El papel del no administrador de ITM en la gestión de riesgos de ITR empresarial

El impacto de la TI en las operaciones comerciales no se puede ignorar en el entorno empresarial actual. La TI no solo ha infundido innovación, sino que también ha permitido a las empresas llegar a nuevos mercados, crear nuevos modelos comerciales, brindar un servicio al cliente más eficiente e integrar cadenas de suministro. Por ejemplo, la incorporación de la tecnología de drones reduce los desafíos logísticos y acelera la distribución para organizaciones como Amazon y Walmart.[1, 2]

Sin embargo, la proliferación de TI en todos los procesos comerciales ha aumentado el riesgo asociado. Por ejemplo, en octubre de 2016, un ciberataque en Twitter, Amazon, Spotify y Reddit provocó interrupciones y cortes del servicio durante aproximadamente dos horas.[3] Además, los ciberataques en Anthem, Home Depot y Target han costado a las organizaciones millones de dólares estadounidenses en acuerdos y han perdido clientes.[4]

Aunque muchos gerentes comerciales tienden a creer que proteger a una organización de los ciberataques es responsabilidad exclusiva del departamento de TI, la mayoría de las amenazas a los sistemas de información son el resultado de fallas de políticas, procedimientos y control en departamentos funcionales que no son de TI. Por ejemplo, los piratas informáticos obtuvieron credenciales de red para el ataque Target a través de un proveedor externo que brindaba servicios de refrigeración, calefacción y aire acondicionado.[5] En otro ejemplo, el equipo defectuoso que controlaba la electricidad fue la causa de una falla del sistema Delta en

2016.[6] Por lo tanto, la gestión de riesgos de TI debe convertirse en un esfuerzo empresarial que abarque todas las funciones de la cadena de valor en lugar de seguir siendo una función de TI.

responsabilidad. Para reducir la exposición al riesgo de TI, las organizaciones no solo deben centrarse en la infraestructura técnica, sino también crear una cultura consciente de los riesgos en toda la organización y, en consecuencia, gestionar personas, procesos y políticas.

En consecuencia, es esencial que los gerentes funcionales que no son de TI se conviertan en campeones de la gestión de riesgos de TI y ayuden al departamento de TI a mitigar el riesgo de TI.

Preocupaciones de riesgo de TI

El objetivo principal de la mayoría de las organizaciones es obtener beneficios proporcionando valor a sus clientes. El valor se deriva en gran medida de las actividades principales de la cadena de valor (es decir, logística de entrada, operaciones, logística de salida, marketing y ventas y servicios).[7] Aunque la cadena de valor puede verse diferente según la naturaleza de la industria (por ejemplo, una organización de fabricación frente a un servicio

organización), es fundamental para la función empresarial general de cualquier organización. Por lo tanto, un
la ruptura de la cadena de valor puede tener consecuencias catastróficas. Con la integración de TI en todos los aspectos de la organización, los factores de riesgo de TI prevalecen en toda la cadena de valor.

Logística entrante

La tecnología se utiliza para aumentar la eficiencia y eficacia de las actividades relacionadas con la recepción, almacenamiento y distribución de insumos para las operaciones. Muchas de las empresas actuales utilizan

Nishani Edirisinghe Vincent, Doctorado, ACMA, CGMA
Es profesor asistente de contabilidad en la Universidad de Tennessee en Chattanooga (EE. UU.). Sus intereses de investigación en el gobierno de TI, la gestión de riesgos de TI y el área amplia de los sistemas de información contable, se derivan de su experiencia profesional como consultora de implementación de sistemas de planificación de recursos empresariales. También es miembro asociado del Chartered Institute of Management Accountants del Reino Unido (ACMA). Se la puede contactar en surani-vincent@utc.edu.

Vinod U. Vincent, DBA, SHRM-SCP, SPHR
Es profesor asistente de administración en Clayton State University (Morrow, Georgia, EE. UU.). Los intereses de investigación de Vincent incluyen cognición gerencial, intuición, toma de decisiones y temas de recursos humanos como la selección de empleados. Su investigación se centra en ampliar la comprensión de la toma de decisiones gerenciales en entornos organizacionales. Vincent tiene más de 12 años de experiencia en la industria de personal sanitario de EE. UU., Donde su experiencia incluye nuevas empresas comerciales, gestión estratégica, gestión de operaciones comerciales, selección de empleados, gestión del desempeño y capacitación y desarrollo de empleados. Puede ser contactado en VinodVincent@clayton.edu.

sistemas de inventario e intercambio electrónico de datos para comunicarse con sus proveedores. Sin embargo, existen amenazas asociadas con la gran dependencia de TI de la logística de entrada. Las amenazas de TI aumentan cuando los límites del sistema se difuminan como resultado de la integración con partes externas. Además, las vulnerabilidades del sistema aumentan al proporcionar puntos de acceso a partes externas. Por ejemplo, en junio de 2016, CHI Franciscan Health Highline Medical Center en Burien, Washington, EE. UU., Informó una filtración de datos en un servidor de red que afectó a más de 18.000 personas. La violación fue el resultado de que uno de sus proveedores dejó la información del paciente accesible a través de Internet desde abril hasta junio de 2016.[8] En consecuencia, el cumplimiento del proveedor es un factor importante que afecta la seguridad del sistema de información de una empresa.

> AMENAZA AUMENTAR
> CUANDO EL SISTEMA
> LOS LÍMITES ESTÁN BORROSOS
> COMO RESULTADO DE
> INTEGRARSE CON
> PARTES EXTERNAS.

Operaciones

Las operaciones incluyen las actividades de transformación que transforman las entradas en salidas. Un objetivo importante en las operaciones es minimizar los costos y maximizar la eficiencia y la eficacia. La mayoría de las organizaciones hoy dependen en gran medida de la automatización y la estandarización para lograr estos objetivos. Sin embargo, el mayor uso de la tecnología para administrar las operaciones amplifica la exposición al riesgo. Por ejemplo, un hotel en Australia tuvo que volver a utilizar cerraduras y llaves tradicionales para las habitaciones de huéspedes después de enfrentarse a varios ciberataques en su sistema de cerradura electrónica.[9] Los piratas informáticos están cada vez más interesados en obtener información confidencial y propiedad intelectual.[10] Por tanto, tanto invertir en nueva tecnología que no tiene una solución probada contra ciberataques como seguir utilizando sistemas heredados que no cuentan con

Las ciberprotecciones aumentan el riesgo de TI. Además, las vulnerabilidades en otras áreas funcionales pueden desencadenar amenazas a los sistemas de información que afectarán las operaciones. Por ejemplo, como resultado de una falla del sistema causada por un corte de energía en un lugar, Delta Airlines canceló más de 400 vuelos durante tres días.[11]

Logística de salida

La logística de salida incluye procesar pedidos, almacenar, transportar y distribuir productos / servicios para el cliente. Un objetivo en la logística de salida es minimizar los costos al tiempo que aumenta la accesibilidad y el valor para los clientes. En consecuencia, la TI se puede utilizar para mejorar la gestión de inventario, las actividades de envío, los cronogramas de entrega, etc. Amazon anunció una entrega de prueba exitosa de productos a uno de sus clientes de prueba en Londres, Reino Unido, utilizando un dron.[12] Además, Walmart ha comenzado a probar drones para la gestión de inventario.[13] Hay beneficios tangibles de utilizar tecnología en la logística de salida. Sin embargo, si no se planifica y ejecuta correctamente, la adopción de nueva tecnología puede provocar fallas, lo que aumenta el riesgo comercial. Por ejemplo, la instalación de un nuevo sistema de cumplimiento automatizado en Sainsbury, una de las cadenas de supermercados más grandes del Reino Unido, fracasó y resultó en una pérdida de beneficios.[14] Por lo tanto, los que no son administradores de TI deben informarse sobre los riesgos asociados con cada alternativa y participar más en la evaluación de la tecnología adecuada para la empresa.

Marketing y ventas

El marketing y las ventas implican métodos utilizados para promover y vender productos y servicios. Los datos del cliente, un componente esencial de una

La estrategia de marketing y ventas son fundamentales para la generación de ingresos. El uso y almacenamiento de grandes cantidades de datos de clientes mediante tecnología conlleva la carga adicional de proteger la información confidencial de los clientes. En 2014, Home Depot experimentó una filtración de datos que afectó a 56 millones de datos de clientes debido a la instalación de software en las cajas registradoras de 2200 tiendas. [15] La violación de datos le costó a la empresa US $ 19,5 millones en reembolsos y servicios de protección de identidad para sus clientes afectados. [dieciséis] El daño potencial debido a acuerdos legales, pérdida de reputación y otros costos requiere que los gerentes de marketing y ventas tengan un conocimiento profundo de las leyes de ciberseguridad, privacidad y confidencialidad, además del conocimiento de los protocolos para reducir efectivamente la exposición al riesgo de TI. [17]

Servicios

Las actividades de servicio incluyen brindar soporte al cliente, servicio de garantía, responder a las consultas de los clientes y capacitarlos. El objetivo de los servicios es mejorar la experiencia del cliente para aumentar la satisfacción del cliente, repetir compras, ventas de productos y servicios complementarios y referencias. La TI se usa ampliamente para mejorar la gestión de las relaciones con los clientes. Muchas empresas están introduciendo aplicaciones móviles (aplicaciones) con acceso a cuentas de clientes y otras herramientas en línea para permitir una mejor experiencia del cliente. Gracias a estas nuevas técnicas, las organizaciones pueden reducir los costos al no tener que mantener grandes centros de llamadas. Sin embargo, las actividades de los clientes, como conectarse a redes desconocidas, instalar aplicaciones móviles desconocidas en sus dispositivos y establecer niveles de seguridad bajos en sus dispositivos, no pueden ser monitoreadas fácilmente por la empresa.

Aunque la TI se puede utilizar para mejorar la eficiencia y la eficacia de las actividades a lo largo de la cadena de valor, existen factores de riesgo definidos asociados con una fuerte dependencia de la TI. Estos factores de riesgo de TI, si se ignoran, pueden amenazar la integridad, la confidencialidad y la seguridad de la información de la organización, aumentando así el riesgo comercial. Para ayudar al departamento de TI a gestionar dicho riesgo, los que no son directores de TI pueden utilizar un marco de mejores prácticas como COBIT. ® 5 [18] para ayudar a identificar las fuentes de riesgo.

> “AUNQUE SE PUEDE UTILIZAR PARA MEJORAR LA EFICIENCIA Y LA EFECTIVIDAD DE LAS ACTIVIDADES EN TODA LA CADENA DE VALOR, EXISTEN FACTORES DE RIESGO DEFINIDOS ASOCIADOS CON UNA GRAN DEPENDENCIA DE ÉL.”

Marco de COBIT 5

COBIT 5 es un marco integral que aborda todos los aspectos del gobierno y la gestión de TI. El marco guía a las organizaciones sobre cómo crear un valor óptimo de TI manteniendo un equilibrio entre la obtención de beneficios y la optimización de los niveles de riesgo y el uso de recursos. [19]

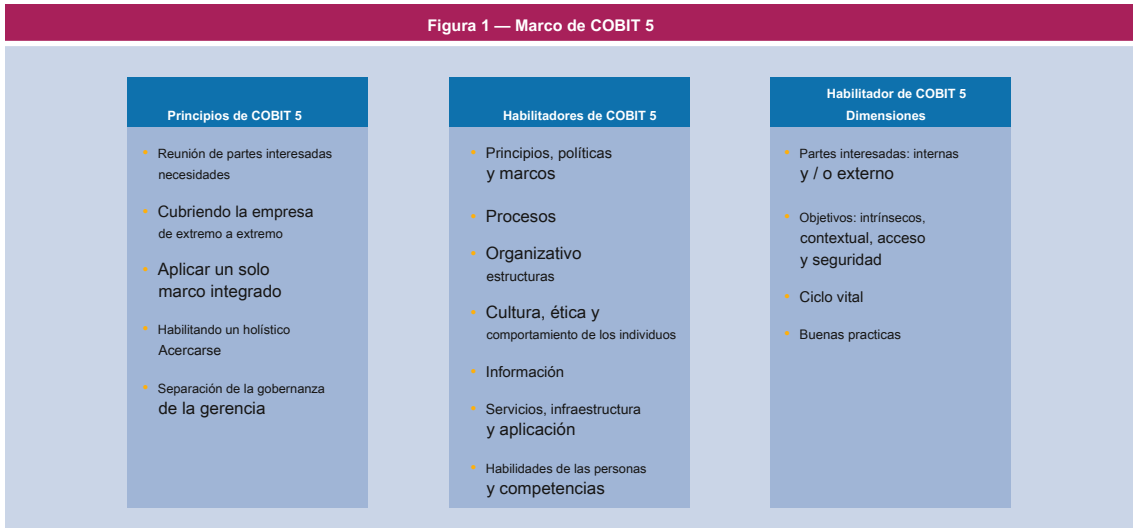
El marco se basa en cinco principios que se basan en una perspectiva de gobierno de TI a nivel empresarial (**figura 1).** Guiado por los cinco principios subyacentes, el marco presenta siete habilitadores, cada uno de los cuales tiene cuatro dimensiones, que, individual y colectivamente, trabajan juntas para lograr un conjunto de metas y objetivos de TI.

Es importante reconocer los facilitadores y su aplicabilidad única para cada organización. Para obtener los beneficios, las organizaciones deben asegurarse de que los facilitadores funcionen como se desea. Con este fin, COBIT 5 alienta a los gerentes a medir el desempeño de los habilitadores a lo largo de las cuatro dimensiones preguntando si se satisfacen las necesidades de las partes interesadas, se logran los objetivos de los habilitadores, se gestiona el ciclo de vida y se aplican y siguen las buenas prácticas. Para ser eficaz, el marco de COBIT 5 debe aplicarse en todas las áreas de la organización.

Aplicación de los habilitadores para evaluar y reducir el riesgo de TI

Además de medir el desempeño, los siete habilitadores se pueden utilizar para ayudar a identificar, evaluar y reducir la exposición al riesgo de TI durante todo el proceso.
organización. Por lo tanto, en colaboración con el departamento de TI, los gerentes funcionales que no son de TI pueden utilizar los siete habilitadores para abordar y guiar los riesgos de TI.

Figura 1 — Marco de COBIT 5



prácticas de gestión dentro de su departamento y en toda la cadena de valor.

Principios, políticas y marcos

Si bien las políticas brindan orientación detallada sobre cómo alinear la toma de decisiones con los principios, los marcos brindan orientación sobre cómo organizar las actividades dentro de una empresa. Una política debe describir lo que se espera de los empleados, cómo manejar las excepciones, cómo medir el desempeño y qué

consecuencias a esperar por incumplimiento. Los gerentes deben identificar y equilibrar las necesidades en conflicto de las partes interesadas internas y externas y diseñar políticas que estén alineadas con la estrategia de la organización. Al establecer políticas, los gerentes también deben considerar cómo se relacionan las políticas con otros habilitadores. Por ejemplo, los procesos son los medios para ejecutar políticas, la estructura organizacional ayuda a implementar políticas y las políticas ayudan o pueden obstaculizar la comunicación de información en una organización.

Los gerentes deben evaluar si las políticas y los marcos existentes en sus respectivos departamentos están siguiendo las buenas prácticas, cumpliendo con las leyes y regulaciones, adaptándose a situaciones específicas y asegurando la información. Los gerentes también deben comprender cómo todas las actividades están interconectadas y cómo todos los departamentos deben trabajar junto con otras divisiones para lograr un objetivo común. Por ejemplo, los gerentes de operaciones deben ser conscientes de que las vulnerabilidades en otras divisiones pueden afectar directamente las operaciones. Al mismo tiempo, debilidades en sus propios sistemas de TI pueden influir negativamente en las divisiones de logística, marketing y ventas de entrada y salida, y de servicios. Por lo tanto, además de implementar políticas que satisfagan las necesidades del departamento, los gerentes funcionales también deben evaluar las políticas generales que deben ser consistentes en toda la empresa, así como las políticas únicas establecidas en otros departamentos e incorporar esas políticas en sus respectivos departamentos cuando sea apropiado. Por ejemplo, una política de TI general sería cambiar las contraseñas con regularidad.

Procesos

Los procesos son una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toman entradas de varias fuentes (incluyendo otros procesos), manipulan las entradas y producen salidas (por ejemplo, productos, servicios). Un proceso tiene un ciclo de vida (es decir, un proceso debe diseñarse, implementarse, monitorearse y redefinirse cuando sea necesario) y cada proceso debe tener una meta (es decir, un resultado deseado). Estos objetivos deben ser intrínsecos (por ejemplo, ¿cómo se alinean con los principios, políticas y buenas prácticas?), Contextuales (por ejemplo, ¿es el proceso flexible, personalizable y adaptable a varias situaciones?), Y accesibles y seguros (por ejemplo, ¿es el proceso accesible solo para usuarios autorizados?). Una vez que se identifican las metas, se deben definir métricas para medir si se satisfacen las necesidades de las partes interesadas, se logran las metas facilitadoras, Se gestiona el ciclo de vida del habilitador y se aplican buenas prácticas. Es importante comprender cómo el habilitador de procesos está conectado con otros habilitadores. Los procesos necesitan

la información para funcionar y producir información como salida, depende de las estructuras organizativas para funcionar, requiere infraestructura y aplicaciones para producir salidas y conectar y desencadenar otros procesos. Además, la cultura de la organización influye en qué tan bien se implementan y se siguen los procesos de manera consistente.

A través de un análisis integral, los gerentes deben identificar los procesos críticos dentro de cada actividad primaria de la cadena de valor. Cada gerente individual puede ayudar creando una lista de procesos existentes y categorizándolos en procesos primarios y secundarios o alto, medio o bajo según la criticidad del proceso para la actividad primaria. En segundo lugar, dado que los procesos pueden abarcar varios departamentos, los gerentes deben identificar y establecer la propiedad del proceso. Al hacerlo, las organizaciones podrán evaluar la exposición al riesgo de cada uno de los procesos centrales e identificar quién es responsable de implementar y

mantenimiento de medidas de reducción de riesgos.

Estructuras organizacionales

La estructura organizacional facilita la toma de decisiones y el flujo de información dentro de una organización. Para optimizar este habilitador, una empresa debe considerar no solo su propia estructura organizacional, sino también las estructuras organizacionales de sus clientes, proveedores, reguladores y otras entidades interesadas. Los gerentes deben evaluar la adecuación de la estructura organizacional para facilitar el funcionamiento eficiente de los procesos; escalada y

distribución de información para la toma de decisiones; prevención, detección y corrección oportuna de amenazas informáticas; y representación adecuada de las necesidades del departamento en las selecciones de inversión en TI a través de la membresía en los comités directivos.

En consecuencia, se deben establecer estructuras organizacionales donde los gerentes funcionales puedan trabajar en estrecha colaboración con el liderazgo de TI para que estén informados sobre el estado actual de la tecnología y los sistemas de información. Es importante implementar y evaluar la delegación de autoridad, los procedimientos de escalamiento, el alcance de los procedimientos operativos y de control, como la frecuencia de las reuniones y la documentación. Los gerentes funcionales deben trabajar en estrecha colaboración con TI para identificar información dentro de cada departamento que podría alertar sobre posibles riesgos y

Establecer una estructura de informes para comunicar la información del personal de línea dentro de cada departamento a TI y *viceversa.* Las estructuras organizativas son críticas para la empresa porque facilitan la función de otros habilitadores.

Cultura, ética y comportamiento de las personas

Se trata de un conjunto de comportamientos individuales y colectivos que determinan el comportamiento de la organización en su conjunto. El entorno cultural tiene un impacto en la adopción, el uso y la gestión de riesgos de la tecnología. Por ejemplo, las organizaciones que asumen más riesgos pueden explotar tecnologías innovadoras para desarrollar nuevos modelos comerciales, mercados y métodos de producción para obtener una ventaja competitiva. Sin embargo, la falta de experiencia con las nuevas tecnologías, la falta de protocolos de seguridad y las implementaciones apresuradas pueden aumentar la exposición al riesgo de TI.

> “LOS GERENTES DEBEN CONSIDERAR INCORPORACIÓN DE ASPECTOS DE LA TI EN LAS EVALUACIONES DE DESEMPEÑO PARA RECOMPENSAR A LOS EMPLEADOS POR EL USO EXCEPCIONAL DE LOS SISTEMAS.”

Por lo tanto, los gerentes funcionales deben ser muy conscientes del riesgo de TI atribuido a la adopción de nuevas tecnologías y establecer protocolos para mitigar esos factores de riesgo. Deben dar ejemplo siguiendo la dirección establecida por la alta dirección, abordando los problemas de riesgo de TI dentro del departamento, comunicándose y colaborando con TI y alentando a los empleados a seguir los procesos establecidos y las mejores prácticas. Los gerentes deben considerar incorporar aspectos de TI en las evaluaciones de desempeño para recompensar a los empleados por el uso excepcional de los sistemas. Además, los gerentes deben considerar cómo se puede abordar rápidamente el comportamiento inaceptable y qué acciones apropiadas deben tomarse.

Información

Una organización tiene información estructurada, no estructurada, automatizada o no automatizada que crea conocimiento y agrega valor a la toma de decisiones. El objetivo de este habilitador es proporcionar

información que sea precisa, relevante y segura. Las buenas prácticas adaptadas para la información pueden variar según los aspectos únicos de cada industria y / u organización. Sin embargo, al desarrollar buenas prácticas, los gerentes deben considerar dónde se almacena la información, cómo se accede a la información, quién puede acceder a la información, cuál es el nivel y tipo de información y qué otra información se necesita para que la información disponible sea útil.

Los gerentes deben evaluar los diferentes tipos de información recopilada, procesada y distribuida de cada proceso. En particular, los gerentes deben reconocer la información confidencial recopilada y almacenada dentro de su departamento respectivo y evaluar la idoneidad de los controles para proteger esa información de usuarios no autorizados. En consecuencia, los gerentes deben identificar quién posee, procesa y usa la información.

Servicios, infraestructura y aplicación

Estos son recursos en una organización que influyen en la entrega de servicios relacionados con TI y pueden ser proporcionados por partes interesadas internas o externas. Los gerentes funcionales deben establecer metas para aplicaciones, infraestructura y tecnología basadas en las necesidades organizacionales y departamentales. Las buenas prácticas relacionadas con este habilitador son de naturaleza técnica e incluyen el establecimiento de principios arquitectónicos (como reutilización, construcción frente a compra, simplicidad, agilidad y apertura), definiciones, repositorio y niveles de servicio.

Los gerentes deben identificar y evaluar los recursos de TI (por ejemplo, equipos, maquinaria, aplicaciones, hardware y redes) que se utilizan en cada departamento. Dado que la infraestructura y las aplicaciones son recursos importantes, el mantenimiento oportuno de estos recursos es imperativo para el desempeño continuo de la organización. Por ejemplo, los equipos que funcionan mal u obsoletos pueden causar amenazas a los sistemas de información de la empresa al prenderse fuego, proporcionar un punto de acceso para los piratas informáticos o desviarse de la configuración normal y causar problemas de calidad en los productos. Por lo tanto, al identificar los servicios críticos y planificar y proporcionar el mantenimiento adecuado a los equipos, los gerentes funcionales pueden ayudar a reducir el riesgo de TI.

Aunque la mayoría de las actividades en este sentido pueden ser de naturaleza técnica, los gerentes funcionales deben ser conscientes de la interrelación de estos recursos de TI, reconocer a las partes interesadas internas y / o externas que interactúan con los recursos y comprender el impacto de las elecciones departamentales con respecto a los recursos de TI en el negocio en general. Otro aspecto importante que necesita la atención de la administración es la informática del usuario final. Con el mayor uso de dispositivos móviles personales en el trabajo, los empleados pueden estar exportando datos a aplicaciones externas para organizar y reportar cierta información de manera comprensible. Aunque estas aplicaciones pueden ser inofensivas, los administradores deben comprender que las aplicaciones independientes pueden aumentar la exposición al riesgo de TI. En consecuencia, los gerentes deben hacer un inventario de las aplicaciones individuales utilizadas, informarse sobre el peligro de exportar datos a otros sistemas, y controlar si los empleados utilizan aplicaciones independientes, como hojas de cálculo y bases de datos de acceso, para mantener la información. Además, los gerentes deben conocer y comunicar los peligros de descargar y mantener varias aplicaciones móviles relacionadas con el entretenimiento, como varios juegos y aplicaciones para ver televisión / películas y escuchar música, en dispositivos utilizados para actividades organizativas.

Personas, habilidades y competencias

Este habilitador enfatiza la importancia de contar con empleados capaces no solo internamente, sino también externamente, incluyendo proveedores, distribuidores y reclutadores. El objetivo es encontrar y retener a personas cali fi cadas con la educación, las habilidades técnicas, la experiencia, el conocimiento y el comportamiento adecuados necesarios para desempeñar eficazmente sus responsabilidades. Es necesario establecer buenas prácticas en las distintas etapas de adquisición y desarrollo del nivel de habilidades de los empleados. Estas prácticas pueden incluir herramientas como verificaciones de antecedentes, pruebas de competencia, pruebas de personalidad, capacitación, educación continua y evaluaciones de desempeño. Además, los gerentes deben evaluar si se mantiene un nivel apropiado de personal y también planificar la rotación de empleados para asegurar que las habilidades y competencias se conserven dentro de la organización.

Los gerentes deben realizar auditorías periódicas para evaluar si los empleados tienen las habilidades necesarias para desempeñar eficazmente sus responsabilidades. Los trabajadores no calificados pueden

causar interrupciones en la maquinaria y obstaculizar las actividades de la cadena de valor de la empresa. Además, no tener las habilidades adecuadas dentro de la organización también puede obligar a la empresa a utilizar sistemas heredados cuando se dispone de sistemas más eficientes y efectivos, restringir la capacidad de invertir en nuevas tecnologías y / o obstaculizar la capacidad de maximizar los beneficios ofrecidos por la empresa. sistemas existentes. Renunciar a estas oportunidades no solo tiene un impacto negativo en el desempeño de la organización, sino que también puede aumentar su exposición al riesgo de TI. Por lo tanto, los gerentes deben evaluar el nivel de habilidad necesario dentro de cada área funcional, trabajar junto con TI para identificar las habilidades necesarias para optimizar la tecnología existente, planificar el futuro con base en los cambios tecnológicos,

> “EL RIESGO NO ES NECESARIAMENTE TÉCNICO Y PUEDE ORIGINARSE EN VARIAS FORMAS DURANTE EL ORGANIZACIÓN.”

Conclusión

El riesgo de TI no es necesariamente técnico y puede originarse de diversas formas en toda la organización. Aunque proteger a una organización del riesgo de TI es principalmente responsabilidad del departamento de TI, dados los numerosos puntos de acceso al sistema de TI de una empresa en toda la cadena de valor, se ha vuelto cada vez más difícil para la división de TI por sí sola mitigar suficientemente la exposición al riesgo de TI. Por lo tanto, los gerentes funcionales que no son de TI deben colaborar más estrechamente con el departamento de TI y ser la primera línea de defensa contra los riesgos de TI. Sin embargo, identificar los riesgos de TI, especialmente para los gerentes no técnicos, puede ser una tarea abrumadora.

Los gerentes funcionales que no son de TI deben evaluar la idoneidad de los principios, políticas y marcos utilizados en cada departamento y comprender el impacto de esas políticas en la gestión de riesgos de TI. Además, los gerentes deben establecer la propiedad de los datos en los procesos y comprender cómo los procesos dentro del departamento están interconectados con otros procesos fuera del departamento y la gestión general de riesgos de TI de la organización. Ya que

Las estructuras organizativas y la cultura influyen en todos los demás habilitadores, los gerentes deben establecer estructuras que faciliten la gestión de riesgos de TI y construir una cultura consciente de los riesgos de TI dentro de cada área funcional. Cada gerente funcional debe identificar la información que se recopila y procesa en cada uno de sus departamentos que pueda ser útil para la gestión de riesgos de TI y comunicar esta información al departamento de TI. Además, la infraestructura, el equipo, el software, el hardware y las aplicaciones utilizados en cada departamento deben evaluarse para identificar cualquier fuente de riesgo que pueda afectar los sistemas de información dentro y fuera del departamento. Por último, contratar y retener empleados calificados y proporcionar la formación adecuada con respecto al riesgo de TI es fundamental para reducir la exposición al riesgo de TI.

Notas finales

1 Johnson, K .; D. Martínez; "Mantenerse al día con la Drones (s) " *Asesor empresarial de JDSupra,* 11 de enero de 2017, *www.jdsupra.com/legalnews/ keep-up-with-the-drones-es-74395 /*

2 O'Brien, M .; “Walmart Testing Drones para DC La gestión del inventario," *Comerciante multicanal,* 6 de junio de 2016, *http://multichannelmerchant.com/ news / walmart-testing-drones-dc-Inventory- gestión-06062016 /*

3 O'Brien, SA; "Ciberataque generalizado Derriba sitios en todo el mundo " *CNN Money,* 21 de octubre de 2016, *http://money.cnn.com/2016/ 10/21 / technology / ddos-attack-popular-sites /*

4 Pierson, B .; “Anthem pagará un récord de $ 115 millones para resolver demandas en EE. UU. por violación de datos ", *Reuters Business News,* 23 de junio de 2017, *https://www.reuters.com/article/us-anthem- ciber-asentamiento / himno-para-pagar-récord-115-milli en-para-resolver-nosotros-demandas-por-violación-de-datos- idUSKBN19E2ML*

5 Krebs, B .; "Los hackers de Target entraron a través de HVAC Company ", KrebsonSecurity, 14 de febrero de 2014, *https://krebsonsecurity.com/2014/02/ hackers-objetivo-irrumpieron-en-via-hvac-company /*

6 Sasso, M .; T. Black; "Fallo del sistema Delta Marks Wake-Up Call for Airline Industry ", Bloomberg Technology, 9 de agosto de 2016, *https://www.bloomberg.com/news/articles/ 2016-08-10 / marcas-de-falla-de-sistemas-delta-s-wake- llamada para la industria de las aerolíneas*

7 Porter, ME; *Ventaja competitiva: creación un desempeño superior sostenido,* The Free Press, Estados Unidos, 1985

8 Landi, H .; "Error del proveedor dejó 18.000 CHI "Información accesible en línea para pacientes del Franciscan Hospital", Healthcare Informatics, 12 de septiembre de 2016, *www.healthcareinformatics.com/news-item/cybersecurity/ proveedor-error-left-18000-chi-franciscan-hospital- información-pacientes*

9 Herrero; "El ransomware bloqueó al hotel Sistema de bloqueo de llave electrónica, " *Mundo de la red,* 29 de enero de 2017, *www.networkworld.com/ article / 3162764 / security / ransomware-lock- hotel-out-of-its-electronic-key-lock-system.html*

10 Sikich, “Informe de fabricación 2016: clave Hallazgo; Los fabricantes son vulnerables a las amenazas cibernéticas ”, abril de 2016, *https://www.sikich.com/ insight / 2016-manufacturing-report /*

11 *Op cit* Sasso y Black

12 *Op cit* Johnson y Martinez

13 *Op cit* O'Brien, M.

14 Clark, L .; "Sainsbury's cancela 260 millones de libras como Los problemas de TI de la cadena de suministro llegan a las utilidades " *ComputerWeekly,* 25 de octubre de 2004, *https://www.computerweekly.com/news/ 2240058411 / Sainsburys- cancela -260m-as- cadena de suministro, problemas, resultados, ganancias*

15 Bose, N .; “Home Depot confirma la seguridad Incumplimiento tras el robo de datos de Target " *Reuters,* 9 de septiembre de 2014, *www.reuters.com/article/ us-usa-home-depot-databreach-idUSKBN0H327 E20140909*

dieciséis Stempel, J .; Home Depot liquida al consumidor Demanda por gran violación de datos de 2014 ", *Reuters,* 8 de marzo de 2016, *www.reuters.com/article/ us-home-depot-breach-solution- idUSKCN0WA24Z*

17 PricewaterhouseCoopers, “The Evolving Sala de juntas: señales de cambio " *www.pwc.com/ us / en / Corporate-Governance / Annual-Corporate- encuesta-directores / activos / pwc-2015-anual- encuesta-directores-corporativos.pdf*

18 ISACA®, COBIT®5, Estados Unidos, 2012, *www.isaca.org/COBIT/Pages/COBIT-5.aspx*

19 *Ibídem.*