Experis™
ManpowerGroup

CÓMO PROTEGER A SU EMPRESA EN UN MERCADO ESCASO DE TALENTO

Seguridad de la información

INTRODUCCIÓN

Debido a destacables fallos de seguridad de gran repercusión mediática, la seguridad de la información ha pasado de estar en un segundo plano en departamentos de informática a ocupar la portada de noticias internacionales. **Se ha convertido en un tema de importancia estratégica tanto para empresas como para la sociedad.** Mientras las empresas luchan por encontrar soluciones, ahora afrontan una amplia escasez de Talento en materia de seguridad que complica aún más una situación ya difícil.

Basado en un estudio sobre las habilidades informáticas a nivel internacional[1] realizado por Experis en 10 mercados principales, en este artículo se exploran las repercusiones de la escasez de Talento en materia de seguridad; para ello, se proporcionan conocimientos sobre los problemas, junto con pautas sobre cómo reducir al máximo los riesgos derivados.

El estudio a nivel internacional de Experis se basó en la información recopilada por parte de personas cuyas responsabilidades incluían las decisiones relacionadas con la contratación. Uno de los hallazgos clave de este estudio es que el 32% de los directivos de departamentos de informática mencionaron la seguridad de la información como una habilidad solicitada y difícil de encontrar, tanto en la actualidad como en los próximos 12 a 18 meses. Esto se compara con el 18% de desarrollo de *software*, que fue la siguiente habilidad más requerida. Una de las principales preocupaciones para los informáticos encuestados es el acceso a suficientes recursos sobre seguridad de la información, lo que destaca el aumento en la importancia fundamental de atraer y retener Talento en materia de seguridad de la información.

1/3 de los directivos de departamentos de informática considera que la seguridad de la información es una habilidad solicitada y difícil de encontrar.

YA NO ES CUESTIÓN DE SABER SI HABRÁ FALLOS EN LA SEGURIDAD DE LA INFORMACIÓN, LA CUESTIÓN ES **“CUÁNDO”** *Y* **“CON QUÉ ALCANCE”**

1. Experis IT Skills Research 2015 (Estudio sobre habilidades informáticas 2015 de Experis)

SITUACIÓN ACTUAL

La seguridad en portada

Ahora más que nunca, la seguridad de la información y las repercusiones que representan los fallos se han convertido en los temas habituales de conversación. El aparentemente infinito desfile de casos de gran repercusión mediática en empresas minoristas líderes, instituciones financieras y organizaciones gubernamentales también sirve para educar a la sociedad sobre las repercusiones reales de los fallos de seguridad a nivel personal, profesional y corporativo. Incluso los medios habituales tratan el tema, con series en horario de máxima audiencia *CSI: Cyber* y *Mr. Robot*, que incorporan diferentes situaciones ficticias de amenaza cibernética inspiradas en historias reales. Con independencia de si los objetivos originales de los ataques cibernéticos eran de carácter financiero, político o personal, en la red sus efectos se han traducido en un aumento de cargos de alta dirección y juntas directivas que se ven **forzados a redirigir cada vez más recursos** al año para gestionar las **amenazas en materia de seguridad de la información**.

3,8 MILLONES de USD
Promedio consolidado del coste total de un fallo de datos.

23% desde 2013

154 USD
Coste provocado por cada registro robado o perdido con información confidencial.

6% desde 2013

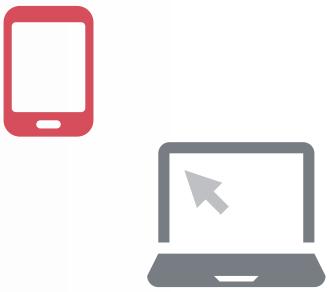
38%
Aumento de los fallos en materia de seguridad en 2015 en comparación con 2014.

Como consecuencia, se ha producido un **aumento en la demanda de Talento en materia de seguridad de la información**, en especial de expertos en la materia de alto nivel necesarios para planificar y llevar a cabo estrategias de seguridad. Se necesitan dichas estrategias para combatir el entorno de amenazas cada vez más sofisticadas al que se enfrenta la mayoría de las empresas.

Cómo mantenerse al día con los avances tecnológicos

Los avances tecnológicos, junto con un mayor grado de interconectividad, han proporcionado a la sociedad ventajas tangibles. Queda claro que la emergente "Internet de las cosas" que fomenta interconectar cada dispositivo ha producido **una explosión en la creación y el intercambio de la información**. La virtualización, la computación en la nube y la expansión de la potencia de procesamiento y el ancho de banda de datos en dispositivos portátiles **han dado lugar a la creación, la recopilación y el uso compartido de diferentes formas de información personal, privada y corporativa**, a menudo a través de modelos comerciales completamente nuevos. Desafortunadamente, muchos usuarios y proveedores no han entendido (y tampoco enfrentado) **las consecuencias de proteger esta información de forma incorrecta y, de manera involuntaria en muchos casos, han creado amplias recopilaciones de datos personales y privados que constituyen el objetivo ideal de los ataques cibernéticos**.

Además, la creciente cultura llamada *Bring-Your-Own-Device* (BYOD, "Traiga su propio dispositivo") ha creado un entorno donde la mayoría de las funciones de gestión de activos son insuficientes para controlar los dispositivos que se usan en el lugar de trabajo. **Esto ha provocado incongruencias de funcionamiento que rápidamente se han convertido en vulnerabilidades en materia de seguridad.** Es obvio que la resistente arquitectura de seguridad perimetral, apreciada por muchos directores de departamentos de informática, ya no protege de manera suficiente los procesos y la información de la empresa. Sin embargo, para proporcionar una gestión más avanzada que no se limite solo a bloquear usuarios mediante *firewalls* y controles de red, se necesita Talento en materia de seguridad que muchas empresas simplemente no poseen.



> **"Muchos usuarios y proveedores no han entendido (y tampoco enfrentado) las consecuencias de proteger incorrectamente esta información..."**
>
> Experis

En punto muerto

Algunos temas clave tratados en la RSA Conference 2015[2] refuerzan el mensaje de que las preocupaciones en materia de seguridad continúan aumentando. En ellos, se indica que, aunque las empresas gastan más dinero en seguridad de la información, desde una perspectiva práctica, están "en punto muerto".

Los fallos aumentan en términos de cantidad, sofisticación y repercusiones. Cada vez más, tanto países como delincuentes organizados ven la infraestructura de las tecnología de la información de sus públicos objetivos como el mejor canal de acceso, lo que proporciona una elevada tasa de retorno y menos probabilidad de ser detenidos. Dependen de que las empresas tengan problemas de *software*, como un diseño de procesos y comunicaciones entre procesos ineficientes, lo que comporta una infraestructura y aplicaciones vulnerables. Además, **áreas de control comunes que se ven afectadas por recursos insuficientes**, como una gestión deficiente de accesos, una gestión de configuración inapropiada, un mantenimiento limitado, errores humanos y supervisión insuficiente crean puntos débiles explotables en empresas que pueden aprovechar atacantes motivados.

Un factor clave que se debe tener en cuenta al evaluar la seguridad es la perspectiva de los atacantes, que es bastante diferente a la de los posibles atacados en lo que respecta al nivel de inversión que consideran rentable. Los atacantes han demostrado ser expertos utilizando equipos de disponibilidad inmediata para aprovechar las debilidades de los objetivos, a menudo con un plan de ataque a largo plazo que pueda desgastar las defensas. **Los piratas informáticos son cada vez más sofisticados**, ya que convierten *malware* en las herramientas y bibliotecas que otras personas usan para desarrollar el software de la aplicación. Si bien los atacantes tienden a tener acceso con mayor frecuencia a través de la perseverancia, también son extremadamente oportunistas, puesto que explotan las vulnerabilidades en cuestión de segundos cuando las condiciones son las adecuadas.

Las grandes empresas como los bancos internacionales gastan cientos de millones de dólares para proteger sus datos. Mientras que este nivel de gastos es, por supuesto, imposible para muchas empresas, también **alejan el Talento de aquellas con menor presupuesto,** lo que provoca que las empresas más pequeñas sean cada vez más vulnerables. Existen cada vez más incidentes de atacantes que usan proveedores externos para comprometer a las empresas e infiltrarse en sus redes de trabajo. A pesar de que la gestión de proveedores externos está mejorando, estos proveedores externos a menudo no se examinan con tanta exhaustividad o frecuencia como seria necesario. Por lo tanto, no se puede tener la certeza de que se esté implementando un nivel suficiente de riesgo aceptable, dado que estos terceros se enfrentan a los mismos desafíos, o mayores, a la hora de acceder a suficientes recursos de seguridad.

Las hazañas de gran repercusión mediática han hecho que las empresas vean que en realidad no poseen suficientes habilidades de detección de seguridad o planes de respuesta de seguridad adecuados dentro de la empresa para abordar de manera proactiva y combatir ataques frecuentes y cada vez más sofisticados. Algunos fallos grandes e industrias recientemente atacadas han activado las respuestas para mayores controles dentro de competidores. Sin embargo, muchas aún se muestran **reticentes a responder rápidamente ante los ataques** y a adoptar medidas defensivas como comunidad. Al menos en parte, esto se debe a la escasez de recursos en materia de seguridad disponibles para desarrollar e implementar las soluciones necesarias. Los mandatos normativos, legislativos y contractuales aparentemente interminables que de forma inevitable aparecen tras fallos importantes también comportan un **aumento de la demanda de Talento en materia de seguridad de la información**.

Mientras algunos consideran las nuevas herramientas de seguridad que emergen una alternativa útil para atraer Talento, **estas a menudo requieren formación o un ciclo de aprendizaje especializados** antes de poder usarse de manera eficaz, lo que agrava la escasez de Talento en lugar de mitigarla.

2. Diapositivas de RSA Conference 2015: https://www.rsaconference.com/writable/presentations/file_upload/prof-m01_status-of-the-industry-2015-global-information-security-workforce-study.pdf

Escasez de Talento global en materia de seguridad

Lamentablemente, el número real de puestos que se publican ha superado de manera tan drástica la fuente de Talento (a nivel mundial) disponible que **las empresas se encuentran cada vez más en una carrera o en una guerra de pujas con sus competidores para atraer y retener escasas y fundamentales habilidades en materia de seguridad**. Esto incluye los puestos de seguridad que no se limitan al dominio del ciberespacio. Cabe reconocer que no todas las habilidades escasean; existe una gran demanda de profesionales de seguridad de la información, que va de redactores de políticas a piratas informáticos éticos e ingenieros de soluciones en materia de seguridad técnica.

En el estudio de Experis se destacó que muchas empresas, para enfrentarse a la escasez de Talento, recurren a asesores externos a fin de aumentar el personal interno. Los encuestados indicaron que el 40% emplea actualmente a asesores externos para asuntos relacionados con la seguridad de la información. De estos encuestados, el 27% planea aumentar el uso de asesores mientras que el 40% mantendrá el mismo nivel, y citaron la rentabilidad, la flexibilidad y el acceso a expertos como las razones por las cuales eligen profesionales externos como opción.

El **27%**

de las organizaciones aumentará el uso de externos

El **40%**

mantendrá el mismo nivel de asesores externos

Un tema crucial es que **la demanda de Talento clave en materia de seguridad supera el crecimiento internacional en la fuente de Talento**. En un estudio realizado por Frost and Sullivan, al que se hace referencia en el 2015 (ISC)2 Global Information Security Workforce Study[3], se destaca un crecimiento internacional previsto para la demanda de profesionales en materia de seguridad de la información que alcanzará los 2,5 millones en 2019, mientras que se prevé que el suministro solo crezca aproximadamente 1 millón. Los datos en este informe pronostican una tasa de crecimiento compuesto anual (TCCA) de aproximadamente el 10% en la demanda de Talento en materia de seguridad, pero solo una TCCA del 5,6% en el suministro de 2014 a 2019. Estas previsiones indican que la situación del Talento de seguridad no es saludable y, **a menos que se tomen medidas para reducir la carencia de Talento, la escasez probablemente empeore con el tiempo**.

Demanda global de

2,5 millones

para 2019

Esta disparidad en la previsión de recursos de 1,5 millones entre los puestos y los candidatos presionará cada vez más los costes de trabajo relacionados con la seguridad de la información, lo que aumenta la presión sobre las empresas que contratan para que reduzcan las pautas de calidad con respecto a lo que se considera un nivel “aceptable” de competencia para cubrir las vacantes a largo plazo. Desafortunadamente, intentar escatimar en gastos para seguridad solo empeorará el problema y comportará un aumento de los riesgos para la empresa.

1,5 millones

de disparidad entre los puestos y los candidatos

3. Information Security Workforce Study (Estudio sobre personal en materia de seguridad de la información): https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

COMPLICACIONES

Como si la situación actual ya no fuera lo suficientemente compleja, empresas de todo tipo deben prepararse para un entorno informativo más complejo y difícil.

Ausencia de liderazgo

Existe una falta de acuerdo general sobre quién debería poseer la seguridad de la información y a qué nivel de la organización debe reportar el director de seguridad de la información (CISO). ¿Acaso el propietario principal debería ser el presidente ejecutivo, el director de informática, el director de finanzas, el director ejecutivo de recursos o el director de seguridad de la información? ¿Acaso el director de seguridad de la información debe responder directamente al presidente ejecutivo o a la Junta directiva? Ante el contexto actual de amenazas, **muchas empresas se dan cuenta de que nadie quiere realmente asumir esta responsabilidad** en el equipo de liderazgo, **aunque en última instancia es un riesgo para los directivos como un todo**.

Una gestión efectiva requiere líneas internas de comunicación en toda la empresa. En el informe especial 2015 de la Bolsa de Valores de Nueva York (NYSE) "Managing Cyber Risk: Are Companies Safeguarding Their Assets?"[4], se indicó que el **42% de los miembros de la junta admitió que solo hablaban ocasionalmente de la seguridad cibernética o informática**. En lo que respecta a la priorización de la contratación de recursos para seguridad, el estudio de Experis muestra disparidades entre los directivos funcionales y los directores de informática de las empresas: el 45% de los vicepresidentes (VP) coloca la seguridad de la información en el primer lugar de la lista de preocupaciones en comparación con el 28% de los directivos de informática (DI).

El **42%**

de los miembros de las juntas solo discuten ocasionalmente la seguridad cibernética o informática

coloca la seguridad de la información en el primer lugar en la lista de preocupaciones

4. Managing Cyber Risk: Are Companies Safeguarding their Assets (Gestionar el riesgo cibernético: ¿las empresas protegen sus activos?): https://www.nyse.com/publicdocs/nyse/listing/NYSE_Governance_Services_ Managing_Cyber_Risk.pdf

Composición desequilibrada del equipo

Las empresas a menudo se esfuerzan por alcanzar la protección suficiente de seguridad porque no cuentan con una **composición del equipo de seguridad** adecuada o una **estrategia de gestión de recursos de seguridad**; en particular, con respecto a la gestión de seguridad de la información. Existen diferentes configuraciones de equipo y estrategias que las empresas pueden implementar hoy en día, como:

personal interno

aumento del equipo con trabajadores eventuales

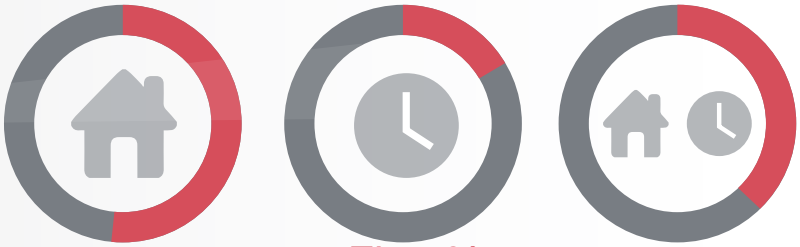
externalización completa de las principales funciones de seguridad a una empresa de servicios de seguridad gestionada con servicio completo

contratación de funciones específicas a través de terceros

soluciones de proyecto

En el estudio de Experis se observó que la **gran mayoría de las empresas defienden una sola estrategia de gestión de recursos, aunque a menudo puede añadir estrés a la efectividad de su personal**[1]. Los resultados indicaron que el 52% de las empresas encuestadas solo emplea a trabajadores permanentes. Este modelo reduce la capacidad de la empresa de incorporar tecnologías de rápida evolución o de reaccionar ante las amenazas emergentes. El 15% de las empresas encuestadas solo emplea a externos. Adoptar un modelo de gestión de recursos que utilice principalmente proveedores de servicio externos para puestos de seguridad y establecer iniciativas de seguridad puede resultar una forma eficaz para que las empresas diseñen un equipo flexible. Sin embargo, este enfoque no está exento de problemas. Según las habilidades disponibles, aún puede requerirse formación para asegurarse de que los equipos externos puedan dar apoyo eficaz a las tecnologías específicas de la empresa. Estas empresas, en última instancia, pueden ver una erosión importante de los conocimientos del equipo de seguridad interno y una toma de consciencia situacional como consecuencia de la falta de contacto directo con el entorno operativo. Esto afectará a su capacidad para lograr cualquier visión a largo plazo de crear un grupo de personal interno completamente cualificado.

La encuesta de Experis muestra que solo el 33% de las empresas defiende una combinación más óptima y equilibrada de los enfoques a la gestión de equipos para seguridad. **Usar un enfoque de gestión de recursos equilibrado no solo ayuda a abordar la escasez con mayor rapidez, sino que también puede exponer los recursos con afinidad para ampliar sus habilidades o capacidades de liderazgo,** lo que crea una reserva interna de Talento en materia de seguridad de la información más robusta a largo plazo.



El **52%**
solo emplea a trabajadores permanentes

El **15%**
solo emplea a asesores externos/ freelances

El **33%**
combina

1. Experis IT Skills Research 2015 (Estudio sobre habilidades informáticas 2015 de Experis)

El Talento con experiencia es escaso

"El hecho es que simplemente no existen suficientes profesionales seniors con experiencia en seguridad para avanzar, ya sea hoy o en el futuro predecible", afirma Michael Gerdes, director del Information Security Center of Expertise en Experis. "En el centro del problema está el hecho desconcertante de que las habilidades consolidadas y la experiencia en seguridad no se pueden enseñar en un programa académico. Se requiere tiempo en los puestos correctos para que se desarrollen". Muchas empresas se están dando cuenta de que es de alguna manera más sencillo encontrar especialistas en seguridad para puestos operativos básicos, o recursos más avanzados para cubrir el global de políticas y visión del espectro, porque estas áreas tienden a usar habilidades que se pueden enseñar y aplicar de inmediato.

La disponibilidad de recursos es mucho más escasa cuando se buscan recursos de alto nivel y con experiencia que puedan crear planes prácticos y gestionar los riesgos de seguridad de la empresa de manera eficaz. El grado necesario de pragmatismo y habilidad para equilibrar de manera eficaz los aspectos prácticos de la cultura empresarial, la efectividad de los controles y los obstáculos de la implementación solo llegan después de que los recursos de seguridad ganen algo de experiencia en el mundo real (estudiantes de la "escuela de la vida").

Una de las complicaciones que impide que la fuente de Talento obtenga la experiencia necesaria es el dilema que se plantean las empresas que buscan una mayor fuente de candidatos, solo para contratar personal con experiencia. Con frecuencia, esta práctica deja a los candidatos sin experiencia sin otra opción que aceptar puestos fuera del ámbito de la seguridad. Cuando no se pueden crear oportunidades para que profesionales junior en seguridad aprendan el oficio de colegas de alto nivel y se conviertan en parte de la fuente de Talento interna, **las empresas fomentan una situación de empleo que erosiona aún más la fuente de Talento a largo plazo**.

"En el centro del problema está el hecho desconcertante de que las habilidades consolidadas y la experiencia en seguridad no se pueden enseñar en un programa académico..."

Michael Gerdes, director del Information Security Center of Expertise en Experis

Fuente de educación fragmentada

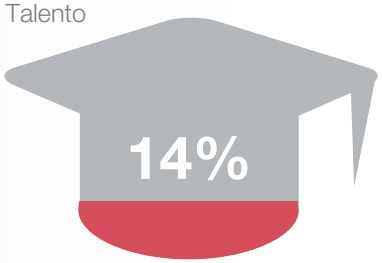
Los sistemas actuales de educación y formación no proporcionan una fuente de Talento suficiente para abordar la demanda actual de recursos en materia de seguridad o el crecimiento esperado de la demanda futura. Lo que es peor aún, es probable que los modelos educativos, basados principalmente en principios de formación y carrera de la era industrial, ya no sean completamente adecuados para cubrir las necesidades y los desafíos de Talento de la era digital.

Los programas tradicionales de grado se ven forzados a ofrecer contenidos que sean consistentes con una misión académica, pero que aún proporcionen contenido relevante, oportuno y de calidad en un entorno de amenazas y riesgos de seguridad que evoluciona rápidamente. Aunque los directivos determinan la demanda buscando profesionales graduados para la mayoría de los puestos, **deben tener en cuenta que los candidatos con títulos recién emitidos suelen necesitar años de experiencia para transformar el conocimiento teórico en habilidades prácticas**. Asimismo, la necesidad de profesionales graduados en muchos puestos de seguridad (p. ej., operaciones de plataforma, configuraciones y mantenimiento) tiende a estar menos justificada en puestos que son altamente técnicos y dependen fundamentalmente de habilidades diferenciadas que se deben aprender y expandir cada vez que las plataformas evolucionan.

LA NECESIDAD DE INNOVAR

Reflexionar sobre el desarrollo del Talento en materia de seguridad

Las empresas deben reflexionar sobre los requisitos educativos asociados a los puestos de seguridad de la información y **plantearse formas alternativas para que el Talento pueda formarse más allá de** los títulos tradicionales. La mejor forma de cubrir esta necesidad de desarrollar Talento es a través del uso de escuelas de formación profesional y escuelas técnicas superiores en materia de seguridad donde la formación rápida **altamente especializada** en habilidades técnicas **aumenta la fuente de Talento en mucho menos tiempo** que los programas convencionales de grado. Si se expanden de la forma adecuada, estos centros de formación en seguridad podrían crear una capacidad adicional para formar Talento valioso en seguridad con habilidades técnicas específicas en mucho menos tiempo y quizás ayudar a corregir la carencia de Talento lo suficientemente rápido como para satisfacer las demandas de los directivos.



Google lidera el camino con equipos en los que hasta un 14% son personas que nunca han ido a la universidad[5].

Las instituciones y empresas deben asociarse para crear candidatos cualificados en materia de seguridad en menos tiempo con el desarrollo de **programas de estudio y trabajo amplios** o becas ofrecidas a través de **asociaciones entre el centro académico y la industria**. Los programas deben proponer puentes para los candidatos de otras disciplinas que desean comenzar una carrera en seguridad.

La educación debe empezar temprano. En el mundo empresarial, se sabe que las empresas de tecnología establecen nuevos límites en la contratación de adolescentes. **Google lidera el camino con equipos en que hasta un 14% son personas que nunca han ido a la universidad[5].** Si bien la seguridad de la información está todavía fuera del alcance para muchos de estos jóvenes, existe una oportunidad para que empresas y centros se replanteen un curso acelerado para estudiantes prometedores.

Ventajas y desventajas de los títulos

En el estudio de Experis también se observó que los directivos de informática en muchos mercados expresaron la necesidad de talento titulado. Los títulos pueden ser útiles para diferenciar el grado de dominio, pero no predicen cuál será el rendimiento de los candidatos en un puesto específico. Las funciones y los posibles especialistas en seguridad de la información valiosos contribuirán con una mejor correlación entre las experiencias del mundo real y el historial laboral que con sus títulos. Además de los títulos, las empresas obtendrían mayores ventajas con programas que proporcionen a los candidatos oportunidades para adquirir la experiencia práctica necesaria a fin de desarrollar sus conocimientos y habilidades.

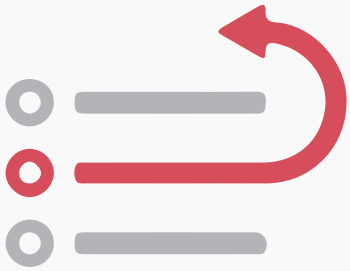
5. Google Has Started Hiring More People Who Didn't Go To College (Google ha comenzado a contratar más personas que no han ido a la universidad). http://www.businessinsider.com/google-hiring-non-graduates-2013-6

RECOMENDACIONES

Queda claro que los métodos actuales de atracción y retención de Talento, composición de grupos de profesionales y educación no siempre son eficaces y, por lo tanto, están exponiendo a algunas empresas a un mayor riesgo. Veamos formas para que su empresa pueda gestionar y expandir su fuente de Talento en materia de seguridad de la información de manera más eficaz y enfrentarse a la amplia escasez de Talento en seguridad:

Convierta en prioridad la gestión de Talento en seguridad

Asegúrese de que la junta directiva está formada y se mantiene informada en lo que respecta a los temas de seguridad de la información, incluido el nivel de recursos necesarios para mitigar riesgos inaceptables. Los directivos deben estar a cargo de la seguridad. El director de seguridad de la información debe ser un líder empresarial eficaz y experto en superar las barreras del idioma que surgen por las diferencias culturales entre los usuarios y los tecnólogos. La planificación de recursos y la gestión de Talento son una parte esencial de la comunicación constante. Esto se debe establecer junto con las líneas de comunicación de la empresa creando un plan flexible y ágil que se pueda adaptar a riesgos de seguridad emergentes y predecibles, así como a los requisitos cambiantes en seguridad propios de los mercados objetivo.



Evalúe a su equipo

Implemente un proceso de revisión anual de resumen de habilidades para identificar y realizar un seguimiento de las habilidades esenciales en materia de seguridad que la empresa actualmente aplique o tenga previstas. De manera parecida, revise el nivel de cobertura que proporcionan los recursos existentes. Mediante este proceso, se obtiene información valiosa que puede ser útil para el desarrollo profesional, la retención de recursos y la planificación de atracción de Talento.

Crecimiento interno

Las habilidades esenciales en materia de seguridad son cada vez más costosas de adquirir y a menudo requieren mucha más atención y retroalimentación para retenerlas. Con frecuencia, se pasa por alto el desarrollo de competencias internas. A menudo, es más coherente añadir esto al plan de crecimiento. Elimina el coste de atracción y se apoya en un profesional del que ya se conoce ajuste cultural a la compañía. Identifique al Talento que tenga algún grado de exposición a temas de seguridad, con independencia de lo indirecta que sea la exposición, y téngalo en cuenta para una formación en múltiples áreas. Cree un programa que ofrezca **oportunidades prácticas en situaciones de la vida real** para obtener los mejores resultados en el menor tiempo posible.

Este es un mercado desequilibrado, por lo que debe asegurarse de crear un entorno estimulante y de ofrecer compensación total para contrarrestar el atractivo de los incentivos que ofrecen otras empresas que buscan impulsar el Talento en seguridad.

Evalúe con detenimiento el nuevo Talento antes de contratarlo

El aumento de la necesidad de Talento en seguridad ha creado un entorno donde los candidatos que buscan trabajo intentan sacar provecho de las palabras de moda frecuentes en materia de seguridad para introducirlas en sus currículums y atraer a empresas de selección de personal. Con frecuencia estos “aspirantes” hacen coincidir sus currículums con la descripción de un puesto de una empresa y saben convencer a las empresas de selección de personal de que cumplen con los requisitos. Por ello, es importante incorporar exámenes por parte del personal de seguridad con experiencia para proporcionar un nivel más de **evaluación que no se limite a las palabras de moda** y así explorar con mayor profundidad las áreas y habilidades funcionales deseadas.

Gestione su canal de atracción de Talento

Piense con originalidad a la hora de evaluar la mejor forma de adquirir recursos adicionales. Muchas necesidades en materia de seguridad son únicas o periódicas en lugar de continuas y es posible que la mejor forma de cubrirlas sea mediante una o más de las siguientes opciones:

- Contratar expertos o liderazgo intelectual
- Realizar asesoría basada en proyectos
- Llevar a cabo iniciativas de contratación temporal según los resultados finales

Los agentes de Talento deben mostrar una profunda experiencia en seguridad de la información y un enfoque innovador para la contratación. Deben tener acceso a fuentes de Talento en seguridad de la información y deben haber establecido relaciones con sus candidatos para conocer sus habilidades y experiencia más allá de las palabras de moda que mencionen en un currículum. Dado el carácter evolutivo de las habilidades necesarias, se debe incluir la revisión regular de los agentes y sus funciones en el plan de la cadena de suministro.

Contemple la posibilidad de implementar el examen técnico como un elemento obligatorio para los consultores externos de selección de personal a fin de reducir al máximo el tiempo valioso del equipo a la hora de revisar los candidatos iniciales.

CONCLUSIÓN

Las empresas no verán el final de la escasez de Talento con experiencia en seguridad de la información en el corto plazo; **por lo tanto, deben usar la imaginación e innovación para buscar formas de aprovechar el Talento que pueden adquirir** (temporal o permanentemente) para obtener las mejores ventajas posibles. El mayor éxito en este esfuerzo se logrará a través de procesos de gestión que incorporen la supervisión y la retroalimentación para facilitar ajustes en los puestos, responsabilidades y búsqueda de Talento.

Debemos reconocer que la seguridad de la información es un campo que evoluciona rápidamente y **debemos prepararnos para más de una batalla**. Cualquier solución (individual o combinada) que decidamos adoptar para terminar con la escasez de Talento **tardará tiempo en desarrollarse y arrojar resultados importantes**.

Reconocer el verdadero alcance del problema es el primer paso para solucionarlo. Tomar consciencia ejecutiva del problema, los enfoques innovadores y flexibles en educación y formación, así como el aumento de la colaboración entre empresas, son las claves para una gestión exitosa del equipo de seguridad. Estas mejoras también se encuentran en el centro de la gestión de desafíos en seguridad de la información a largo plazo.

ACERCA DE EXPERIS:

Experis es la consultoría de ManpowerGroup especializada en soluciones de atracción de Talento. Su profundo conocimiento sectorial le permite entender los desafíos a los que se enfrentan los negocios y tener acceso a profesionales altamente cualificados. Ofrece soluciones globales de atracción para ayudar a las empresas a afrontar la escasez de Talento.

En concreto, Experis IT está especializada en Soluciones IT basadas en Talento y enfocada a resolver cualquier necesidad en el ámbito del área IT: consultoría, *headhunting,* selección de personal (*interim* y *permanent*), asistencia técnica, desarrollo de *software*, gestión de proyectos, servicios de *quality assurance* y *outsourcing* de servicios (ITO y BPO), tanto a nivel nacional como internacional.

Para obtener más información, visite **www.experis.es**.

Experis™
ManpowerGroup