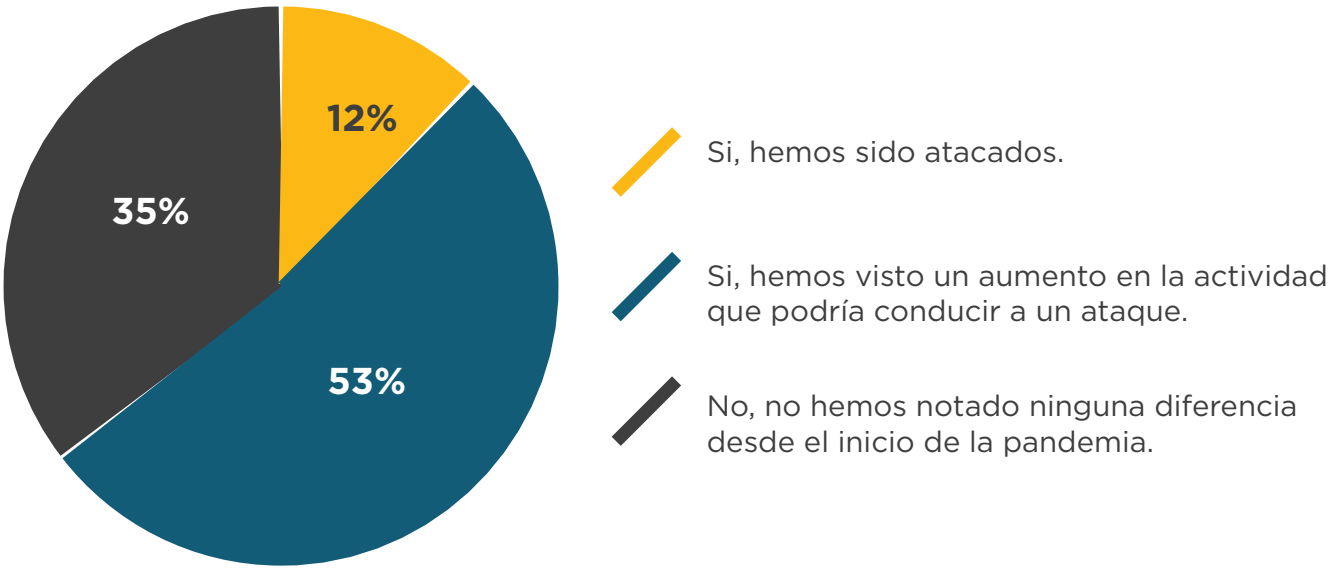
La opinión abrumadora de nuestros expertos es que los ataques de phishing están aumentando, con una tendencia que apunta a los ciberataques que involucran la información de inicio de sesión de los empleados en su plataforma de trabajo virtual. Estos principalmente solicitan a los usuarios sus inicios de sesión en herramientas como Microsoft Office 365 o Dropbox.

Según Bakkar, la ingeniería social también está aumentando. Él dice que los trabajadores remotos pueden ser más vulnerables a los correos electrónicos de phishing que hacen que las personas hagan clic en un enlace. Esto es especialmente cierto con los empleados que asisten a eventos físicos o virtuales y dejan una huella digital. Bakkar compartió una ocasión reciente en la que los hackers siguieron a su objetivo -un asistente a un evento- en las redes sociales para ver lo que estaba haciendo. Después le enviaron un correo electrónico aparentemente de la organización del evento con el mensaje "aquí está su factura". En este caso, el objetivo sabía que debía verificar minuciosamente la solicitud antes de pagar la factura. Sin embargo, muchos trabajadores a distancia nuevos pueden simplemente abrir el documento o hacer clic en un enlace de pago. El hecho de que muchos de nuestros procesos hayan cambiado en un corto período de tiempo y se hayan vuelto menos personales debido a su naturaleza remota y digital, es más fácil diseñar un ataque en redes sociales.

Asimismo el aislamiento social juega un papel en esta situación, ya que, en un entorno de oficina, Ud. le pediría a un colega su opinión o iría a la oficina del asistente administrativo para verificar que lo que recibió sea correcto si tiene un momento de duda. Pero los trabajadores a distancia deben tomar esas pequeñas decisiones por su cuenta y a menudo las consecuencias pueden ser desastrosas.

Figura 2: Organizaciones notaron un aumento de actividad cibernética sospechosa

Pregunta: ¿Han notado tu o los miembros del staff en tu organización alguna actividad cibernética inusual y/o ataques desde el inicio de la pandemia?



LAS EMPRESAS ESTÁN SUPERANDO LOS OBSTÁCULOS DE PROTECCIÓN DE DATOS

Una vez que la continuidad de la actividad comercial fue abordada, las compañías recurrieron a la seguridad. Pero no existe una única solución para este complejo problema. En cambio, los profesionales deben evaluar una variedad de problemas urgentes y luego desarrollar un enfoque que funcione fuera de la oficina. Cuando se les pidió que clasificaran cinco acciones para fortalecer la seguridad cibernética en orden de prioridad, los encuestados proporcionaron la siguiente clasificación. Los expertos de HLB comentaron de cada una lo siguiente:

1. **Realizar una evaluación de riesgos de seguridad interna:**
Cambiar la infraestructura para permitir la disponibilidad de datos hace que las empresas estén más expuestas, por lo que nuestros encuestados mencionaron que las evaluaciones de riesgos de seguridad interna son una prioridad principal.

2. **Actualizar la capacitación en ciberseguridad para la fuerza laboral:**
Los atacantes aprovechan las vulnerabilidades en software como Microsoft Office 365 y Zoom. Como resultado, es necesario revisar los programas y objetivos de capacitación. Muchas empresas ya lanzaron videos adicionales de capacitación en seguridad cibernética para enfrentar nuevos desafíos a medida que se adoptaron nuevas formas de trabajo.

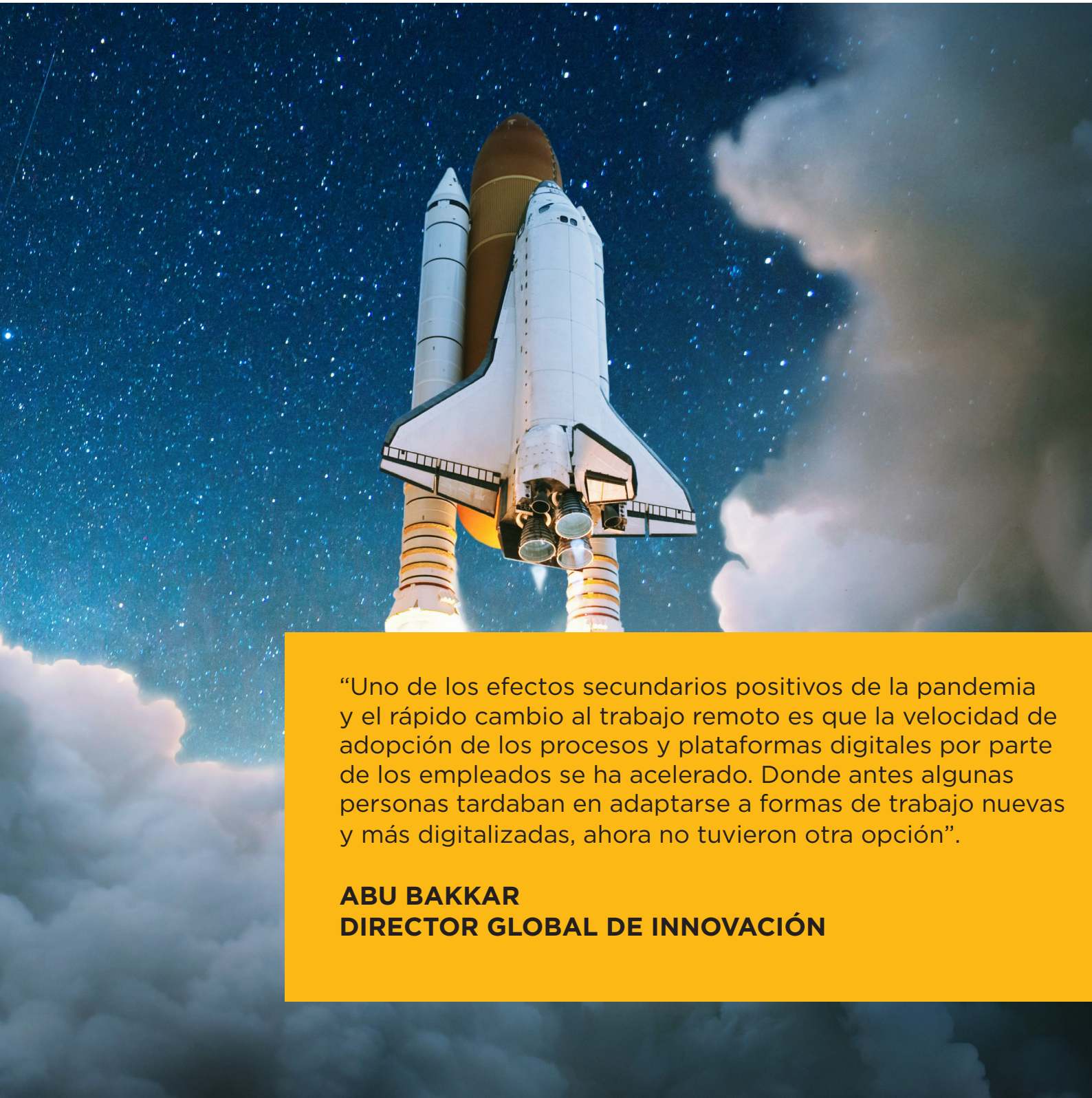
3. **Desarrollar un plan de respuesta a incidentes de ciberseguridad:**
Muchos planes de respuesta a incidentes de seguridad cibernética se relacionan directamente con las oficinas corporativas, no con lugares de trabajo remotos, lo que hace que sea esencial para los directores generales reevaluar sus procedimientos de informes y respuestas.

4. **Revisar las estrategias de la nube informática:**
A medida que las organizaciones atraviesan varias etapas de transformación digital, los tres principios de la seguridad de la información resultan vitales. Para enfrentar este desafío, los ejecutivos deben comprender dónde se integran la disponibilidad, la confidencialidad y la integridad de los datos en las oficinas en el hogar.

5. Realizar evaluaciones de riesgos de ciberseguridad de terceros:

Aunque nuestros encuestados enumeraron este nivel bajo en sus listas de prioridades, nuestros expertos señalan cómo los riesgos de seguridad incluyen nuestras interacciones con proveedores externos.

Nuestra cadena de suministro interconectada significa que lo que le sucede a su proveedor puede afectar a cualquier número de miembros de su equipo remoto o a toda la empresa.



"Uno de los efectos secundarios positivos de la pandemia y el rápido cambio al trabajo remoto es que la velocidad de adopción de los procesos y plataformas digitales por parte de los empleados se ha acelerado. Donde antes algunas personas tardaban en adaptarse a formas de trabajo nuevas y más digitalizadas, ahora no tuvieron otra opción".

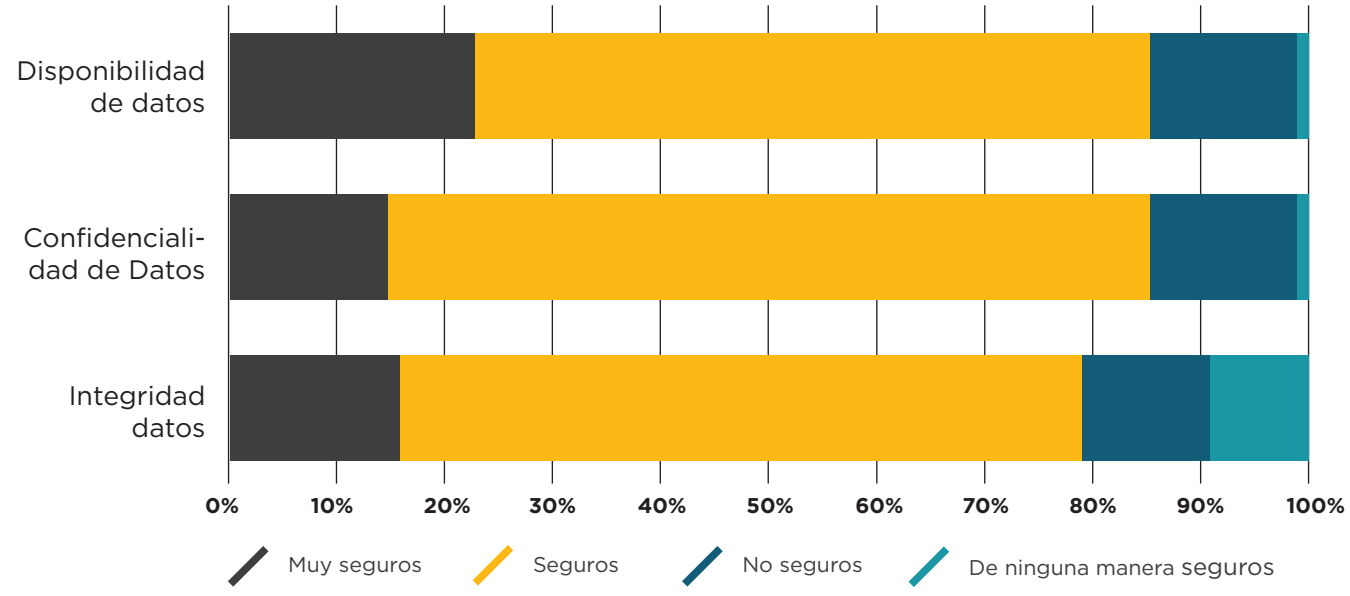
ABU BAKKAR
DIRECTOR GLOBAL DE INNOVACIÓN

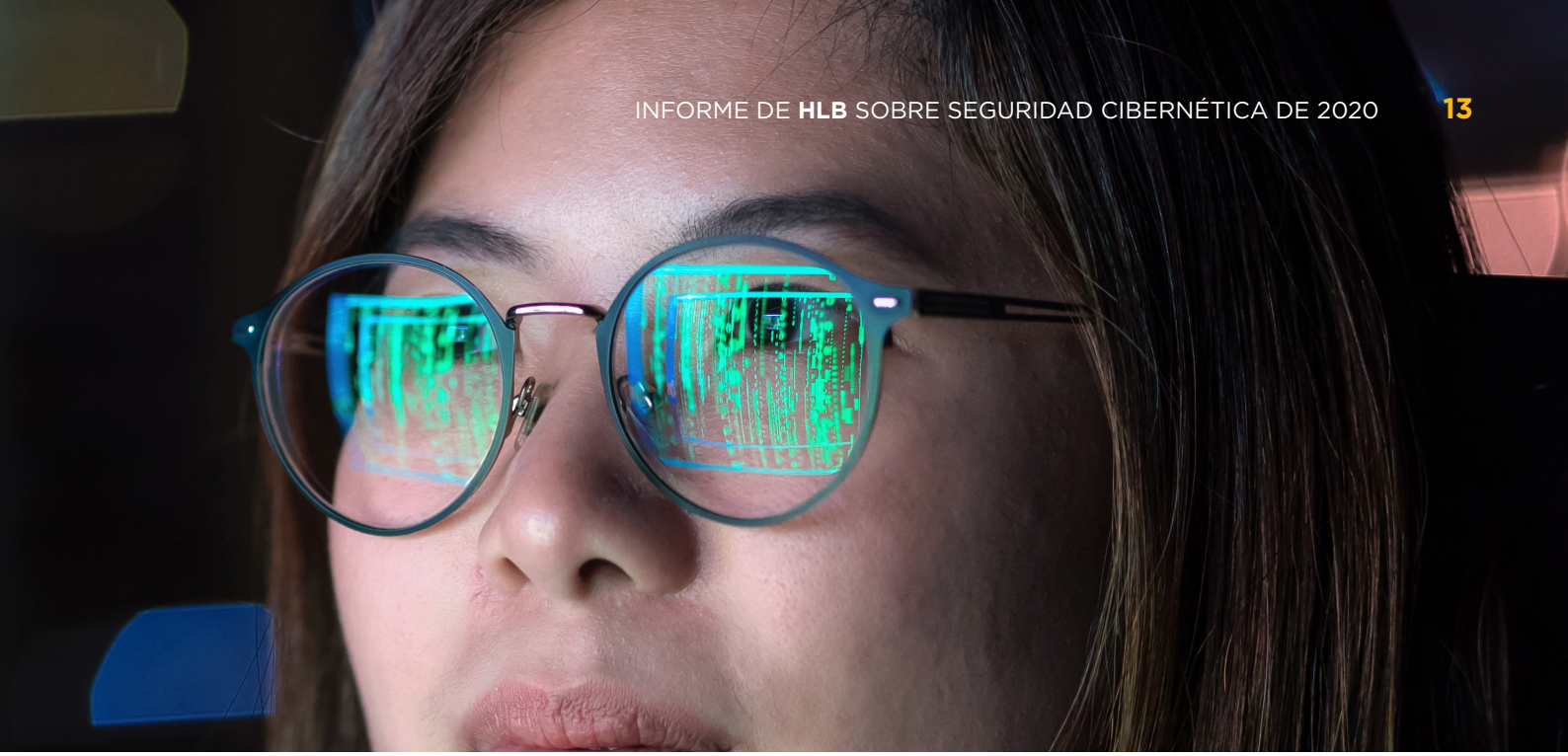
FORTALECER SU ESTRATEGIA DE GESTIÓN DE CIBERRIESGOS

Cuando se les preguntó sobre el nivel de seguridad en los tres principios de la seguridad de la información, uno de cada cinco encuestados no cree que sus sistemas en línea sean seguros. En un entorno de trabajo normal, es simplemente inaceptable un nivel de seguridad inferior al 100%. Pero con el trabajo remoto, vemos que el 21% de los encuestados cuestionan la integridad de sus datos. Bourke señala: “Desde la perspectiva del mes de la ciberseguridad, vale la pena señalar que la pregunta sobre la confidencialidad de los datos debería haberse respondido con un 100% de seguridad. Tenemos reglas y reglamentos, como el GDPR (Reglamento General de Protección de Datos), por lo que deberíamos estar seguros”. Sin embargo, algunas compañías tienen problemas para administrar la seguridad de los datos como lo harían en circunstancias normales y aún no se han adaptado por completo.

Figura 3: Uno de cada cinco no considera que los que los principios de seguridad de la información sean 100% seguros.

Pregunta: ¿Qué tan Seguro consideras los siguientes 3 principios de seguridad de la información en tu organización?





Para gestionar el riesgo cibernético, es necesario adaptar los tres principios de la seguridad de la información a los entornos de trabajo remotos:

Confidencialidad de los datos. La idea es garantizar que la información sólo se proporcione a quienes estén autorizados para gestionarla o verla. Las medidas están diseñadas para proteger contra la divulgación no autorizada de información. En un entorno de oficina, estas son más fáciles de aplicar, mientras que cuando los usuarios trabajan a distancia se vuelve cada vez más complejo y arriesgado.

Integridad de los datos. Las partes interesadas y los empleados de todos los niveles deben tener confianza en los sistemas y los datos. Adicionalmente, la integridad de los datos es un componente clave para cumplir con las normas de cumplimiento reglamentario. Garantizar la calidad de los datos que recopila y mantenerlos actualizados se reduce al acceso interno y a la gestión de datos. El principio de integridad está diseñado para garantizar que se pueda confiar en que los datos son precisos y que no se han modificado de manera inadecuada.

Disponibilidad de datos. El objeto de la disponibilidad es asegurar que los datos estén disponibles para ser utilizados cuando se necesiten para tomar decisiones. Para que el trabajo remoto funcione, su personal requiere acceder a los datos que requieren para desempeñar su trabajo. Es tan simple como eso. Pero equilibrar la disponibilidad con la confidencialidad y la integridad requiere una planeación estratégica y una infraestructura.

Toda amenaza a la seguridad no es necesariamente maliciosa. Los usuarios con buenas intenciones han causado importantes violaciones de seguridad, por lo que la capacitación sobre seguridad es fundamental. El acceso a los datos debe otorgarse a los usuarios según el principio de privilegio mínimo, lo que significa que el nivel de acceso otorgado a los usuarios debe limitarse a lo que requieren para cumplir con sus funciones.

LECCIONES APRENDIDAS DEL CONFINAMIENTO

Cuando se produjo la pandemia y muchos países adoptaron medidas de confinamiento para evitar que el COVID-19 se propagara, la prioridad de los líderes empresariales fue la continuidad de la actividad comercial. Sin embargo, las lecciones aprendidas en la gestión del riesgo cibernético continúan basándose en los temas comunes de agilidad y resiliencia.

LECCIÓN 1: Mejorar la capacitación y el soporte en ciberseguridad

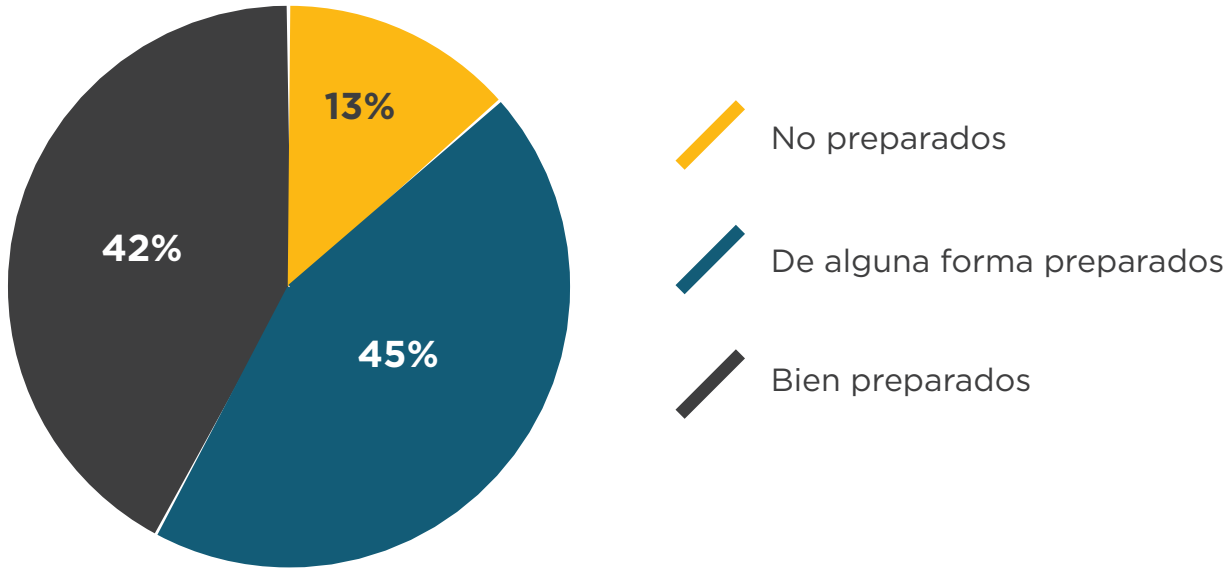
Se necesita un enfoque de 360 grados para gestionar las amenazas cibernéticas. La capacitación de la fuerza laboral ocupó el segundo lugar en términos de prioridad, según lo indicado por nuestros encuestados. Morales informa un aumento en las preguntas de los líderes empresariales sobre la creación y el cumplimiento de reglas para oficinas remotas. Esta es un área complicada, porque "puede tener un contrato de confidencialidad para su empleado, pero no puede tener un contrato de confidencialidad para un compañero de vida, un primo o cualquier otra persona en el hogar". Tenga en cuenta que las personas pueden filtrar información de forma no intencionada o sin intenciones maliciosas. Por lo tanto, la prevención de filtraciones de información confidencial puede complicarse en entornos remotos.

Sin embargo, una mayor conciencia y capacitación pueden combatir este problema, además de abordar el mayor riesgo de estafas de phishing y otros ciberataques. Adolfo explica: "El aislamiento de las personas es un factor de riesgo. Hemos aislado a las personas y tienen que tomar decisiones por sí mismas". El hecho de que esto las hace más vulnerables es algo de lo que quizás no sean conscientes y es algo que debe abordarse en la capacitación en seguridad adecuada para las circunstancias actuales.

Además, Bakkar afirma: "Su fuerza laboral es su activo más importante, pero también su mayor desventaja. Puede aumentar las medidas de protección, pero si su personal no está capacitado, entonces les darán acceso a las personas equivocadas y exponen su empresa a vulnerabilidades". Combata esto evaluando sus canales de soporte, encuestando a sus empleados e identificando formas de ayudarlos a desempeñar el trabajo remoto de manera segura.

Figura 4: Niveles de preparación para un cierre de emergencia

Pregunta: ¿en qué medida tu nivel de infraestructura en tecnologías de la información y protocolos de seguridad cibernética estaban preparados para un cierre de emergencia y trabajo remoto?



LECCIÓN 2: No espere a preparar la infraestructura de TI y los protocolos de ciberseguridad

Si bien el 42% de los profesionales de TI afirman que la infraestructura de TI y los protocolos de seguridad cibernética de sus organizaciones estaban bien preparados para operar las actividades comerciales de forma remota, la mayoría afirmó que estaban algo preparados (45%) o nada preparados (13%) para el confinamiento. Bakkar dice: "Todo sucedió en tan poco tiempo. Si su infraestructura no está configurada y lista, entonces tendrá problemas con la confidencialidad de los datos y con la determinación de quién tiene acceso a qué".

La infraestructura juega un papel crucial en la confidencialidad de los datos, por lo que ahora que los datos son accesibles en más lugares, los profesionales están bajo presión para abordar su enfoque de la ciberseguridad y las normas de cumplimiento reglamentario mientras las personas trabajan a distancia. Según Gartner[1], las empresas deben invertir "para proteger las tecnologías que respaldan sus resultados comerciales. Comprender los resultados más importantes de una compañía, sus procesos y sus resultados tecnológicos más importantes es el primer paso para poner un contexto empresarial en torno a la ciberseguridad".

1. Gartner, 2020. *The Gartner Business Risk Model: A Framework for Integrating Risk and Performance*

LECCIÓN 3: Pensar en una solución a largo plazo, no en soluciones a corto plazo

Las compañías no anticiparon el periodo de tiempo que la fuerza laboral estaría trabajando de forma remota. Si bien la disponibilidad de datos fue la primera preocupación, ahora que el trabajo remoto parece que llegó para quedarse, la seguridad de los datos debe fortalecerse. Bourke menciona: "Es posible que los CTO se hayan preparado para que los empleados trabajen de forma remota, pero no estaban preparados para las preocupaciones sobre seguridad cibernética en torno a los empleados que trabajan de forma remota durante un período de tiempo prolongado. No anticiparon los problemas de ciberseguridad en un período de meses o quizás un año o más".

Ya sea que crea Ud. que el trabajo remoto es una solución temporal mientras el mundo lucha contra una pandemia o que está aquí para quedarse para siempre, Ud. debe comenzar a pensar en la solución a largo plazo. Así como las empresas están revisando sus arrendamientos de espacio de oficina y planean reducir la cantidad de espacio de oficina que utilizan, los CTO deberían planear la ciberseguridad en un mundo donde las personas no regresarán a un único entorno de oficina controlado.

LECCIÓN 4: Evaluar periódicamente las amenazas y vulnerabilidades de la nube informática

Un estudio reciente realizado por Oracle[2] informa que dos tercios de los altos ejecutivos dicen que la nube nativa es parte integral de la competitividad de sus empresas. La forma en que operamos hoy y accedemos a los datos es diferente a la forma en que trabajábamos hace un año. Adolfo nota un aumento considerable en las solicitudes de evaluaciones de seguridad interna. "El enfoque de todos está en la seguridad interna. La pandemia ha hecho surgir esta valoración; todos quieren saber si son buenos. Entonces, cuando ingresamos y hacemos estas evaluaciones, encontramos exposición en áreas no anticipadas antes de la pandemia".

Aunque la disponibilidad de datos era esencial para la continuidad de la actividad comercial, la confidencialidad y la integridad de los datos se han vuelto más difíciles de controlar. Es probable que las circunstancias cambien constantemente y por lo tanto es aconsejable realizar evaluaciones periódicas de las vulnerabilidades. En particular en lo que se refiere a la nube informática.

2. Oracle, 2020. *Cloud 2020: Cloud Accelerates with Urgency*

"Todos somos parte del ecosistema empresarial. Esto significa que estamos muy interrelacionados y dependemos de nuestros proveedores. Entonces, cuando un proveedor nuestro se ve afectado por un ciberataque, esto también nos afectará".

GUSTAVO ADOLFO
SOCIO, HLB DIGITAL

LECCIÓN 5: Abordar el riesgo cibernético es un ejercicio para toda la empresa

Como hemos señalado, una de las principales prioridades actuales para los profesionales de TI es realizar una evaluación interna de riesgos. Pero las conversaciones no deben estar limitadas sólo a los líderes empresariales. Es fundamental iniciar una conversación en toda la empresa sobre los tres principios de seguridad de la información. Tradicionalmente, las transformaciones digitales llevan mucho tiempo. Pero en las circunstancias actuales, la adopción de tecnología digital se ha acelerado. Para que todos se unan a su estrategia de ciberseguridad, primero es necesario obtener la aceptación de los responsables de la toma de decisiones. Luego, capacítelos para que todos los demás respalden su programa.

Es importante evitar la toma de decisiones reactivas basadas en el miedo. A menudo, esto es el resultado de hacer al personal y a las partes interesadas las preguntas equivocadas que conducen a inversiones deficientes en ciberseguridad. El enfoque final debe estar en abordar el comportamiento de los empleados y ayudarlos a darse cuenta de cómo afectan la seguridad en su conjunto.

LAS PRINCIPALES CONCLUSIONES: CIBERSEGURIDAD Y TRABAJO REMOTO

Entonces, ¿qué puede hacer su compañía para promover la conciencia de la seguridad cibernética durante la era del trabajo a distancia? Nuestros expertos ofrecen sus mejores consejos para administrar sus riesgos cibernéticos mientras dan soporte a su fuerza laboral virtual.

RECONOCER LOS RIESGOS

Carlos Morales sugiere que un problema subyacente en la mayoría de las preocupaciones de seguridad cibernética es que muchas empresas no se dan cuenta de sus vulnerabilidades. Los líderes empresariales se centran en la continuidad y en dar a las personas acceso a los datos que requieren para trabajar. Pero es esencial reconocer que las circunstancias actuales aumentan el riesgo y pueden dar lugar a una violación de datos o problemas de privacidad.

EVALUAR TODO SU PROCESO DE CIBERSEGURIDAD

Jim Bourke recomienda volver a revisar la capacitación en ciberseguridad para la fuerza laboral. Y si no ha realizado una evaluación de ciberseguridad en los últimos seis meses, debe hacer una de inmediato. Por último, es esencial volver a examinar su riesgo cibernético dentro y fuera de su compañía. Por ejemplo, Ud. confía en sus proveedores y sus clientes. Sus preocupaciones de seguridad se vuelven suyas.

> “El primer paso para abordar los riesgos cibernéticos es reconocer que existen y que son un verdadero hilo conductor de la actividad comercial. Y eso es algo que, al menos en Centroamérica, no creo que siempre se reconozca”.
>
> **CARLOS MORALES**
> **SOCIO, HLB DIGITAL**

ANALIZAR LAS INTERACCIONES DIGITALES DENTRO Y FUERA DE SU EMPRESA

Gustavo Adolfo está de acuerdo con Bourke y agrega que las evaluaciones de riesgo deben basarse en el análisis de datos para determinar si se han violado las reglas o si se produjo una actividad inusual o parámetros anormales en las actividades comerciales. Porque es posible que los encuestados que informaron que no hay filtraciones de datos o cambios en la actividad que pudieran conducir a una filtración, simplemente no las hayan notado. Además, nuestro ecosistema empresarial y los eventos actuales destacan la dependencia que tenemos con los proveedores. Estas empresas de terceros están integradas en nuestra cadena de suministro o en nuestras operaciones diarias, lo que las hace más críticas que en años anteriores. Es posible que los ciberdelincuentes encuentren un camino hacia su empresa a través de sus proveedores.

81% ESTÁ ESTUDIANDO ACUERDOS LABORALES MÁS FLEXIBLES[3]

CONSTRUIR LA SEGURIDAD CIBERNÉTICA EN SU ESTRATEGIA COMERCIAL

Según Abu Bakker, la ciberseguridad no se trata sólo de protocolos; debe ser parte de su estrategia comercial general. Los CEO deben trabajar en estrecha colaboración con sus CTO y consultores de TI y determinar la inversión requerida en esta área. Las organizaciones requieren la tecnología adecuada, por lo que la adopción de la nube es fundamental. Pero sus equipos deben saber cómo utilizarla, por lo que la capacitación es igualmente importante. Al combinar todas las facetas en su estrategia, Ud. presentará un enfoque coherente y completo de la ciberseguridad.

3. HLB International, 2020. *HLB Survey of Business Leaders: The Execution Challenge for New Decade*

PRÓXIMOS PASOS: IDENTIFIQUE SUS RIESGOS DE CIBERSEGURIDAD Y LAS CONTRAMEDIDAS

Entonces, ¿es Ud. uno del 53% de los profesionales de TI que ha notado un aumento en la actividad que podría conducir a una violación de datos? ¿O podría haber pasado desapercibida en su empresa? A medida que los ataques continúan aumentando a nivel mundial, los ejecutivos deben adaptar las operaciones para tener en cuenta los cambios y al mismo tiempo encontrar formas innovadoras de crear resiliencia en todos los aspectos de una empresa. Dé sus siguientes pasos:

- Comience con una lista de verificación de evaluación de riesgos en la nube.
- Evalúe los riesgos de los proveedores externos.
- Analice conjuntos de datos para ver si ya se han producido violaciones.
- Identifique el papel que juegan sus medidas de ciberseguridad en su estrategia comercial.
- Desarrolle la capacitación en ciberseguridad para la fuerza laboral remota.

CONTÁCTENOS

Nuestros expertos en ciberseguridad están listos para ayudarle a identificar riesgos y asegurar su negocio en el ambiente actual de trabajo a distancia.
Trabajamos en 158 países alrededor del mundo.
Póngase en contacto con nosotros:

Abu Bakkar
Global Chief Innovation Officer

a.bakkar@hlb.global

Jim Bourke
Global Advisory Leader

j.bourke@hlb.global

Gustavo Adolfo
Socio, HLB Digital

g.solis@hlbdigital.global

Almerindo Graziano
Socio, HLB Digital

a.graziano@hlbdigital.global

Carlos Morales
Socio, HLB Digital

c.morales@hlbdigital.global

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

THE GLOBAL ADVISORY AND ACCOUNTING NETWORK