Un hito en la lucha para proteger las tecnologías comerciales y de doble uso en Estados Unidos fue la promulgación de la Economic Espionage Act (EEA) de 1996. La ley transformó en una ofensa federal robar secretos comerciales y dio al FBI la autoridad para investigar el espionaje económico. La ley fue redactada con el aporte de ASIS International y su Consejo de Protección de la Información Privada, ahora el Consejo de Protección del Activo de Información (http://www.asisonline.org/councils/SPI.xml).

Con los años, mientras que las tecnologías empleadas en el espionaje han avanzado enormemente, las tácticas y técnicas generales se han mantenido muy consistentes. Incluso los planteamientos defendidos por Sun Tzu y Frederick Taylor siguen siendo ampliamente usados hoy en día.

## 1.3 ENFOQUE DE GESTIÓN DEL RIESGO PARA LA IAP

Todas las organizaciones poseen y usan los activos de información que merecen protección. La naturaleza de esa protección debiera basarse en un buen enfoque de la gestión del riesgo.

El siguiente es un proceso de evaluación para uso en la IAP:

- Identificar los activos de información.
- Valorizar los activos de información (asignando un valor cuantitativo, como dólares, o un valor cualitativo, como alto, medio o bajo).
- Evaluar amenazas para los activos de información. Evaluar los probables adversarios.
- Evaluar la probabilidad de ocurrencia de las amenazas.
- Identificar las vulnerabilidades existentes y las previstas.
- Evaluar el impacto de un evento de pérdida o divulgación en la organización.

- Identificar los controles de seguridad existentes y planificados u otras opciones para enfrentar el riesgo.
- Evaluar y priorizar los riesgos, basado en su probabilidad e impacto organizacional.

Una estrategia de protección de la información debe ser diseñada para apoyar los objetivos, la estrategia y la cronología de la organización. Tal como señala el autor Ira Winkler (2005, p.35):

> Sólo cuando usted comprende los verdaderos componentes del riesgo puede crear una estrategia efectiva y apropiada para proteger su organización y gestionar sus riesgos. Abordando sus vulnerabilidades y *optimizando*, en lugar de *maximizando*, sus esfuerzos de contraespionaje, usted puede mejorar enormemente su seguridad.
>
> Por lo que el objetivo de su programa de seguridad es optimizar el riesgo, nunca minimizarlo. Esta es una diferencia extremadamente importante.

### 1.3.1 EL ACTUAL ENTORNO GLOBAL DE LA INFORMACIÓN

En términos de intercambio de información, el mundo está interconectado como nunca antes. Debido a este nivel de interconectividad enorme –de hecho global-, las amenazas a los activos de información han llegado a ser más difusas y difíciles de reconocer y pueden actuar más rápido. El nivel de riesgo está aumentando. Como señala Michael D. Moberly, ex presidente del Consejo de Protección de Activos de Información de ASIS International (2006):

> Una lamentable realidad de las transacciones comerciales internacionales es que la probabilidad de que una compañía...experimente alguna forma...de infracción, apropiación indebida, falsificación o piratería de productos, es cada vez mayor.

Hoy en día, los activos de información que están en peligro son casi siempre imposibles de recordar o contener en términos de

 

diseminación (ASIS International, *Trends*, 2007, p.41). Ellos pueden estar en cualquier parte o en todas partes en un instante.

La Office of the National Counterintelligence Executive de Estados Unidos, en su *Annual Report on Foreign Economic Collection and Industrial Espionage* (2006), reconoció los desafíos del entorno global de la información cuando afirmó:

> La feroz competencia económica global permanente alimentará el robo de tecnología comercial...[y] las adquisiciones ilegales de elementos militares y de doble uso...En la medida que la globalización continúa presionando a las compañías estadounidenses para mover importantes tecnologías e incluso instalaciones de investigación y desarrollo en el extranjero, lugares en terceros países pueden llegar a ser cada vez más importantes para la adquisición de tecnología de Estados Unidos. Tanto la seguridad como el marco legal para la protección de las tecnologías en el exterior tienden a ser más débiles...

### 1.3.2 CATEGORÍAS DE AMENAZAS Y EJEMPLOS

Un elemento clave del modelo de evaluación de riesgos es un estudio exhaustivo de las amenazas existentes y proyectadas. Ellas pueden incluir las amenazas intencionales, naturales e involuntarias.

#### Amenazas Intencionales

Históricamente, gran parte de la atención se ha centrado en las amenazas intencionales. Para evaluarlas, uno identifica los potenciales adversarios y evalúa sus capacidades e intenciones de dirigirse hacia los activos de información clave. Es importante pensar en términos amplios cuando se consideran los potenciales adversarios. Además de los competidores extranjeros y nacionales, los adversarios pueden incluir gobiernos extranjeros, grupos activistas, grupos terroristas, organizaciones criminales, agentes de información y vándalos.

El FBI (2011) entrega el siguiente resumen del entorno de amenazas actuales:

> La Guerra Fría no ha terminado, simplemente se ha trasladado a un nuevo escenario: el mercado global. El FBI estima que cada año billones de dólares se pierden por los competidores extranjeros y nacionales que deliberadamente apuntan a la inteligencia

económica en la floreciente industria y tecnologías estadounidenses, y que sacrifican la inteligencia al dejar de lado las tecnologías explotando las fuentes abiertas de información y los secretos comerciales de la compañía. Los competidores extranjeros que buscan criminalmente información económica, por lo general operan de tres maneras:

1. Ellos apuntan agresivamente y reclutan personas informadas (a menudo de los mismos antecedentes nacionales) trabajando para empresas estadounidenses e instituciones de investigación;
2. Ellos realizan inteligencia económica a través de operaciones como soborno, intrusiones cibernéticas, robo, hurgando en la basura (en búsqueda de propiedad intelectual o prototipos desechados), interceptando teléfonos y;
3. Ellos establecen relaciones de negocios aparentemente inocentes entre compañías extranjeras e industrias de Estados Unidos para reunir inteligencia económica incluyendo los secretos comerciales.

La investigación sobre las capacidades e intenciones de los adversarios puede ser desarrollada internamente o mediante un consultor de confianza o una empresa de análisis de amenazas.

## Amenazas Naturales

Después de los desastres naturales, muchas compañías se disuelven, no porque perdieron sus instalaciones, sino porque perdieron su información. Por lo general, no tenían un plan de preparación eficaz (incluyendo un respaldo de la información crítica fuera de la instalación y un sitio listo (hot site) o semi-listo (warm site) como parte de un plan integral de continuidad del negocio. A menudo, las compañías que dejan de operar son pequeñas, de un solo sitio, sin funciones robustas de seguridad y gestión de riesgos. Todas la entidades, grandes y pequeñas, deben prepararse para desastres naturales que puedan afectar gravemente sus operaciones.

## Amenazas Involuntarias

Tal vez, las amenazas que con mayor frecuencia se pasan por alto son las amenazas involuntarias. Estas también son las más difíciles de identificar y evaluar, pero no pueden ser ignoradas. Como señala Winkler (2004, pp.53-54):

> A pesar que la gente quiere escuchar acerca de los terroristas y hackers (piratas informáticos), el hecho es que las pérdidas más grandes son de la gente en el espejo (people in the mirror)...Las personas cometen errores y esos errores lo más probable es que les hagan daño...Los errores humanos y los accidentes...causan cientos de billones de dólares (en pérdidas) al año. Cuando no se han anticipado apropiadamente, los incidentes pueden literalmente destruir una vida o una compañía.

Las amenazas involuntarias pueden ser atribuidas a un inadecuado entrenamiento de los empleados, malos entendidos, falta de atención a los detalles, aplicación relajada de la seguridad, presión para producir entregas, insuficiente personal u otros factores. Por lo tanto, es esencial desarrollar, promulgar y hacer cumplir políticas prácticas para la IAP.

Unas cuantas amenazas específicas merecen ser mencionadas, porque son prevalentes o representan una tendencia. Los siguientes temas deben ser considerados, según corresponda, cuando se realiza una evaluación de riesgos de IAP o para desarrollar estrategias de mitigación.

### Minería de Datos

De acuerdo a *Trends in Proprietary Information Loss* (ASIS International, 2007), el informe de una encuesta realizada por ASIS International, la minería de datos (basada en un software de recopilación de datos de fuentes abiertas e información pública) se ha convertido en una amenaza importante. Del mismo modo, la Office of the National Counterintelligence Executive (2006) expresa las siguientes preocupaciones por el futuro:

> La continua expansión de vínculos internacionales...crearán agentes mundiales especializados en el movimiento de tecnologías a través de las fronteras y socavando la capacidad...para controlar las exportaciones.

> Una gran preocupación es el hecho que las naciones mejor preparadas para usar las herramientas cibernéticas para acceder a las tecnologías estadounidenses también son los países que tradicionalmente han sido los más agresivos.

Las entidades del sector gubernamental y privado están usando cada vez más las herramientas automatizadas para recopilar, filtrar, organizar, analizar y diseminar la información. Un resultado es el crecimiento de los agentes de información. Otro es el desarrollo sitios Web de cursos de recopilación, libros de cómo hacerlo e incluso "inicie su propio negocio casero" en el tema de la minería de datos y corretaje de información. De mayor preocupación es que grupos terroristas internacionales están utilizando la minería de datos y las técnicas avanzadas de gestión del conocimiento para apoyar su obtención de inteligencia y planificación de actividades de ataque.

## Personas Informadas (Insiders)

*Trends in Proprietary Information Loss* (ASIS International, 2007) encontró que la explotación de relaciones de confianza también es una creciente amenaza. Las personas en ese tipo de relaciones incluyen a proveedores, clientes, socios de empresas mixtas (joint venture), subcontratistas y proveedores externalizados. Asimismo, un informe del Defense Personnel Security Research Center (Kramer, Heuer & Crawford, 2005) señala:

> Debido a su conocimiento de las agencias públicas y compañías privadas que los emplean, su familiaridad con los sistemas computacionales que contienen información clasificada y patentada, y su conciencia del valor de la información protegida en el mercado global, los insiders constituyen una importante área de vulnerabilidad para la seguridad nacional...
>
> La revolución de la información, la competencia económica global, la evolución de los nuevos y no tradicionales adversarios de inteligencia y otros cambios en el entorno nacional e internacional, han convergido para crear un campo inusual y fértil para el espionaje de los insiders. Las principales conclusiones de esta investigación son las siguientes:
>
> - Los avances tecnológicos en el almacenamiento y recuperación de la información están mejorando dramáticamente la capacidad de los insiders para acceder y robar información clasificada y patentada.
> - El mercado global para la información protegida de Estados Unidos se está expandiendo. Los insiders estadounidenses pueden vender tipos de información a una amplia gama de compradores extranjeros como nunca antes.

 

- La internacionalización de la ciencia y el comercio está colocando más empleados en posiciones estratégicas para establecer contactos con científicos, empresarios y recolectores de inteligencia extranjeros, y para transferirles material científico y tecnológico.
- El aumento de la frecuencia de viajes internacionales está creando una nueva oportunidad para los vendedores de información motivados para establecer contacto con y transferir información a entidades extranjeras. Los compradores extranjeros tienen mayores oportunidades para contactar y evaluar las vulnerabilidades del personal estadounidense con acceso a información protegida.
- La expansión global de Internet está proporcionando nuevas oportunidades para el espionaje interno. Internet permite a los vendedores y buscadores de información permanecer en el anonimato y proporciona los medios por los cuales se pueden transmitir grandes cantidades de material digitalizado a terceros en el extranjero de manera segura.
- Los estadounidenses son más vulnerables a experimentar graves crisis financieras debido a hábitos de gasto agresivo de los consumidores y otros factores. Los problemas financieros son una fuente común de motivación para el espionaje interno.
- La creciente popularidad de las apuestas y la prevalencia de los trastornos del juego sugieren que un mayor número de insiders cometerán delitos en el lugar de trabajo, tales como el espionaje, para pagar deudas y mantener las actividades de juego.
- Debido a que la lealtad organizacional está disminuyendo, menos empleados pueden ser disuadidos de cometer espionaje debido a al sentido de obligación con sus empleadores. Las condiciones cambiantes en el lugar de trabajo en Estados Unidos sugiere que un mayor número de insiders pueden ser motivados a robar información de sus empleadores para vengarse por el maltrato recibido.
- Ahora, más insiders tienen vínculos étnicos con otros países, se comunican con sus amigos y familiares en el extranjero, e interactúan con empresarios y gobiernos extranjeros. Las conexiones en el extranjero le proporcionan a los insiders oportunidades para transmitir información fuera de Estados Unidos, y los vínculos extranjeros pueden proporcionar la motivación para hacerlo.

- Más estadounidense ven la sociedad humana como un sistema evolutivo de diversidad étnica e ideológica, de grupos y personas interdependientes. Si bien esto es beneficioso en muchos aspectos, también es posible que algunos insiders con una orientación global en los asuntos mundiales, verán el espionaje, en circunstancias extremas, como moralmente justificable si ellos sienten que compartiendo la información beneficiarán la comunidad mundial.

Un estudio de 49 incidentes de insiders concluyó lo siguiente (United States Secret Service, 2005, pp.11-16):

- De los autores, el 59 por ciento eran ex empleados o contratistas de la organización afectada, mientras que el 41 por ciento eran actuales empleados o contratistas.
- El rango de edad de los autores era de 17 a 60 años.
- Tres de diez autores tenían registros de arrestos anteriores.
- Un evento negativo relacionado con el trabajo gatilló sus acciones en casi todos los casos.
- En el 80 por ciento de los casos, el autor llamó la atención de la gerencia debido a comportamientos inapropiados antes del incidente (v.gr, atrasos, ausencias, discusiones con los compañeros de trabajo, o un deficiente desempeño laboral).
- En el 31 por ciento de los casos, otros tenían información acerca de los planes del autor de causar daño; en el 20 por ciento de los incidentes se realizó una amenaza directa.

## Falsificación y Piratería

Desde los tejanos (jeans) y las carteras hasta los productos químicos y farmacéuticos, la falsificación y la piratería son problemas cada vez mayores, con implicancias tanto económicas como de seguridad. En una declaración reciente, la United States General Accountability Office (2007) afirmó que:

> Los esfuerzos del gobierno para proteger y hacer valer los derechos de propiedad intelectual (IP de ahora en adelante, por sus siglas en inglés), en el país y en el extranjero son cruciales para prevenir billones de dólares en pérdidas para la industria estadounidense y los

 

los propietarios de derechos IP y para evitar los riesgos de salud y seguridad asociados al comercio de productos falsificados y pirateados.

La amenaza de falsificación y piratería tiene grandes consecuencias, particularmente sobre las pequeñas empresas, las cuales están entrando cada vez más al mercado global y operando internacionalmente. Como señala Moberly (2006):

> Emprendimientos, empresas en etapa inicial y pequeñas y medianas empresas que son ricas en activos intangibles, por lo general no reconocen el alcance o impacto económico de la falsificación y piratería a nivel mundial. Tampoco parecen darse cuenta de cuán reactivas son la mayoría de las defensas convencionales (v.gr., patentes, derechos de autor, marcas registradas) frente a la piratería de nanosegundos y la falsificación.

### 1.3.3 EVALUACIÓN DEL RIESGO Y DUE DILIGENCE[1]

A veces, en el mundo de los negocios se dice que "usted no puede gestionarlo si no puede medirlo". Las evaluaciones de riesgos deben identificar los riesgos, cuantificarlos y priorizarlos de acuerdo al criterio de aceptación del riesgo de la organización. Los resultados de la evaluación deben ayudar en la selección y priorización de las acciones para gestionar los riesgos.

Se deben realizar evaluaciones regularmente e incluir un seguimiento de los riesgos para enfrentar los cambios en los requerimientos de seguridad, así como los cambios en la naturaleza de los activos de información, amenazas, frecuencia de ocurrencia de la amenaza, vulnerabilidades e impactos. Además, el seguimiento ayuda a evaluar la efectividad de la seguridad y otras medidas de mitigación de riesgo.

---

[1] Nota del Traductor: el término en general se utiliza para referirse a la investigación de empresas o personas. No existe una traducción oficial, las más comunes son "debida diligencia", "auditoría", o se mantiene el uso del término en inglés, el cual se utilizará en este trabajo de traducción.

### 1.3.4 LOGRAR EL COMPROMISO

EL compromiso de los ejecutivos es esencial para la IAP. Debido a que la información, los activos intangibles y la propiedad intelectual son parte integral de casi cualquier organización, se podría esperar que fuera fácil convencer a los ejecutivos de adoptar y apoyar un programa de protección de activos de información. Sin embargo, a menudo es difícil lograr tal compromiso, debido a la naturaleza intangible de los activos. Por lo tanto, los profesionales de IAP deben esforzarse para tener un argumento de negocios (business case) convincente a favor de estrategias proactivas, dedicación de recursos y la capacidad de hacer aportes al proceso de toma de decisiones del negocio –en otras palabras, para conseguir un puesto en la mesa.

Un paso hacia este fin es articular los impactos en el negocio de un evento de pérdidas. De acuerdo a *Trends in Proprietary Information Loss* (ASIS International, 2007), los principales impactos en el negocio son los siguientes:

- pérdida de la reputación/imagen/predisposición comercial de la empresa
- pérdida de la ventaja competitiva de un producto/servicio
- reducción del retorno o rentabilidad proyectada/anticipada
- pérdida de las tecnología o procesos fundamentales del negocio
- pérdida de ventajas competitivas en múltiples productos/servicios

Otros impactos de la pérdida de información patentada incluyen la pérdida de uso, propiedad o control de los derechos de propiedad intelectual, así como la pérdida de información confidencial o prototipos que facilitarían la falsificación del producto.

El personal de gestión de seguridad también puede destacar que la IAP beneficia el negocio porque hace lo siguiente (Moberly, 2007):

- mejora la supervisión fiduciaria, el control y la administración de activos intangibles clave

 

- alinea los activos de información con las operaciones del negocio y la visión estratégica de la organización
- permite una asignación más eficiente de los recursos de seguridad tradicionales y de TI
- permite una búsqueda más oportuna de los compromisos de los activos de información y de las violaciones a los derechos de propiedad intelectual (IPR de ahora en adelante, por sus siglas en inglés)
- sirve como ventaja en la negociación de la cobertura y de las primas de seguros de propiedad intelectual (IP) y de tecnología de información (TI)
- proporciona consistencia en los informes reglamentarios de activos intangibles
- estandariza el manejo interno y externo de los activos intangibles
- identifica las fuentes internas y externas clave de activos intangibles y capital intelectual

Otros enfoques sugeridos por Moberly incluyen el uso de métodos cuantitativos por parte de los profesionales de IAP cuando sea posible y asumir el rol de un recurso de negocios (uno facilitador, no un impedimento) para la empresa. Finalmente, la responsabilidad por la protección de los activos de información recae en los líderes de una organización.

Gerentes de nivel medio, también, deben ser convencidos para que un programa IAP tenga éxito (Winkler, 2005):

> Obtener el apoyo de la gerencia de primer y segundo nivel es fundamental. Los gerentes que ven a los empleados todos los días son los que realmente estarán allí para darse cuenta cuando las personas siguen las prácticas de seguridad y cuando no. Estas son las personas que más pueden influir en seguridad.

Finalmente, el programa de IAP debe ser asimilado por cualquier otra persona –dentro o fuera de la empresa- que tenga acceso a los activos de información de la compañía.

## 1.4 MÉTODOS PARA LA MITIGACIÓN DEL RIESGO

Gran parte del siguiente contenido proviene de *Information Asset Protection Guideline* (2007) de ASIS International.

### 1.4.1 PRÁCTICAS BÁSICAS DE PROTECCIÓN

El FBI (2011) enumera los siguientes pasos para proteger una empresa del espionaje:

- Reconocer que hay una amenaza interior y una exterior a su empresa.
- Identificar y valorar los secretos comerciales.
- Implementar un plan proactivo para proteger los secretos comerciales.
- Tener versiones físicas y electrónicas de los secretos comerciales.
- Circunscribir el conocimiento intelectual sobre la base de la "necesidad de saber".
- Hacer una capacitación a los empleados sobre el plan de propiedad intelectual y de seguridad de la compañía.

Las medidas que siguen son consistentes con el enfoque del FBI. La mayoría puede ser aplicada a cualquier organización privada o pública.

**Sensibilización y Políticas de la IAP**

Políticas claras, prácticas y bien promulgadas fortalecen cualquier programa de seguridad. Al desarrollar una política, hay varios pasos vitales:

- La dirección de la organización debe demostrar su compromiso con la IAP, proporcionando los recursos apropiados y exigiendo a todas las unidades de la empresa que

 

desarrollen las estrategias para alinear los negocios y los objetivos de protección.

- Un grupo, persona o departamento específico debe ser asignado a la gestión y auditoría de la política
- Se les debe exigir adherirse a la política a todas las unidades de la empresa, personal, empleados temporales, proveedores, consultores, contratistas y socios del negocio.
- Se debe entregar en forma reiterada una capacitación de la IAP en las sesiones de orientación para los nuevos empleados; durante las inspecciones, en conferencias con todo el personal, y visitas a otras instalaciones; en la intranet de la empresa; los boletines; y como parte de la capacitación de TI o de recursos humanos.
- Los esfuerzos de sensibilización y capacitación de la IAP deben ser documentados.

Es importante identificar qué información debe ser protegida y cuándo, y luego identificar las muchas formas que puede tomar esta información durante su ciclo de vida. Sólo un cierto segmento de la información de la organización puede justificar la protección. Una vez que esa información es identificada, se debe clasificar de modo que los activos de información más importantes reciban el mayor grado de protección.

La declaración de la política establece el tono para la organización y, si se hace cumplir, puede apoyar acciones legales si se vuelve necesario. La política debe clarificar que la información es uno de los recursos más importantes de la organización, que toda la información necesita ser evaluada apropiadamente según su sensibilidad, y que las medidas de protección deben ser suficientes para garantizar la confidencialidad, integridad, disponibilidad, responsabilidad, capacidad de recuperación, auditabilidad y autenticación de la información, tanto en el entorno físico y cibernético. Se deben realizar al azar para asegurar el cumplimiento de la política de IAP.
En el Anexo A se encuentra un ejemplo de declaración de política para IAP.

## Identificación y Marca de la Información Protegida

La información que merece protección debe ser adecuadamente identificada y marcada. Se usan varios niveles para distinguir el grado de sensibilidad o el grado de protección que requiere: confidencial,

restringida, limitada, no pública, etc. La mayoría de las organizaciones usan dos o cuatro niveles de sensibilidad.

Por ejemplo, muchas empresas dividen la información en tres categorías: aprobada para divulgación externa (acceso sin restricción), interna (limitada a los empleados y contratistas) y confidencial (limitada por una necesidad de conocimiento específica). La información puede ser electrónica, oral, escrita u otras formas. Siempre que sea práctico, el material debe ser marcado o etiquetado. Generalmente, quien originó la información determina el nivel de clasificación y los usuarios autorizados no pueden divulgar los contenidos sin la aprobación del propietario.

El acceso a la información interna debe restringirse al personal de la compañía u otras personas que hayan firmado un acuerdo de no divulgación. Las normas para autorizar el acceso también pueden incluir una investigación de antecedentes satisfactoria. El acceso de un empleado se debe basar en su función de trabajo actual y en la necesidad de conocimiento, no solamente en el cargo o nivel de gerencia.

### 1.4.2 SEGURIDAD FÍSICA

Los profesionales de IAP deben coordinar estrechamente con el personal de seguridad física para armonizar los esfuerzos de protección en varias categorías.

**Protección en Capas (Defensa en Profundidad)**

Este concepto, que aplica una visión de anillos o capas concéntricas de protección para cualquier activo, comúnmente se utiliza más en términos de seguridad física. El mismo enfoque, no obstante, debe ser empleado en la protección de los activos de información sensible. La defensa en profundidad puede ser vista desde tres perspectivas diferentes, en las cuales los anillos concéntricos o capas de protección representan lo siguiente:

- Incremento de los niveles de confianza para aquellos a quienes se les da acceso a capas sucesivas. Por ejemplo, un miembro del personal de mantenimiento probablemente tendrá un nivel de confianza menor (y por lo tanto acceso) que el director de

investigación y desarrollo de la empresa. Basado en sus respectivos niveles de confianza, cada uno de ellos tendría niveles de acceso apropiados, pero diferentes, a la información o instalaciones.

- Diferentes tecnologías o medidas de seguridad que operan concertadamente. Mediante la aplicación de tecnologías o medidas de seguridad superpuestas y diversas, el personal de seguridad puede identificar y llenar los vacíos en la cobertura de protección. Los beneficios deben ser sopesados con los costos.
- Capas sucesivas empleadas para demorar, detectar y disuadir a los intrusos. Cada capa de protección sucesiva puede demorar aún más a un adversario, ofrecer una oportunidad adicional para detectar la intrusión y disuadir al adversario de avanzar.

Estas perspectivas aplican igualmente a los sistemas de protección automatizados y a la información en otras formas (disco duro, proceso, conocimiento, intangible, etc.).

Para implementar la protección en capas, un profesional de IAP debe hacer lo siguiente:

- Aplicar múltiples niveles o capas de medidas de protección a los activos de información críticos, apropiados a su sensibilidad y exposición a la pérdida.
- Garantizar que los sucesivos niveles o capas de medidas de protección se complementen en lugar de entrar en conflicto entre ellas.
- Elaborar una estrategia coordinada que integre diferentes familias de medidas de protección, tales como seguridad física, personal de seguridad, seguridad técnica, control de acceso, educación y concienciación, y políticas y procedimientos.

Normalmente, las instalaciones y los sistemas de información de la compañía deben contar con protección de entrada no autorizada en todo momento. El acceso a información interna o confidencial debe requerir autenticación vía presentación de credenciales de acceso única, previamente autorizadas, físicas y lógicas. El nivel de acceso

otorgado debe ser consistente con el nivel de información que la persona necesita para su trabajo.

**Manejo de Documentos y Registros**
Estas funciones representan la gestión diaria de la información sensible en papel o en forma electrónica. Se recomiendan los siguientes pasos de protección:

- Colocar trituradoras o receptáculos seguros de recolección cerca de las impresoras, fotocopiadoras y máquinas de fax.
- Colocar avisos en esas áreas para recordar a los empleados que deben destruir las copias sobrantes o con error de impresión.
- Cuando corresponda, documentar cualquier transferencia (interna y externa) de registros o documentos sensitivos.
- Seleccionar cuidadosamente los contratistas que destruyen registros, documentos o información sensible.
- Destruir registros e información sensible de manera que impida una reconstrucción consistente con su nivel de sensibilidad, y documentar la fecha y lugar de destrucción.
- Destruir los registros obsoletos regularmente, conforme a la programación de retención de registros.
- Destruir los registros incidentales y duplicados sobre una base regular.
- Almacenar los medios en espera de destrucción en contenedores seguros.
- Si es posible, evitar desechar los medios destruidos en receptáculos de basura accesibles al público.
- Cuando los registros y la información estén siendo transportadas, protegerlos con contenedores cerrados, sellos, escoltas, etiquetas de identificación de radiofrecuencia, registros de transporte y otros medios.

En el Anexo E se presenta más información sobre la eliminación y destrucción de documentos.

 

## Protección de la Información en Forma Física

- Prototipos y modelos
  - A estos se les debe otorgar la misma seguridad física, control de acceso, clasificación, investigación de antecedentes de los empleados, verificación y documentación que a los otros activos de información.
  - Los prototipos, modelos y artículos de prueba obsoletos deben ser destruidos de modo que no se pueda realizar ingeniería reversa.
  - Los contratistas y proveedores encargados de prototipos, modelos o artículos de prueba deben ser contractualmente obligados a protegerlos de acuerdo a las políticas y procedimientos del propietario. Además, se les deben dar las instrucciones para la devolución o disposición de los artículos cuando ya no se necesiten.

- Equipos y Procesos de Fabricación
  - El acceso a las instalaciones de producción o procesamiento se debe restringir a los empleados que necesitan acceso para llevar a cabo sus responsabilidades
  - Se debe restringir la fotografía en las áreas de producción o procesamiento
  - Los contratistas con acceso a las áreas de producción o procesamiento deberían firmar acuerdos de no divulgación como los que se requieren para el manejo de otra información sensible
  - Los empleados, contratistas y visitantes que entran a las áreas de producción o procesamiento deben mostrar sus credenciales de identificación indicando su estado y nivel de acceso autorizado. Además, los visitantes deben ser obligados a firmar en un sistema automatizado de control de visitas o registro de visitas
  - Los equipos de producción obsoletos o dañados, así como la chatarra, deben ser eliminados de manera que no se

ponga en peligro o se divulgue información respecto al área de producción o procesamiento.

- La información relacionada con la actividad del muelle de carga (como materiales y cantidades recibidas en los envíos) también pueden requerir protección

- Compartimentación y barreras físicas o visuales
  - La información de diferentes clasificaciones deben ser almacenadas separadamente
  - Se deben usar protecciones como barreras y cubiertas cuando la información sensible pueda ser expuesta a la vista de personas no autorizadas

### 1.4.3 PERSONAL DE SEGURIDAD

La seguridad del personal juega un rol clave en un IAP. Esto incluye aspectos como investigación de due diligence de potenciales socios, investigaciones estándar de selección previas al empleo e investigación de antecedentes de subcontratistas, proveedores y consultores.

El proceso de selección a menudo está fuera del control de seguridad, gestión de riesgos o las funciones de IAP, y en su lugar pueden ser manejados por los departamento de recursos humanos o legal. Un desafío adicional es que esas investigaciones por lo general requieren largos plazos. Por lo tanto, los procedimientos a veces son eludidos, y posiblemente ponen los activos de información en mayor riesgo.

Para superar estos desafíos, el profesional de IAP debe establecer un canal de comunicación eficaz con los otros elementos organizacionales involucrados en estas funciones de selección; garantizar que la investigación de antecedentes cubra todas las potenciales personas de confianza con quienes la información protegida pudiera ser compartida; y revisar periódicamente la selección de personal, due diligence y procedimientos de investigación de antecedentes.

 

### 1.4.4 PROTECCIÓN DE LA PRIVACIDAD

Todas las organizaciones manejan información privada que pertenece a sus empleados, la gerencia, sus relaciones, clientes u otras personas. En algunas organizaciones esto incluye información que es clasificada como "Información de Identificación Personal" o "PII" (por sus siglas en inglés). Para mantener la confianza y cumplir los requerimientos legales, los profesionales de IAP deben hacer lo siguiente:

- Establecer políticas de privacidad específicas y designar un empleado responsable de implementar y administrar el programa de privacidad.
- Evaluar la información de privacidad relacionada con los empleados, proveedores, clientes y otras personas, y determinar los requerimientos legales y reglamentarios.
- Asegurar los sistemas establecidos para proteger la privacidad de empleados y clientes.
- Proporcionar un mecanismo para investigar el compromiso de la privacidad de la información (incluyendo el robo de identidad) e informar los incidentes a las personas u organizaciones afectadas (víctimas) según corresponda.
- Revisar las directrices federales, estatales e internacionales aplicables, tales como aquellas mostradas en el sitio Web de U.S. Federal Trade Commission (www.ftc.gov/privacy) y en varias directivas de protección de los datos de la Union Europea para garantizar el total cumplimiento con las leyes y reglamentos aplicables.
- Marcar claramente la privacidad de la información para indicar cómo se usará la información y cómo se pondrá a disposición de otros, qué notificaciones y acciones se deben realizar si se ve comprometida y las instrucciones para su destrucción o disposición cuando la información ya no sea necesaria.
- Realizar un programa de auditoría para garantizar que las políticas de privacidad se han implementado apropiadamente.

### 1.4.5 PRÁCTICAS EMPRESARIALES

ASIS International sostiene que la seguridad es una función de negocios. Por lo tanto, los principios de IAP deben ser incorporados a las prácticas cotidianas y a la cultura de la empresa. Por otra parte, los aspectos clave de la misión y filosofía de negocios de la organización deben ser incluidas en la estrategia de la IAP. Los siguientes son algunos pasos para la armonización de la IAP y las prácticas generales de negocios:

- Coordinar las materias de IAP con todos los medios apropiados de la compañía: legal, recursos humanos, seguridad, gestión de riesgos, protección, TI, investigación y desarrollo, contrataciones, marketing, relaciones públicas, capacitación, logística, inteligencia competitiva, relaciones internacionales, contabilidad y finanzas, instalaciones y otros.
- Incorporar la IAP en el plan de continuidad del negocio de la organización para garantizar que la información crítica conserva su disponibilidad, confidencialidad e integridad durante todas las fases de situaciones de crisis, incluyendo la respuesta y recuperación.
- Incorporar el material relacionado a la IAP en los programas de capacitación y desarrollo profesional de los empleados.
- Comunicar los asuntos de la IAP a todos los niveles de gestión.

Una actividad de negocios que plantea riesgos especiales para la información de una compañía es el establecimiento de relaciones (tales como sociedades o acuerdos de externalización) con otras compañías, nacional e internacionalmente. En esas relaciones, las compañías pueden bajar la guardia sin darse cuenta respecto a la protección de la información. En estados Unidos, miles de compañías de fachada se han establecido, a menudo a través de gobiernos extranjeros, para recolectar información de las empresas estadounidenses. Por lo tanto, es esencial realizar investigaciones de due diligence antes de asociarse con –y compartir información con- otras compañías.

 