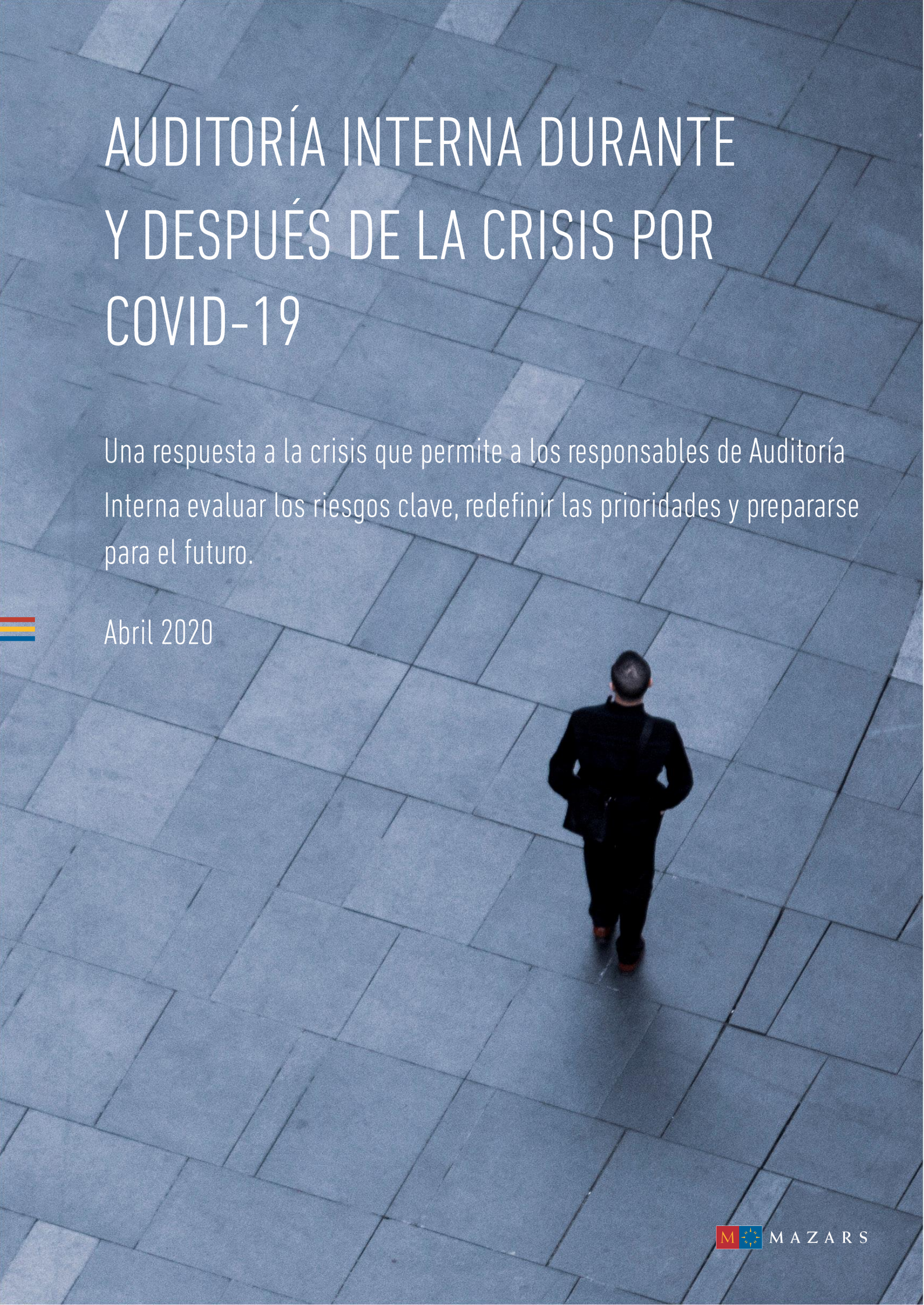
AUDITORÍA INTERNA DURANTE Y DESPUÉS DE LA CRISIS POR COVID-19

Una respuesta a la crisis que permite a los responsables de Auditoría Interna evaluar los riesgos clave, redefinir las prioridades y prepararse para el futuro.

Abril 2020



MAZARS

Estimada comunidad de Auditoría Interna,

Publicamos este documento en tiempos difíciles. El mundo, tal como lo conocemos, parece haberse detenido, y enfrentamos luchas sin precedentes, tanto en el frente de la salud, como en el económico. A lo largo de este período, el papel de la auditoría interna será fundamental.

El presente documento ha sido redactado para permitir que los auditores internos brinden servicios personalizados, relevantes y alineados con la orientación de la industria, como la del Instituto de Auditores Internos. Las siguientes páginas incluyen asesoramiento sobre áreas a evaluar y sugerencias prácticas sobre cómo relacionarse con sus partes interesadas.

Como este es un momento de crisis global, hemos trabajado juntos como una comunidad integral para brindarle esta información. Esperamos que sea de utilidad y en caso de tener alguna pregunta o deseara platicar más al respecto, no dude en ponerse en contacto.

Como siempre, les deseo salud y por favor cuídense.

Mercedes Rodríguez
Country Managing Partner

Contenido

01	El rol de la Auditoría Interna durante el Covid-19	4
02	Comprender y evaluar la gama completa de riesgos inmediatos	6
03	Evaluar la resiliencia organizacional	11
04	Asesorar sobre riesgos futuros y pensar más allá de los riesgos inmediatos	12
05	Continuar monitoreando y actualizando las necesidades de la organización y el plan de auditoría	13
06	Cómo podemos ayudarle	14

01

El rol de la auditoría interna durante el Covid-19

¿Qué significa "business as usual" en estos tiempos sin precedentes?

La pandemia de Covid-19 ha tenido efectos disruptivos y sin precedentes en individuos, empresas, gobiernos y sociedades. Debido a ello, muchas organizaciones han pasado a tener empleados que trabajan desde casa y han adoptado nuevos modelos operativos para continuar con el negocio.

Estas excepcionales circunstancias, requieren un enfoque renovado de la auditoría interna (AI) que considere el conjunto específico de habilidades, competencias, supervisión y conocimiento que aporta la AI. Ésta no puede simplemente insistir en entregar planes de auditoría existentes para las organizaciones. Las organizaciones están atravesando disrupciones y cambios significativos, y es poco probable que los planes de auditoría sean adecuados para su propósito ahora.

¿Cómo debería adaptar su enfoque la AI?

La AI debe evaluar completamente los impactos operativos que enfrentan las organizaciones y los nuevos entornos de control en los que están operando (principalmente, trabajo remoto y en línea) y ajustar el plan de auditoría en consecuencia. Ésto, con el objetivo de que la AI pueda proporcionar contribuciones específicas y valiosas a las organizaciones en sus áreas prioritarias inmediatas en los próximos meses.

Las organizaciones deben comprender y mitigar los riesgos de crisis que enfrentan actualmente en el contexto de sus propias obligaciones, actividades, objetivos y valores. La AI debe proporcionar información relevante y ser garantía para la gestión de los riesgos emergentes debido a la crisis.

La AI también debe ser proactiva y continuar desempeñando un papel importante para ayudar a las organizaciones a comprender el impacto del COVID-19 en su entorno de control. Esto incluye ayudar a las organizaciones a construir y dar forma a sus entornos de control en el contexto de los acuerdos del trabajo remoto, así como proporcionar información y garantías sobre la eficacia de esos controles. La AI tiene la función de proporcionar asesoramiento de consultoría y soporte de primera línea bajo los Estándares Globales de Auditoría Interna.

¿Cómo debería la AI continuar con sus actividades de aseguramiento y asesoramiento?

La AI debe emprender las siguientes acciones clave:

- Comprender y evaluar la gama completa de riesgos inmediatos:
  - Gobierno, comunicaciones e informes
  - Gestión de riesgos y problemas
  - Entorno de controles
  - Riesgos operacionales
  - Capital humano: salud, seguridad y bienestar
- Evaluar la gestión de crisis y los planes de continuidad del negocio, incluidos los acuerdos de TI.
- Asesorar sobre riesgos futuros y pensar más allá de los riesgos inmediatos.
- Adaptarse al trabajo remoto, y continuar brindando servicios efectivos.
- Continuar monitoreando y actualizando las necesidades de la organización y el plan de auditoría.

La AI debería proporcionar soporte directo a la administración, incluyendo su participación en discusiones de alto nivel. Esto con el objetivo de que la AI proporcione aportaciones valiosas y oportunas durante estos tiempos sin precedentes, en lugar de brindar auditoría y aseguramiento "después del evento", a través de revisiones "post-mortem" en un futuro.

Este es un momento en que la AI puede agregar valor real y apoyar a las organizaciones y partes interesadas en tiempos difíciles y desafiantes.

02

Comprender y evaluar la gama completa de riesgos inmediatos

Los Consejos y los Comités de Auditoría quieren asegurarse de que las organizaciones hayan podido adaptarse a las disrupciones provocadas por la pandemia de COVID-19. La AI debe dar soporte a través de las siguientes acciones:

- Comprender y evaluar los posibles impactos para las organizaciones en función de los riesgos inmediatos que enfrentan. La AI puede facilitar la evaluación de riesgos.
- Considerar los desafíos inmediatos, por ejemplo, los problemas que enfrentan las organizaciones actualmente, validar si las actividades de mitigación son suficientes, así como considerar los riesgos que enfrentan. Es probable que los problemas inmediatos tengan mayor prioridad que los riesgos potenciales.
- Ayudar al Consejo y a la dirección de alto nivel a reevaluar los riesgos y a determinar si las actividades de mitigación de los asuntos actuales son suficientes.
- Reenfocar el negocio en lo que más importa.
- Brindar apoyo y asesoramiento sobre los desafíos clave que pueden enfrentar, incluidas las medidas gubernamentales de las que podrían beneficiarse.

Hay una serie de riesgos inmediatos que las organizaciones deberían de estar evaluando y mitigando desde ahora, incluidos:

- Gobierno, comunicaciones e informes.
- Gestión de riesgos y problemas.
- Ambiente de controles.
- Riesgos operacionales.
- Salud, seguridad y bienestar.

En las siguientes páginas se revisa cada una de estas áreas con más detalle.

Guía práctica para los auditores:

- A corto plazo, los auditores deben **descartar el registro de riesgos corporativos** (ya que probablemente esté desactualizado) e involucrarse directamente con las partes interesadas para comprender los desafíos que enfrentan. Levante el teléfono y verifique cómo se encuentran las principales partes interesadas.
- **Considere el panorama general,** es probable que algunas organizaciones se enfrenten a amenazas existenciales y la AI debería considerar el escenario actual más amplio y las limitaciones bajo las cuales las organizaciones están operando.
- **Restablezca las prioridades del plan de auditoría.** Probablemente lo que está considerado como más importante en su plan de auditoría, ya no está relacionado con los principales riesgos que enfrenta la organización. Se debe realizar una reevaluación rápida, pero exhaustiva de los principales riesgos, y en consecuencia, debe revisarse el plan de auditoría.
- **Presionar para entregar el plan de auditoría existente, no es el mejor enfoque.** Hay varias formas de apoyar a las organizaciones, incluido el trabajo de asesoramiento / proyecto hasta asistir a reuniones de la administración y brindar apoyo y orientación directa.
- **Las auditorías deben centrarse sólo en las preguntas clave cuando se planifican.** Las auditorías no deben avanzar como si la situación fuera "business as usual". Los auditores deben hacer preguntas difíciles sobre las áreas esenciales a cubrir y centrarse en ellas. Es poco probable que las organizaciones deseen revisar áreas de baja prioridad durante los próximos tres a seis meses.
- **Los auditores deben reducir la cantidad de aportes de las partes interesadas y producir informes breves y precisos.**
- **Los informes de auditoría deben recomendar que sólo se remedien las cuestiones más críticas; cualquier otra cosa probablemente será cuestionada.**
- **La AI debería considerar la adopción de enfoques ágiles,** por ejemplo, la priorización a corto plazo de las áreas de auditoría con revisiones periódicas y actualizaciones del plan de auditoría, alineadas con las necesidades de las organizaciones.
- **La AI puede acelerar el uso de análisis para entregar el trabajo de forma remota y aumentar la cobertura.**
- **La AI debería discutir el uso de su presupuesto de una manera diferente,** por ejemplo, apoyo directo para actividades clave como la gestión de soporte, nuevos sistemas y procesos.

Consulte el Hub de Mazars sobre Covid-19, que incluye información de interés y medidas gubernamentales:
www.mazars.co.uk/Home/Services/COVID-19-Your-Business

Gobierno, comunicaciones e informes

Las organizaciones que han adaptado rápidamente su enfoque a la gobernanza, las comunicaciones y los informes probablemente estarán mejor ubicadas para comprender y mitigar los impactos operativos. La AI debe dar soporte a través de las siguientes acciones:

- Evaluar si existen responsabilidades claras entre el Consejo, los Comités de Auditoría y Riesgo y el equipo de administración.
- Evaluar si el Consejo está recibiendo información oportuna y relevante.
- Ayudar a la Administración a desarrollar mensajes centralizados y oportunos de los líderes a los empleados para infundir confianza y calma, contrarrestando el miedo y la información errónea.

Gestión de riesgos y problemas

Los Consejos y los Comités de Auditoría quieren saber y tener la seguridad de que las organizaciones han podido adaptar rápidamente su enfoque operativo y que está funcionando de manera efectiva.

La AI debería considerar la mejor manera de contribuir a los procesos de gestión de riesgos. Por ejemplo, dar información a grupos / reuniones de gestión de riesgos y facilitar el proceso de evaluación de riesgos.

Esto es particularmente importante para los procesos de gestión de riesgos y problemas a los que la AI debería dar soporte, a través de las siguientes acciones:

- Revisar las capacidades de gestión del riesgo operativo, como la gestión de crisis, la continuidad del negocio, el riesgo de terceros y los seguros.
- Verificar que todos los miembros clave del equipo hayan sido identificados y entiendan completamente sus deberes y que confíen en su capacidad para llevar a cabo las responsabilidades.

Guía práctica para los auditores

- Evaluar si la administración cuenta con recursos adecuados interna o externamente para ayudar a evaluar y mitigar el riesgo. Determinar si la administración está planeando horizontes de tiempo más largos; esto debería ser un mínimo de 6 meses con las medidas gubernamentales vigentes.
- Evaluar si los procesos de gobernanza y presentación de informes se han adaptado al trabajo remoto. Esto incluye si lo que se informa y escala hacia arriba es apropiado y se enfoca en las áreas de alto riesgo o alta prioridad, es decir, las áreas operativas más afectadas.
- Ofrecer apoyo a las organizaciones que no se limite exclusivamente a la AI. Puede ser que las unidades organizacionales tengan personal insuficiente por varias razones (incluido el personal que está de incapacidad por enfemedad) y requieran más “manos”. Por lo tanto, pueden requerir especialistas en riesgos, controles y cumplimiento para reforzar los equipos internos en toda la empresa.

Guía práctica para los auditores

- Comprender los procesos de gestión de riesgos y problemas, incluidos los informes y el escalamiento. ¿La organización valora la gestión de riesgos? ¿Cómo ha cambiado desde que comenzó el trabajo remoto?
- ¿En qué medida impacta Covid-19 en el marco de gestión de riesgos existente y los registros de riesgos correspondientes? ¿La organización está trabajando proactivamente para identificar posibles riesgos, impacto y respuestas de mitigación?
- Si las capacidades de gestión de riesgos operativos no existen o son insuficientes, ofrezca involucrar a la gestión de riesgos y a profesionales de la AI para ayudar en el desarrollo y la implementación de un marco de gestión de riesgos.

Entorno de control

Los Consejos y los Comités de Auditoría querrán garantías de que las organizaciones han podido adaptar de manera rápida y efectiva su enfoque operacional y el entorno de control a las nuevas formas de trabajo implementadas en respuesta a Covid-19.

Esto es especialmente importante para el mantenimiento del entorno de control que la AI debería soportar mediante las siguientes acciones:

- Comprender cómo las organizaciones han implementado e incorporado un nuevo entorno de control en estas circunstancias desafiantes.
- Asegurar que existan controles clave (ajustados), tales como un nivel mínimo de segregación de funciones, evidencia de revisiones y aprobaciones de la administración.
- Se debe considerar otorgar entrenamiento, soporte y supervisión, revisión e informes adicionales de la administración.

Guía práctica para los auditores

- Los auditores no deben depender del archivo del año pasado o en el banco de controles esperados, al evaluar nuevos entornos de control.
- Los auditores deben volver a una página en blanco, documentar y evaluar los procesos para capturar los controles, antes de evaluar si mitigan los riesgos actuales.
- Algunas preguntas que los auditores deben considerar son:
  - ¿Los controles clave están cubiertos y diseñados de manera efectiva en los procesos primarios?
  - ¿Deben considerarse controles adicionales con respecto a la exposición de la organización a las influencias internas y externas?
  - ¿Cómo se puede mantener la supervisión de los empleados cuando el personal trabaja de forma remota?
  - ¿Se han considerado y diseñado controles de gestión adicionales, como el riesgo y el cumplimiento?
  - ¿Se han diseñado e implementado nuevos informes de gestión?

Riesgos Operacionales

Las partes interesadas dentro de las organizaciones querrán asegurarse de que las unidades de negocio y los equipos entiendan sus riesgos operativos clave y hayan implementado medidas efectivas para mitigar esos riesgos. Esto podría aplicarse, más no limitarse, a las siguientes áreas:

- **Comportamiento del cliente.** Es probable que esto reduzca la demanda y las ventas, lo que resulta en menores ingresos e impactos en el flujo de efectivo. Esto podría resultar en una amenaza para las organizaciones.
- **Cadenas de suministro.** Podría haber interrupciones en las cadenas de suministro que resulten en riesgos para la producción. Las organizaciones deberían:
  - Determinar qué socios comerciales y proveedores pueden verse más afectados, y si los proveedores alternativos pueden proporcionar una solución para satisfacer las necesidades comerciales.
  - Evaluar si los proveedores tienen planes documentados para la continuidad de la unidad de negocios y la recuperación de desastres de tecnología de la información, incluyendo para negocios críticos.
  - Cambiar la combinación de producción y planear nuevos métodos de entrega para llegar a los clientes.
- **Capital y liquidez.** La AI debería comprender los requisitos de capital de trabajo, frente a los supuestos de planificación de escenarios y los flujos de efectivo previstos. Esto incluye evaluar si las organizaciones han hecho uso de esquemas gubernamentales.
- **Cumplimiento contractual.** Existe el riesgo de que las obligaciones contractuales se vean afectadas. Las organizaciones deberían:
  - Consultar a sus asesores legales y revisar sus contratos para determinar el impacto y los derechos que tienen.
  - Tomar medidas razonables para mitigar el impacto de Covid-19. Es posible que necesiten cuantificar la cantidad de daño financiero y el impacto en sus relaciones comerciales a largo plazo.
  - Revisar sus pólizas de seguro existentes para averiguar si las pérdidas en que incurran, en relación con Covid-19 pueden cubrirse bajo los términos existentes.

Guía práctica para los auditores

- La AI debe evaluar cómo las organizaciones están reaccionando a los cambios, incluyendo los procesos y controles de gobernanza asociados, como pueden ser:
  - Capital y liquidez
  - Cobros en efectivo
  - Pagos a proveedores
  - Producción
  - Gestión de proveedores
- La AI debería evaluar con qué eficiencia se están llevando a cabo los procesos de gestión del cambio.
- La AI debería evaluar si las organizaciones se han hecho las preguntas difíciles para comprender realmente los impactos operativos de Covid-19. Esto incluye la implementación de acciones a corto, mediano y largo plazo.
- La AI debería asesorar sobre liquidez y gestión financiera y, en particular, centrarse en el riesgo contractual.

Consulte el Hub de Mazars sobre Covid-19, que incluye orientación sobre la gestión del flujo de efectivo:

www.mazars.co.uk/Home/Services/COVID-19-Your-Business/Covid-19-Cash-Flow-Management

Capital Humano - Salud, seguridad y bienestar

Los empleadores tienen las mismas responsabilidades de salud y seguridad para los trabajadores remotos, que para cualquier otro trabajador. Con las medidas de distanciamiento social y autoaislamiento del gobierno, ahora existen mayores riesgos para el bienestar mental y físico de las personas.

Las organizaciones han adoptado rápidamente el trabajo remoto para la gran mayoría de la fuerza laboral, a fin de seguir las pautas gubernamentales y garantizar que las operaciones puedan continuar. Como consecuencia, los controles de salud y seguridad típicos, podrían no haberse realizado por completo. Se espera que el bloqueo gubernamental actual se mantenga vigente durante un período prolongado y, en menor medida, más allá del período de verano.

Por lo tanto, las organizaciones querrán la garantía del área de AI de que están brindando el apoyo adecuado a sus empleados para que puedan trabajar en un entorno seguro. Esto incluye poner en práctica medidas para apoyar el bienestar mental de los empleados, además de su bienestar físico.

Guía práctica para los auditores

Cuando alguien trabaja desde casa, de forma permanente o temporal, la AI puede ayudar a las organizaciones a considerar:

- ¿Cómo se mantendrán en contacto con los trabajadores a domicilio?
- ¿Qué actividades laborales realizarán y podrán realizar (y durante cuánto tiempo)?
- ¿Se puede realizar esta actividad de manera segura?
- ¿Deben establecerse medidas de control para protegerlos?

Los auditores deben evaluar si las "soluciones" utilizadas durante el período de bloqueo están normalizadas y controladas adecuadamente.

Los auditores deberían evaluar si el impacto en las nuevas formas de trabajo ha sido considerado por los procesos de gestión de Recursos Humanos y desempeño, tales como las evaluaciones anuales de desempeño y el enfoque de la capacitación y el coaching.

Consulte el Hub de Mazars sobre Covid-19, que incluye orientación sobre el talento en su negocio:

www.mazars.co.uk/Home/Services/COVID-19-Your-Busines
Business/Covid-19-People-In-Your-Business

03

Evaluar la resiliencia organizacional

La AI debería considerar qué impacto está teniendo Covid-19 en la capacidad de resiliencia de una organización, incluida la gestión de crisis y planes de continuidad del negocio existentes. Ésto evaluará si hay vacíos en esos planes. La AI podría proveer aseguramiento sobre la efectividad de acciones de crisis seleccionadas.

La AI debería considerar cuándo revisaron por última vez estos acuerdos y si se podría proporcionar algún otro consejo, apoyo o aseguramiento. Ésto implicaría evaluar las lecciones aprendidas de cómo esos planes funcionaron en la práctica.

La AI también podría considerar qué disposiciones están implementando las organizaciones para la fase de "recuperación" y cómo cumplirán con las demandas a medida que se levanten las restricciones, etc.

Las organizaciones ya deberían haber implementado los planes existentes de gestión de crisis y continuidad del negocio. Para muchas organizaciones, tener que operar con la mayoría de la fuerza laboral trabajando de forma remota, no es algo planeado. Esto trae una serie de desafíos de TI que la AI debería evaluar, por ejemplo:

La AI debería evaluar los riesgos cambiantes relacionados con una mayor dependencia y uso de TI como facilitador principal en la crisis, que puede incluir las siguientes áreas:

- Si la configuración de seguridad para las conexiones remotas y los mecanismos de acceso individual seguros están implementados y funcionan de manera efectiva.
- Determinar si cuentan con la capacidad de red para una gran cantidad de empleados trabajando de forma remota durante un período prolongado.

Debido a una mayor flexibilidad de trabajo y acuerdos remotos, las personas requieren un mayor acceso a los sistemas, incluida la cobertura cuando las personas no están trabajando. Por lo tanto, se deben mantener controles críticos de acceso del usuario. La AI debería considerar los controles de monitoreo establecidos, si existe una segregación apropiada de funciones y pistas de auditoría para los cambios de acceso.

Guía práctica para los auditores

Como se señaló anteriormente, muchas organizaciones habrán implementado e incorporado nuevos entornos de control. Estos han sido soportados por los auditores de TI y deben evaluar lo siguiente:

- Si hay suficiente capacidad de TI para prestar los servicios requeridos.
- Si existen medidas de seguridad apropiadas.
- Que los controles han sido diseñados e implementados adecuadamente.

Todavía es valioso revisar la gestión de crisis y los planes de continuidad del negocio para identificar cualquier brecha y determinar la mejor manera de garantizar que las partes interesadas estén informadas de las actividades de la organización. Esto incluye educar al personal sobre los protocolos a seguir en caso de que ocurra un brote local o medidas adicionales introducidas por el gobierno.

Consulte el Hub de Mazars Sobre Covid-19,

www.mazars.co.uk/Home/Services/COVID-19-Your-Business/Covid-19-Business-Continuity-Measures

04

Asesorar sobre riesgos futuros y pensar más allá de los riesgos inmediatos

Si bien las organizaciones a menudo se centran en sus riesgos y desafíos inmediatos, la AI debería ayudar a las organizaciones a pensar más allá. Esto podría ser para los riesgos más amplios que las organizaciones podrían enfrentar al adaptarse a la "nueva normalidad".

Estos riesgos podrían incluir ciberfraude, cultura y capital humano, cadena de suministro, salud y seguridad y amenazas a la reputación. Dado el rápido cambio de muchas organizaciones para trabajar de forma remota, éstas deberían considerar inicialmente el riesgo de fraude:

- El cambio de controles, ya sea intencional o no, también puede provocar la elusión de dichos controles, suavizar los principios de segregación de funciones o anular los procedimientos de aprobación habituales.
- Las desviaciones del modo "business as usual" y la posible racionalización de los recursos, a menudo dan como resultado un menor nivel de control. Ésto, junto con el aumento de las presiones operativas, podría crear comportamientos oportunistas por parte de los individuos.

La AI debería evaluar y ayudar a las organizaciones a interpretar los cambios regulatorios, como los requisitos bancarios para aumentar las pruebas de estrés de cartera o la documentación de continuidad.

La AI también debe proporcionar asesoramiento sobre la comunicación y las prácticas de auditoría revisadas. Puede ser necesario ayudar a las organizaciones a comunicarse con las partes interesadas y adoptar las nuevas orientaciones relativas a la evidencia virtual de auditoría.

Además, será necesario ayudar a las organizaciones a evaluar si las transformaciones de control se han incorporado adecuadamente. La AI puede evaluar si los controles continúan funcionando según lo previsto y si la documentación es adecuada. Esto puede incluir políticas de trabajo remoto, autorización y reconciliación de transacciones, y seguridad física, entre otros temas.

Guía práctica para los auditores

- Los auditores internos deben utilizar el conocimiento de organizaciones similares (a través de relaciones entre pares o socios co-source) para asesorar sobre cómo otras organizaciones enfrentan desafíos similares.
- Los auditores internos deben transmitir las mejores prácticas entre las organizaciones, incluidos los riesgos futuros que esperan.
- Con respecto al riesgo potencial de fraude, la AI debe considerar las siguientes preguntas:
  - ¿Existe una evaluación de riesgo de fraude en la organización? ¿Se ha actualizado para reflejar amenazas y riesgos para Covid-19?
  - ¿Ha considerado la organización qué procesos tienen un mayor riesgo de fraude?
  - ¿Están cubiertos y diseñados de forma efectiva en los procesos los controles clave?
  - ¿Cómo se puede controlar o chequear a los empleados si trabajan desde casa?
  - ¿Existe suficiente conciencia de las áreas donde hay posibilidad de fraude, como la facturación y los pagos?
  - ¿La organización ha considerado la implementación de contramedidas de baja fricción para prevenir el riesgo de fraude? Estos pueden incluir controles electrónicos para identificar y verificar la cuenta del solicitante / empresa / beneficiario, o el uso de cláusulas de prevención de fraude por adelantado en los formularios y procesos de solicitud.

05

Continuar monitoreando y actualizando las necesidades de la organización y el plan de auditoría

La AI debería trabajar en estrecha colaboración con la administración para monitorear continuamente lo que sucede dentro y fuera de las organizaciones.

La AI debería apoyar a las organizaciones para comenzar a ver más allá de la crisis actual y considerar la planificación de la reanudación del negocio. Es posible que muchas organizaciones se den cuenta de que sus planes de reanudación del negocio son inadecuados. Además, es factible que los cambios en los modelos de negocio requieran nuevas estrategias de reanudación y planes estratégicos.

En el futuro, es probable que las organizaciones analicen sus procesos para garantizar que se puedan llevar a cabo de forma ágil y remota. Esto incluirá una mayor digitalización y automatización. Seguramente será necesario que las organizaciones reevalúen los procesos manuales y planifiquen una mayor automatización, no sólo para mejorar la eficiencia y el rendimiento de los costos, sino también para reducir el riesgo de depender de los recursos en sitio. La automatización de procesos robóticos (RPA) puede incluir el diseño y la implementación de áreas operativas, así como del área de AI. Puede haber áreas que la AI debería evaluar sobre la gobernanza, el riesgo y los controles en torno a estos procesos transformados.

La AI debe ser ágil y ajustar los planes en consecuencia y, cuando sea posible, trabajar con otras funciones dentro de la organización, como el riesgo y el cumplimiento.

La AI puede ayudar a las organizaciones a construir un enfoque integrado para proporcionar información, seguridad para el Consejo y el Comité de Auditoría.

Guía práctica para los auditores

- Los auditores deben entablar un diálogo continuo y frecuente con las partes interesadas para monitorear y comprender los desafíos que enfrentan.
- Los auditores deben incrementar el número de reuniones para ver el progreso, llamar regularmente y verificar cómo se encuentran las partes interesadas clave.
- Los auditores deben continuar enfocándose en el panorama general y no estar sujetos a los planes de la AI. Éstos deben ajustarse y modificarse, a medida que las organizaciones enfrentan diferentes desafíos.
- Además de los servicios estándar de AI, podrían ofrecerse servicios de asesoría o recursos para asumir roles de negocio, si fuera necesario.

06

Cómo podemos ayudar

Hay muchas maneras en que las organizaciones deben prepararse para la "nueva normalidad" y operar después de que la pandemia retroceda. Estos podrían ser impulsados por:

- Cambios en la estrategia
- Cambios en el modelo operativo
- Cambios en la estrategia y arquitectura de TI, incluida la automatización de los procesos
- Cambios en las relaciones e interacciones con clientes y proveedores
- Cambios en el entorno laboral

Hay numerosos impulsores para el cambio dentro de las organizaciones. Contamos con las habilidades y la capacidad para apoyar a las organizaciones de varias maneras, a través de trabajos de auditoría interna, asesoramiento o consultoría.

Las siguientes páginas incluyen algunas de nuestras ofertas de servicios principales, que las organizaciones pueden encontrar útiles, para ayudar a navegar a través de estos tiempos desafiantes, y sin precedentes.

Resiliencia organizacional

Las organizaciones operan en un entorno de constante cambio, con la necesidad de prepararse y planificar una amplia gama de riesgos estratégicos y operativos, respondiendo rápidamente a las crisis. La creación de resiliencia es un imperativo para todas las organizaciones, y requiere una combinación efectiva de gestión de riesgos y mejora continua. Cada organización, independientemente de su tamaño o forma, necesita un marco de resiliencia organizacional que aborde las siguientes áreas. Podemos ayudar a las organizaciones a documentar un marco o brindar seguridad sobre los marcos existentes.

GOBERNANZA

Proporcionar supervisión, toma de decisiones y dirección estratégica, en la crisis y el cambio.

GESTIÓN DE RIESGOS Y PROBLEMAS

Identificar, evaluar y mitigar los riesgos para reducir la probabilidad de impacto.

RECUPERACIÓN DE DESASTRES

Recuperación de la infraestructura, los sistemas, las aplicaciones y los datos tras una crisis.

GESTIÓN DEL CAMBIO

Pasar a nuevas formas de trabajo para aprovechar las oportunidades, responder a los riesgos o crisis, y mejorar continuamente.

GESTIÓN DE CRISIS

Responder a una crisis mediante un control, comunicación y gestión eficaces.

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Habilitar una respuesta eficaz a las crisis para que se puedan seguir prestando servicios importantes.

06

Nuestros Servicios

Resiliencia de TI

La resiliencia de TI "apropiada" puede prevenir o retrasar la necesidad de usar su Plan de Recuperación de Desastres de TI en primera instancia. La resiliencia de TI debe centrarse en:

- **Tecnología.** Resiliencia en los componentes y dispositivos, eliminando puntos únicos de falla y escalabilidad.
- **Personal de TI.** Riesgo de personal clave, capacidad del staff y terceros.
- **Procesos de TI.** Alineación con los estándares de TI, incluida la respuesta a incidentes y la gestión de capacidad y disponibilidad.

La Recuperación de Desastres de TI tradicional supone la pérdida de una aplicación clave o una interrupción total de TI (por ejemplo, una falla del centro de datos) y detalla los procesos que TI seguiría para recuperarlos en línea, con los plazos acordados. Es poco probable que el DRP detalle cómo gestionar un cambio fundamental, casi de la noche a la mañana, en la forma en que los usuarios y clientes consumen servicios de TI.

Los planes tradicionales de Continuidad del Negocio (BCP) suponen la pérdida de un solo edificio de oficinas, en lugar de un cierre completo de todos los edificios de oficinas a la vez, o que el gobierno legisle un cierre económico nacional, por un período de tiempo indefinido.

El Covid-19 es inusual porque cambió fundamentalmente la forma en que una organización usaría TI, sin causar ningún desastre o falla, real o directa relacionada con TI. En cambio vemos:

- Presiones a la capacidad de la red y soluciones de trabajo remoto.
- Aumento del tráfico a los sitios web.
- Mayor demanda a la mesa de ayuda o de servicio de TI (Service Desk).

El Covid-19 será un probable catalizador para cambiar permanentemente los patrones de trabajo, incluyendo:

- Menos viajes / consumismo = reducción de emisiones y contaminación.
- Las empresas se ven obligadas o aprenden a adoptar el trabajo remoto, de manera más regular.
- Las empresas pueden descubrir que sus empleados no desean volver a trabajar todo el tiempo en la oficina, una vez que se levanten los cierres.

El trabajo remoto y las futuras presiones de costos / ingresos, también podrían dar lugar a otros cambios comerciales, como:

- Estrategia de negocios
- Reestructuración
- Estrategia de alojamiento - (racionalización de edificios comerciales)

Todos estos cambios podrían alterar fundamentalmente las necesidades de TI de una organización que requieren una reevaluación de:

1 **Resiliencia de TI / alineación de DRP y BCP** **Covid-19 lecciones de TI aprendidas.** ¿Qué salió bien y qué no tan bien? ¿Los proveedores de TI lo apoyaron como esperaba?
   - **Resiliencia de TI.** ¿Es su capacidad de resiliencia de TI apropiada para su negocio?
   - **Recuperación de Desastres de TI.** ¿Qué procesos DRP existen y son apropiados para la dirección futura del negocio?
   - **Alineación del Plan de Continuidad del Negocio (BCP).** ¿Su DRP está alineado con su BCP?

2 **Arquitectura de TI.**
   - ¿Es la arquitectura de TI correcta para la dirección futura del negocio?

3 **Estrategia de TI.**
   - ¿Covid-19 provocará un cambio en las estrategias de negocio y digitales que deben reflejarse en toda su función de TI?

Si la estrategia de negocio sufrirá cambios como resultado del Covid-19, considere completar lo anterior en orden inverso. La resiliencia de TI aún debe revisarse a corto plazo, también con un enfoque específico en la estabilidad de TI.

Aseguramiento del cambio y del programa

Todas las organizaciones han emprendido cambios como resultado del Covid-19 y muchas lo ven como un desafío, pero también es una oportunidad para rediseñar el proceso para que sean más eficientes. Esto es algo que puede llevarse a cabo de forma remota y eliminar puntos de falla. Las organizaciones implementarán iniciativas y programas de cambio para ofrecer el entorno operativo "normal" y post pandemia.

Por lo tanto, tener aseguramiento efectivo del cambio y del programa, es esencial para evaluar si los riesgos clave del cambio se gestionan de manera efectiva. Nuestra metodología de aseguramiento del cambio y del programa, considera las tres áreas clave, descritas a continuación:

- Gestión del programa. ¿El programa o proyecto está adecuadamente definido, planificado, dotado de recursos, presupuestado, administrado, gobernado y alineado con estrategias y otras iniciativas de cambio?
- Gestión del cambio. ¿Es apropiado el esfuerzo de gestión del cambio con referencia a los enfoques de prácticas líderes esperados?
- "Business as usual". ¿Están siendo efectivamente gestionadas y mitigadas las potenciales disrupciones a las actividades "business as usual" causadas por el programa o proyecto?

Enfoque de evaluación

PLANEACIÓN Y PREPARACIÓN

- ¿Está claro el caso de negocio?
- ¿Los objetivos son claros y se pueden medir?
- ¿Existe un plan de programa de alto nivel que esté actualizado?

GOBERNANZA Y ESTRUCTURA

- ¿Existe un programa de Consejo apropiado?
- ¿Este Consejo está informado y es eficaz?

CONTROLES Y CALIDAD

- ¿Se ha actualizado el caso de negocio a lo largo del programa?
- ¿Están implementados los controles de cambio?

GESTIÓN DE RIESGO

- ¿Se identifican y evalúan los riesgos?
- ¿Se revisan y reportan periódicamente las acciones?

INFORME Y COMUNICACIÓN

- ¿Se informa periódicamente de manera eficaz?
- ¿Se ha definido y aplicado adecuadamente una estrategia de comunicación?

IMPLEMENTACIÓN

- ¿Existen planes de implementación detallados?
- ¿Se ha definido una estrategia de prueba?

ENTREGABLES CLAVE

- ¿Están definidos los entregables clave?
- ¿Tienen la calidad apropiada?

CIERRE DEL PROGRAMA

- ¿Hay planes para el cierre del programa?
- ¿Se ha planificado un ejercicio de lecciones aprendidas?

Nuestro enfoque incluye evaluaciones de programas o proyectos e "inmersiones profundas" en áreas clave de preocupación. Se puede realizar una evaluación en cualquier momento, ya sea un período específico en el tiempo, o actualizar de forma iterativa para proporcionar aseguramiento continuo durante el ciclo de vida del proyecto. Las inmersiones profundas también se pueden realizar en cualquier punto y tendrían un alcance limitado, con un enfoque de profundidad total en un área de riesgo específica.

Enfoque de inmersión

Hackeo ético

¿Conoce todas las vulnerabilidades de las que su organización podría ser víctima?

La AI debería considerar qué impacto está teniendo el Covid-19 en la seguridad de TI de la organización y evaluar si existen brechas. Hemos visto que la situación del Covid-19 es aprovechada para realizar ataques cibernéticos, incluyendo phishing, ataques al correo electrónico empresarial, malware, ransomware y sitios maliciosos. Los sitios con información de coronavirus están en aumento, y son objetivos de amenazas criminales que apuntan cada vez a más negocios para obtener información financiera o solicitudes de transferencia de dinero.

Las pruebas de penetración son ataques simulados realizados por nuestro equipo de profesionales, que emplean las mismas técnicas que los atacantes.

Estas pruebas revelan si sus sistemas o aplicaciones resistirán ataques hostiles y si las vulnerabilidades descubiertas pueden conducir a una mayor intrusión y explotación.

Al tener personal que trabaja de forma remota, el brote de Covid-19 ha puesto en primer plano los riesgos de seguridad cibernética relacionados con el trabajo remoto. Sin las defensas perimetrales y las capas de controles de las redes internas, las computadoras de los usuarios están directamente expuestas a nuevos ataques y la conciencia de seguridad del usuario se ha vuelto aún más relevante.

Mientras tanto, aunque los equipos de TI están adaptando sus conjuntos de herramientas para administrar de forma remota las computadoras, la infraestructura de la compañía expuesta al Internet, sigue siendo incansablemente sondeada y atacada. Por lo tanto, las empresas corren el riesgo de verse comprometidas, perder o divulgar datos confidenciales y violar la protección de datos y las regulaciones, así como de un potencial daño a su reputación. Por lo tanto, esto representa un área importante de enfoque para la alta administración.

¿Cómo podemos ayudar?

Mazars ha desarrollado un enfoque único de nuestros servicios de gran calidad, implementándolos en una variedad de entornos y escenarios complejos.

Usando nuestras habilidades en pruebas de penetración, podemos replicar las tácticas, técnicas y procedimientos de atacantes sofisticados para identificar vulnerabilidades, antes de que puedan ser explotadas. Esto proporciona las capacidades de protección y detección que una organización requiere para repeler la próxima generación de vulnerabilidades.

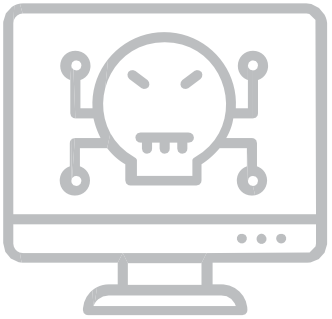
Nuestro equipo de pruebas especializado ofrece un enfoque holístico hacia la gestión de la actividad de amenazas de una organización.

Nuestros servicios van más allá de las pruebas de penetración, para explorar los aspectos de respuesta y recuperación y probar la seguridad en su conjunto, al replicar las últimas tácticas, técnicas y procedimientos de ataque (TTP).

A medida que se intensifica la pandemia, los ciberdelincuentes continúan aprovechando las oportunidades, y los ataques de phishing y el ransomware aumentarán.

Nuestros servicios de seguridad ayudan a las empresas a descubrir vulnerabilidades y evaluar riesgos, que incluyen:

- Refuerzo de la seguridad del trabajo remoto, incluidas las computadoras de los usuarios finales, la solución de acceso remoto y los dispositivos móviles.
- Pruebas de penetración de aplicaciones web.
- Pruebas de penetración de infraestructura externa.
- Ejercicios de phishing que reflejan campañas de la vida real.



Automatización Robótica de Procesos (RPA): su fuerza de trabajo digital

Las medidas adoptadas en todos los países para prevenir la propagación del coronavirus están teniendo un gran impacto en las organizaciones de todos los sectores. En circunstancias habituales, se esperaría que brinden sus productos y servicios, sin interrupciones y en línea con la orientación del gobierno, pero, como sabemos, hay una serie de desafíos para lograrlo en la crisis actual.

Las organizaciones con las que hemos hablado prevén un pico o disminución enorme en la demanda de sus servicios y están explorando formas de llevar a cabo el trabajo requerido para servir a sus clientes de manera rentable, al mismo tiempo que equilibran eso con la probabilidad de una capacidad limitada del personal. Sin embargo, existe la oportunidad de optimizar sus operaciones, reducir costos y aumentar la eficiencia de sus servicios de compromiso con el cliente, y una de las consideraciones clave para esto es el despliegue de su fuerza de trabajo digital.

¿Qué es la fuerza laboral digital?

Una fuerza de trabajo digital es un conjunto de robots de software, generalmente conocidos como Automatización Robótica de Procesos o RPA. Esta tecnología ya se usa en muchas organizaciones para ejecutar actividades monótonas y repetitivas, por ejemplo, dentro de los procesos de soporte. Un robot de software ejecuta estas actividades en lugar de sus empleados, sin requerir cambios grandes e impactantes en su entorno de TI. Este desarrollo se puede hacer en un período de tiempo relativamente corto (a menudo en semanas). Una vez instalado, la gran ventaja es que un robot de software puede ser productivo las 24 horas, los 7 días de la semana, sin errores, brindando servicios, sin interrupciones. Además, el RPA puede funcionar sobre las aplicaciones heredadas existentes, lo que le ahorra costos en cualquier nueva actualización del sistema o proyecto de implementación.

¿Cómo puede ayudar la fuerza laboral digital?

La fuerza de trabajo digital puede realizar muchas de sus actividades principales y de soporte, incluidas, entre otras, las siguientes.

- **Administración de**
- **ingresos.**
- **Customer engagement.**
- **Gestión de contratos.**
- **Funciones de recursos humanos** como nómina, gestión de beneficios, gestión de registros de educación y formación, contratación y nuevos procesos de incorporación.
- **Funciones de TI** tales como infraestructura / monitoreo de aplicaciones, administración de carpetas y archivos, usuarios / directorios y administración de versiones, monitoreo de redes y soporte de escritorio.
- **Funciones financieras** como conciliaciones, procesamiento de reclamos, pagos de gastos, gestión de devoluciones y procesamiento de inventario.

¿Cómo podemos ayudarle en Mazars?

Mazars tiene amplia experiencia en todos los sectores y puede aprovechar nuestras capacidades de RPA y bibliotecas de robots para desarrollar e implementar su fuerza de trabajo digital. Estamos asociados con todos los principales proveedores de software RPA y, al mismo tiempo, somos independientes, por lo que usted tendrá la seguridad de que estamos trabajando con el mejor software para sus necesidades particulares.

Podemos trabajar de forma remota, utilizando nuestras herramientas de trabajo remotas, como MS Teams, Huddle, y el desarrollo y despliegue de RPA remotos utilizando nuestros centros de desarrollo en Eslovaquia, Brasil, India y México. El uso de bibliotecas de robots y desarrollo remoto acorta el tiempo considerablemente y reduce el costo total de este desarrollo. Nuestros servicios de mantenimiento pueden ayudarlo cuando sea necesario, incluso después de la implementación de robots en su entorno.

Monitoreo continuo

A medida que la pandemia evoluciona, las organizaciones están reconsiderando sus formas convencionales de operar negocios para crear una nueva normalidad para el futuro. Igualmente, las funciones de auditoría interna y cumplimiento tienen que innovar y evolucionar rápidamente, para ser relevantes en la crisis actual y la nueva normalidad. Para cumplir con las expectativas del negocio, las funciones de auditoría interna y cumplimiento están explorando formas de proporcionar información de manera oportuna, reducir los costos generales de las pruebas de control e identificar oportunidades de mejora en todo el negocio. Una consideración clave es automatizar las pruebas de controles utilizando análisis de datos y utilizar la visualización para involucrar a sus partes interesadas, y Mazars Curious, nuestra herramienta de monitoreo continuo, satisface esta necesidad.

¿Qué es Curious?

Curious es nuestra herramienta de análisis de procesos de negocio patentada que combina el poder de los siguientes beneficios en un solo lugar:

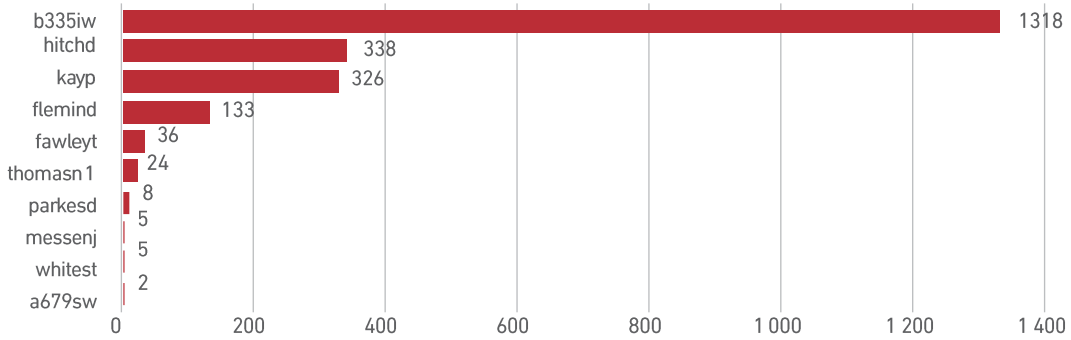
- Controles de monitoreo
- Desempeño del proceso
- Detección de fraude

Curious Test Suite tiene más de 100 pruebas y paneles relevantes, que cubren varias áreas de procesos estándar y subprocesos, incluyendo los siguientes:

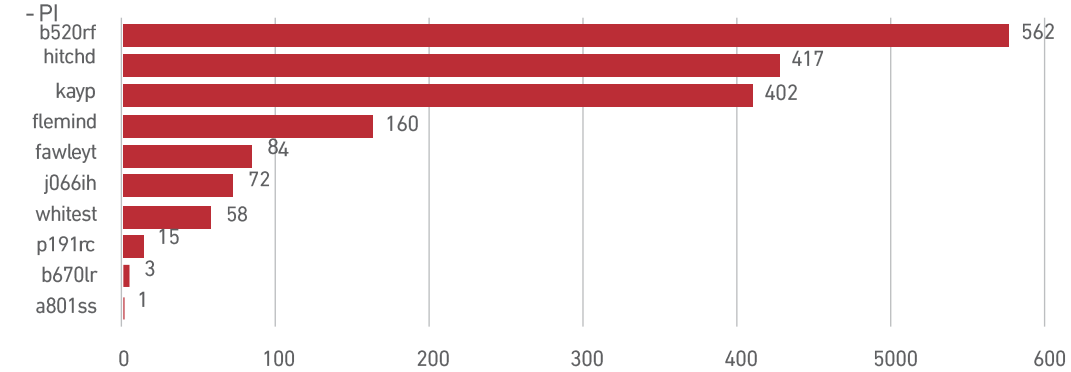
- Ventas
- Compras
- Cuentas por pagar
- Cuentas por cobrar
- Análisis de gastos
- Nómina

Control de procesos - Límites de aprobación

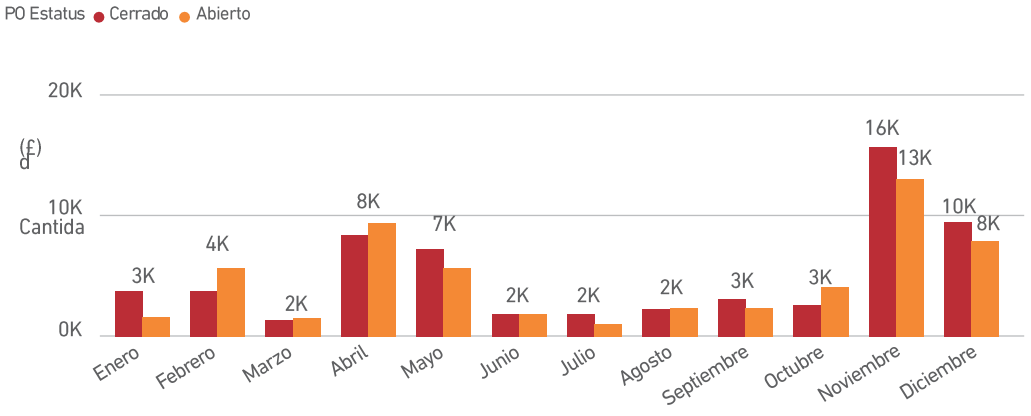
Top 10 de violaciones del límite de aprobación - Por usuario y número de Transacciones - PO



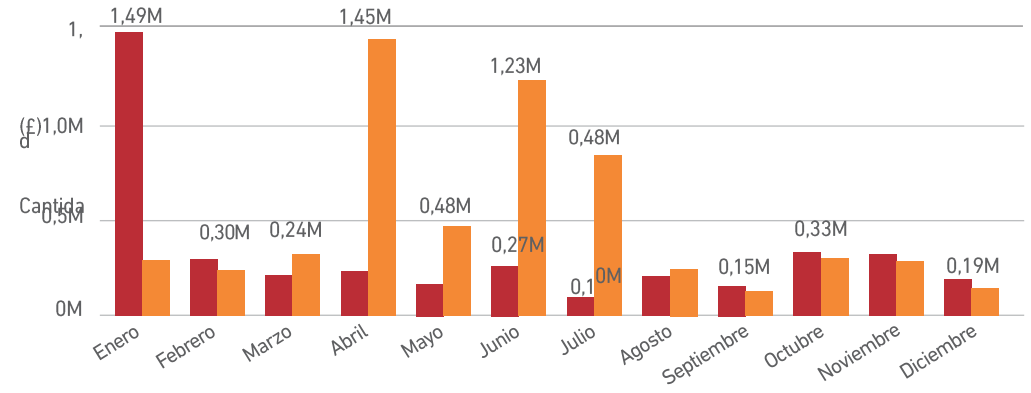
Top 10 de violaciones del límite de aprobación - Por usuario y número de Transacciones - PI



Violación de los límites de aprobación - Tendencia mensual de las órdenes de compra (Drilldown)



Violación de los límites de aprobación - Tendencia mensual de PI (dDrilldown)



Curious se puede implementar in situ, aprovechando sus inversiones existentes en TI, o como un servicio totalmente administrado.

¿Cómo le puede ayudar Curious?

El departamento de administración o de AI podría utilizar Curious para monitorear los sistemas de TI, procesar transacciones y controles de forma frecuente o continua, durante un período determinado. Curious puede reducir drásticamente el tiempo requerido para innovar y ayudar a acelerar la transformación impulsada por la analítica, ya que se puede implementar y personalizar fácilmente para satisfacer sus necesidades.

¿Cómo puede ayudar Mazars?

Podemos implementar rápidamente una prueba de concepto (PoC) con tarifas fijas en pocas semanas, que demostrará el valor de Curious para su organización. Una vez que se establezca la PoC, podríamos ayudarlo a crear un caso de negocio y ampliarlo para cubrir varias áreas de proceso en su organización. Podemos implementar Curious utilizando nuestras herramientas de trabajo remotas, como MS Teams, Huddle y el entorno basado en la nube, con un tiempo mínimo de su personal. Nuestros precios también tienen planes flexibles para brindarle diferentes opciones para satisfacer sus necesidades y ser el catalizador para que se embarque en un viaje de transformación impulsado por la analítica.

Contáctenos

Mercedes Rodríguez
Country Managing Partner

+58 212 951 09 11
Correo: mercedes.rodriguez@mazars.com.ve

Adrianza, Rodríguez, Céfalo &
Asociados (Mazars Venezuela)
Av. Tamanaco de El Rosal, Torre
Extebandes, Piso 1, Urb. El Rosal,
Caracas.
www.mazars.com.ve

Gracias a nuestra sociedad global por sus contribuciones:

REINO UNIDO

Keith Bonjour Asistente del Gerente
Keith.Bonjour@mazars.co.uk

Graeme Clarke Director
Graeme.Clarke@mazars.co.uk

Matt Dalton Socio
Matt.Dalton@mazars.co.uk

Christian Fell Gerente
Christian.Fell@mazars.co.uk

Alan Frost Director
Alan.Frost@mazars.co.uk

Andrew Hoyle Socio
Andrew.Hoyle@mazars.co.uk

Sam Patel Socio
Sam.Patel@mazars.co.uk

Syed Shah Gerente Senior
Syed.Shah@mazars.co.uk

Anish Venugopal Gerente Senior
Anish.Venugopal@mazars.co.uk

INDIA

Ravindra Rao Socio
Ravindra.Rao@mazars.in

ALEMANIA

Kai Beckman Director
Kai.Beckman@mazars.de

MÉXICO

Enrique Romero Socio
Enrique.Romero@mazars.com.mx

HOLANDA

Michel Kee Socio
Michel.Kee@mazars.nl

SUDÁFRICA

Ghitesh Deva Socio
Ghitesh.Deva@mazars.co.za

EUA

Peter Shablik Director
Peter.Schablik@mazarsusa.com

Mazars es una sociedad integrada internacionalmente, especializada en servicios de auditoría, impuestos y asesoramiento*. Operando en **91 países y territorios** alrededor del mundo, contamos con la experiencia de **40,400 profesionales** - 24,400 en la sociedad integrada de Mazars y 16,000 a través de Mazars North America Alliance - para asistir a los clientes en cada etapa de su desarrollo.
*Donde es permitido, bajo las legislaciones aplicables del país.

MAZARS