Recurso Humano, Activo Crítico en las Empresas Proveedoras de Servicios de Seguridad de la Información

Suárez López, Diana Patricia
Universidad Piloto de Colombia
sudias7@hotmail.com

Resumen— Este documento busca evidenciar como las fallas en el control y cuidado del recurso humano, uno de los activos más críticos en las empresas proveedoras de servicios de seguridad de la información, pueden causar incidentes de seguridad como fuga de información en empresa donde estos recursos laboran y en los clientes de la empresa, o incurrir en gastos elevados para la compañía por conceptos de entrenamiento de personal nuevo, pérdida de credibilidad por parte de los clientes a los cuales la organización presta sus servicios por posibles falencias de conocimiento de los recursos nuevos, fallas en la ejecución de procesos de la organización y perdida de ventas a causa de la llegada de nuevas empresas que proveen el mismo servicio con recursos entrenados provenientes de otros proveedores de servicios de seguridad de la información. Adicionalmente, este artículo muestra algunas alternativas que podrían ayudar a las organizaciones a mitigar el riesgo que implica la gestión de los recursos humanos.

Abstract— This document searches to show how faults in the control and care of human resources, one of the most critical assets in the service providers of information security, can cause security incidents as leak of information company where these resources works and the customers of the company, or incur in high costs of the company for concepts of training new staff, loss of credibility of the customers to whom the organization serves by possible weaknesses of knowledge of the new human resources of the company, failures in the execution of the company processes and lost sales due to arrival of new companies providing the same service with trained resources which come of other security information providers. Additionally, this article shows some alternatives that could help organizations mitigate the risk involved of human resource management.

Índice de Términos— Fuga de información, incidente, riesgo, normatividad

I. INTRODUCCIÓN

Aunque la información es uno de los activos más críticos para las organizaciones, el recurso humano también se debe considerar como un activo crítico, el personal en una empresa es quien maneja la información, quien tiene el conocimiento del negocio, de los clientes y de los procesos.

En las empresas que proveen servicios de seguridad de la información, gran parte del portafolio de servicios es ejecutado por el recurso humano contratado, como es el caso de servicios de consultoría, implementación y soporte, prácticamente estas áreas se convierten en unas de las más importantes fuentes de facturación de este tipo de organizaciones, sin dejar al lado áreas importantes como la parte administrativa, financiera y comercial quienes tienen acceso a información crítica no solo de la empresa si no de los clientes que contratan servicios profesionales con la misma.

Si una organización no cuida el recurso humano, no solamente se expone a que nuevas empresas emergentes con el mismo propósito u objetivo de negocio robe este activo valioso, si no que se expone a riesgos de seguridad como es el caso de fuga de información crítica de la empresa y de sus clientes llegando a ocasionar riesgos como multas, pérdida de credibilidad, pérdida de clientes, baja en ventas entre otras.

Otro ítem importante por lo cual se hace necesario

tener un buen cuidado de este activo, es la reinversión en procesos de capacitación y línea de aprendizaje del recurso humano nuevo, esto cuando se presentan altos índices de rotación de personal dentro de la organización.

II. FUGA DE INFORMACIÓN

La fuga de información es un reto difícil de enfrentar, la confidencial de la información de una organización es expuesta o divulgada a personas no autorizadas causando pérdidas considerables a la misma, según estudios efectuados por Symantec en 2012 [1] y a información provista en la V encuesta de seguridad informática de ACIS e ISACA efectuada en 2014 [2], aproximadamente el entre el 56% al 61% de incidentes de seguridad corresponden a incidentes de fuga de información de las organizaciones.

Cuando se efectúan búsquedas de incidentes relacionados con fuga de información, generalmente muchos de los ejemplos expuestos corresponden a robo de información de empleados inconformes con la organización los cuales utilizan medios como correo electrónico personal, USB, discos duros entre otros, para poder sacar información de la compañía donde laboran y venderla a otras organizaciones, también se encuentra información relacionada con productos o herramientas que ayudan a la organización a protegerse de este tipo de incidentes, como es el caso de los firewall con módulos de DLP, sistemas de filtrado web con protección de fuga de información y Endpoints entre otros, pero ¿Qué pasa o como se controla la información que maneja el personal que labora en empresas que brindan servicios de seguridad de la información precisamente a otras empresas que buscan protección de este tipo de incidentes?.

Algunas regulaciones como la circular 042 de la Superintendencia Financiera y la ley 1581 correspondiente a la protección de datos personales, entre otras, hacen que muchas empresas día a día contraten servicios de empresas dedicadas a temas de seguridad de la información, ya sea para implementar y soportar herramientas que ayudan a la protección de su información del negocio en sí o de sus clientes o para brindar asesorías y/o consultorías que permitan cumplir con las regulaciones y normatividad establecidas por la ley acorde a su objetivo de negocio y su razón económica.

Aunque generalmente se efectúan acuerdos de confidencialidad al iniciar las actividades definidas a nivel contractual, que en caso de incumplimiento llevaría a multas económicas, ¿Cómo se asegura la empresa que contrata el servicio que un funcionario de la empresa contratada no efectué un mal uso de la información proporcionada para la actividad que debe desarrollar? ¿Cómo evitar que el costo del daño en caso de existir una fuga de información, no sea mayor que la multa económica que tendría que pagar el proveedor?

Así como se generan nuevas regulaciones y requerimientos de protección de la información, crecen los requerimientos de servicios de seguridad de la información en el mercado, ocasionando la generación de nuevas empresas prestadoras de este tipo de servicios y por ende la generación de más oportunidades laborales para las personas que trabajan en este medio. Si no se cuenta con procesos adecuados de cuidado del personal por parte de las organizaciones actuales pueden existir riesgos de empleados descontentos los cuales utilicen no solo su conocimiento en seguridad de la información para conseguir empleos más lucrativos o con mejor posicionamiento, sino también la información de la empresa para la cual laboran, como listados de clientes, detalles de diseños, fallas en procesos internos que puedan afectar la reputación de la organización y puedan ser aprovechados por las empresas emergentes para ganar clientes y aumentar sus ventas

Acorde al estudio efectuado por Symantec en el 2012 [1] el 59% de los ex-empleados se llevan información de las compañías, entre la cual se encuentran listados de clientes, contactos, información de empleados actuales e información financiera, el mismo estudio nos indica que el 68% de esos ex-empleados que se llevan información pensaban utilizar los datos robados en el nuevo empleo.

No solamente se puede pensar que el recurso humano de cuidado en una empresa que provee servicios de seguridad de la información

corresponde al área técnica o área de ingeniería, todo el personal es importante, por ejemplo, en una empresa generalmente las personas que manejan información crítica como facturación, contabilidad, manejo de contratos corresponden al área administrativa, al igual que información como listas de precios, estrategias de mercado, clientes claves la maneja generalmente el área comercial de dichas organizaciones, si no se tiene cuidado con este personal y controles adecuados como firmas de acuerdos de confidencialidad en los contratos, puede presentarse incidentes de fuga de información ocasionando graves pérdidas para la organización.

III. PÉRDIDA DE CREDIBILIDAD

La pérdida de credibilidad hacia una empresa no solo se puede presentar por incidentes de fuga de información u otro tipo de incidentes de seguridad, para el caso de las empresas que proveen servicios de seguridad de la información, es esencial contar con recurso idóneo para la prestación de los servicios ofrecidos y pactados a nivel contractual con sus clientes.

Si la empresa no cuenta con el personal idóneo (capacitado y certificado) o si cuenta con el mismo pero no cuenta con una política adecuada de retención y cuidado del personal y este rota constantemente, es inminente que recursos nuevos que posiblemente no cuentan con los conocimientos técnicos suficientes estén al frente de la prestación del servicio, generando posibles riesgos de incidentes de seguridad.

Aunque se piense que esto no es visible ante los clientes, si lo es, generalmente que rote el personal constantemente aumenta los niveles de desconfianza de los clientes hacia la empresa y aumentan el riesgo perdida de los clientes los cuales deciden renovar los servicios con la empresa que contrato al personal que antes le brindaba el servicio.

IV. MEDIDAS DE CONTROL

A. Responsabilidad Contractual

Establecer claramente a nivel contractual la responsabilidad de la empresa y del empleado referente a la seguridad de la información, como lo indica la norma ISO 27001 [3] en el control A.8, en donde se mencionan medidas como la firma de acuerdos de confidencialidad o no divulgación por parte de los empleados, contratistas o terceros que van a tener acceso a información sensible como la información de la organización o sus clientes, previo al acceso a la misma por parte del funcionario o contar con procesos disciplinarios establecidos y divulgados los cuales son aplicables a los funcionarios que cometan violaciones a la seguridad de la información, entre otros.

B. Procesos de Selección Adecuados

Contar con un proceso adecuado de selección de personal donde se efectúen tareas como la verificación de referencias personales y laborales, verificación de estudios realizados, ejecución de estudios de seguridad al personal que aspire a un cargo en la organización y pruebas de polígrafo, este ítem también es recomendado dentro de la norma ISO 27001 [3], hay que recordar que el personal que se contrate no solo va a tener acceso a información de la empresa, también podría tener acceso a información de los clientes con los cuales se tenga acuerdos contractuales. Se debe contar con un proceso de validación de referencias o firmas de acuerdos de responsabilidad para recursos que no estén directamente contratados por la organización, es decir, terceros.

C. Plan de Carrera

Contar con planes de carrera para el personal. En muchas ocasiones las personas no solo buscan el beneficio económico en las empresas donde laboran, también buscan el crecimiento profesional, sobre todo cuando se trabaja en áreas de tecnología.

Contar con un plan de carrera claro donde se especifique los requerimientos a los empleados para subir de cargo o mejorar sus condiciones laborales es fundamental. Es de anotar, que si se cuenta con un plan de carrera ya definido por parte de la empresa, este socializa a los empleados y posteriormente la empresa no cumple con lo pactado, esto puede llegar a generar inconformidades por parte de los empleados, ocasionando pérdida de credibilidad del personal hacia la organización.

D. Estudios de Mercado

Efectuar estudios de mercado permite a las empresas que proveen servicios revisar no solo si el personal está calificado acorde a las necesidades del negocio, si no también validar si las remuneraciones a nivel salarial están acorde a lo ofrecido por el mercado, especialmente en las empresas que son competencia directa. Si las organizaciones no efectúan estudios de mercado constantemente, por lo menos cada seis o doce meses, parte de la rotación del personal posiblemente se dará por la búsqueda de mejores condiciones salariales por parte de los empleados.

V. CONCLUSIONES

Contar con un recurso humano conforme no solo le permite a las organizaciones que proveen servicios de seguridad de la información tener más competitividad en el mercado, bajar costos de entrenamiento, evitar mala reputación por no contar con recursos especializados y evitar incidentes de seguridad como fuga de información.

Por los requerimientos actuales del mercado de la seguridad de la información, se debe contar con medidas de cuidado de personal adecuadas que permitan a las empresas que proveen servicios de seguridad de la información ofrecer a sus clientes la seguridad referente al cuidado de la información que ellos suministran para la prestación del servicio ofrecido.

REFERENCIAS

[1] Fuga de Información un Negocio en Crecimiento, Symantec, 2012
[2] V Encuesta de Seguridad Informática, ACIS, ISACA, 2014
[3] Norma ISO 27001 Sistemas de Gestión de la Seguridad de la Información.

Autor
Diana Patricia Suarez Lopez
Ingeniera de Sistemas Universidad INCCA de Colombia
Experiencia en implementación y soporte de plataformas de seguridad informática como firewalls, herramientas de filtrado web y de correo, herramientas de administración de privilegios de usuarios entre otras.