1.4.8 PREVENCIÓN Y DETECCIÓN DE LA FALSIFICACIÓN Y COPIA ILEGAL

Los siguientes pasos pueden ayudar a los profesionales de IAP a prevenir y detectar la falsificación y copia ilegal:

- Monitorear Internet para identificar los productos falsificados.
- Entrenar a los empleados para observar productos falsificados y sospechosos conocidos, competidores u otros esquemas comunes.
- Exigir a todos los empleados, proveedores, subcontratistas que firmen acuerdos de no divulgación (NDA por sus siglas en inglés).
- Emplear tecnología anti-falsificación.
- Numerar todos los informes y memorandos técnicos.
- Realizar regularmente auditorias de cumplimiento y control de inventario, dentro y fuera de la organización.
- Trabajar con los organismos encargados de hacer cumplir la ley y las agencias fiscales en la detección, conciencia, alertas e intercambio de información
- Considerar la participación en el programa U.S. Customs and Border Protection (CBP) Intellectual Property Rights e-Recordation (https://apps.cbp.gov/e-recordations). Bajo el programa, los dueños de propiedad intelectual pueden registrar sus derechos de autor y marcas aunque mediante un proceso de registro electrónico. Este programa de inscripción permite a CBP detener cualquier producto registrado sospechoso de ser una violación de los derechos de autor o leyes de marca registrada de Estados Unidos, y a notificar al propietario del activo.

1.5 PROTECCIONES LEGALES

En Estados Unidos, la privacidad de la información protegida está regulada específicamente por la Health Insurance Portability and Accountability Act (HIPAA), la Ley de Privacidad y Ley de los Servicios Financieros (Gramm-Leach-Bliley Act); en la Unión Europea por la Data Protection Directive; y por otras leyes y reglamentos en todo el mundo[2]. Todos los programas exitosos de IAP asignan a un especialista la responsabilidad de monitorear la legislación y reglamentos en trámite relacionados con la protección de los activos de información. Es muy importante evaluar cualquier posible efecto que esos cambios puedan tener en la organización.

A continuación se enumeran los temas a discutir con el asesor legal de la organización:

- tomar medidas coercitivas sobre cualquier patente, derecho de autor, o violación a una marca comercial/de servicio
- conocer los actuales protocolos legales y jurisprudencia para ayudar a determinar la pérdida de beneficios (lucro cesante) y daños financieros y decidir las estrategias de protección apropiadas
- conocer el estado de protección de los derechos de propiedad intelectual y la naturaleza de las violaciones en cada jurisdicción donde la organización planea hacer negocios

Además, los propietarios de los activos de información deben reconocer que las protecciones legales son eficaces sólo si el propietario está dispuesto a perseguir el recurso cuando se produce una violación. Esta actividad puede consumir una gran cantidad de tiempo y recursos financieros. Los propietarios de los activos deben analizar por anticipado el criterio previsto para resolver violaciones cuando ocurran.

Según la Patent and Trademark Office de Estados Unidos (2007), una patente es un derecho de propiedad concedido a un inventor para excluir a otros de fabricar el invento, usarlo, ofrecerlo para la venta, o venderlo el invento por tiempo limitado; una marca comercial consiste de palabras, nombres, símbolos, dispositivos, o imágenes aplicadas a productos o usadas en relación a bienes o servicios para identificar su origen; y un derecho de autor es usado para proteger la expresión de ideas en obras literarias, artísticas y musicales.

La mejor manera de empezar a abordar la infracción de patentes, derechos de autor y marcas comerciales es registrando esos derechos. Es responsabilidad del dueño de la propiedad intelectual conocer y cumplir los requisitos relacionados con la protección de esos derechos en cada jurisdicción relevante. Es importante buscar la ayuda de un experto cuando se registren patentes, marcas comerciales y derechos de autor y cuando se enfrente una potencial infracción. También puede ser útil la participación en organizaciones de lucha contra la falsificación.

El Departamento de Estado de Estados Unidos proporciona asesoría en los temas de derechos de propiedad intelectual en muchos países, generalmente listados bajo "IPR Tool Kit" (kit de herramientas de derechos de propiedad intelectual) en el sitio Web de la embajada específica. Por ejemplo, los temas de derechos de propiedad intelectual en China se discuten en http://beijing.usembassychina.org.cn/ipr.html.

1.5.1 DERECHOS DE AUTOR

Según el derecho internacional, los derechos de autor no tienen que ser registrados para ser protegidos. No obstante, un autor o poseedor de derechos de autor puede formalizar su propiedad a través del registro de gobierno, el cual puede ayudar en cualquier acción de cumplimiento posterior.

El titular de los derechos de autor no debe permitir que el control de los derechos caiga en manos de los agentes o distribuidores de la organización. Es importante hacer lo siguiente:

- Incorporar los derechos de autor en los contratos y estrategias de marketing.

- Suscribir contratos escritos que exijan que agentes, proveedores, distribuidores y empleados protejan los derechos de autor.
- Negarse a ceder o autorizar los derechos de autor hasta que las consecuencias sean totalmente comprendidas.
- Asegurarse que los derechos de autor se mantienen en la organización hasta el término de la cesión, licencia, transacción o inversión.

Si una organización descubre que su derecho de autor ha sido violado, es esencial adoptar medidas inmediatamente. Las herramientas de respuesta incluyen:

- contratación de un asesor legal;
- informar a las autoridades correspondientes;
- realizar investigaciones, allanamientos e incautaciones; y
- iniciar litigios civiles, procedimientos administrativos y procesos criminales.

Al decidir qué herramientas usar, ayuda el formularse las siguientes preguntas:

- ¿El derecho de autor está registrado o susceptible de protección en el país en particular?
- ¿El daño se está causando en ese país o en el extranjero?
- ¿Cuál es el origen del daño: competidores, empleados, agentes o contratistas?

1.5.2 MARCA COMERCIAL, IMAGEN COMERCIAL, MARCA DE SERVICIO

Los nuevos participantes del mercado deben desarrollar una estrategia para proteger la propiedad intelectual de la compañía en las primeras etapas de planificación de la actividad comercial en cualquier país. El registro de las marcas comerciales antes de que el producto entre en la

corriente del comercio en cualquier país es el medio más importante para asegurarse que la marca es susceptible de protección bajo las leyes de ese país y garantizar que la infracción de la marca comercial puede ser remediada a través de procedimientos administrativos o judiciales. También es importante aplicar la marca comercial o de servicio apropiada y los avisos a materiales producidos por la compañía.

Cuando se realizan negocios fuera del país de origen de la organización, la mejor arma es la prevención. Los siguientes son algunos pasos prácticos:

- Familiarizarse con los derechos de la organización antes que el producto cruce la frontera.
- Desarrollar y registrar una versión en el idioma del país anfitrión. De lo contrario, el mercado puede hacerlo, creando un apodo para el producto. A la compañía puede que no le guste ese nombre, o alguien más en el país puede registrarlo, obligando a la compañía a comprar los derechos.
- Registrar la marca comercial en los países vecinos para proporcionar la protección para una potencial expansión y evitar que otros registren las marcas en productos que los consumidores pueden confundir con los de la compañía.
- Realizar una investigación para identificar los productos que infringen la marca comercial o que tenga una marca registrada tan similar que se puede confundir con la de la compañía, pero registrada por un tercero.

1.5.3 PATENTES

Un inventor puede proteger una invención patentándola o considerándola un secreto comercial. Las patentes conllevan una serie de beneficios, pero requieren que el inventor divulgue públicamente los elementos de la invención, y una patente dura sólo 20 años. Por el contrario, un secreto comercial no es divulgado y puede durar indefinidamente. Además, mientras que el robo de un secreto comercial puede violar leyes criminales, no existen leyes criminales relacionadas a la infracción de patentes (United States Department of

Justice, 2006). Lo que sigue es un enfoque para la protección de invenciones:

- Seguir las directrices del secreto comercial para todos los procesos o productos recientemente descubiertos hasta que la patente haya sido emitida.
- Asegurarse que la protección de la patente es adquirida en todas las jurisdicciones correspondientes.
- Considerar el uso de la U.S. International Trade Commission como un lugar para resolver las controversias sobre patentes.

1.5.4 SECRETOS COMERCIALES

Los secretos comerciales no necesitan ser registrados en ninguna agencia externa, así el propietario puede mantener un mayor grado de control sobre el activo. Para que la información sea considerada un secreto comercial, el propietario debe ser capaz de probar que la información añadió un valor o beneficio al propietario, el secreto comercial fue específicamente identificado y el propietario proporcionó un nivel razonable de protección al secreto comercial. El término "razonable" implica un alto estándar; el propietario debe demostrar un programa de seguridad robusto y medidas de protección estrictas que estén clara y consistentemente definidas, comunicadas y que se hagan cumplir.

Los siguientes pasos deben ayudar a la organización a proteger sus secretos comerciales:

- Documentar la identificación y valoración de los secretos comerciales, su rol en el establecimiento de una ventaja competitiva en la industria y el alcance total de las medidas de protección instituidas para protegerlos.
- Asegurar que existen medidas de seguridad, tradicionales y cibernéticas, razonables para evitar el acceso no autorizado a los secretos comerciales.
- Realizar auditorias de seguridad aleatorias y periódicas, para asegurar su cumplimiento

- Llevar a cabo acuerdos de no divulgación con los empleados, proveedores, consultores, y otras personas antes de cualquier divulgación.
- Establecer los criterios de necesidad-de-conocimiento para garantizar que las personas tengan acceso sólo a la información específica que necesitan para hacer sus trabajos.
- Instituir notificaciones de información de advertencia eficaces para garantizar que las personas están conscientes de lo que exactamente necesita ser protegido.
- Adoptar medidas apropiadas para la destrucción de materiales que ya no se necesiten.

1.5.6 ACUERDOS DE NO DIVULGACIÓN Y CONTRATOS

Los acuerdos escritos de no divulgación (NDA) garantizan un comprensión común y una obligación legal respecto a la protección de los activos de información. Los NDA deben reconocer que cualquier información sobre cualquier medio que registre comunicaciones comerciales o transacciones es considerado un registro oficial ante las leyes y será manejado de acuerdo a las políticas y procedimientos relacionados con los activos de información. Las obligaciones de confidencialidad pueden necesitar ser extendidas a los miembros del consejo, empleados, agentes u otras personas.

Todos los empleados deben firmar una NDA como una condición de empleo. Mediante el acuerdo, ellos deben reconocer que todos los activos de información relacionados con el empleador, proveedores y clientes son considerados confidenciales. El NDA de los empleados también debe incluir la verificación de que el empleado ha leído, entendido y se atendrá a las políticas y procedimientos de IAP. Cuando su empleo termine, a los empleados se les debe recordar que su obligación bajo el NDA continúa.

Del mismo modo, un contratista, subcontratista, consultor o proveedor con acceso a los activos de información deben estar contractualmente obligados a proteger la información en la misma medida en que se encuentra protegida en la empresa.

1.6 MEDIDAS TÉCNICAS DE PROTECCIÓN

Esta sección aborda los medios de mitigación de las amenazas de recolección técnica. La incorporación de medidas tradicionales de protección con estos métodos técnicos representa una aplicación de convergencia en la protección de activos. Muchos de estos métodos descritos aquí requieren conocimientos especializados, y puede ser necesario externalizar algunos servicios. Es esencial seleccionar cuidadosamente los socios para externalización, ya que ellos necesariamente obtendrán acceso a información sensible.

1.6.1 CONTRAMEDIDAS DE VIGILANCIA TÉCNICA

Las contramedidas de vigilancia técnica (TSCM de ahora en adelante, por sus siglas en inglés) son servicios, equipos y técnicas diseñadas para localizar, identificar y neutralizar actividades de vigilancia técnica (escuchas clandestinas). Las TSCM deben ser parte de la estrategia global de protección de la organización.

Como parte de los esfuerzos de TSCM, los profesionales de IAP deben disponer inspecciones periódicas de los equipos de telecomunicaciones, cables y terminales con equipos, métodos y personal capaz de detectar las amenazas actuales. Las oficinas y salas de reuniones deben ser inspeccionadas regular y aleatoriamente para detectar vulnerabilidades de vigilancia técnica y también inmediatamente antes de cualquier conversación sensible.

1.6.2 PROTECCIÓN EN UN ENTORNO DE TI

Esta sección presenta los aspectos más destacados de los problemas de seguridad de TI relacionados con los programas de IAP. La seguridad de TI está cubierta en mayor detalle en otras secciones de *Protección de Activos*.

Debido a que existe mucha información en forma electrónica, los profesionales de IAP deben considerar la protección de redes (alámbricas e inalámbricas) y también de las computadoras independientes. Lo más eficaz es un enfoque estratificado que integre

las medidas de protección físicas, de procedimientos y lógicas. Los siguientes son algunos pasos recomendados:

- Cambiar las contraseñas por defecto, nombres de usuarios y cuentas administrativas.
- Asignar adecuadamente los privilegios administrativos. Los administradores deben usar cuentas sin privilegios cuando no están realizando la administración del sistema.
- Limitar y monitorear los accesos físicos a los componentes de la red.
- Asegurar una separación de responsabilidades para el personal de TI cuando sea posible.

- Instalar y actualizar el software de antivirus y cortafuegos en los servidores de la red y los dispositivos de clientes (computadoras portátiles, estaciones de trabajo y dispositivos electrónicos personales). Los cortafuegos pueden proteger la información de intrusiones externas e internas.
- Implementar protocolos formales de gestión de parches y gestión de configuración.
- Capacitar a los usuarios en la conciencia de seguridad informática, incluyendo los riesgos asociado a accesos remotos, accesos móviles y tecnología inalámbrica.
- Exigir a las organizaciones externas con acceso a los sistemas de información de la compañía que mantengan una postura de seguridad equivalente.

Un sistema de detección de intrusión (IDS de ahora en adelante, por sus siglas en inglés) supervisa programas maliciosos y cambios no autorizados de archivos y configuraciones. También supervisan el tráfico de la red y proporcionan alarmas para los ataques a la red. Para algunos entornos, se debe considerar un sistema de prevención de intrusión, especialmente donde el personal podría no estar disponible para monitorear activamente o actuar en las alertas del IDS. Adicionalmente, se pueden configurar sistemas de prevención de extrusión para prevenir la salida de información no autorizada.

Especial atención se debe dar a la protección de datos y al control de acceso en entornos informáticos en la nube y/o cuando terceros tengan

algún acceso legítimo a los recursos informáticos o contenido de la información. Esto también aplica cuando una organización emplea un respaldo en línea, una almacenamiento de datos o proveedor de administración de archivos.

Los profesionales de IAP también deben estar conscientes de lo siguiente:

- **Control de acceso lógico a la red**. Este es el proceso por el cual los usuarios son identificados y se les otorga privilegios para la información, sistemas, o recursos.
- **Seguridad de las aplicaciones**. Las aplicaciones comerciales modernas generalmente consisten de un código personalizado, software de terceros y uno o más servidores. La integración inadecuada de estos componentes puede resultar en una vulnerabilidad que posteriormente puede ser explotada para obtener acceso no autorizado a los datos.
- **Desinfección de los sistemas de información y medios de comunicación**. La desinfección es el proceso de eliminación de datos de un medio de almacenamiento (como un disco duro) antes de que el medio sea reutilizado. Los métodos incluyen sobrescribir y desmagnetización (borrado magnético). Una alternativa es la destrucción física.
- **Encriptación.** La encriptación obscurece el significado de la información alterándola o codificándola de tal manera que sólo pueda ser decodificada por las personas a quienes va destinada
- **Firma digital.** Esta autentifica la identidad del remitente de un mensaje. Las firmas digitales son especialmente importantes para el comercio electrónico y los correos electrónicos.
- **Entorno inalámbrico.** Las redes de área local inalámbricas (WLAN de ahora en adelante, por sus siglas en inglés) son convenientes pero pueden introducir riesgos. Ellas por lo general son consideradas menos seguras que las redes

1.7 RESPUESTA Y RECUPERACIÓN DESPUÉS DE UNA PÉRDIDA DE INFORMACIÓN

Los siguientes son pasos clave a tomar después de una pérdida de información:

Investigación

- Investigar exhaustivamente la información comprometida ya conocida y la que se sospecha para apoyar a los encargados de hacer cumplir la ley, las causas judiciales, recuperación de activos, identificación de la causa raíz del incidente, prevención de futuros incidentes y evaluación de las pérdidas o daños.
- Establecer un plan de investigación y coordinar con el asesor.
- Identificar los recursos de investigación que se requieren de las fuentes internas o externas.
- Establecer y mantener enlaces con los organismos encargados de hacer cumplir la ley y los proveedores de servicios de investigación así como con diversas fuentes de información.

Evaluación del Daño

- Tan pronto y lo más completamente posible, determinar cuál es la información que ha sido comprometida.
- Determinar las implicancias del compromiso en términos de pérdidas económicas, demora en los proyectos, impacto

operacional, imagen corporativa, confianza de los accionistas, responsabilidad legal y relaciones corporativas (con socios, proveedores, vendedores, subcontratistas, etc.).

- Informar el impacto real y potencial al nivel de gerencia correspondiente.

Recuperación y Seguimiento

- Darse cuenta que los dos elementos primordiales de la recuperación son (1) volver el negocio a las operaciones normales tan pronto como sea posible y (2) implementar medidas para evitar una recurrencia del problema.
- Implementar cualquier parte aplicable del plan de continuidad de negocios de la organización.
- Realizar un análisis de la causa raíz e implementar acciones correctivas basadas en sus conclusiones. Mantener una base de datos de incidentes (incluyendo denuncias y presuntos incidentes) para apoyar el análisis de la causa raíz y analizar cualquier tendencia.