AMENAZA U OPORTUNIDAD: AFRONTAMIENTO DEL PANORAMA DEL RIESGO CIBERNÉTICO EN LA ERA DEL TRABAJO HÍBRIDO

HLB CYBERSECURITY REPORT 2021

HLB THE GLOBAL ADVISORY AND ACCOUNTING NETWORK

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

Conforme salimos de los cierres de emergencia y las restricciones del Gobierno ocasionadas por la COVID-19, más empresas en todo el mundo están adoptando los modelos híbridos de trabajo. Al hacerlo, la dirección de tecnología y la gerencia de TI enfrenta mayores riesgos y vulnerabilidades a los ciberataques y las filtraciones de datos.

En vista del Mes de la Conciencia sobre Ciberseguridad 2021, encuestamos a 136 profesionales de TI y entrevistamos a expertos(as) de ciberseguridad de HLB acerca del panorama actual de riesgo cibernético, las lecciones que se aprendieron en los cierres de emergencia y el camino a seguir para los(as) directores(as) de tecnología para protegerse contra el crimen cibernético en la era del trabajo híbrido.

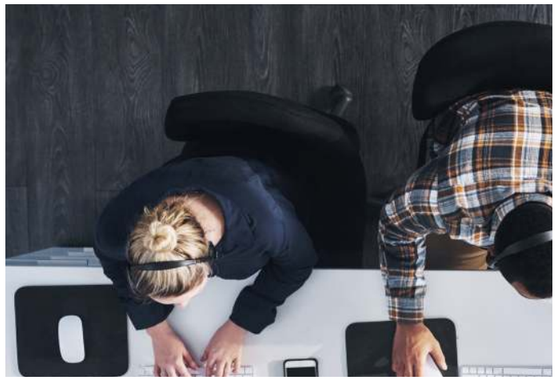
CONTENIDO

DE LA CONTINUIDAD EMPRESARIAL A LA CIBERSEGURIDAD: AYER Y HOY

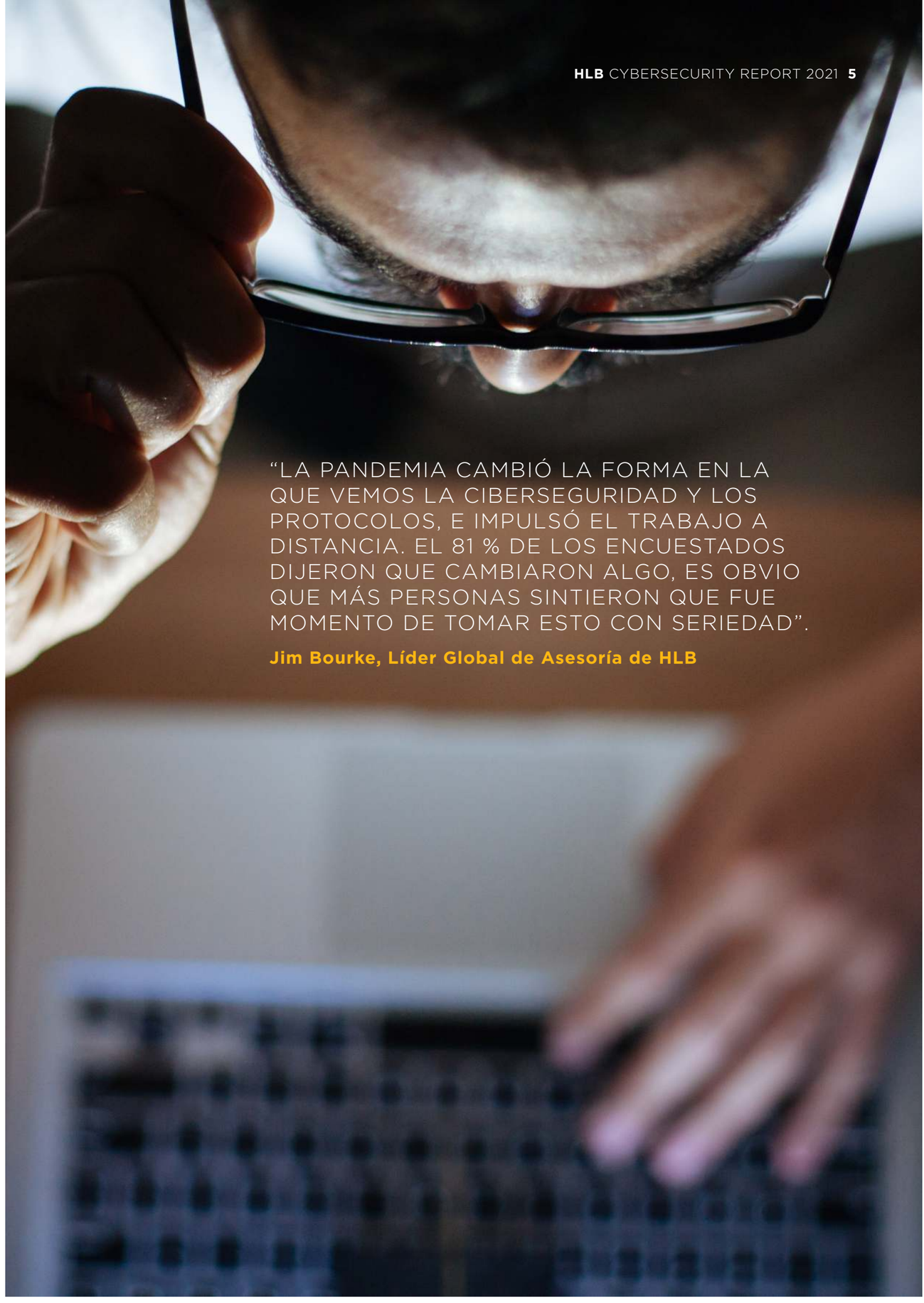
En 2020, los(as) líderes se centraron en implementar tecnologías y lograr que el personal se mantuviera trabajando, aunque fuera a distancia. Esto requirió migrar a la computación en la nube, asegurar una conexión de alta velocidad y dispositivos adecuados para el personal La ciberseguridad era importante, pero el primer paso era implementar con éxito el trabajo a distancia.

El 53 % de las personas participantes en la encuesta HLB de 2020[1] indicó que estaban al tanto de actividades inusuales y ataques cibernéticos desde el inicio de la pandemia. En consecuencia, la prioridad principal en el 2020 fue realizar una evaluación interna de riesgos.

Un año después, los ciberataques continúan en aumento y las empresas siguen enfrentando la interrupción que causó la COVID-19. Ahora los(as) empleados(as) se encuentran en un modelo híbrido de trabajo, mientras que los(as) líderes pasaron de la reacción a la acción preventiva. En vez de evaluar y arreglar los problemas de seguridad conforme ocurren, la mayoría de directores de tecnología aseguran en la encuesta HLB 2021 que ahora dan prioridad al desarrollo de un plan de respuesta a los incidentes.



1 HLB International, 2021. HLB Cybersecurity Report 2020: Navigating the cyber-risk landscape in the age of remote working



"LA PANDEMIA CAMBIÓ LA FORMA EN LA QUE VEMOS LA CIBERSEGURIDAD Y LOS PROTOCOLOS, E IMPULSÓ EL TRABAJO A DISTANCIA. EL 81 % DE LOS ENCUESTADOS DIJERON QUE CAMBIARON ALGO, ES OBVIO QUE MÁS PERSONAS SINTIERON QUE FUE MOMENTO DE TOMAR ESTO CON SERIEDAD".

Jim Bourke, Líder Global de Asesoría de HLB

GESTIÓN DE LOS RIESGOS CIBERNÉTICOS: EL TRABAJO HÍBRIDO ES EL FUTURO LABORAL

La COVID-19 derribó barreras culturales y tecnológicas que impedían el trabajo a distancia en el pasado, lo cual puso en movimiento un cambio estructural para cada empresa. Las personas participantes en nuestra encuesta de 2021 hicieron cambios para apoyar el trabajo híbrido del personal. El 44% indicó que se siente bien preparada para el trabajo híbrido y otro 44% indicó que se siente preparada en cierta medida.

De acuerdo con McKinsey & Company[2], desde 2019 el número de personas que desean trabajar desde las instalaciones de su empresa disminuyó 25%, mientras que es probable que el 30% cambie de trabajo si se le obliga a volver completamente a las instalaciones.

En nuestro sector, con personal altamente capacitado y calificado, las investigaciones[3] muestran que más del 20% de la fuerza laboral podría trabajar a distancia entre tres y cinco días a la semana de forma igualmente eficaz que si trabajaran desde una oficina. Los servicios de contabilidad, fiscales y de asesoramiento tienen un potencial alto para teletrabajar, ya que se dedica entre el 50 y el 75% del tiempo a actividades que pueden realizarse a distancia sin pérdida de productividad. Gartner mencionó que, “Se pronostica que el 51% deel personal intelectual en todo el mundo trabaje a distancia, lo cual representa un aumento del 27% en comparación con el personal intelectual que lo hacía en 2019”.

Los(as) directivos(as) ejecutivos(as) reconocen las oportunidades de un modelo de trabajo híbrido: desde la reducción de los costos de bienes raíces, hasta la retención del personal. Pearl Meyer[4] observó que casi “el 40% de las empresas informaron tener mayor productividad y casi el 50% no informó ningún cambio”.

Para 2022, Gartner estimó que “el 31% del personal en el mundo entero trabajará a distancia (una combinación de trabajo híbrido y completamente a distancia)”. Este estimado varía según la ubicación, dentro del cual, el personal que trabaja a distancia representa el 53% de la fuerza laboral en EE. UU., el 52% en Europa y el Reino Unido, el 37% en Alemania, el 33% en Francia, el 30% en India y el 28% en China.

Sin embargo, una fuerza laboral de trabajo híbrido requiere de entornos adaptables. Los espacios de trabajo adaptables capacitan al personal para trabajar donde y cuando sea más productivo. Los entornos flexibles proporcionan áreas bien diseñadas y equipadas en las instalaciones, mientras que garantizan que los equipos que trabajan desde casa tengan la tecnología y las herramientas necesarias para realizar sus labores.

Las empresas recurren a la nube para dar soporte a la fuerza laboral de trabajo híbrido. Pero añadir terminales a distancia y aumentar la dependencia en el software en línea representa un riesgo de ciberseguridad considerable. Al mirar hacia el futuro laboral, las soluciones de ciberseguridad representan un papel destacado en el éxito del modelo de trabajo híbrido.

2 McKinsey & Company, 2021. What employees are saying about the future of remote work
3 Gartner, 2021. Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021
4 Pearl Meyer, 2021. Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021

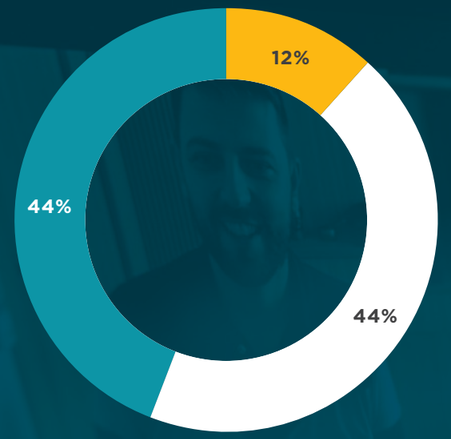


FIGURA 1: NIVELES DE PREPARACIÓN PARA EL MODELO DE TRABAJO HÍBRIDO

P: ¿EN QUÉ MEDIDA ESTÁN PREPARADOS SUS PROTOCOLOS EN TORNO A LA INFRAESTRUCTURA DE TI Y LA CIBERSEGURIDAD PARA UN MODELO DE OPERACIÓN HÍBRIDO?

- NADA PREPARADOS. NUESTRO PERSONAL TODAVIA TRABAJA DESDE LA OFICINA DE NUESTRAS INSTALACIONES Y LO HACE EN UN MODELO DE SEGURIDAD DE PERIMETRO CORPORATIVO.
- ALGO PREPARADO. UTILIZAMOS NUEVA TECNOLOGIA COMO SOPORTE PARA NUESTRO PERSONAL A DISTANCIA Y EN LA OFICINA DE NUESTRAS INSTALACIONES.
- BIEN PREPARADOS. IMPLEMENTAMOS EL TRABAJO HIBRIDO Y CAMBIAMOS NUESTRA INFRAESTRUCTURA TECNOLÓGICA PARA CONTAR CON UNA ARQUITECTURA DE CERO CONFIANZA.

PROBLEMAS DE SEGURIDAD Y LUGARES DE TRABAJO HÍBRIDOS

En una anterior encuesta de líderes empresariales[5], preguntamos a los(as) directivos(as) la medida en la que les preocupaban los riesgos de su negocio relacionados con los problemas de ciberseguridad. Aunque el 47 % sentía preocupación o mucha preocupación, destacaron múltiples problemas desde diferentes perspectivas como las consecuencias de la COVID-19, la inestabilidad económica y geopolítica, y la interrupción de la cadena de suministro.

Aunque estos temas son válidos, los datos demuestran que la ciberseguridad debería ser una prioridad, especialmente en los lugares de trabajo híbridos. De acuerdo con McAfee[6], el número de “amenazas de agentes externos dirigidos a los servicios de la nube aumentaron un 630 %, de los cuales, la mayoría de los incidentes surgieron a causa del robo de datos de identificación. Asimismo, el tráfico de la nube desde dispositivos no gestionados se duplicó; lo que sugiere la necesidad de control del acceso a la nube por tipo de dispositivo por parte de los(as) directores(as) de tecnología.

Añadir terminales fuera de las instalaciones requiere más recursos para monitorearlas. Y es más difícil conseguir visibilidad a las actividades del personal y la forma en la que trata a los posibles incidentes de seguridad cuando no está en las instalaciones.

Al mismo tiempo, las medidas de seguridad de proveedores externos afectan también a las empresas. Por lo tanto, los(as) líderes deben reevaluar las alianzas tecnológicas para confirmar que sus proveedores de software también estén preparados para un ataque de ransomware.

AJUSTE DE LAS ESTRATEGIAS Y LOS PROTOCOLOS DE CIBERSEGURIDAD

Mientras que las compañías desean retener el talento al ofrecer flexibilidad, también necesitan proteger a sus empresas de las ciber amenazas. Para hacerlo, la mayoría de las personas participantes en la encuesta HLB de 2021 indicó que alteró sus estrategias y protocolos de ciberseguridad. El 43% mencionó que los cambió en cierta medida y el 39% informó que los cambió de forma drástica. Solo el 17% aseguró no haber realizado ningún cambio desde el inicio de la pandemia.

Estos resultados son equivalentes a los de la encuesta de 2020, en la que el 88% indicó que cambió sus políticas y planes de ciberseguridad. Sin embargo, el número de participantes que indicó que los cambió de forma drástica aumentó un 14% en 2021.

De las personas participantes que informaron cambios drásticos, el 66 % ahora supervisa la ciberseguridad a nivel de la dirección. Esto es significativo, ya que, históricamente, la ciberseguridad se percibió como una tarea de TI, con menos participación de los(as) ejecutivos(as) superiores. Pero las investigaciones muestran que una estrategia que comienza en los niveles más altos es fundamental para la ciberseguridad. Bourke afirma, “La conciencia ahora es más amplia, y se hace responsable a la alta dirección, no solo a TI. Anteriormente, los(a) directores(as) ejecutivos(as) tradicionales dependían de TI para mantener la protección. Ya no es así”.

5 HLB International, 2021. HLB Survey of Business Leaders 2021: Achieving the post-pandemic vision: leaner, greener and keener
6 McAffee, 2021. Cloud Adoption and Risk Report

“ES NECESARIO REALIZAR LA CIBERSEGURIDAD A UN NIVEL MÁS ALTO. EJECUTAR LAS ACCIONES A NIVEL DE LA DIRECCIÓN. DE LO CONTRARIO, NO LOGRA LA TRACCIÓN QUE NECESITA”.

Abu Bakkar, Director General de Innovación de HLB

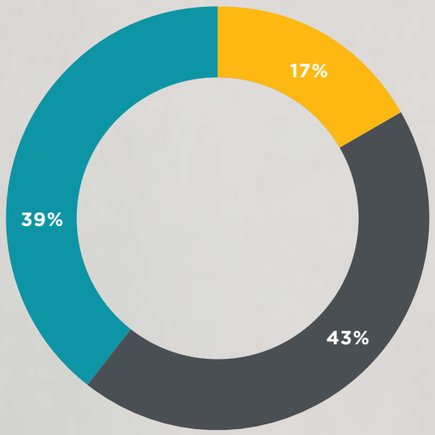


FIGURA 2: LAS ESTRATEGIAS DE CIBERSEGURIDAD CAMBIARON COMO RESPUESTA A LA COVID-19

P: ¿EN QUÉ MEDIDA CAMBIARON LOS PROTOCOLOS Y LAS ESTRATEGIAS EN TORNO A LA CIBERSEGURIDAD EN SU EMPRESA DESDE EL INICIO DE LA PANDEMIA?

- PERMANECIERON IGUAL
- CAMBIARON EN CIERTA MEDIDA
- CAMBIARON DRÁSTICAMENTE

Abu Bakkar, director general de innovación de HLB, añade: “Es necesario realizar la ciberseguridad a un nivel más alto. Ejecutar las acciones a nivel de la dirección. De lo contrario, no logra la tracción que necesita”. Sin embargo, Bourke menciona, “Si se lleva a cabo a nivel de la dirección, ¿qué están haciendo? Especialmente si no desean subcontratar su ciberseguridad”. En otras palabras, es fundamental aclarar los papeles de los miembros directivos y encontrar la desconexión entre el equipo de TI y lo que el/la director(a) ejecutivo(a) cree que hacen.

Además, el 28% de las personas participantes informaron sobre la implementación de un marco operativo. Normalmente, un marco operativo incluye la continuidad empresarial y un plan de recuperación ante desastres.

Requiere el soporte de los(as) ejecutivos(as), ya que es una gran tarea que involucra cambios en las políticas y los procedimientos. Bakkar menciona que “implementar un marco operativo suena sencillo, pero no lo es. Se necesita ayuda y apoyo, ya que hay demasiadas políticas y procedimientos, y muchas cosas que cambiar”. Carlos Camacho, socio de HLB Digital, añade: “No es solo un año, es la mentalidad la que hace la diferencia”.

En contraste, solo el 6% de los cambios drásticos incluyen la subcontratación de la ciberseguridad. El bajo porcentaje podría provenir del deseo de los(as) ejecutivos(as) de trabajar con socios conocidos y su recelo acerca de a quién integran a su proceso de ciberseguridad. Para los(as) proveedores(as) y asesores(as) de seguridad, la baja saturación del mercado podría ofrecer oportunidades para futuras asociaciones.

Del 42% que indicó que hizo cambios, el 39% aumentó la capacitación del personal, el 36% aumentó su presupuesto y el 12% invirtió en un programa de resistencia cibernética. De acuerdo con Bourke, “El mayor riesgo involucra al personal, por lo que son importantes los programas de capacitación”. También encontramos que, mientras que el 14% seleccionó “Otra respuesta”, al inspeccionar sus respuestas escritas, indicaron que sus cambios fueron una combinación de las tres opciones.

PREPARACIÓN PARA EL TRABAJO HÍBRIDO

El año pasado, muchos(as) participantes de la encuesta mencionaron la importancia de lograr las condiciones de trabajo a distancia para el personal, como proporcionarles las herramientas y los recursos necesarios para realizar su trabajo tal como si estuvieran en oficina. Sin embargo, muchos(as) líderes no conocían la duración del periodo en el que su fuerza laboral permanecería a distancia y no buscaban soluciones a largo plazo. Por consiguiente, al inicio de la pandemia no fue una prioridad la inversión en protocolos más estrictos de ciberseguridad.

Ahora que el trabajo fluye con mayor soltura y los ciberataques prominentes están en las noticias, los(as) líderes buscan adoptar medidas más sólidas en torno a la seguridad para proteger a su negocio.

EL PERSONAL SE ENCUENTRA EN EL NÚCLEO DE LA CIBERSEGURIDAD DE SU EMPRESA

Aunque las empresas implementen muchas medidas de seguridad, el personal representa finalmente uno de los papeles más significativos. Carlos Morales, socio de HLB Digital dijo, “Ahora las personas comprenden que la ciberseguridad no es un problema computacional. Es un problema humano”.

Y, con demasiada frecuencia, es el personal el punto débil de la ciberseguridad. Bourke explica, “En mayor medida, los fallos de ciberseguridad comenzaron con el personal y esto impulsó la importancia de desarrollar un plan de respuesta a los incidentes”. El Informe de Investigaciones sobre la Filtración de Datos de Verizon[7] de 2021 encontró que “El 85% de las filtraciones involucran un elemento humano y el 61% de las filtraciones involucraron datos de identificación”. Asimismo, “El 88 % de las filtraciones de datos en el Reino Unido fueron a causa de errores humanos, no ciberataques”, de acuerdo con los datos que se obtuvieron de la Information Commissioner’s Office (ICO) del Reino Unido.

Mientras que las herramientas pueden proporcionar la imprescindible visibilidad a las prácticas del personal en torno a las contraseñas, los(as) líderes deben centrarse en la capacitación y la concientización de los miembros del equipo. Nuestra encuesta descubrió que el 57% de las personas participantes se toman en serio la capacitación del personal y cuentan con una política que no permite excepciones. En contraste, el 33% de los(as) profesionales de TI que encuestamos afirman que capacitan a su personal, pero lidian constantemente con la falta de cumplimiento. En esto subyace la gran dificultad de las empresas para lograr el cumplimiento del personal, especialmente al usar un modelo de trabajo híbrido.

Ya que algunos de los mayores riesgos provienen de las personas, es importante comprender las amenazas que aparecen con las áreas de trabajo híbridas. A partir de esto, los(as) líderes deberían prestar atención a los desafíos para implementar las medidas de seguridad y concebir soluciones.

AMENAZAS A LOS ENTORNOS HÍBRIDOS

La ingeniería social y los fraudes electrónicos (phishing) ocasionan problemas de seguridad para las empresas. En algunos casos, los correos electrónicos comprometidos de los proveedores (VEC, por sus siglas en inglés) dificultan el rastreo de las direcciones de correo electrónico falsas. Esto ocurre con frecuencia a través de datos de identificación de correo electrónico robados u obtenidos mediante un fraude electrónico.

Cada vez más, vemos correos electrónicos empresariales comprometidos (BEC, por sus siglas en inglés). Estas comunicaciones parecen provenir de un(a) empleado(a) o gerente(a) interno(a) y solicitan información confidencial o el pago de una factura. Las intrusiones a las computadoras de escritorio a distancia provienen a menudo de errores de configuración. Como se menciona en el estudio de McAfee, los dispositivos para trabajar desde casa aumentan la complejidad de la gestión de la ciberseguridad. Las empresas sin visibilidad y control de las terminales enfrentan mayores riesgos cibernéticos que aquellas con un plan de protección de terminales integral.

7 Verizon, 2021. Data Breach Investigations Report

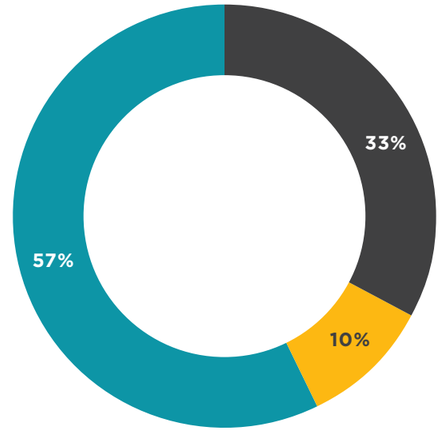


FIGURA 3: CAPACITACIÓN EN CIBERSEGURIDAD PARA EL PERSONAL

P: ¿CUÁL ES SU ESTRATEGIA EN RELACIÓN CON LA CAPACITACIÓN DE SU PERSONAL EN MATERIA DE CIBERSEGURIDAD?

- CAPACITAMOS A NUESTRO PERSONAL, PERO SIEMPRE LIDIAMOS CON LA FALTA DE CUMPLIMIENTO
- LA FOMENTAMOS, PERO NO ES OBLIGATORIA
- LA TOMAMOS CON SERIEDAD Y TENEMOS UNA POLÍTICA DE NO EXCEPCIONES

BARRERAS COMUNES PARA LAS MEDIDAS DE SEGURIDAD DEL PERSONAL

Ya que un tercio de los(as) directores(as) de tecnología e información lidia con la falta de cumplimiento, es fundamental comprender la raíz del problema. Hay muchas razones por las cuales el personal no sigue los protocolos de ciberseguridad, entre ellas el que son procesos inconvenientes o confusos. Además, el personal de áreas distintas a TI podría no estar al tanto de los diferentes tipos de amenazas o comprender las consecuencias de las fallas de seguridad. Aunque más del 90% afirmó que capacita a su personal, Bourke menciona que “el 33% tiene problemas de falta de cumplimiento, lo que destaca la razón por la que una política que no permite las excepciones es esencial. Solo se necesita que una persona cometa un error”.

El personal de trabajo híbrido podría confiar en el internet inalámbrico para trabajar desde cualquier lugar y, si la decisión está entre no trabajar o arriesgarse con el wifi público, se genera una situación complicada. Morales dice, “Las personas habitualmente no están conscientes de que trabajar de forma remota o desde cualquier lugar podría presentar un riesgo”.

Por otro lado, el personal de trabajo híbrido podría no contar con las herramientas tecnológicas para realizar sus labores de forma segura, como gestionadores de contraseñas, autenticadores de dos factores y redes virtuales privadas (VPN, por sus siglas en inglés). Si las empresas ofrecen una política que permite usar un dispositivo propio, hay una mayor probabilidad de que estos dispositivos se utilicen para realizar tareas personales y profesionales.

Por último, la capacitación del personal puede ser deficiente. El personal puede ver la capacitación como una tarea que tiene que completar, no como una actividad de aprendizaje. Algunas personas podrían reproducir sin audio los videos requeridos y pasar el examen sin dificultades con la ayuda de los motores de búsqueda en línea. Otras personas podrían no comprender los extensos documentos de las políticas antes de firmarlos.

En comparación, los programas exitosos son incluyentes, fáciles de usar y continuos. Vienen en diferentes formatos y, como los lugares de trabajo adaptativos, la capacitación en materia de ciberseguridad faculta al personal para aprender en el momento y lugar de su elección, y de forma adecuada para su nivel de habilidad y estilo.

SOLUCIONES PARA SUPERAR LOS OBSTÁCULOS EN TORNO A LA CIBERSEGURIDAD

Carlos Camacho dice, “Ese elemento humano necesita capacitación. Porque la capacitación es la clave para el cambio en el patrón humano”. Es por esto por lo que las mejores soluciones de ciberseguridad buscan desarrollar mejores hábitos, alterando procesos y aumentando el conocimiento. Además, cuando preguntamos sobre las acciones que se tomaron para proteger a su empresa, recibimos docenas de respuestas relacionadas con la capacitación del personal, lo que demuestra que centrarse en los(as) empleados(as) es fundamental para combatir las amenazas cibernéticas.

Como todas las medidas de ciberseguridad, la higiene cibernética del personal se apoya en una estrategia de tres frentes: las personas, la tecnología y el entorno. Las personas necesitan capacitación para detectar los correos electrónicos falsos de phishing, como programas de capacitación en línea obligatorios. Asimismo, la dirección debe poner el ejemplo y mantener abiertas las líneas de comunicación con el fin de realmente transmitir el mensaje de la importancia de la ciberseguridad. Aproximadamente un cuarto de las personas participantes cambió el nivel de la toma de decisiones, ahora tomar las medidas en torno a la ciberseguridad se da a nivel de dirección, lo que sugiere que los(as) líderes reconocen la importancia de una estrategia que comienza en los más altos niveles.

En las respuestas escritas, las personas encuestadas informaron sobre el uso de varias soluciones para mejorar el conocimiento del personal, incluidos los talleres, la capacitación en línea y los servicios de capacitación de terceros, intensivos y en toda la empresa.

De acuerdo con Bakkar, algunas empresas "utilizan a una compañía de capacitación que proporciona videos educativos. Y, sin importar si usted es socio(a), profesional o parte del personal, si no toma esos videos y los ve, no tendrá acceso a su computadora portátil o a la red".

El entorno laboral, sin importar la ubicación, debe asegurarse. Las VPN de acceso a distancia son una solución. Otorgar solo los permisos de acceso necesarios es otra. Otros(as) directores(as) de tecnología nos dijeron que tomaron medidas para evitar la navegación personal y el uso de filtros de contenido y herramientas de monitoreo dentro de los dispositivos empresariales.

La tecnología también representa un papel. Por ejemplo, las aplicaciones de autenticación de dos factores o factores múltiples, o la habilitación de 2FA en las herramientas existentes puede reducir significativamente la piratería de las cuentas. Los programas de gestión de contraseñas facilitan el cumplimiento de sus políticas en torno a estas. Utilizar medidas estándares de ciberseguridad, como firewalls, sistemas de prevención de intrusiones (IPS, por sus siglas en inglés), sistemas de detección de intrusiones (IDS, ídem) y el monitoreo de las terminales, también ayuda a proteger la información de sus equipos y empresarial. Además, adoptar políticas e implementar los marcos operativos del National Institute of Standards and Technology (NIST) y la International Organization for Standarization (ISO) es fundamental para reducir los riesgos cibernéticos.

De acuerdo con Bakkar, algunas empresas

"UTILIZAN A UNA COMPAÑÍA DE CAPACITACIÓN QUE PROPORCIONA VIDEOS EDUCATIVOS. Y, SIN IMPORTAR SI USTED ES SOCIO(A), PROFESIONAL O PARTE DEL PERSONAL, SI NO TOMA ESOS VIDEOS Y LOS VE, NO TENDRÁ ACCESO A SU COMPUTADORA PORTÁTIL O A LA RED"

EL FORTALECIMIENTO DE SU ESTRATEGIA DE GESTIÓN DE LOS RIESGOS CIBERNÉTICOS

Como se mencionó con anterioridad, en el 2020, la mayoría de las personas participantes indicó que su prioridad principal era realizar una evaluación interna de riesgos. Sin embargo, dicho objetivo cayó al número cuatro en nuestra encuesta de 2021. En cambio, la acción estratégica de mayor importancia es desarrollar un plan de respuesta ante incidentes. En la encuesta de este año, las personas avanzaron de la evaluación de riesgos a desear, ahora, descubrir la forma de responder a ellos.

Aunque las empresas tienen estrategias distintas en torno a la transformación digital, incluidos los objetivos y la cronología, la capacitación del personal sigue en el número dos de nuestra lista de prioridad, la cual es igual a la del año pasado.

Para que los(as) directores(as) de tecnología tomen una decisión acerca de sus siguientes pasos, el primer lugar para comenzar es ejecutar una evaluación interna de riesgos. A partir de ahí, los(as) líderes deberían dar prioridad a las tácticas para mitigar las amenazas, capacitar al personal y responder a los incidentes.

DESARROLLO DE UN PLAN DE RESPUESTA A LOS INCIDENTES

El año pasado, los planes de continuidad de las empresas se centraron en la reincorporación al trabajo de los(as) empleados(as). Este año, el 88% de los(as) ejecutivos(as) se encuentran en cierta medida preparados(as) para el trabajo híbrido. Como resultado, su prioridad principal es diseñar un plan de respuesta a los incidentes. Con la idea de que un ciberataque es inminente, los(as) líderes buscan formas de limitar la interrupción mediante el monitoreo proactivo y las respuestas uniformes, en caso de una filtración.

Bakkar menciona, "La continuidad empresarial es enorme. Hay que asegurarse de que la empresa sea capaz de estar en funcionamiento lo más rápido posible después de un incidente. No hay forma de detener al 100% un ciberataque. Se pueden mitigar la mayoría de las cosas, pero si se tiene un buen plan de respuesta, se sabe que también se mitiga con la continuidad empresarial".

CAPACITACIÓN EN MATERIA DE CIBERSEGURIDAD PARA LAS ESTRATEGIAS DE LA FUERZA LABORAL

De acuerdo con Camacho y Morales, las personas son tanto la fortaleza como la debilidad. Por lo tanto, la prevención y la respuesta a los incidentes depende, en parte, de su personal. Nuestra encuesta HLB de 2021 encontró que el 90 % de las personas participantes capacita al personal. Sin embargo, no todas consiguieron con éxito el cumplimiento de los(as) empleados(as), lo que sugiere que existe la necesidad de revisar los programas actuales de capacitación y afrontar sus debilidades.

8 HLB International, 2021. HLB Cybersecurity Report 2020: Navigating the cyber-risk landscape in the age of remote working

9 HLB International, 2021. HLB Survey of Business Leaders 2021: Achieving the post-pandemic vision: leaner, greener and keener

57%

DE LOS ENCUESTADOS SE TOMAN EN SERIO LA EDUCACIÓN EN CIBERSEGURIDAD PARA SU PERSONAL Y NO TIENEN UNA POLÍTICA DE EXCEPCIÓN.

De acuerdo con Bourke, “El 56% se lo toma en serio y afirma que no tolerará excepciones, lo cual es un buen inicio. En HLB, somos el asesor de confianza, y nuestros clientes confían en que nosotros protegeremos sus datos confidenciales. Por lo tanto, nos tomamos en serio el acceso a los documentos y a la información. No deseamos correr el riesgo de un posible peligro”.

Las políticas en materia de ciberseguridad deberían cubrir los dispositivos móviles y de escritorio, las descargas de aplicaciones de terceros, el uso de las redes sociales y la seguridad del correo electrónico. Asimismo, los cursos continuos deberían repasar las normas de protección de datos y las consecuencias de incumplir los protocolos de ciberseguridad a nivel del personal y directivo.

Sin embargo, bombardear al personal con material de lectura o largos videos es menos útil que los modelos y las simulaciones interactivas para la capacitación. La comunicación de los(as) directivos(as) también es esencial. Los(as) ejecutivos(as) deberían informar a los equipos acerca de los fraudes más recientes dirigidos a su sector y puestos laborales, y hablar acerca de lo que se ha estado haciendo a nivel directivo para proteger al personal y a la empresa en conjunto. Las conversaciones frecuentes mantienen la ciberseguridad siempre en mente y, al hacerlo, aumenta la concientización del personal.

Por último, la capacitación del personal solo llegará a este punto, a menos de que la respalden los recursos que los(as) empleados(as) necesitan. Para este fin, los(as) directores(as) de tecnología podrían considerar encuestar a sus equipos para evaluar su comprensión de las medidas de ciberseguridad y preguntar cuáles son sus preocupaciones. Los(as) empleadores(as) deberían proporcionar apoyo uno(a) a uno(a) para ayudar al personal a actualizar o mejorar la seguridad en su oficina en casa y en sus dispositivos.

ANÁLISIS DE LAS ESTRATEGIAS DE COMPUTACIÓN EN LA NUBE

Las personas participantes clasificaron en tercer lugar la revisión de las estrategias de la computación en la nube en nuestra encuesta HLB9. De acuerdo con Gartner[10], “a nivel global, el gasto de usuario final en servicios de la nube pública aumentará un 23.1% en 2021”. Gartner estima que “al menos el 40% de todo el uso de acceso a distancia provendrá predominantemente del acceso a redes de cero confianza (ZTNA, por sus siglas en inglés), en comparación con el casi 5% a finales de 2020”. Aunque Gartner pronostica la continuación del uso de la VPN, dice, “El ZTNA se convertirá en la primera tecnología de reemplazo”.

Bakkar afirma, “Cambiar a una arquitectura de cero confianza es una gran, gran tarea. Hay que cambiar procesos, políticas, hardware y sistemas. No es un cambio barato ni rápido. Cambiar al ZTNA significa que no se confía en nada hasta que se atraviesan los procesos internos de seguridad, como 2FA. Solo cuando el usuario final obtiene la “confianza”, puede acceder a las redes y las aplicaciones.

REALIZACIÓN DE UNA EVALUACIÓN INTERNA DE RIESGOS

En 2020, más de la mitad de las personas participantes en la encuesta estaban al tanto de situaciones cibernéticas anormales y el 12% había experimentado una filtración. Sin embargo, muchos cibercrímenes pasan desapercibidos durante meses o años. Y es casi imposible dar prioridad a los objetivos de ciberseguridad y saber dónde colocar sus fondos presupuestales sin realizar primero una evaluación interna de riesgos.

Ya que la mayoría de las personas participantes en la encuesta de este año están tomando medidas inmediatas para mejorar la ciberseguridad, hay una buena posibilidad de que hayan realizado una evaluación interna de riesgos y se basen en ella. Pero es importante notar que los equipos de TI deberían realizar

con regularidad evaluaciones de amenazas. Algunas empresas podrían preferir subcontratar la evaluación para garantizar que se realiza de forma correcta y oportuna.

EVALUACIÓN DE RIESGOS DE CIBERSEGURIDAD DE TERCEROS (PROVEEDORES)

Las evaluaciones de proveedores también tuvieron un lugar bajo en nuestra encuesta de 2020, conforme los(as) líderes dieron prioridad a las acciones internas por encima de lo que hacen los demás. Sin embargo, el año pasado, grandes corporativos, como Marriott, P&N Bank y General Electric enfrentaron ataques después de la filtración de un proveedor externo. De acuerdo con el informe Mastercard RiskRecon[11], los(as) líderes consideran que los ataques a la mayoría de sus proveedores ocasionarían un riesgo o un efecto grave en su empresa.

Sin embargo, el informe afirma que el 57% de las personas participantes adujeron a la falta de personal sus dificultades para mantener la gestión de riesgos de proveedores externos. Debido a los presupuestos ajustados y a la falta de fuerza laboral, es desafiante realizar evaluaciones y monitorear el cumplimiento de los proveedores. Al mismo tiempo, hay una oportunidad para los proveedores de evaluaciones para apoyar a los rezagados con sus evaluaciones y planificación.

FIGURA 4: DESARROLLAR UN PLAN DE RESPUESTA ANTE INCIDENTES ES AHORA UNA PRIORIDAD PRINCIPAL

P: CLASIFIQUE POR ORDEN DE PRIORIDAD LAS SIGUIENTES ACCIONES PARA FORTALECER LA CIBERSEGURIDAD:

LAS PERSONAS PARTICIPANTES CLASIFICARON LAS ACCIONES EN EL ORDEN SIGUIENTE:

1. DESARROLLAR UN PLAN DE RESPUESTA A LOS INCIDENTES
2. PROPORCIONAR CAPACITACIÓN EN MATERIA DE CIBERSEGURIDAD PARA LAS ESTRATEGIAS DE LA FUERZA LABORAL
3. REALIZAR UN ANÁLISIS DE NUESTRAS ESTRATEGIAS DE COMPUTACIÓN EN LA NUBE
4. REALIZAR UNA EVALUACIÓN INTERNA DE RIESGOS
5. REALIZAR UNA EVALUACIÓN DE RIESGOS A TRAVÉS DE UNA ENTIDAD EXTERNA

10 Gartner, 2021. Gartner Forecasts 51% of Global Knowledge Workers Will Be Remote by the End of 2021

11 Mastercard: Riskrecon, 2021. The State of Third-Party Risk Management

UNA CONVERSACIÓN HONESTA: CÓMO AFRONTAN LOS(AS) DIRECTORES(AS) DE TECNOLOGÍA LOS DESAFÍOS DE CIBERSEGURIDAD

Preguntamos a las personas participantes de este año: ¿Qué medidas específicas ha estado tomando para proteger a su empresa de los ataques de ciberseguridad más frecuentes, como phishing o ransomware? Sus respuestas nos muestran el alcance y la importancia de varias estrategias y la dedicación a una estrategia de capas múltiples.

A continuación, verá formas en las que las personas participantes de la encuesta HLB de 2021 afrontan la ciberseguridad en su empresa:

Servicios de ciberseguridad: Muchas dependen de asesores(as) de confianza, como expertos(as) en ciberseguridad. Contratan a empresas de ciberseguridad para liberar a su equipo interno para dar prioridad al firmware y a los parches. Las empresas externas también apoyan con evaluaciones y capacitación del personal.

Empleados(as) de TI: Las personas participantes implementan equipos especializados con la responsabilidad principal de gestionar los incidentes de phishing y ransomware. Están preparadas para identificar, rastrear y aislar las amenazas para proteger la información de los(as) clientes en la nube.

Dirección de seguridad de TI: Varias crearon un nuevo puesto laboral de TI. Esta posición se coordina con cada gerente(a) de sistema de TI y supervisa todas las tareas relacionadas con la cibernética, lo que incluye garantizar que los dispositivos tengan clientes finales gestionados de forma actual y centralizada.

Analítica: Las personas participantes también aumentaron su uso de la analítica y el informe de situaciones de seguridad. El monitoreo y la acción con base en los tres principios de la seguridad de la información (confidencialidad de datos, integridad y disponibilidad) son fundamentales.

Herramientas de ciberseguridad: Los(as) directores(as) de tecnología implementan varias herramientas tecnológicas para dar apoyo a los esfuerzos de ciberseguridad, como el uso de servicios en la nube para la recuperación frente a desastres, poner en cuarentena los correos electrónicos desconocidos, el uso de verificación de cuenta para correos electrónicos y el encriptado de datos.

Políticas y protocolos: Las empresas adoptan procedimientos claros para informar y lidiar con los correos electrónicos sospechosos, protocolos para el control de versiones y la retención de archivos, y mantener un plan de recuperación de rápida respuesta.

Capacitación del personal: Con estrategias que van desde las capacitaciones obligatorias para el acceso a las redes, hasta los talleres a nivel empresarial, las personas participantes se centran en aumentar la conciencia y desarrollar buenos hábitos de higiene cibernética.

LA CIBERSEGURIDAD: LA OPORTUNIDAD FRENTE A LA AMENAZA

En la encuesta de este año les preguntamos a las personas participantes si veían a la ciberseguridad como una amenaza o una oportunidad. El 45% la vio como una oportunidad para ofrecer servicios de asesoría, en comparación con el 44.85% que la vio como una amenaza que consume recursos empresariales. Menos del 10% de las personas participantes no anticipa cambios drásticos, mientras que más del 90% cree que las amenazas continuarán creciendo a ritmo acelerado.

Bakkar afirma, "Yo creo que tiene que haber un riesgo para crear una oportunidad. Si todo fuera perfecto, no habría ninguna oportunidad". Para los(as) líderes, quienes toman medidas a nivel de dirección y tienen un marco operativo en funcionamiento, las oportunidades son inmensas. Son los(as) líderes del sector y pueden ofrecer servicios de asesoría, informes cibernéticos sobre auditorias de TI, servicios de centro de operaciones de seguridad, y contratos de riesgo y control de TI.

Ya que menos del 3% de las personas participantes utiliza un servicio de ciberseguridad externo, hay una oportunidad significativa en esta área para demostrar el valor de sus servicios como socio de tecnología de confianza.

Al mismo tiempo, la ciberseguridad representa una amenaza. Es costoso implementar cambios, proporcionar recursos suficientes y dar prioridad a la ciberseguridad. Si estos gastos se reducen de las áreas que generan ingresos, los(as) líderes podrían preocuparse a causa de la sustentabilidad del programa. En consecuencia, las personas participantes sienten la preocupación de que un aumento repentino en las amenazas esté por venir.

45%

VERLO COMO UNA OPORTUNIDAD PARA OFRECER SERVICIOS DE ASESORÍA

10%

DE LOS ENCUESTADOS NO ESPERAN CAMBIOS DRÁSTICOS

PASOS SIGUIENTES: ASEGURAR EL FUTURO

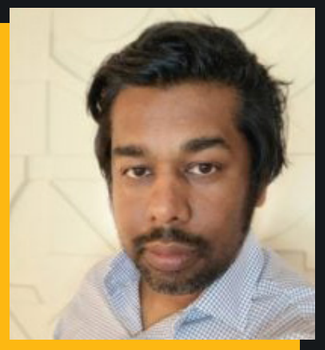
Algunas empresas dirigen el sector apresurándose a ajustar los protocolos y desarrollar marcos operativos. Otras se retrasan, pero buscan las mejores prácticas y las soluciones rápidas, mientras avanzan en el desarrollo de lugares de trabajo híbridos seguros. Por último, una minoría de líderes hizo cambios mínimos y sigue manteniendo al personal en un ambiente seguro, en las instalaciones dentro del perímetro corporativo. En este caso, el sector, el tamaño de la empresa o la ubicación geográfica podría reducir la necesidad de tener personal a distancia, herramientas basadas en la nube o medidas de seguridad fuera de las instalaciones.

Sin embargo, es un hecho que los ciberataques siguen en aumento, sin importar el tamaño o el sector de las empresas. Y los(as) creadores(as) de amenazas sofisticadas siguen encontrando formas de obtener acceso a los datos y programas fundamentales para las empresas. Mientras que una estrategia fragmentada funciona como solución temporal, una estrategia integral de ciberseguridad, operada a nivel de la dirección, es vital para las empresas con una fuerza laboral que trabajará de forma híbrida a largo plazo.

Además, una de las mejores medidas que los(as) líderes pueden tomar es diseñar programas de concientización y capacitación del personal, que incluyan campañas para destacar amenazas específicas y módulos interactivos centrados en el desarrollo de buenos hábitos. Conforme su empresa navega el panorama del riesgo cibernético, nuestros(as) asesores(as) de confianza pueden serle de ayuda. Póngase en contacto con nosotros para conocer la forma de aprovechar las oportunidades mientras se mitigan las amenazas.

CONTÁCTENOS

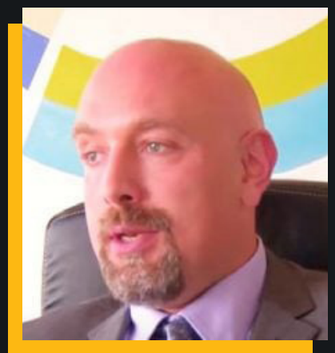
Nuestros expertos en ciberseguridad están listos para ayudar a identificar riesgos y proteger su negocio en el entorno de trabajo remoto actual. Operamos en 159 países en todo el mundo. Contáctenos:



ABU BAKKAR
Chief Innovation Officer
a.bakkar@hlb.global

JIM BOURKE
Global Advisory Leader
j.bourke@hlb.global

CARLOS CAMACHO
HLB Digital
c.camacho@hlbdigital.global



ALMERINDO GRAZIANO
HLB Digital
a.graziano@hlbdigital.global

CARLOS MORALES
HLB Digital
c.morales@hlbdigital.global

GUSTAVO SOLIS
HLB Digital
g.solis@hlbdigital.global

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

THE GLOBAL ADVISORY AND ACCOUNTING NETWORK