Fuga de datos a nivel mundial: Riesgos y errores comunes de los empleados

Resumen ejecutivo

Hoy en día las empresas son cada vez más distribuidas y móviles, lo cual les obliga a enfrentar desafíos en la protección de su información confidencial. Con el objeto de comprender esta situación, Cisco encargó a InsightExpress, una compañía independiente de investigación de mercado, que realizara un estudio que abarcara a empleados y profesionales de TI en diversos países. Como parte del estudio, se realizaron encuestas en 10 países que Cisco seleccionó debido a las diferencias en sus culturas sociales y comerciales. En cada país, se encuestó a 100 usuarios finales y 100 profesionales de TI, cubriendo así a un total de 2000 personas. La investigación descubrió que a pesar de las políticas, procedimientos y herramientas de seguridad actualmente en uso, los empleados de todo el mundo exhiben conductas arriesgadas que ponen en peligro los datos personales y empresariales. Tales conductas incluyeron:

- **Uso de aplicaciones no autorizadas:** el 70% de los profesionales de TI cree que el uso de programas no autorizados fue responsable de hasta la mitad de los incidentes de pérdida de información en sus empresas.
- **Uso indebido de computadoras de la empresa:** el 44% de los empleados comparte dispositivos de trabajo con otras personas sin supervisión.
- **Acceso no autorizado tanto físico como a través de la red:** el 39% de los profesionales de TI afirmó que ha debido abordar el acceso no autorizado por parte de un empleado a zonas de la red o de las instalaciones de la empresa.
- **Seguridad de trabajadores remotos:** el 46% de los empleados admitió haber transferido archivos entre computadoras del trabajo y personales al trabajar desde el hogar.
- **Uso indebido de contraseñas:** el 18% de los empleados comparte contraseñas con sus colegas. El porcentaje aumenta al 25% en China, India e Italia.

Para reducir la fuga de datos, las empresas deben integrar la seguridad en su cultura empresarial y evaluar constantemente los riesgos de cada interacción con redes, dispositivos, aplicaciones, datos y, por supuesto, otros usuarios.

Introducción

Los empleados de todo el mundo utilizan las redes comerciales para comunicarse, colaborar ente sí y acceder a información. Las empresas ávidas de aumentar su productividad buscan integrar cada vez más las comunicaciones de red con las operaciones comerciales, e incentivan a que sus empleados aprovechen tecnologías tales como dispositivos inalámbricos y puntos de acceso públicos. La productividad aumenta, pero la colaboración basada en la red coloca la información empresarial en un entorno más amplio que es más vulnerable y difícil de proteger.

Los datos almacenados en la red empresarial también corren riesgo puesto que están más accesibles que nunca. Las organizaciones facilitan el acceso a sus bases de datos a fin de compartir y almacenar información, y la tecnología de compresión ha permitido puntos terminales de mayor capacidad (y mayor riesgo). Un dispositivo móvil de 80 MB ahora almacena 6000 documentos de Microsoft Word o 720.000 correos electrónicos, y los nuevos dispositivos extraíbles de 64 GB permiten copiar un disco duro entero en un dispositivo del tamaño de un paquete de chicle.

Estos dispositivos hacen más fácil que los empleados, partners o ladrones de datos accedan, muevan o pierdan propiedad intelectual o datos de clientes. Además de tener más información en riesgo, las empresas de hoy sufren consecuencias más graves si estos datos se pierden o ven comprometidos. La pérdida de propiedad intelectual, como diseños de productos privados, datos financieros, planes de fusiones y adquisiciones, puede dañar la reputación de una empresa, debilitar su marca, o menoscabar su ventaja competitiva. Las infracciones a los requisitos normativos que regulan el manejo de datos confidenciales de clientes pueden mermar la confianza de los clientes y acarrear multas.

Las empresas inteligentes instituyen políticas de seguridad y capacitan a sus empleados sobre el riesgo de pérdida de información, pero la eficacia de dichas medidas es cuestionable. En los últimos dos años, se informó sobre la pérdida o robo de más de 250 millones de registros confidenciales;1 y dichas pérdidas no siempre se deben a amenazas externas. Ya sea a sabiendas o no, en forma inocente o maliciosa, los empleados exhiben conductas que incrementan el riesgo de perder datos.

Para reducir la fuga de datos y proteger la información empresarial, las organizaciones de TI deben comprender cómo la conducta de los empleados puede acrecentar los riesgos y deben tomar medidas para fomentar una cultura empresarial consciente de la seguridad en la que los empleados acaten las políticas y los procedimientos.

Encuesta detallada revela conductas arriesgadas

Para comprender mejor las conductas de los empleados que ponen en riesgo los recursos empresariales, Cisco encargó a InsightExpress, una compañía independiente de investigación de mercado, que realizara un estudio en diversos países representativos para detectar los errores comunes que cometen los empleados y que favorecen la fuga de información. Se realizaron dos encuestas en 10 países: Estados Unidos, Reino Unido, Francia, Alemania, Italia, Japón, China, India, Australia y Brasil. Como el objetivo del estudio era examinar las tendencias de conducta de empleados a nivel mundial, los 10 países se seleccionaron por tener culturas sociales y comerciales distintivas, así como por el tiempo que la fuerza laboral de cada uno llevaba utilizando Internet y redes empresariales basadas en IP. En cada país, se encuestó a 100 empleados y 100 profesionales de TI, cubriendo así a un total de 2000 personas.

Los resultados de la encuesta revelaron diversas conductas de riesgo y un desdén generalizado por las políticas de seguridad. Uno de los descubrimientos más notables fue la frecuencia de determinadas conductas en diferentes partes del mundo. Por ejemplo:

- China presenta tal nivel de abuso tecnológico que los responsables de tomar decisiones de TI auditan las computadoras en busca de contenido no autorizado.
- En Japón, el 65% de los usuarios finales no acata de manera constante las políticas de TI de su empresa, y el estudio indica que el abuso tecnológico por parte de los usuarios finales está en aumento.
- Los usuarios finales en India tienden a emplear el correo electrónico y la mensajería instantánea para fines personales y modifican la configuración de seguridad de TI en las computadoras empresariales para poder ver sitios web no autorizados.
- Los empleados en Brasil utilizan las computadoras empresariales para fines de comunicación personal y para actividades como descargar música.
- Los usuarios de Francia tienen la tasa más baja de cumplimiento de políticas de TI de todos los países encuestados, ya que sólo el 16% de los empleados afirmó cumplir de manera constante las políticas de seguridad.

El nivel de conciencia que tienen los administradores de TI en relación con las conductas arriesgadas de los empleados también varía entre los diferentes países. En China, los administradores de TI confrontan directamente a los empleados por el desacato a las políticas de seguridad. Los profesionales de TI en India tienen poca conciencia sobre el grado en que los

empleados menoscaban la seguridad, ya que menos de la mitad de ellos cree que los usuarios finales utilizan aplicaciones y programas no autorizados en las computadoras de sus empresas. Brasil demostró la mayor correlación entre el abuso de TI por parte de los empleados y la percepción de dicha conducta por parte de los responsables de tomar decisiones de TI, ya que dichos encargados evalúan y actualizan las políticas empresariales con mayor frecuencia que en ningún otro país que haya participado en la encuesta.

1 http://www.privacyrights.org, 2008

Estas diferencias representan un desafío para las empresas multinacionales que intentan mantener políticas de seguridad centralizadas en todos sus sitios distribuidos y departamentos de TI. Y a medida que más empleados se unan a la tendencia mundial de trabajar desde el hogar y mientras están de viaje, la separación entre la vida laboral y personal continuará desdibujándose. La combinación entre las conductas culturales y el uso de teléfonos móviles, equipos portátiles, aplicaciones Web 2.0, video y otros medios sociales en el hogar, el trabajo y de viaje crea un entorno aún más complejo de resguardar. Las organizaciones de alcance mundial deben comprender el entorno laboral actual y tomar en cuenta las diferencias culturales en cuanto al comportamiento y su impacto sobre la vulnerabilidad de la información, y adaptar localmente la educación, las políticas y las decisiones tecnológicas según corresponda.

Revelación de conductas arriesgadas

Los empleados revelaron una impresionante serie de conductas que ponen en riesgo la información y los recursos empresariales, a pesar de las políticas que establecen procedimientos correctos. Los siguientes ejemplos muestran como los empleados pierden y filtran información ya sea a sabiendas o no.

Uso de aplicaciones no autorizadas

El uso de aplicaciones no autorizadas en las redes empresariales puede constituir un riesgo para la información empresarial confidencial y la información personal de los empleados. El correo electrónico personal es la aplicación no autorizada que más se utiliza, seguida de actividades bancarias en línea, pago en línea de cuentas, compras en línea y mensajería instantánea.

Estas aplicaciones implican un alto riesgo de pérdida de información por parte de los empleados y de robo de datos por parte de piratas informáticos debido a que con frecuencia no son supervisadas y no se adhieren a las normas de seguridad de la empresa. Además, el uso de estas aplicaciones conlleva el riesgo de contagio de sitios maliciosos.

- El 78% de los empleados accedió a correo electrónico personal desde computadoras empresariales. Este número aproximadamente duplica el nivel de uso autorizado.
- El 63% de los empleados admite usar una computadora laboral para uso personal todos los días, y el 83% admite hacerlo de vez en cuando.
- El 70% de los profesionales de TI cree que el uso de programas no autorizados fue responsable de hasta la mitad de los incidentes de pérdida de información en sus empresas. Esta creencia está más extendida en los Estados Unidos (74%), Brasil (75%) e India (79%).

Uso indebido de computadoras de la empresa

Muchos empleados usan a sabiendas computadoras empresariales en formas reñidas con las políticas de seguridad de TI. Algunos ejemplos incluyen alterar las configuraciones de seguridad y compartir dispositivos laborales e información confidencial con personas ajenas a la empresa. Los empleados anulan las configuraciones de TI para descargar música, comprar en línea, pagar cuentas y, en algunos casos, acceder a juegos de azar y pornografía en línea. Aproximadamente un

cuarto de los empleados encuestados admitió compartir información confidencial con amigos, familiares o incluso extraños, y casi la mitad de ellos comparte sin supervisión dispositivos laborales con personas ajenas a la empresa. Estas conductas facilitan que propiedad intelectual de la empresa llegue a manos de personas que constituyen una grave amenaza para la seguridad y la rentabilidad empresarial.

- Desacato de políticas empresariales y anulación de configuraciones de seguridad de TI

  China: 42%
  Brasil: 26%
  India: 20%

- Compartir información empresarial confidencial fuera de la empresa

  Brasil: 47%
  India: 27%
  Reino Unido: 26%
  Italia: 22%
  Alemania: 24%

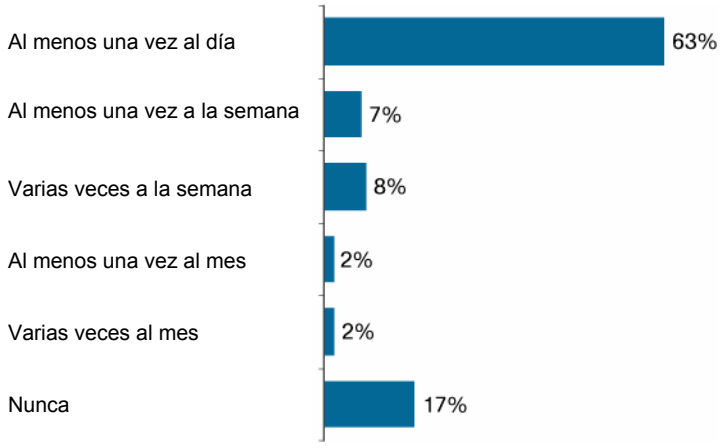
- Compartir dispositivos laborales con personas ajenas a la empresa sin supervisión

  China: 43%
  India: 28%

- En total: 44% (el 32% de los encuestados compartió dispositivos laborales con colegas y el 19% lo hizo con amigos y familiares ajenos a la empresa)

La figura 1 muestra la frecuencia con que los empleados utilizan computadoras de sus empresas para actividades personales.

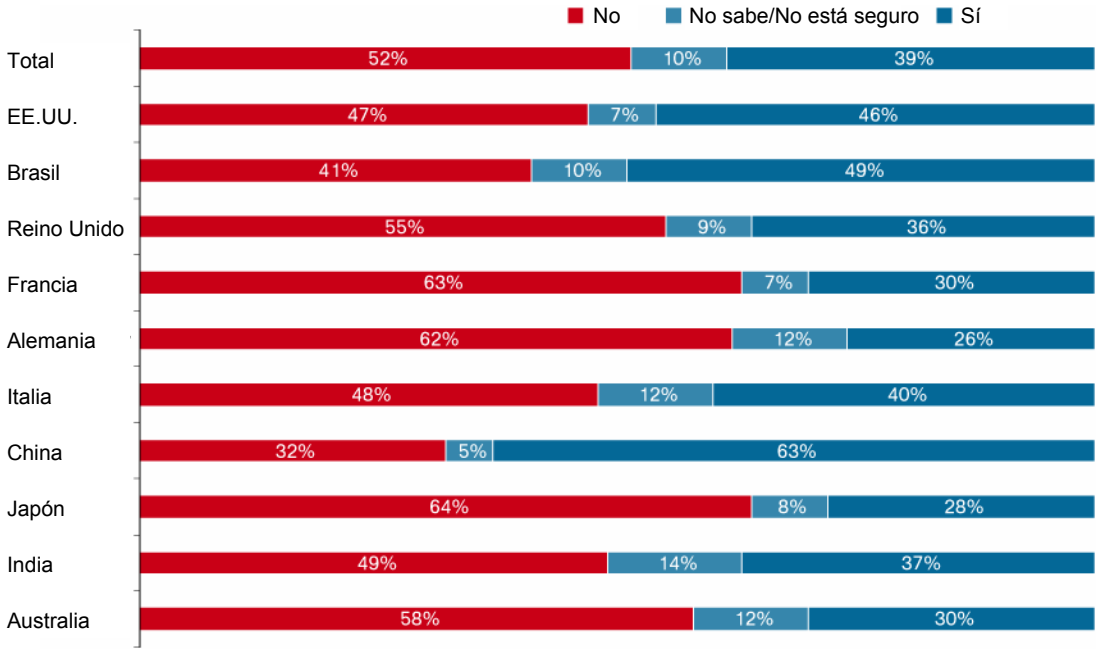
Figura 1. Frecuencia de uso personal



Acceso no autorizado tanto físico como a través de la red

Muchos trabajadores permiten que personas desconocidas ingresen a dependencias de la empresa con ellos, o permiten que personas ajenas a la empresa deambulen libremente por las instalaciones empresariales sin supervisión. Estas acciones facilitan que personas no autorizadas físicamente roben recursos de la empresa o accedan a información confidencial. A veces, los mismos empleados acceden a zonas no autorizadas de la red o las instalaciones empresariales. La figura 2 muestra la cantidad de veces que el personal de TI tuvo que enfrentar el acceso no autorizado a la red o las instalaciones por parte de un empleado:

Figura 2. Los responsables de tomar decisiones de TI enfrentan accesos no autorizados tanto físicos como a través de la



- El 39% de los profesionales de TI afirmó que ha enfrentado accesos no autorizados por parte de un empleado a zonas no autorizadas de la red o de las instalaciones empresariales. Esto fue cierto para casi la mitad de ellos en Brasil (49%) y Estados Unidos (46%), y el 63% en China. Aunque Japón (28%) y Alemania (26%) presentaron el menor número de incidentes, en todos los países al menos un cuarto de los profesionales de TI ha enfrentado esta situación.
- El acceso no autorizado tanto físico como a través de redes fue más frecuente en las empresas medianas y grandes (46%), pero en las pequeñas empresas estos incidentes también se producen con frecuencia (32%).
- El 22% de los empleados en Alemania permite que personas ajenas a la empresa deambulen sin supervisión por las oficinas.

Seguridad de trabajadores remotos

Debido a que las empresas actualmente operan en forma cada vez más distribuida, los empleados móviles aumentan el riesgo potencial de pérdida de información. Conductas tales como transferir archivos de un dispositivo laboral a una computadora doméstica que no esté protegida según las normas del departamento de TI, usar medios de comunicación personales que no sean tan seguros como medios de comunicación empresariales, hablar sobre temas confidenciales de la empresa en lugares donde otras personas puedan escucharlos, y no utilizar un protector de privacidad en un equipo portátil al trabajar en un lugar público, facilitan el robo de información. Los empleados tampoco protegen debidamente los dispositivos de almacenamiento y los equipos portátiles, que pueden perderse o ser robados.

- El 46% de los empleados admitió transferir archivos entre computadoras laborales y personales al trabajar desde el hogar.
- Más del 75% de los empleados no utiliza un protector de privacidad al trabajar en un lugar público. Esta cifra es mucho más alta en Brasil, China e India, que son los países que presentan las conductas más irresponsables.
- El 68% de las personas no se preocupa de bajar la voz al hablar por teléfono en lugares públicos fuera de la oficina.
- El 13% de las personas que trabaja en el hogar admite que no puede conectarse a la red empresarial, por lo que envía comunicaciones laborales a clientes, partners y colegas mediante su correo electrónico personal.

Uso indebido de contraseñas y procedimientos de inicio/cierre de sesión

Cerrar la sesión y usar contraseñas son algunos de los métodos más antiguos y simples de la seguridad informática. Cuesta imaginar que a estas alturas haya usuarios que pasen por alto estos pasos básicos de seguridad, pero lo hacen…y en cifras sorprendentes. Al menos uno de cada tres empleados afirmó que deja su computadora con sesiones activas y desbloqueada cuando se aleja de su escritorio, como por ejemplo para almorzar o regresar a su hogar al fin de la jornada. Otra práctica común consiste en dejar un equipo portátil sobre el escritorio toda la noche, a veces sin cerrar la sesión. Uno de cada cinco empleados almacena datos de inicio de sesión y contraseñas en su computadora o los anota y deja en su escritorio, en un cajón sin llave, o en notas pegadas en su computadora.

Cualquiera de estas infracciones al protocolo de seguridad ofrece peligrosas oportunidades a los atacantes. En conjunto, no sólo dejan la puerta abierta a amenazas potenciales, sino que invitan el ingreso de atacantes. Por ejemplo, cuando un empleado deja un sistema con la sesión activa sobre un escritorio y con su contraseña adjunta, invita a que un intruso robe su computadora en ese momento e información confidencial en el futuro. Si el empleado utilizó dicha computadora para uso personal, el atacante también podrá acceder a dicha información.

- El 28% de los empelados en China almacena información de inicio de sesión y contraseñas de cuentas financieras personales en sus dispositivos laborales.
- El 18% de los empleados comparte contraseñas con sus colegas y esta tasa aumenta al 25% en China, India e Italia.
- El 10% de los empleados en India, el Reino Unido e Italia conserva notas escritas con información de inicio de sesión y contraseñas en el escritorio de trabajo, por lo que incluso si no hay sesiones activas, un atacante podría acceder a información confidencial si roba su computadora.
- El 5% de los empleados en el Reino Unido y Francia conserva en forma impresa contraseñas de cuentas personales y financieras en el escritorio de trabajo, por lo que su información podría ser robada mediante cualquier otra computadora incluso si su computadora laboral está debidamente protegida.

¿Por qué los empleados ponen la información en riesgo?

Generar estadísticas que muestren cuántos empleados exhiben conductas que merman la seguridad de la información es un ejercicio valioso, pero lo realmente importante es comprender cómo cambiar dichas conductas y aumentar la seguridad. Para ello, las empresas deben comprender qué piensan los empleados sobre la seguridad y por qué ignoran o vulneran los procedimientos empresariales.

La encuesta de InsightExpress fue más allá de las estadísticas y preguntó a los empleados por qué se comportaban de una forma que ponía en riesgo la información. Luego, la encuesta presentó las respuestas en el contexto de empresas grandes y pequeñas, diferentes culturas y las perspectivas de los empleados y los profesionales de TI.

Los resultados de la encuesta revelaron en general que a menudo el incumplimiento de las normas por parte de los empleados pesa más que la importancia que le dan a cumplir con las políticas de seguridad. Por ejemplo, cuando la encuesta les preguntó a los empleados por qué comparten información empresarial confidencial, el 44% de ellos respondió que “necesitaba cotejar ideas con otras personas”. Otras de las razones fueron: “Necesitaba desahogarme” (30%) y “No vi nada malo en ello” (29%). Cuando se les preguntó por qué alteraban las configuraciones de seguridad en sus computadoras en un claro desacato de las medidas de seguridad de sus empresas, la respuesta fue más descarada, ya que el 35% cree que eso “no le incumbe a nadie”. Y estos empleados incluyeron al personal de TI en su respuesta. El cincuenta y dos por ciento simplemente respondió que quería ver sitios no autorizados, sin importar que esto contradijera la política empresarial. El treinta y cinco por ciento sintió que nadie se iba a enterar.

La figura 3 muestra en forma gráfica **las razones que dan los empleados para alterar las configuraciones de seguridad de sus computadoras.**

Figura 3. Razones para alterar las configuraciones de seguridad

A veces la razón de poner la información en riesgo fue monetaria. Simplemente, para una familia u hogar es más económico usar una computadora suministrada por el empleador. Esta es una razón muy poderosa en culturas donde vive junta la familia extendida, pero aumenta la posibilidad de que personas que no sean empleados accedan a información de la empresa.

Por supuesto, en algunos casos, el problema no es que el empleado ignore la amenaza, sino que el empleado en sí constituye la amenaza. Si un empleado se siente infeliz en su trabajo, descontento con su jefe, o vengativo por alguna razón, puede convertirse en una “amenaza interna” capaz de dañar o causar una fuga de información en forma deliberada.

A pesar del esfuerzo del departamento de TI, es posible que algunos empleados no comprendan los procedimientos de seguridad establecidos en sus entornos laborales. La comparación entre el uso que le dan los empleados a los servicios de comunicación y los usos autorizados por sus departamentos de TI revela algunas diferencias interesantes. Lo más evidente, es que un porcentaje significativamente mayor de usuarios finales utiliza correo electrónico personal en el trabajo (49%) en comparación con la proporción que afirma que dicha práctica es aprobada por la empresa (40%). En China y Japón, esta brecha es aún mayor.

Las cifras de la encuesta indican que a pesar de que muchas empresas han intentado evitar la filtración de información por parte de sus empleados, sus esfuerzos no están dando los resultados deseados.

Cómo prevenir la fuga de información

Las amenazas contra la seguridad de la información continúan evolucionando. La piratería informática se está convirtiendo de manera creciente en una profesión delictiva y la colaboración adversaria es una actividad con fines de lucro. Gran parte del peligro proviene de Internet, que es un componente crucial de la infraestructura empresarial actual. Y en este entorno peligroso, se generan fugas de información por parte de los empleados a pesar de los grandes esfuerzos que realizan los profesionales de TI para impedirlo.

Debido a que la fuga de información por parte de los empleados se debe principalmente a la ignorancia, el desacato y la apatía, claramente no existe una solución mágica para salvaguardar la información empresarial, especialmente cuando las empresas y sus datos se tornan cada vez más móviles y operan con límites virtuales en vez de físicos. La forma más eficaz de prevenir la fuga de información es mediante un esfuerzo continuo y generalizado que sea holístico y estratégico.

Muchas empresas se equivocan al confiar exclusivamente en la tecnología, o al iniciar un programa de seguridad con una avalancha tecnológica. La mejor tecnología de seguridad del mundo no producirá un buen retorno de inversión si no se cuenta con una sólida base de procesos, políticas y educación en materia de seguridad.

Las empresas deben comenzar por evaluar la conducta de los empleados y los riesgos asociados basándose en factores tales como el país y el panorama de amenazas. Luego de acuerdo con dicha evaluación pueden diseñarse planes de educación sobre amenazas, capacitación en seguridad y procesos comerciales. Ése es el momento de realizar inversiones pertinentes en tecnología de seguridad.

Esta estrategia integral es la mejor forma de lograr un nivel de seguridad sostenible. Establece la base para evaluar los riesgos de cada interacción entre usuarios y redes, puntos terminales, aplicaciones, datos y, por supuesto, otros usuarios. Pero lo más importante es que hace que la seguridad sea una parte integral de la cultura empresarial, tal como lo es para la infraestructura de TI.

A continuación se indican algunas medidas tangibles que pueden implementarse para evitar la fuga de información.

Conozca su información y adminístrela bien — Como el propósito de la colaboración es abrir y compartir información, proteger los datos comienza por entender cómo las personas interactúan con ellos todos los días.
Usted puede:

- Establecer herramientas y procesos que rastreen el movimiento de datos para saber dónde se almacenan, cómo se accede a ellos y quiénes los utilizan.
- Identificar los tipos de datos que requieren un régimen especial de protección tanto en el interior como exterior de su empresa.
- Considerar nuevos métodos de seguridad para las herramientas y capacidades de nueva generación.

Proteja la información empresarial como si fuera su posesión más valiosa — Enséñele a sus empleados que la información empresarial es esencialmente dinero: perder o favorecer la fuga de datos empresariales es lo mismo que tirar dinero a la basura y dejar que la competencia lo encuentre y utilice en su contra. Y es muy probable que la información se use para perjudicar a la empresa en cuanto a su marca, ingresos, cotización bursátil y confianza del mercado. Los empleados deben comprender y poner en práctica los siguientes procedimientos básicos de seguridad:

- Para proteger los sistemas utilice sólo aplicaciones y métodos de acceso autorizados, mantenga actualizado el software de seguridad además de las aplicaciones antivirus, respete

y conserve las configuraciones de seguridad, comprenda las consecuencias de aceptar o rechazar las acciones emergentes de Cisco® Security Agent, y prepárese para los distintos métodos de ataque como el correo no deseado, software malicioso y phishing.
- Para proteger los dispositivos portátiles, manténgalos con usted o bloqueados en todo momento, no comparta sus dispositivos laborales ni los utilice para actividades personales, no envíe información confidencial desde sistemas laborales a dispositivos personales, y no acceda a sitios inapropiados ni descargue información indebida.
- Para evitar el acceso no autorizado a información, cierre sesiones o bloquee los sistemas cuando se aleje momentáneamente de su computadora o se vaya a casa al final de la jornada, utilice buenas técnicas de creación de contraseñas, no comparta sus contraseñas con nadie y almacénelas en forma segura.
- Para evitar el robo de información cuando esté de viaje, baje la voz cuando tenga que hablar sobre información confidencial en público, use filtros de privacidad para evitar que alguien vea sobre su hombro, use una red VPN y nunca use una impresora compartida a menos que usted esté presente para recoger enseguida lo que imprimió.

Institucionalice códigos estándar de conducta segura en su empresa — Las políticas de seguridad con respecto a la información son una parte integral del código de buena conducta empresarial y todos deben leerlas, comprenderlas y acatarlas. Los profesionales de TI deben pensar en forma global y actuar en forma local estableciendo objetivos de política generales y formulando planes de educación localizados adaptados según la cultura y el panorama de amenazas del país. Los empleados deben comprender que son fundamentales para conservar la seguridad de la empresa y aceptar la responsabilidad de protegerla. Sacrificar el nivel de calidad y seguridad en pos de la conveniencia es un error que las empresas no pueden permitirse cometer. Todos los empleados deben:

- Regirse por el código de buena conducta comercial de la empresa al llevar a cabo sus actividades laborales cotidianas, especialmente aquéllas relacionadas con la seguridad de la información.
- Estar constantemente atentos al entorno y pensar en la seguridad en cada acción que realicen en la oficina, el hogar y cuando estén de viaje.
- Aprender cómo manejar los diferentes niveles de confidencialidad para los documentos de su empresa. Esto incluye comprender las diferencias entre información “pública”, “confidencial”, “sumamente confidencial” y “restringida”.

Fomente una cultura y un entorno de honestidad y confianza — Los empleados deben sentirse cómodos con el panorama de seguridad de la empresa para poder poner en práctica las directivas de seguridad. Deben saber a qué organización de seguridad informar sobre conductas sospechosas, ataques reconocibles o incidentes de seguridad (incluso si fueron causados por ellos mismos), y deben sentirse cómodos iniciando dicho contacto. Los profesionales de TI deben enseñar a los empleados:

- Cómo evitar los errores de seguridad destacando las áreas de mayor vulnerabilidad.
- Prácticas adecuadas para proteger los sistemas y los datos.
- Qué constituye un incidente de seguridad informática y cómo informar de ello.

Establezca prácticas que fomenten la conciencia y educación sobre la seguridad en su empresa — Crear conciencia sobre los temas de seguridad es fundamental para lograr el apoyo de los empleados. Cuando un empleado cree que los programas de seguridad son importantes, es más probable que acate los procedimientos pertinentes. Un plan de educación debe:

- Instruir y capacitar a los empleados con respecto a las expectativas que tiene la empresa en relación con la protección de datos.
- Incluir capacitación y prácticas de seguridad en la orientación de nuevos empleados.

- Capacitar a los empleados sobre las medidas de seguridad que deben considerar al responder el teléfono y al conectarse a sitios Web 2.0, redes sociales y sitios de colaboración.
- Capacitar a los empleados sobre temas de seguridad física, como permitir que sólo empleados con credenciales de seguridad accedan a los edificios.

Un futuro seguro

Prevenir la fuga de información es un desafío que incumbe a toda la empresa. Mientras más personas comprendan dicho desafío, desde profesionales de TI, ejecutivos a empleados de todos los niveles de responsabilidad, mejor podrá proteger la empresa sus recursos cruciales. La meta es que cada persona, en cada nivel, esté convencida de que la seguridad empresarial es fundamental, comprenda las políticas y los procedimientos para lograr un entorno seguro y ponga en práctica las medidas necesarias cada día. Tal cambio cultural es todo un proceso —y según la encuesta de InsightExpress, uno al que las empresas de todo el mundo deben dedicar más recursos—. Con la voluntad y las inversiones suficientes, las empresas pueden reducir la fuga de información. La recompensa valdrá el esfuerzo.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**