LINK SERVICES

En particular la empresa Link Services definió un Sistema de Gestión de Seguridad de la Información, conforme a la ISO 27001:2005 contrató a LS Consultores para que le hiciera una auditoría del SGSI dado que está pensando en obtener la certificación por parte del ente autorizado en Colombia, para tres procesos descritos.

En principio Link Services definió la política del SGSI, los objetivos y los planes de gestión correspondientes, la alta dirección fue muy diligente en la elaboración del documento y en su publicación, para que dicho SGSI fuese de conocimiento amplio de las personas claves de la compañía. En particular Link decidió que un Ingeniero del área comercial se hiciere cargo de asegurar el cumplimiento de los procesos. El Ingeniero Díaz ha desarrollado toda su carrera en el área comercial, vendiendo equipos de seguridad y los conoce muy bien. Adicional a ello es certificado como Auditor Interno ISO 9001:2008 y cuenta con otras certificaciones entre ellas PMI que según la alta dirección lo avalan para ejercer esta función.

El Ingeniero Díaz dentro de la gestión de seguridad, ha realizado un análisis muy importante que permite brindar una valoración de la seguridad y que se garantice la financiación adecuada para entregar los equipos a los diversos clientes. En dicho análisis ha realizado tareas tales como planear la seguridad, planear la gestión de incidentes ha tomado cursos para actualizarse sobre legislación y normatividad y planear su cumplimiento.

Así mismo el Ingeniero Díaz, cuenta con un equipo de personas quienes son considerados los dueños de los procesos de seguridad y cuentan con la debida educación, formación y capacitación de acuerdo a los perfiles establecidos para los cargos que ostentan al interior de BS. El Ing. Ruiz, encargado de la seguridad de los Datacenter, El Ing. Navarro, encargado de la seguridad de los servidores y la Ing. Prada

que se encarga de la seguridad de las redes. Todos son Ingenieros de Sistemas certificados CISA y CISSP, la Dra. Prada cuenta con un certificado PMI, el cual le ha servido para planear el proyecto de Seguridad en Comercio Electrónico. Los auditores de LS Consultores decidieron revisar los registros asociados a estas personas y, teniendo en cuenta que en su documentación todos deben tener tarjeta profesional, encontró que en la carpeta del Ingeniero Ruiz no está una copia de

dicho documento, sin embargo se encontró una notificación en un correo electrónico donde el ingeniero comenta que su documento está en trámite. No obstante dicho e-mail tiene fecha de hace más de 7 meses de vigencia.

En particular el Ing. Díaz entrega informes a la alta dirección sobre la gestión de seguridad, deja claramente registro de todas las situaciones y contingencias asociadas a la seguridad que se pueden presentar y cada uno de los ingenieros mencionados firma como Vo. Bo. cada reporte.

El personal de LS Consultores, decidió indagar por el proceso la administración de seguridad de los servidores en particular y se encontró con que no ha habido mayores situaciones, pues el trabajo al parecer ha sido muy sencillo. Hay que resaltar que en los últimos seis meses han cambiado servidores y por ende su capacidad, además han tenido una serie de inconvenientes y problemas de espacio en disco. Así mismo los informes de capacidad y rendimiento han llegado incompletos y en algunos casos no reflejan como se ha mantenido la operación de los servidores y por ende la prestación de los servicios al interior de la compañía.

Así mismo los auditores de LS encontraron que la compañía Link está implementando un SGCN (Sistema de Gestión de Continuidad de Negocios) y ya realizó el análisis de impacto en el negocio pero al revisar la relación costo/beneficio, decidieron cambiarle un poco el alcance al plan y por ende han entrado en un retraso importante en el proyecto inicialmente planeado. Actualmente la compañía no cuenta con un plan que asegure la continuidad de la prestación de los servicios de tecnología, especialmente los relacionados con Datacenter, sin embargo firmó un contrato a dos años con otra compañía que cuenta con un Datacenter TIER IV, pero el análisis dio para que se mantuviese como un “Middle Site”, es decir que se deban tomar acciones de configuración y conexión, en otras palabras no hay alta disponibilidad. Hasta el momento no ha sido necesario utilizar el Site.

Por último LS Consultores preguntó por la lista de proveedores de Link y pudo establecer que la lista existe, se encuentra documentada, registrada, autorizada y publicada. Al indagar se pudo establecer también que el proveedor del Site Alterno ya se encuentra incluido en la lista pero no se encontró el nombre del contacto o a quién recurrir en caso de una situación contingente, ni tampoco un

registro que confirme que estos proveedores se comprometen con el cumplimiento de la política de seguridad de Link Services.

Finaliza la revisión y se procederá a emitir un informe de la auditoría por parte de LS Consultores.

En el anterior caso, no imagine, no asuma, ni especule nada, solamente aténgase a lo que el caso propone, no hay más información y es con base en ella que usted debe trabajar, para tal efecto, establezca lo siguiente:

1. ¿Qué numerales de la norma ISO27001 se ven reflejados como “no cumplimiento” en este caso?
2. Teniendo en cuenta lo aprendido sobre seguridad de la información y COBIT, como podrían solucionarse dichas falencias?