Ciencias de los Sistemas de Información y Seguridad

Handbook T-I

Solares-Soto, Pedro F.

Director

ECORFAN®

Volumen I

Para futuros volúmenes:
http://www.ecorfan.org/handbooks

ECORFAN Ciencias de los Sistemas de Información y Seguridad

El Handbook ofrecerá los volúmenes de contribuciones seleccionadas de investigadores que contribuyan a la actividad de difusión científica de ECORFAN en su área de investigación en Ciencias de los Sistemas de Información y Seguridad. Además de tener una evaluación total, en las manos de los editores de la Universidad Iberoamericana que colaboraron con calidad y puntualidad en sus capítulos, cada contribución individual fue arbitrada a estándares internacionales (RENIECYT-LATINDEX-DIALNET-ResearchGate-DULCINEA-CLASE- Sudoc- HISPANA-SHERPA-UNIVERSIA-eREVISTAS-ScholarGoogle-DOI-REBID-Mendeley), el Handbook propone así a la comunidad académica, los informes recientes sobre los nuevos progresos en las áreas más interesantes y prometedoras de investigación en Ciencias de los Sistemas de Información y Seguridad.

Solares-Soto, Pedro F.

Editor

Ciencias de los Sistemas de Información y Seguridad

Universidad Iberoamericana. Diciembre, 2016.

ECORFAN®

Editor

Solares-Soto, Pedro F.

Universidad Iberoamericana

ISBN-978-607-8324-85-9
Sello Editorial ECORFAN: 607-8324
Número de Control HCSIS: 2016-01
Clasificación HCSIS (2016): 091216-0101

Prefacio

Actualmente las Tecnologías de la Información (TI) están disponibles para casi todos. En las últimas décadas su impacto se ha extendido ampliamente en todos los campos de las actividades humanas. Los investigadores han recurrido a las TI como una forma de cumplir necesidades de una sociedad moderna, y esto ha creado una gran expectación en una amplia gama de actores que van desde las empresas a los institutos de educación superior. En aras de contribuir con estas necesidades esta obra presenta diversos trabajos referentes al desarrollo de un sistema de información para pequeñas empresas del sector salud, emprendimiento para empresas de TI, administración de servicios de TI y aspectos de seguridad de TI, todos ellos desarrollados por alumnos y profesores tanto de la Universidad Iberoamericana como de la Unidad Profesional Interdisciplinaria de Ingeniería Ciencias Sociales y Administrativas del Instituto Politécnico Nacional.

Sin lugar a dudas, la divulgación de la innovación y la investigación en tecnologías de la información traerán incontables beneficios que contribuirán a la creación de estrategias para una mejor calidad de vida en la sociedad donde la tecnología es la llave para abrir la puerta al futuro.

Olvera, Gordillo, Acosta presentan Propuesta de un sistema integral de gestión de citas y facturación electrónica para pymes del sector salud en México, *Galván* presenta Gestión de riesgos de seguridad en ACME, *Medellín* presenta Una perspectiva de Silicon Valley-La Ciudad Tecnológica, *Velázquez* presenta La gestión de servicios de TI orientada al cliente, *González* presenta El valor de contar con buen service desk, *Ramos* presenta El bienestar laboral y la felicidad como factores para la productividad y retención de los colaboradores de tecnologías de información en las organizaciones, *Cárdenas, Solares* presenta SGSI en las sociedades de información crediticia.

Quisiéramos agradecer a los revisores anónimos por sus informes y muchos otros que contribuyeron enormemente para la publicación en éstos procedimientos repasando los manuscritos que fueron sometidos. Finalmente, deseamos expresar nuestra gratitud a la Universidad Iberoamericana en el proceso de preparar esta edición del volumen.

Solares-Soto, Pedro F.

Ciudad de México. Diciembre, 2016.

Contenido Pág.

Propuesta de un sistema integral de gestión de citas y facturación electrónica para pymes del sector salud en México

OLVERA, Gabriela, GORDILLO, Abraham, ACOSTA, Elizabeth

G.Olvera, E.Acosta, A.Gordillo

Unidad Profesional Interdisciplinaria de Ingeniería Ciencias Sociales y Administrativas - Instituto Politécnico Nacional

P. Solares (eds.) Ciencias de los Sistemas de Información y Seguridad. Handbook T-I. -©ECORFAN, Ciudad de México, 2016.

Abstract

Nowadays Small and Medium-sized Enterprises (SMEs) of the health sector in Mexico (medical clinic, rehabilitation clinics, veterinary clinics) face several problems of internal control. One of them is that they do not have an information system for managing the patient's agenda which is an important process since it is the beginning of contact with customers. In addition, other important process and obligation that SMEs face is to generate and send electronic invoices.

To help solve these situations, it is proposed the implementation of a comprehensive information system that has the integrated features: appointments' management and control, sending Short Message Service (SMS) to patients to confirm appointments and the generation and sending of electronic invoices. Thus, the proposal of this information system allows integrating appointments' control and management processes with electronic billing. Results show that the medical clinic can reduce appointment' management cost as well as electronic billing. The information system helps to simplify the tasks of remembering and confirming appointments by sending timely notifications either by e-mail or by SMS, thus allows reducing the time of sending electronic invoices to the patient, all these contribute to medical clinics provide better patient care.

1 Introducción

Hoy en día, las Pequeñas y Medianas Empresas (PyME) del sector salud de México, tales como consultorios y torres médicas, clínicas de rehabilitación, clínicas veterinarias, entre otras, se enfrentan a diversos problemas de control interno, los cuales están relacionados con el servicio que dan a sus clientes, uno de ellos es que no cuentan con una herramienta informática para la gestión de la agenda de pacientes, el cual es un importante proceso de negocio ya que es el inicio del contacto con los clientes.

En muchas de estas PyME, esta actividad se realizan de manera manual, es decir, que el área de recepción para pacientes, administra y controla la agenda de citas de manera tradicional, utilizando la mayoría de las veces una libreta para el registro correspondiente, sin embargo, esta forma no proporciona de manera integral todo el servicio que un cliente necesita, y que el negocio debe proporcionar, ya que no se saben datos finos, tales como quienes son los pacientes más frecuentes, que días son los que normalmente tienen consulta, si estas son por la mañana o por la tarde, que medico les atiende, cuanto facturan estos pacientes, etc., es por ello que se justifica el contar con un sistema que automatice estas actividades que de manera tradicional sería muy difícil obtener.

Además, otra importante obligación que las PyME del sector salud requieren cumplir, es generar y enviar facturas electrónicas también conocidas como Comprobante Fiscal Digital por Internet (CFDI), esto es un requerimiento de Ley que en México existe por disposición oficial por parte del Sistema de Administración Tributaria (SAT) a partir del 1º de abril de 2014 en donde se declaró que el único esquema válido de comprobación fiscal es la factura electrónica (CFDI), (Servicio de Administración Tributaria, 2014).

Y es que actualmente estas actividades se realizan totalmente independientes, es decir, mientras que las recepcionistas controlan lo relacionado con la agenda de pacientes y citas, el área administrativa controla lo relacionado con la facturación provocando con ello que no se cuente con información integrada que comparta los datos de los pacientes y citas con los ingresos derivados de estos, lo único que se tiene es una simple combinación de informes. Y en clínicas y consultorios donde existe una demanda grande de operaciones resulta complicado su gestión y control.

Para ayudar a resolver esta situación se propone el diseño e implementación de un sistema de información integral que cuente con las siguientes características integradas: gestión y control de citas, envío de notificaciones, mediante mensajes cortos a sus aparatos móviles, SMS (por sus siglas en inglés), para confirmar citas y como recordatorio para el paciente, y la generación y envío de facturas electrónicas (CFDI). Así, la propuesta de este sistema de información permite integrar los procesos de control y gestión de citas y de facturación electrónica, lo que puede ayudar a reducir costos de servicio de telefonía para gestión de citas así como de facturación electrónica, asimismo, el sistema ayuda a simplificar las tareas de recordar y confirmar las citas mediante notificaciones oportunas ya sea por correo electrónico o bien mediante el Servicio de Mensajes Cortos (SMS) para teléfonos móviles y así permite disminuir el tiempo de envío de CFDI al paciente, todo ello contribuye a que las consultorios y clínicas médicas otorguen una mejor atención al paciente.

El hecho de contar con un sistema de información que automatice estas actividades trae grandes beneficios a la empresa, por ejemplo, se pueden generar reportes de facturación por período, de clientes atendidos, de citas por período, etc.

Como parte de este trabajo se realizó un estudio de pertinencia a través de una investigación documental tanto en revistas especializadas como en Internet para encontrar la oferta de sistemas de información o aplicativos orientados al sector salud que ayudara a resolver las problemáticas descritas anteriormente (control de citas, envió de SMS y facturación electrónica) de manera integral.

Los resultados no identificaron alguna aplicación de software para el sector médico que contara en su totalidad con las características buscadas, ya fueran sistemas de esquemas de licenciamiento (de pago) o de software libre (gratuito), (ver Tabla 1). Actualmente existen aplicativos que ofrecen servicios para el control de citas, desde aquellos gratuitos que ofrecen únicamente un manejo de citas, hasta aquellos con licencias que además de la gestión de las citas, ofrecen una gran variedad de servicios dirigidos al manejo del expediente e historia clínica de los pacientes.

Tabla 1 Sistemas para el control de citas para el sector salud

Características	citas	vía SMS	Electrónica	con Costo
SAAM	✓	X	x	✓
Medikal Manik	✓	X	x	✓
iiMed	✓	X	x	✓
Neomedic-2012	✓	X	x	✓
Medby	✓	X	x	✓
Consultorio Virtual	✓	X	x	✓
Control de Pacientes	✓	X	x	X
Patient Manager	✓	X	x	✓
MyConsulta	✓	✓	x	✓
QCinicas	✓	✓	x	✓
Doctordoctor	✓	✓	x	✓
SML	✓	✓	x	✓
MedicalApp	✓	X	✓	✓
Jagarmedical	✓	X	✓	✓
Contactarme	✓	✓	x	✓

Facturación electrónica

Una de las obligaciones de los prestadores de servicio, es que proporcionen a sus clientes facturas electrónicas, cuando le son requeridas, muchos de estos negocios, prefieren no realizar este trabajo, y pagan este servicio transfiriéndolo a terceros, estos, son normalmente despachos de contadores, que piden al área de recepción de los negocios que registren los datos de los clientes, y se los envían normalmente al final del mes en curso, por algún medio, y a su vez ellos, realizarán el trabajo ante el SAT, para enviar finalmente la factura electrónica a los clientes.

Bajo el esquema anterior la administración de los consultorios o de los médicos pierden control sobre los datos y la explotación de los mismo, solo se conforman con que les manejen el aspecto fiscal.

Estos negocios tienen otras posibilidades de trabajo, las cuales se analizan a continuación:

a. utilizar la aplicación gratuita del SAT.

b. utilizar la aplicación gratuita de algún proveedor.

En cuanto al servicio ofrecido por el SAT (Sistema de Administración Tributaria, 2014) éste permite capturar y certificar un comprobante a la vez y entre las funcionalidades y características con las que cuenta están:

- Compatible con diversas plataformas y navegadores
- Contempla todo el ciclo de generación de una factura electrónica (captura, sellado y certificación digital)
- El proceso de certificación del SAT a la factura electrónica es en línea.
- Permite capturar los requisitos de las facturas electrónicas de acuerdo con lo que establecen las disposiciones fiscales, así como la integración de “leyendas fiscales” y del Comprobante Electrónico de Pago (CEP), vinculado con el Sistema de Pago Electrónico Interbancario (SPEI).
- Genera el comprobante en su formato electrónico (XML) y la representación impresa.
- Permite consultar y recuperar las facturas electrónicas (CFDI).
- Almacena comprobantes en captura hasta por 72 horas.

Sin embargo el servicio no administra catálogos de clientes o productos, ni integra addendas comerciales, por lo que debido al volumen de operaciones de algunos contribuyentes o quienes requieran la incorporación de complementos adicionales o addendas, deberán utilizar los servicios prestados por los Proveedores Autorizados de Certificación (PAC) para la certificación de sus comprobantes, éstas empresas tienen como obligación enviar al SAT copia de los CFDI que validen de sus clientes y para lo cual el SAT tiene un listado de proveedores autorizados disponibles en su página de Internet (Reyes, 2013). Asimismo, se deben conservar en archivo digital cinco años las facturas emitidas en cada ejercicio (Castro, Colín y Luna, 2014). El servicio tampoco realiza cálculos de impuestos ni certifica facturas electrónicas (CFDI) generadas por otros sistemas.

Respecto a la opción gratuita de algunos proveedores, estás ofrecen lo mismo que la opción gratuita del SAT, por lo que tampoco se pueden integrar con un sistema del cliente.

Para realizar una factura electrónica es necesario 1. Contar con un Certificado de Sello Digital (CSD), 2. Generar el CFDI en un archivo *.XML, 3. Sellar el CFDI, 4. Timbrar el CFDI.

El Certificado de Sello Digital (CSD) es provisto por el SAT y que está compuesto por una llave privada, en forma de archivo con extensión .key, el cual está protegido con contraseña y una llave pública, en un archivo con extensión .cer. Cabe mencionar que este archivo se obtiene a través de la aplicación gratuita del SAT llamada SOLCEDI.

Para generar el CFDI en un archivo XML. Cabe señalar que el archivo XML que se tiene que generar deberá cumplir con las especificaciones definidas dentro del Anexo 20 de la Resolución Miscelánea Fiscal del 2010 publicado por el SAT, el cual especifica: la estructura que deber tener el CFDI, la forma de generación del sello digital y el uso del complemento obligatorio: Timbre Fiscal Digital.

Para realizar el XML siguiendo la estructura definida, se obtiene el esquema XML definido por el SAT, el cual se encuentra disponible en la dirección: http://www.sat.gob.mx/sitio_internet/cfd/3/cfdv3.xsd. A partir de este esquema se crea el archivo XML.

El siguiente paso es generar el sello digital con lo cual se garantiza la integridad y autenticidad del mismo. Para ello se requiere de 1. Generar la cadena original del comprobante, 2. Obtener la llave privada, 3. Sellar la cadena original, 4. Agregar sello al comprobante. Cabe señalar que para el paso 1 el SAT público un XSLT que genera la cadena original de la forma que se encuentra especificada dentro del Anexo 20, para lo cual se requiere de aplicar una transformación XSLT al archivo XML que se generó anteriormente.

Hasta este momento, se tiene un comprobante creado y firmado como se indica en el Anexo 20 del SAT, pero todavía no es válido ya que no contiene un timbre fiscal digital. Entonces, se requiere de enviar el archivo XML generado a una empresa PAC, para que esta lo verifique y genere el Timbre Fiscal Digital (TFD), el cual se debe incluir dentro del archivo XML.

Todos los PAC implementan un servicio web estándar que definió el SAT y que realiza lo siguiente: 1. Recibe el comprobante firmado, 2. Valida el comprobante y 3. Genera el timbre fiscal digital.

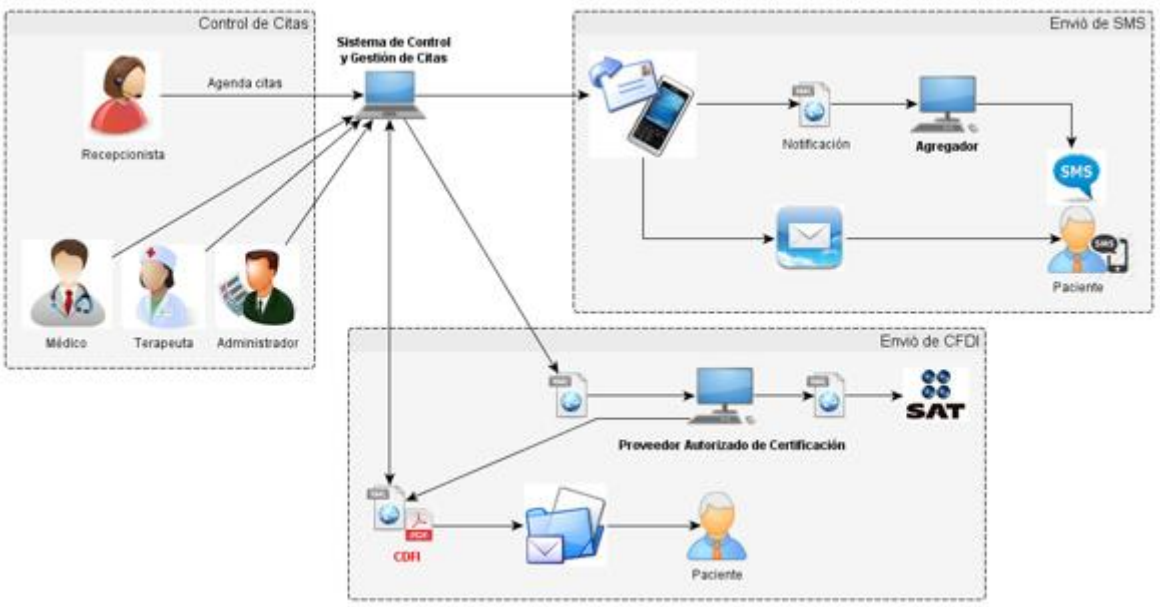
1.1 Propuesta de solución

Las Pymes del sector salud cuentan con el siguiente personal, uno o varios médicos que atiende la consulta, terapeutas de rehabilitación, recepcionistas, contador encargado de los procesos administrativos.

El proceso de negocio actual, funciona de la siguiente manera, los pacientes se comunican vía telefónica al consultorio o clínica médica para agendar una cita. Las recepcionistas atienden las llamadas y agendan las citas en una libreta. Las recepcionistas confirman las citas vía telefónica. El paciente llega a su cita, es atendido y paga su consulta y/o terapia. Las recepcionistas solicitan al contador la generación y envío de las facturas electrónicas.

De acuerdo al proceso descrito anteriormente, se propone la arquitectura del sistema de información integral de Control y Gestión de Citas (SICGC), que permita el envío de notificaciones vía SMS, así como el envío de facturas electrónicas (CFDI). Ver Figura 1.

Figura 1 Sistema para el Control y Gestión de Citas Basado en SMS



Con la propuesta del SICGC, podemos ver, tres grandes subsistemas o procesos, los cuales si son valorados por la administración de los consultorios, es posible que si en sus objetivos, existe alguno de crecimiento y desarrollo del negocio, se puedan alinear, de tal forma, que logren alcanzar ventaja competitiva.

La nueva conceptualización incluyendo tecnologías de la información (TI) al negocio, conceptualizado en la figura 1, ahora puede leerse de la siguiente manera: los pacientes se comunican vía telefónica al consultorio o clínica para agendar una cita. Las recepcionistas atienden las llamadas y agendan las citas en el sistema. El sistema envía notificaciones para recordar y confirmar las citas. El paciente llega a su cita, es atendido y paga su consulta y/o terapia. El sistema genera y envía las facturas electrónicas.

El SICGC, al desglosarse en procesos, estaría siendo conceptualizado cada uno de ellos de la siguiente manera:

Proceso de agendar citas

Para agendar una cita en el sistema de información propuesto, el paciente realiza una cita, comunicándose vía telefónica con la recepcionista, con la implementación del sistema, entonces, tanto el personal médico como el área administrativa podrán tener acceso a la información de la agenda de manera inmediata para un mejor control y seguimiento de los pacientes y citas como se muestra en la Figura 1.1.

Figura 1.1 Agenda

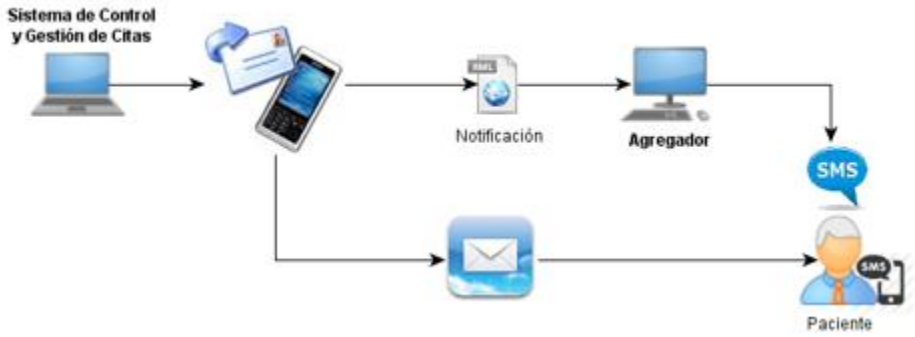
Proceso de envío de notificaciones SMS

La estrategia de envió de notificaciones vía SMS se pueden realizar mediante la contratación de los servicios de empresas conocidas como agregadores, las cuales se dedican al envío masivo de mensajes SMS, se puede contratar desde varios cientos hasta millones de mensajes, que funcionan con una sola compañía o bien que los pueden enviar a diferentes compañías y en un gran rango de precios que va desde los $0.50 centavos por mensaje y hasta $1 peso, dependiendo básicamente del volumen contratado y de los servicios incluidos entre los cuales casi todos ofrecen un API, (Application Program Interface, conjunto de rutinas, protocolos, y herramientas para construir aplicaciones de software) para integración con sistemas propios.

El envío de notificaciones vía SMS como recordatorio de citas es de gran utilidad, en México, por ejemplo, el ISSSTE utiliza un sistema de notificación para recordar a sus derechohabientes respecto de sus citas médicas ya sea vía SMS o correo electrónico. Este servicio también ha funcionado en los centros médicos del Seguro Social en Costa Rica, donde se usan los mensajes de texto para recordar a los pacientes de su cita, lo cual permitió a las unidades médicas que aplican este sistema reducir el ausentismo en un 25% (Diario La Nación, 2013).

Para el envío de las notificaciones vía mensajes de texto SMS el sistema integra una interfaz que permite la comunicación con la empresa agregador, de manera que sean enviadas los mensajes SMS como se muestra en la Figura 1.2.

Figura 1.2 Envío de notificaciones vía mensajes SMS al teléfono móvil del paciente



Como la Figura 1.3 muestra, el SICGC envía notificaciones por correo electrónico y mensajes SMS. El sistema genera un archivo en formato *.xml con el texto de la notificación, y se envía por Internet al agregador. La empresa agregador se encarga de enviar la notificación al paciente mediante un mensaje SMS. Por su parte el sistema envía la notificación mediante correo electrónico al paciente.

Proceso para la generación y envío de factura electrónica (CFDI)

En cuanto a la generación y envió de factura electrónica el sistema también contará con una interfaz que permita la comunicación con el PAC que ya se tenga contratado para la generación de CFDI, de manera que este genera la factura y el sistema posteriormente la envié vía correo electrónico al paciente.

Figura 1.3 Envío de la factura electrónica (CFDI)

El Sistema de gestión y control de citas genera el archivo en formato *.xml y se envía por Internet al PAC. El PAC se encarga de validar, asignar folio, incorporar sello del SAT y enviar una copia del comprobante fiscal al SAT una vez certificado. El PAC, regresa el archivo *.xml al sistema, con todos los elementos que lo acreditan como CFDI. El sistema recibe la factura y la envía por correo al paciente.

1.2 Arquitectura del sistema

(Programacion.net) La arquitectura que se propone para diseñar y construir el Sistema de Gestión y Control de Citas es una arquitectura multicapa no distribuida, la cual dividirá el sistema en distintas unidades funcionales: cliente, presentación, lógica de negocio, integración, y Sistema de Información Empresarial (EIS), con lo que se asegura una división clara de responsabilidades y hace que el sistema sea fácilmente mantenible y extensible.

La capa del cliente es donde se consumen y presentan los modelos de datos. Para una aplicación Web, la capa cliente normalmente es un navegador Web, y para el sistema propuesto también podrán ser dispositivos móviles, para consultar la agenda, exclusivamente.

La capa de presentación es la que expone los servicios de la capa de lógica de negocio a los usuarios, procesa las peticiones de los clientes, interactúa con la capa de lógica de negocio, y selecciona la siguiente vista a mostrar.

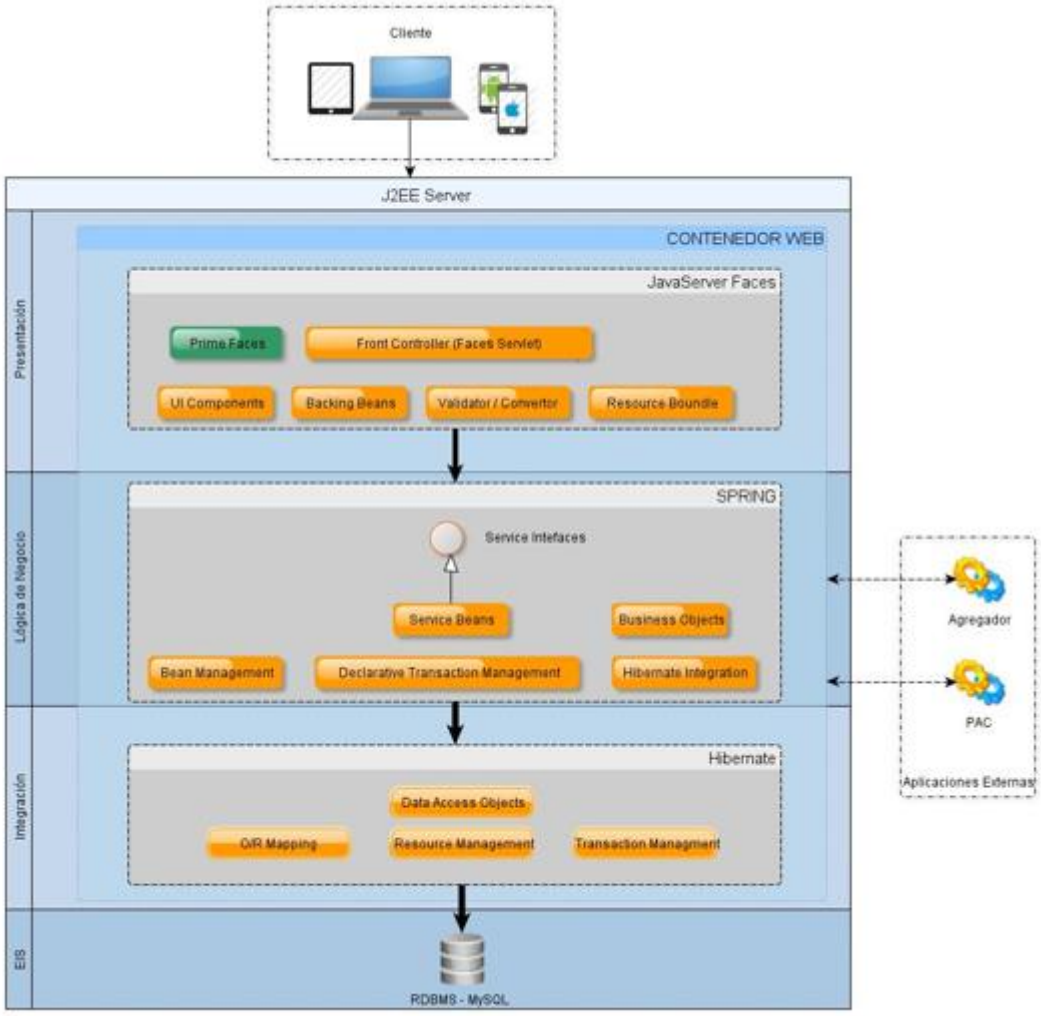
La capa de la lógica de negocio contiene los objetos y servicios de negocio de la aplicación. Recibe las peticiones de la capa de presentación, procesa la lógica de negocio basada en dichas peticiones, y media en los accesos a los recursos de la capa EIS.

Los componentes de la capa de lógica de negocio se benefician de la mayoría de los servicios a nivel de sistema como el control de seguridad, de transacciones y de recursos.

La capa de integración es el puente de comunicación entre la capa de lógica de negocio y la capa EIS. Es decir, encapsula la lógica para interactuar con la capa EIS.

Los datos de la aplicación persisten en la capa EIS, la cual puede contener bases de datos relacionales, bases de datos orientadas a objetos, o sistemas legados. En la Figura 1.4 se observa la distribución de cada capa.

Figura 1.4 Arquitectura del sistema de información integral



Como se observa en Figura 5, la arquitectura del sistema se despliega en capas, mismas que muestran las tecnologías elegidas para cada capa. Para el sistema de información propuesto la capa de presentación, de lógica de negocio y de integración, están ubicadas físicamente en el mismo contenedor Web.

Propuesta técnica

El sistema es un aplicativo Web desarrollado en Java 1.6 debido a que esto permitirá tener acceso desde cualquier punto en el Internet, además de las siguientes razones:

- El manejador de base de datos es MySQL

- La mayoría de los Agregadores y Pac’s cuenta con infraestructura compatible con Java.
- Es orientado a objetos, lo que permite la reutilización y simplificación del código.
- Es multiplaforma, lo que permite que el desarrollo no sea solo para Windows.
- Es gratuito.
- Tiene una gran cantidad de librerías disponibles, como por ejemplo para envió y recepción de SMS o correo electrónico.
- Se puede reutilizar para plataforma Android.

Pantallas principales del sistema

Se presentan las pantallas iniciales del sistema, las cuales permiten el acceso al mismo y contemplar el contenido integral de módulos que maneja, como una muestra de la sencillez con que se diseñó y que cualquier PyME del ramo puede utilizar si así desea hacerlo.

La Figura 1.5, muestra la pantalla de bienvenida al usuario y permite realizar la autenticación dentro del sistema, así como la recuperación de contraseña en caso de ser necesario. Es importante destacar que una correcta autenticación, además de proporcionar un nivel básico de seguridad, no permite el acceso a personal no autorizado, también nos brinda en conjunto con la bitácora del sistema, la posibilidad en caso de ser necesario de identificar unívocamente todas aquellas acciones realizadas por cada usuario.

Figura 1.5 Pantalla de bienvenida y acceso al sistema

La Figura 1.7 presenta el acceso a la pantalla principal de trabajo del área de recepción dentro de esta pantalla se llevan a cabo las principales funciones del sistema:

- Gestión de la Agenda
- Generación y Envió de Factura Electrónica
- Envió de notificaciones

En esta pantalla se pueden llevar a cabo también las acciones de crear, modificar o cancelar citas, sin embargo a diferencia de una gestión manual de la misma, está agenda tiene la ventaja de permitir:

- Visualización de la Agenda en 3 niveles: Día, Semana o Mes.
- Visualización y manejo de la Agenda de manera simultánea. (la Agenda se encuentra dentro de una aplicación WEB)
- Gestión de tantas Agendas como se requieran (por médico, por consultorio etc.)
- Envío automático de notificaciones (las notificaciones se envían 24 horas antes de la programación de la cita)
- Generación y envió automático de facturas electrónicas. (La factura se genera toda vez que la consulta ha concluido y ha sido pagada)

Figura 1.6 Pantalla principal para el perfil de recepcionista

Cada una de las opciones de esta pantalla genera sus propios archivos, de acuerdo a un diseño de bases de datos, a partir de los cuales es posible generar los reportes que los médicos o administradores requieran para su control interno y su toma de decisiones.

1.3 Resultados

Las pruebas que se han realizado con este sistema, con una clínica, en la Ciudad de México, ha dado resultados satisfactorios entre los que se pueden mencionar, de manera inicial, son:

- Agilización en los procesos de gestión de citas, gracias a la visualización simultánea de la Agenda en los distintos consultorios. Anteriormente cuando el paciente requería una cita, debía llamar al consultorio específico para agendar una cita, ahora puede llamar a cualquier consultorio.

- Agilización del proceso de facturación pues ya no es necesario que cada vez que el paciente requiere una factura, llene a mano un formato con sus datos fiscales.

- Generación de reportes, especialmente en correspondiente al de Terapias, pues ya no se tiene que generar manualmente dicho reporte todos los viernes, la importancia de este reporte radica en que a partir de él se calcula el pago de los Terapeutas pues va relacionado con la cantidad de terapias realizadas en la semana.

1.4 Conclusiones

En el contexto de las Pymes de cualquier sector, incluyendo aquellas del sector salud, uno de sus procesos de negocio que es vital para su crecimiento y fortalecimiento, es la administración de la agenda, la cual incluye, la confirmación y recordatorio de citas, la solicitud y envió de facturas electrónicas (CFDI) y la generación de reportes; sin embargo, es muy común que éstas actividades se realicen de manera manual e independiente, provocando con ello que no se cuente con información integrada que beneficie a la administración del negocio.

Con la implementación del sistema de información se logra que se agilicen los procesos cruciales, beneficiando en muchos sentidos a la atención de los clientes, los cuales constituyen el principal ingreso en negocios de este tipo.

Los consultorios médicos ofrecerán a los clientes un servicio, ágil y eficiente, tanto para sacar sus citas o reprogramarlas, y mandarles recordatorios a sus dispositivos móviles, además que de manera automática, en cuanto el paciente pague se le enviará inmediatamente su factura a su correo personal, esto sin duda redundará en elevar la calidad, la productividad y la competitividad de los negocios.

Sin lugar a dudas, el factor económico es decisivo al momento de elegir la opción más rentable de un sistema integral. Se puede señalar que la elección de una propuesta como la descrita en este documento es por mucho un beneficio para las PyME, ya que no tienen que invertir grandes cantidades de dinero en tecnología, lo que puede resultar muy atractivo ya que en algunos meses pueden recuperar la inversión.

Respecto a la tecnología usada para el diseño y desarrollo del sistema, se puede mencionar que aunque las TI se encuentran en constante avance, los servicios Web continúan siendo la opción más usada para acoplar sistemas e integrar funcionalidades tales como la factura electrónica, lo que garantiza que la aplicación puede ser utilizada en cualquier plataforma de software que se tenga.

El sistema desarrollado queda a nivel de prototipo, en la Sección de Estudios de Posgrado de la UPIICSA del Instituto Politécnico Nacional, en los correos de los autores para pruebas y desarrollos más amplios, incluye también la documentación necesaria para analizar su diseño y desarrollo.

1.5 Referencias

Castro Cruz Georgina, Colín Azahar Noemí, Luna Carbajal Armando (2014). México en la nueva tendencia de la facturación electrónica. Revista Académica de Economía No. 199. ISSN 1696-8352.

Observatorio de la Economía Latinoamericana. www.eumed.net.

Consultorio Virtual. (2014). Consultorio Virtual. Recuperado el 8 de Octubre de 2014, de http://www.consultorio-virtual.com/

Control de Pacientes. (2014). Control de Pacientes. Recuperado el 8 de Octubre de 2014, de http://controldepacientes.com/

Datateam Consulting, S.A. de C.V. (2014). Medikal Manik. Recuperado el 7 de Octubre de 2014, de http://medicalmanik.com/

Diario La Nación. (2013). Recuperado el 7 de Noviembre de 2014, de http://www.nacion.com/

Reyes Ramos, O. (2013). Nuevas Tendencias en el Negocio Electrónico. México: Palibrio

Programacion.net. (2016). Recuperado el 15 de 02 de 2016, de http://programacion.net/articulo/integracion_de_jsf_spring_e_hibernate_para_crear_una_aplicacion_web_del_mundo_real_307/3

Servicio de Administración Tributaria (2014). Recuperado el 10 de Octubre de 2015, de http://www.sat.gob.mx

Gestión de riesgos de seguridad en ACME

GALVÁN, Gabriela

G. Galván

Universidad Iberoamericana

P. Solares (eds.) Ciencias de los Sistemas de Información y Seguridad. Handbook T-I. -©ECORFAN, Ciudad de México, 2016.

Abstract

ACME, is a Mexican Company dedicated to marketing high value solutions based on technology information services, with market knowledge for more than 15 years of experience. It has ISO9001 certification, for the delivery of IT services and solutions in the Mexican market. The objective of the present work is to know the level of risk to which the organization is exposed by information security risks for the delivery of Managed Services and based on the analysis determine the necessary controls to mitigate the risk to which the organization is exposed to ensure the value of the company and the projected growth for this group of services based on ISO / IEC 27005 (Information security risk management).

2 Introducción

El uso de las tecnologías de la información (TI) se ha intensificado en las organizaciones independiente de la naturaleza y actividad de las mismas, estás se encuentran en constante evolución adaptándose a las nuevas necesidades de las organizaciones y así mismo dando lugar a otras relacionadas con su operación diaria. Adicionalmente su masificación las han convertido en blanco de ataques; los riesgos asociados a estas se intensifican y transforman y por ello se hace necesario crear y adaptar constantemente los medios y métodos utilizados para conservar la seguridad de la información que las organizaciones quieren proteger.

Derivado del crecimiento en el ofrecimiento de Servicios Administrados en el mercado de Mexicano, ACME identifica la necesidad de fortalecer la tecnología, procesos, procedimientos y el recurso humano especializado de TI para la entrega de este grupo de servicios. La estrategia de la organización es iniciar con una evaluación para conocer el nivel de riesgos de seguridad al que está expuesta para poder determinar los controles necesarios que permitan mitigar el riesgo y de esta forma asegurar el valor de la empresa y el crecimiento proyectado para el grupo de Servicios Administrados con base en ISO/IEC 27005 (Information security risk management).

El resultado del presente trabajo mostrará las áreas de oportunidad para una mejor gestión de riesgos de seguridad en la organización que permita que la entrega de Servicios Administrados cumpla con los estándares de calidad necesarios para asegurar el crecimiento del 20% en el próximo año que permita que la empresa fortalezca su posición en el mercado mexicano.

2.1 Metodología

Alineación ISO27005 con modelo PHVA

La metodología para el presente análisis se alinea con el modelo PHVA con la finalidad de establecer un proceso de gestión que se enfoque en la mejora continua siguiendo el esquema presentado a continuación:

Planificar. Se establecen los objetivos, procesos y procedimientos para el proceso de gestión de riesgos tecnológicos. La finalidad de la planeación es la entrega de resultados acordes con las políticas y objetivos globales de la organización. Así mismo, se establece el plan de comunicaciones y el análisis del contexto organizacional actual para definir el alcance de la gestión de riesgos tecnológicos.

Hacer. Corresponde a la implementación y operación de los controles, procesos y procedimientos (incluye la operación e implementación de las políticas definidas), lo correspondiente a la valoración y tratamiento de los riesgos.

Verificar. Evaluar y medir el desempeño de los procesos contra la política y los objetivos de seguridad e informar sobre los resultados.

Actuar. Establecer la política para la gestión de riesgos tecnológicos e implementar los cambios requeridos para la mejora de los procesos. Como parte de las fases verificar y actuar, se incluye el monitoreo y mejora continua, donde se verifican los cambios y el cumplimientos de los indicadores que fueran establecidos desde la planificación.

Como se mencionó anteriormente, la metodología a usar tiene su base en ISO 27005 e ISO 31000, dado su enfoque en gestión de riesgos y siendo parte de los estándares de la familia ISO fue posible establecer una alineación con el l modelo PHVA (Tabla 2).

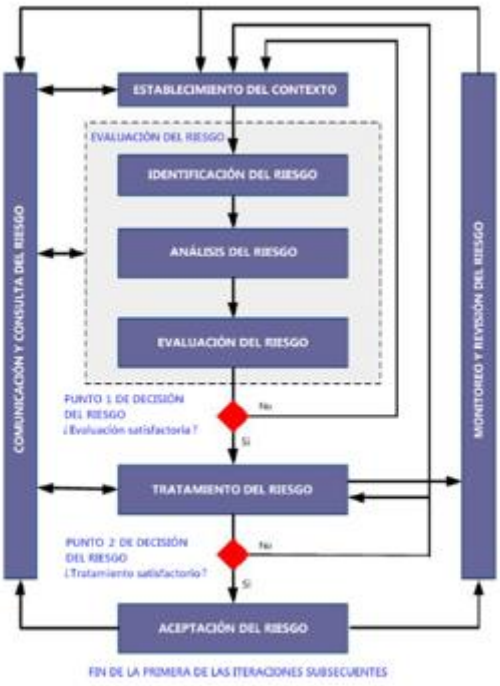
Tabla 2 Alineación de estándar ISO 27005 con modelo PHVA

<table>
<tr><th>PHVA</th><th colspan="2">ISO 27005</th></tr>
<tr><td rowspan="6">Planear</td><td colspan="2">Definir plan de gestión de riesgos</td></tr>
<tr><td colspan="2">Establecimiento del contexto</td></tr>
<tr><td rowspan="3">Valoración Riesgo</td><td>Identificación del riesgo</td></tr>
<tr><td>Estimación del riesgo</td></tr>
<tr><td>Evaluación del riesgo</td></tr>
<tr><td colspan="2">Desarrollar el plan de tratamiento del riesgo</td></tr>
<tr><td colspan="2">Aceptación del riesgo</td></tr>
<tr><td rowspan="2">Hacer</td><td colspan="2">Implementar el plan de tratamiento</td></tr>
<tr><td colspan="2">Implementar plan de comunicación del riesgo</td></tr>
<tr><td>Verificar</td><td colspan="2">Monitoreo y revisión del riesgo</td></tr>
<tr><td>Actuar</td><td colspan="2">Mantener y mejorar el proceso de gestión</td></tr>
</table>

La metodología sigue los pasos del proceso de gestión de riesgos de acuerdo a ISO 27005, la cual contempla las siguientes etapas (Figura 2).

- Establecimiento de plan de comunicación interno y externo
- Definición del contexto organizacional
- Evaluación de riesgos
- Tratamiento de riesgos
- Monitoreo y revisión de riesgos

Figura 2 Proceso de Gestión de Riesgos ISO 27005



2.2 Plan de Comunicación

Establecimiento de plan de comunicación interno y externo

El plan de comunicación se debe realizar a nivel interno (áreas de la organización, empleados, directivos, socios) y externo (clientes, proveedores, entes reguladores, todos los anteriores si así se requiere), teniendo en cuenta las definiciones sobre la existencia del riesgo, los objetivos de la gestión, el debido informe de los avances del proceso y todo aquello que se considere necesario.

El plan de comunicación debe crear conciencia en seguridad, si está bien estructurado permitirá lograr los objetivos de la gestión de forma satisfactoria, obtener información de soporte al análisis y colaborar en la planificación del proceso de gestión de riesgos.

El plan de comunicación propuesto se compone de acciones de comunicación desde el inicio de la implementación hasta su cierre y durante la operación del esquema de gestión (Tabla 2.1).

Tabla 2.1 Plan de comunicación

Etapa	Tema	Objetivo	Periodicidad	Audiencia	Medio	Responsable
Inicio Implementación	Presentación esquema Gestión de Riesgos Seguridad	1. Entendimiento esquema de riesgos 2. Entendimiento conceptos riesgos 3. Beneficios gestión de riesgos 4. Presentación organigrama del proyecto de implementación	Una vez al inicio	Personal Interno Proveedores	Presentación Banner	Gerente Seguridad
Durante Implementación	Campaña de Concientización	1. Sensibilizar a colaboradores sobre los diferentes problemas asociados a los riesgos de seguridad y su inadecuada gestión. 2.Difundir los beneficios de la Gestión Integral de Riesgos de Seguridad para lograr que la organización se involucre en sus diferentes etapas de implementación. 3. Fomentar prácticas para minimizar los riesgos de seguridad 4. Promover la detección de riesgos de seguridad 5. Dar visibilidad de los hallazgos y soluciones, así como los beneficios adquiridos	Mensual	Personal Interno Proveedores	Presentación Correos Talleres	Gerente Seguridad Gerentes de área
	Presentación avance	1. Informar sobre el estado de la implementación 2. Informar sobre los entregables comprometidos 3. Informar atrasos, riesgos o situaciones destacables 4. Informar compromisos siguiente periodo 5. Obtener retroalimentación y mantener la participación de todos los involucrados en la organización 6. Establecer acciones preventivas / correctivas necesarias	Quincenal	Equipo Implementación	Presentación	Gerente Seguridad
Final Implementación	Presentación Cierre de Implementación	1. Informar cumplimiento de los objetivos de la implementación 2. Formalizar esquema final de Gestión de Riesgos de Seguridad 3. Formalizar inicio de operación	Una vez al cierre	Personal Interno Proveedores	Presentación	Gerente Seguridad
Durante Operación	Presentación indicadores	1. Informar a la dirección del desempeño del esquema de gestión necesarias 2. Determinar acciones preventivas o correctivas	Semestral	Dirección Equipo Seguridad	Presentación	Gerente Seguridad

2.3 Definición del contexto organizacional

Misión

Ser el referente mexicano para los productos de consultoría y servicios de alto valor agregando en las TIC´s que genere un sistema sustentable, apreciado entre nuestros clientes, colaboradores, proveedores y accionistas.

Visión

Transformar la industria de los proveedores de soluciones en las Tecnologías de Información y Comunicaciones (TIC´s), a través de una propuesta diferenciada, en función de la sinergia entre las estrategias de negocio de los clientes, su innovación y la oferta tecnológica.

Filosofía

Leer oportunamente los cambios en la industria, en el mercado y en los clientes, para poder adecuar el mejor portafolio de soluciones y competencias que permitan a nuestro ecosistema desarrollarse económicamente.”

Política de Calidad

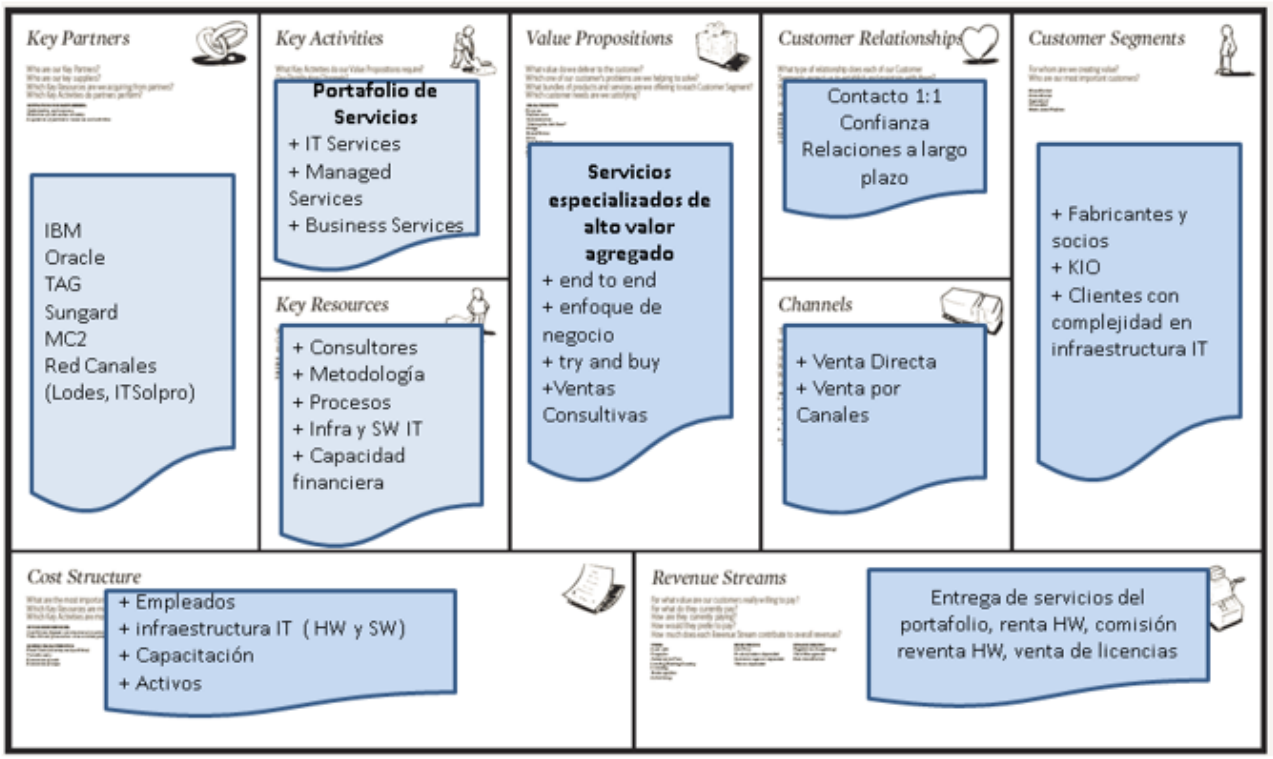
Asegurar, que mediante nuestras soluciones, las Tecnologías de la Información y Comunicación coadyuven al logro de las estrategias de negocio de nuestros clientes sin perder de vista la mejora continua de nuestro Sistema de Gestión de Calidad.

Modelo de Negocio

ACME genera ingresos y utilidades mediante servicios especializados en TI que resuelven los problemas de negocio de sus clientes. Típicamente ACME apoya reduciendo el costo operacional o permitiendo la habilitación de nuevas capacidades que generen ingresos en el negocio de los clientes.

Los servicios de ACME permiten a los clientes optimizar su ambiente de TI a través de la eficiencia, la flexibilidad y la productividad, al mismo tiempo que se genera reducción de costos.

Tabla 2.2



Clientes Objetivo. Se cubren clientes principalmente en las industrias de Servicios Financieros, Distribución y Productos de Consumo. Tienen como característica principal una infraestructura de TI compleja y por lo mismo, el valor de la inversión en estos activos es muy grande.

Portafolio de Servicios

ACME cuenta con un portafolio dinámico, sólido y actual que incluye soluciones de corto y largo plazo, con soluciones relevantes del mercado y un enfoque de ahorro y calidad con foco en servicios administrados.

El portafolio cuenta con 3 grandes pilares; IT Services, Managed Services y Business Services, las cuales son soportadas en su implementación por metodologías y mejores prácticas de las TICs , al igual que múltiples especialidades donde se garantiza que se cuenta con certificaciones en todas ellas.

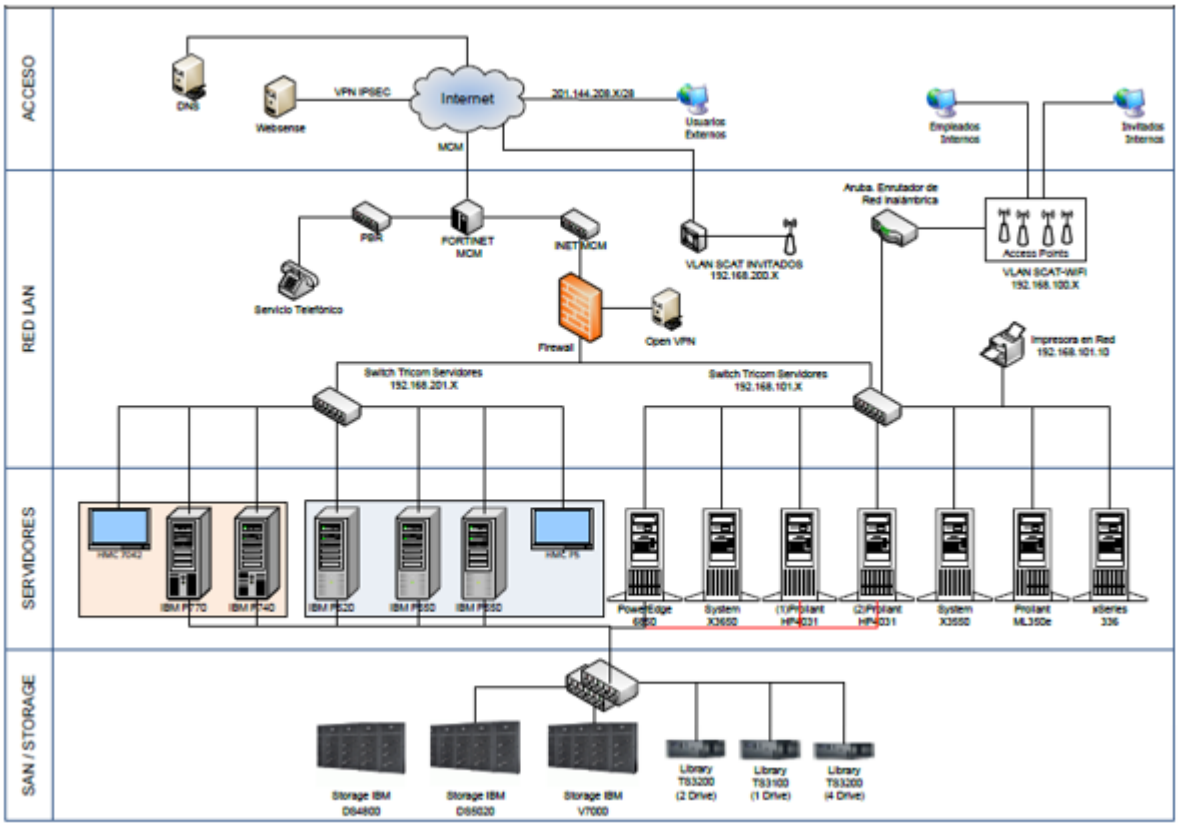
El alcance de este análisis se limita al grupo de Servicios Administrados que forma parte del pilar de “Managed Services que se muestra en la Figura 2.1.

Figura 2.1 Detalle por grupo de servicios

2.4 Análisis de Riesgos

Alcance

Figura 2.2 Infraestructura involucrada para el alcance del análisis



Evaluación de Riesgos

En la etapa de evaluación de riesgos se identifican los activos que se quieren proteger y sus debilidades, así como las amenazas a las cuales se encuentran expuestos. Se tomaron en cuenta los activos relevantes, señalando los daños que pueden implicar las amenazas, la determinación de las probabilidades e impactos.

Para los activos y escenarios de riesgos identificados se valoraron los siguientes elementos:

- Consecuencia
- Dificultad de acceso al activo
- Confidencialidad
- Integridad
- Disponibilidad
- Explotación de la amenaza
- Control implementado
- Reporte de la amenaza

El resultado de las valoraciones arrojó el nivel de riesgo inicial y riesgo residual para cada escenario de riesgo.

Tabla 2.3 Riesgos del SITE

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
1	SITE	Robo o daño intencionado de equipos que puede afectar la disponibilidad de los servicios	Falta de control de acceso al site para personal interno o ajeno a la empresa	BAJO	ALTO	BAJO	PARCIAL	NINGUNA	PARCIAL	DISPONIBILIDAD	NO PROBADA	PERMANENTE	NO CONFIRMADO	53.66%	17.52%
2		Daño parcial o total de equipo en caso de un incendio	Falta de sistema de incendios (Extintores)	BAJO	ALTO	ALTO	COMPLETA	NINGUNA	COMPLETA	DISPONIBILIDAD	NO PROBADA	NINGUNO	NO CONFIRMADO	68.01%	35.30%
3		Daño o degradación del equipo de cómputo por sobrecalentamiento y/o humedad	Falta de mantenimiento al sistema de aire acondicionado	ALTO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	80.99%	80.99%
4		Indisponibilidad del servicio por Falta de energía	Insuficiencia del Power Supply por fallas en baterías para soportar más de 7 min el suministro de energía	ALTO	ALTO	ALTO	NINGUNA	NINGUNA	COMPLETA	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	82.91%	82.91%
5		Indisponibilidad del servicio por fallas en cableado	Falta de un cableado estructurado de quipos	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	59.96%	59.96%
6		Acumulación de polvo u otros residuos que dañan los componentes de la infraestructura	Falta de limpieza periódica	BAJO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	38.94%	19.86%

Tabla 2.4 Riesgos hardware general

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
7	HARDWARE GENERAL	Falla del equipo que puede afectar la disponibilidad de los servicios	Falta de póliza de mantenimiento y soporte	ALTO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	80.99%	80.99%
8		Caída de ambientes críticos	Falta de esquema de alta disponibilidad para ambientes críticos	ALTO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	80.99%	80.99%
9		Obsolescencia tecnológica	Falta de plan de renovación de tecnología para asegurar el buen desempeño de los ambientes	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	59.96%	59.96%
10		Perdida o mal manejo de información en desecho de equipos	Falta de control en eliminación de desechos	BAJO	ALTO	ALTO	NINGUNA	NINGUNA	NINGUNA	NORMAL	PRUEBA DE CONCEPTO	PERMANENTE	IDENTIFICADO	13.58%	13.58%

Tabla 2.5 Riesgos de acceso y servidores

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
11	ACCESO DNS (Nube) Websense (Nube) Internet	Problemas de acceso en cambios de IP's	Accesos Hardcoded	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	59.96%	48.74%
12		Dependencia de internet para otorgar servicios	Punto único de falla en ISP (Internet)	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	COMPLETA	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	66.38%	66.38%
13	SERVIDORES Equipos Power Equipos X (Vmware,Linux yWindows)	Vencimiento equipos en comodato	Ambientes productivos de clientes se encuentran instalados en equipos prestados y no hay equipos propios para migrar ambientes	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PRUEBA DE CONCEPTO	NINGUNO	IDENTIFICADO	59.96%	49.49%
14		Deficiencia en la operación	Falta de capacidad de equipos	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	59.96%	59.96%

Tabla 2.6 Riesgos de red y almacenamiento/biblioteca

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
15	RED Switches de LAN	Empleados y clientes no pueden acceder a los ambientes	Punto único de falla Firewall	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	COMPLETA	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	66.38%	66.38%
16			Punto único de falla en Switches LAN	MEDIO	ALTO	ALTO	NINGUNA	NINGUNA	COMPLETA	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	66.38%	66.38%
17	ALMACENAMIENTO/BIBLIOTECA Storage V7000 Storage DS5020 Bibliotecas IBM TS3200, TS3100 Switches de SAN	Incumplimiento RTO y RPO, posible perdida de información	Incapacidad para poder realizar los respaldos comprometidos por falta de cintas LTO4	ALTO	ALTO	ALTO	NINGUNA	NINGUNA	COMPLETA	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	82.91%	78.38%

Tabla 2.7 Riesgos de software

ID	Activo	Amenaza	Vulnerabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
18	SOFTWARE	Errores o fallas del software (Mal funcionamiento)	Falta de control de cambios	MEDIO	BAJO	NINGUNA	PARCIAL	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	38.13%	28.28%
19		Errores de uso	Falta de documentación o actualización para operación de los sistemas y servicios	ALTO	BAJO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	60.75%	60.75%
20			Asignación incorrecta de accesos	MEDIO	BAJO	NINGUNA	NINGUNA	NINGUNA	NORMAL	PROBADA	NINGUNO	CONFIRMADO	42.50%	42.50%
21			Configuración incorrecta	MEDIO	BAJO	NINGUNA	NINGUNA	NINGUNA	NORMAL	PROBADA	NINGUNO	NO CONFIRMADO	25.00%	25.00%
22		Pérdida de versiones de respaldos	Falta de políticas de respaldo adecuada	ALTO	BAJO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	60.75%	60.75%
23		Problemas de no licenciamiento adecuada de software	Falta de control en descarga de software	MEDIO	BAJO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	INMEDIATO	CONFIRMADO	33.75%	31.56%

Tabla 2.8 Riesgos del personal

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
24	PERSONAL	Incumplimiento en los SLA's de cliente	Falta de atención a clientes por ausencia del personal	BAJO	ALTO	ALTO	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	38.94%	19.86%
25		Penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA´s	Procedimientos de reclutamiento inadecuados	MEDIO	MEDIO	ALTO	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	41.63%	29.16%
26			Capacitación inadecuada	MEDIO	MEDIO	ALTO	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	PROBADA	PERMANENTE	CONFIRMADO	41.63%	29.16%
27		Robo de documentos o medios de almacenamiento	Trabajo no supervisado de proveedores	MEDIO	MEDIO	ALTO	PARCIAL	NINGUNA	NINGUNA	CONFIDENCIALIDAD	PROBADA	PERMANENTE	CONFIRMADO	33.31%	27.08%

Tabla 2.9 Riesgos de administración – 1a parte

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
28	ADMINISTRACION	Abuso de derechos, robo, eliminación y/o modificación de información	Falta de procedimientos registro y cancelación de usuarios	ALTO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	PERMANENTE	CONFIRMADO	76.50%	76.50%
29			Falta de previsiones referentes a seguridad en contratos con clientes, proveedores y empleados	MEDIO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	DISPONIBILIDAD	FUNCIONAL	NINGUNO	IDENTIFICADO	45.00%	45.00%
30		Penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA´s	Falta de auditorias regulares (supervisión)	MEDIO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	NINGUNO	CONFIRMADO	45.00%	45.00%
31			Falta de monitoreo de operaciones	MEDIO	ALTO	N/A	NINGUNA	NINGUNA	PARCIAL	DISPONIBILIDAD	PROBADA	NINGUNO	CONFIRMADO	45.00%	45.00%
32			Falta de actualización de procedimientos operativos	ALTO	MEDIO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	NINGUNO	CONFIRMADO	42.50%	42.50%

Tabla 2.10 Riesgos de administración – 2a parte

ID	Activo	Amenaza	Vulnerabilidad	Probabilidad	Consecuencia	Dificultad de acceso al Activo	Confidencialidad	Integridad	Disponibilidad	Ponderación de CID	Explotación de la amenaza	Control Implementado	Reporte de la amenaza	Riesgo Inicial	Riesgo Residual
33	ADMINISTRACION	Pérdida parcial o total del Site	Falta de plan de continuidad	ALTO	ALTO	N/A	NINGUNA	NINGUNA	NINGUNA	NORMAL	PROBADA	NINGUNO	CONFIRMADO	76.50%	76.50%
34		Perdida de evidencia	Falta de logs de operadores y administradores	ALTO	ALTO	N/A	NINGUNA	NINGUNA	NINGUNA	NORMAL	PROBADA	NINGUNO	CONFIRMADO	76.50%	76.50%
35		Modificación no autorizada, no intencional de la información y mal uso de los activos de información	Falta de clasificación de la información	ALTO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	NINGUNO	CONFIRMADO	76.50%	76.50%
36			Falta de definición de responsabilidad de seguridad en perfiles de puestos	ALTO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	NINGUNO	CONFIRMADO	76.50%	76.50%
37			Falta de segregación de funciones	ALTO	ALTO	N/A	PARCIAL	PARCIAL	PARCIAL	NORMAL	PROBADA	NINGUNO	CONFIRMADO	76.50%	76.50%

Resumen Evaluación de Riesgos

La valoración de riesgos en su conjunto muestra que el nivel de riesgo inicial de la organización no cumple con la tolerancia al riesgo establecido del 30%, el 62% de los escenarios son de riesgo MUY ALTO y un 32% con riesgo ALTO, es decir el 94% de los riesgos están fuera del limite establecido, en promedio el nivel de riesgo es del 58% (Figura 5).

El riesgo residual muestra una ligera mejora bajando a 75% los riesgos arriba del limite establecido con un promedio del 53% (Tabla 2.11).

Tabla 2.11 Resumen evaluación de riesgos

TIPO RIESGO	RANGO	RIESGO INICIAL		RIESGO RESIDUAL	
		Cant	%	Cant	%
Verde (Riesgo BAJO)	0-10%	0	0	0	0
Azul (Riesgo MEDIO)	11-30%	2	5%	9	24%
Amarillo (Riesgo ALTO)	31-50%	12	32%	9	24%
Rojo (Riesgo MUY ALTO)	51-100%	23	62%	19	51%
		37	100%	37	100%
Promedio			58%		53%

La organización establece que la prioridad del tratamiento de riesgos es la siguiente (Tabla 2.12).

Tabla 2.12 Prioridad tratamiento de riesgos

PRIORIDAD	NIVEL RIESGO	FECHA COMPROMISO
1	Rojo (Riesgo MUY ALTO)	mar-17
2	Amarillo (Riesgo ALTO)	jun-17
3	Azul (Riesgo MEDIO)	sep-17

Tratamiento de Riesgos

Como parte del tratamiento se definen las posibles acciones a seguir sobre los riesgos y de acuerdo a la prioridad establecida se determinan los beneficios, responsables, recursos, fechas compromiso e inversión requerida considerando las restricciones de presupuesto.

Los tratamientos recomendados deben incluir un análisis costo-beneficio (incluyendo costos de implementación y mantenimiento), sin embargo por falta de tiempo no se incluyen en este trabajo, sólo se especifica si se requiere inversión pero no se indica el monto de dicha inversión.
Los tratamientos propuestos se listan a continuación:

Tabla 2.13 Tratamiento riesgos del SITE

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
1	SITE	Robo o daño intencionado de equipos que puede afectar la disponibilidad de los servicios	Falta de control de acceso al site para personal interno o ajeno a la empresa	1. Cerradura en entrada al SITE 2. Autorización de acceso con asignando de un gafete 3. Bitácora de accesos (Nombre, fecha, motivo, hora entrada y salida)	Migrar infraestructura a un Data Center que cumpla con los componentes indispensables que aseguren un desempeño optimo de los equipos, así como prevenir la pérdida, daño, robo o comprometer la disponibilidad de los sistemas y servicios.	1. Seguridad sobre los equipos 2. Menor inversión por pagos mensuales que renovar SITE propio 3. Instalaciones bajo las mejores prácticas (espacio, aire acondicionado, sistema incendios, cableado, limpieza) que aseguren el óptimo funcionamiento de los equipos 4. Mejor servicio a clientes 5. Asegurar el cumplimiento de los SLA's comprometidos	Director de Operaciones	Personal Interno Proveedor	31-mar-17	Pago mensual de servicios	28.76%
2		Daño parcial o total de equipo en caso de un incendio	Falta de sistema de incendios (Extintores)								28.76%
3		Daño o degradación del equipo de cómputo por sobrecalentamiento y/o humedad	Falta de mantenimiento al sistema de aire acondicionado								23.67%
4		Indisponibilidad del servicio por Falta de energía	Insuficiencia del Power Supply por fallas en baterías para soportar más de 7 min el suministro de energía								49.04%
5		Indisponibilidad del servicio por fallas en cableado	Falta de un cableado estructurado de quipos								38.94%
6		Acumulación de polvo u otros residuos que dañan los componentes de la infraestructura	Falta de limpieza periódica	Una vez a la semana, personal técnico ayuda y supervisa al personal de limpieza para el aseo del SITE							19.06%

Tabla 2.14 Tratamiento riesgos de hardware general

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
7	HARDWARE GENERAL	Falla del equipo que puede afectar la disponibilidad de los servicios	Falta de póliza de mantenimiento y soporte		Contratación póliza de mantenimiento y soporte para asegurar el desempeño optimo de los equipos y soporte en caso de contingencias que permita minimizar el impacto en la disponibilidad de los sistemas y servicios	1. Mejor servicio a clientes 2. Asegurar optimo desempeño de los equipos 3. Asegurar el cumplimiento de los SLA´s comprometidos	Director Operaciones	Personal Interno Proveedor	31-mar-17	Pago mensual de servicios	58.99%
8		Caída de ambientes críticos	Falta de esquema de alta disponibilidad para ambientes críticos		Implementación de esquemas de alta disponibilidad en ambientes críticos que permita cumplir los SLA´s comprometidos	1. Mejor servicio a clientes 2. Asegurar el cumplimiento de los SLA´s comprometidos	Director Operaciones	Personal Interno	31-mar-17	Compra de HW y SW	23.67%
9		Obsolescencia tecnológica	Falta de plan de renovación de tecnología para asegurar el buen desempeño de los ambientes		No hay presupuesto, la organización asume el riesgo. Se integrará presupuesto en el 2018						59.96%
10		Perdida o mal manejo de información en desecho de equipos	Falta de control en eliminación de desechos	Definición procedimiento ante el SGC (Sistema de Gestión de Calidad) para eliminación de desechos considerando el manejo adecuado de la información		1. Asegurar el resguardo de la información para no comprometer la confidencialidad, integridad y disponibilidad					13.58%

Tabla 2.15 Tratamiento riesgos acceso y servidores

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
11	ACCESO DNS (Nube) Websense (Nube) Internet	Problemas de acceso en cambios de IP's	Accesos Hardcoded	Cambiar configuración de clientes VPN softcoded y realizar la migración de clientes		1. Asegurar el acceso a los sistemas y servicios durante mantenimiento de IP's para no impactar disponibilidad de servicios					23.67%
12		Dependencia de internet para otorgar servicios	Punto único de falla en ISP (Internet)		No hay presupuesto, la organización asume el riesgo. Se integrará presupuesto en el 2018						28.04%
13	SERVIDORES Equipos Power Equipos X (Vmware,Linux y Windows)	Vencimiento equipos en comodato	Ambientes productivos de clientes se encuentran instalados en equipos prestados y no hay equipos propios para migrar ambientes		Compra de equipo para reemplazo equipos en comodato para migrar a equipo propio y asegurar la disponibilidad de los servicios	1. Asegurar operación de ambientes productivos 2. Asegurar el cumplimiento de los SLA´s comprometidos	Director Operaciones	Personal Interno	30-jun-17	Compra HW y SW	23.67%
14		Deficiencia en la operación	Falta de capacidad de equipos		Realizar análisis de capacidades y proyecciones de los requisitos futuros para determinar los requisitos de capacidad que garanticen el desempeño optimo de los equipos	1. Mejor desempeño en sistemas y servicios 2. Asegurar el cumplimiento de los SLA´s comprometidos	Director Operaciones	Personal Interno	31-mar-17	Compra HW y SW	23.67%

Tabla 2.16 Tratamiento riesgos red y almacenamiento/biblioteca

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
15	**RED Switches de LAN**	Empleados y clientes no pueden acceder a los ambientes	Punto único de falla Firewall		Implementar redundancia en firewall que asegure el accesos a los sistemas y servicios	1. Eliminar punto único de falla 2. Asegurar el cumplimiento de los SLA´s comprometidos	Director Operaciones	Personal Interno	31-mar-17	Compra HW y SW	**28.04%**
16			Punto único de falla en Switches LAN		Implementar redundancia en swithes LAN que asegure el acceso a los sistemas y servicios	1. Eliminar punto único de falla 2. Asegurar operación de sistemas y servicios de acuerdo a los SLA´s comprometidos	Director Operaciones	Personal Interno	31-mar-17	Compra HW y SW	**28.04%**
17	**ALMACENAMIENTO/BIBLIOTECA Storage V7000 Storage DS5020 Bibliotecas IBM TS3200, TS3100 Switches de SAN**	Incumplimiento RTO y RPO, posible perdida de información	Incapacidad para poder realizar los respaldos comprometidos por falta de cintas LTO4	Compra de cintas LTO4		1. Asegurar cumplimiento de RTO y RPO comprometidos					**22.58%**

Tabla 2.17 Tratamiento riesgos de software

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
18	**SOFTWARE**	Errores o fallas del software (Mal funcionamiento)	Falta de control de cambios	Creación procedimiento de control de cambios		1. Mejorar servicio por errores o fallas del SW 2. Asegurar el cumplimiento de los SLA´s comprometidos					**28.28%**
19		Errores de uso	Falta de documentación o actualización para operación de los sistemas y servicios		Creación o actualización de documentación de operación	1. Minimizar errores en la operación 2. Asegurar el cumplimiento de los SLA´s comprometidos	Gerente Área	Personal Interno	31-mar-17	N/A	**24.21%**
20			Asignación incorrecta de accesos		Creación de procedimientos para asignación de accesos por roles ante el SGC	1. Asegurar asignación correcta de accesos 2. Salvaguardar la integridad, confidencialidad y disponibilidad de la información	Gerente SGC	Personal Interno	30-jun-17	N/A	**7.58%**
21			Configuración incorrecta								**25.00%**
22		Pérdida de versiones de respaldos	Falta de políticas de respaldo adecuada		Implementar TSM para asegurar que los respaldos d e la información, software e imágenes de sistemas se realizan regularmente de acuerdo con la política de respaldos acordada	1. Asegurar la disponibilidad de respaldos 2. Asegurar el cumplimiento de los SLA´s comprometidos	Gerente Infraestructura	Personal Interno	31-mar-17	N/A	**21.53%**
23		Problemas de no licenciamiento adecuada de software	Falta de control en descarga de software	Restricción de descarga de SW		1. Asegurar que la descarga de SW s cumpla con el licenciamiento adecuado para no poner en riesgo la operación de sistemas y servicios					**13.45%**

Tabla 2.18 Tratamiento riesgos del personal

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
25	**PERSONAL**	Penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA´s	Procedimientos de reclutamiento inadecuados	Cambio a procedimiento de reclutamiento para incluir examen práctico y segunda entrevista por otro gerente además del gerente de área		1. Asegurar un mejor reclutamiento de personal 2. Minimizar las penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA´s					**29.16%**
26			Capacitación inadecuada	Creación de política de no asignar a un recurso a un actividad hasta que haya realizado la tarea con supervisión del gerente y este confirme que cumple con la competencia requerida		1. Asegurar que los recursos cumplen con las competencias requeridas para la operación 2. Minimizar las penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA´s					**29.16%**
27		Robo de documentos o medios de almacenamiento	Trabajo no supervisado de proveedores	Política de custodiar en todo momento a proveedores además de asegurar la autorización del gerente de área		1. Asegurar que el trabajo de proveedores sea supervisado para evitar robo de documentos o medios de almacenamiento					**27.08%**

Tabla 2.19 Tratamiento riesgos de administración – 1ra parte

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
28	ADMINISTRACION	Abuso de derechos, robo, eliminación y/o modificación de información	Falta de procedimientos registro y cancelación de usuarios	Cambios en procedimiento para el ingreso y salida de personal incluyendo la validación del alta y cancelación de usuarios por el gerente responsable		1. Asegurar que el alta de usuarios corresponde a las funciones que va a desempeñar y que a la salida se revoquen todos los accesos para salvaguardar la información de abuso de					13.50%
29			Falta de previsiones referentes a seguridad en contratos con clientes, proveedores y empleados		1.Definir políticas de seguridad de la información e integrar en los acuerdos contractuales con clientes, proveedores y empleados las responsabilidades para seguridad de la información	1. Garantizar la protección de la información que sea accesible por los clientes, proveedores y empleados	Director de Operaciones	Personal Interno	30-jun-17	N/A	13.50%
30		Penalizaciones, falta de pago o cancelación de contratos por incumplimiento de SLA's	Falta de auditorias regulares (supervisión)		Definir procedimientos para realizar auditorias con el objetivo de minimizar las interrupciones a los sistemas y servicios	1. Asegurar que se identifican las mejoras necesarias para minimizar las interrupciones de sistemas y servicios	Gerente SGC	Personal Interno	30-jun-17	N/A	13.50%
31			Falta de monitoreo de operaciones		Implementar herramientas, procesos y procedimientos que informen el estado de las operaciones para tomar las acciones necesarias para minimizar las fallas en la	1. Contar con la información suficiente para tomar las acciones de mejora que minimicen las interrupciones de sistemas y servicios	Gerente de Operaciones	Personal Interno	30-jun-17	Compra HW y SW	13.50%
32			Falta de actualización de procedimientos operativos		Revisión y actualización de procedimientos operativos por cada gerente de área	1. Operación eficiente que se vea reflejada en una buena atención a clientes	Gerentes de área	Personal Interno	30-jun-17	N/A	7.50%

Tabla 2.10 Tratamiento riesgos de administración – 2da parte

ID	Activo	Amenaza	Vulnerabilidad	Control Implementado	Acciones de Tratamiento	Beneficio	Responsable	Recursos	Fecha	Inversión	Riesgo Residual Calculado
33	ADMINISTRACION	Pérdida parcial o total del Site	Falta de plan de continuidad		Definir, implementar y mantener procesos, procedimientos y controles para garantizar la continuidad durante una situación adversa que asegure el cumplimiento de los SLA's	1. Asegurar la continuidad del servicio que permita cumplir los SLA's comprometidos en una situación de emergencia	Director de Operaciones	Personal Interno	31-mar-17	N/A	13.50%
34		Perdida de evidencia	Falta de logs de operadores y administradores		Definir los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información de evidencia	1.Garantizar que se cuenta con procesos definidos para contar con evidencia que soporte la administración de incidentes en las operaciones	Director de Operaciones	Personal Interno	31-mar-17	N/A	13.50%
35		Modificación no autorizada, no intencional de la información y mal uso de los activos de información	Falta de clasificación de la información		Definir esquema de clasificación para implementar un apropiado conjunto de procedimientos para la clasificación y etiquetado de la información	1. Asegurar que la información reciba un apropiado nivel de protección de acuerdo con su importancia para la organización	Director de Operaciones Gerentes de área	Personal Interno	31-mar-17	N/A	13.50%
36			Falta de definición de responsabilidad de seguridad en perfiles de puestos		Definir todas las responsabilidades de la seguridad de la información y asignarse en perfiles de puesto	1. Asegurara la conciencia en empleados sobre sus responsabilidades de seguridad de la información para minimizar incidentes en la operación	Director de Operaciones	Personal Interno	31-mar-17	N/A	13.50%
37			Falta de segregación de funciones		Definir tareas en conflicto y áreas de responsabilidad que deben segregarse para reducir la modificación no autorizada, no intencional o mal uso de los activos de la organización	1. Reducir las oportunidades de mal uso de la información	Director de Operaciones Gerentes de área	Personal Interno	31-mar-17	N/A	13.50%

Resumen Tratamiento de riesgos

Se realizó la valoración de los riesgos asumiendo que las acciones de tratamiento se lleven a cabo con el objetivo de determinar si las acciones de tratamiento establecidas darán como resultado el cumplimiento del nivel de riesgo autorizado por la organización, el nuevo riesgo residual calculado muestra que la organización asume 2 riesgos arriba del 30% por restricciones de presupuesto, el 84% de los riesgos se mantienen dentro del límite establecido, de manera global el nivel de riesgo promedio del 24% permitirá que la organización cumpla con sus objetivos de crecimiento definidos para el año 2017 (Figura 2.2).

Tabla 2.11 Tratamiento riesgos del SITE

TIPO RIESGO	RANGO	RIESGO INICIAL		RIESGO RESIDUAL		RIESGO RESIDUAL CALCULADO	
		Cant	%	Cant	%	Cant	%
Verde (Riesgo BAJO)	0-10%	0	0	0	0	2	5%
Azul (Riesgo MEDIO)	11-30%	2	5%	9	24%	31	84%
Amarillo (Riesgo	31-50%	12	32%	9	24%	2	5%
Rojo (Riesgo MUY	51-100%	23	62%	19	51%	2	5%
		37	100%	37	100%	37	100%
Promedio			58%		53%		24%

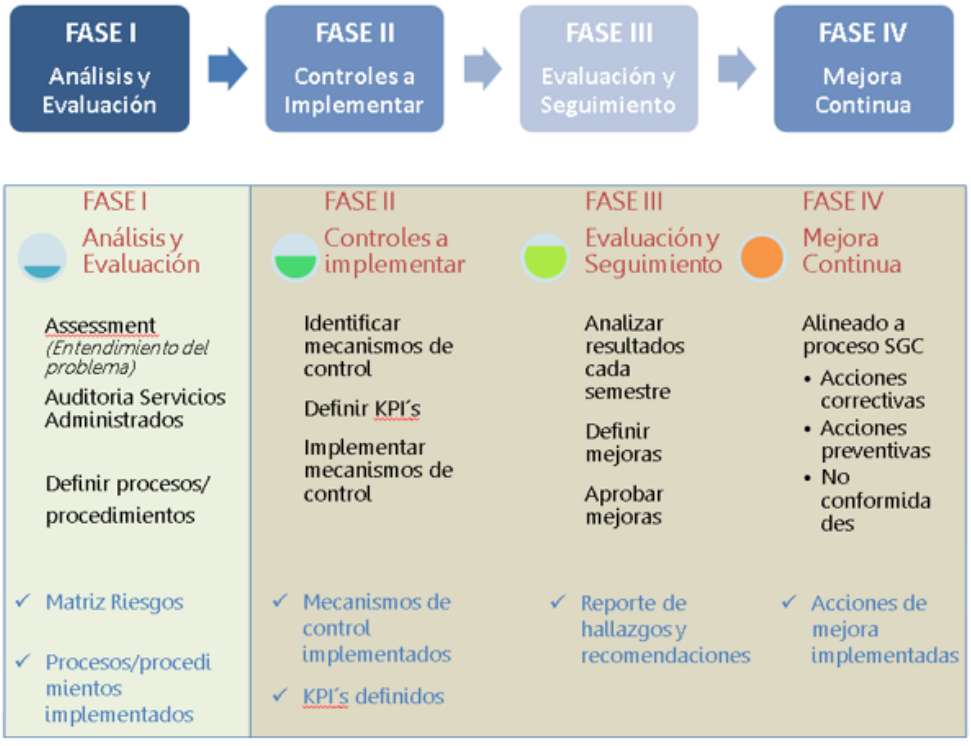
Monitoreo y Mejora Continua del Proceso de Gestión

Es una decisión de la dirección formalizar el análisis de riesgos en la organización, como primera etapa el alcance será el análisis de riesgos para la entrega de Servicios Administrados y paulatinamente se implementará para todos los servicios en la organización.

Con el monitoreo y la mejora continua se busca asegurar la constante revisión sobre la gestión de riesgos para dar cumplimiento a los procesos de mitigación definidos. También, permitirá agregar al análisis riesgos nuevos que puedan aparecer luego de la definición de los planes teniendo en cuenta posibles cambios internos y externos

La implementación se realizará con la siguiente metodología de trabajo, para cada fase se realizarán actividades específicas y se generarán entregables. El seguimiento se realizará de forma semestral.

Figura 2.2 Actividades y entregables por fase



2.5 Conclusiones

Es irrefutable los beneficios de un análisis de riesgos de seguridad, el análisis y los hallazgos del presente trabajo son la base de cambios importantes en la organización, se concluye que los principales ejes de atención para lograr una implementación exitosa son:

- Compromiso de la dirección
- Formalizar la función de gestión de riesgos
- Construir un sistema para la gestión de riesgos
- Permear en la organización que la gestión de riesgos de seguridad se vea como una herramienta para ser más competitivos y no de cumplimiento
- Mejorar con el tiempo los procesos con controles efectivos
- Mostrar resultados semestralmente

Si bien esta implementación supone un importante consumo de recursos y un gran desafío, también se considera que los beneficios de tener una mayor comprensión de las fuentes de riesgos y el nivel de exposición permitirá que la empresa de pasos firmes hacia una mejora continua, disminuyendo la incertidumbre en el logro de los objetivos estratégicos de la organización y de esa forma se asegure su competitividad y rentabilidad para permanecer en el mercado.

2.6 Referencias

ISO (International Standard Organization). (2011). Gestión del riesgo – Principios directrices. Estándar de Seguridad ISO 31000.

ISO (International Standard Organization). (2008). Tecnología de la información – Técnicas de seguridad – Gestión del riesgo de seguridad de la información. Estándar de Seguridad ISO/IEC 27005.

NIST (National Institute of Standards and Technology). (2002). NIST SP 800-30. Guía de Gestión de riesgo para sistemas de tecnología de la Información – Recomendaciones del Instituto Nacional de Estándares y Tecnología.

Ramírez Castro, Alexandra. (2012). Desarrollo de una metodología para la gestión del riesgo tecnológico a partir de ISO 31000 e ISO 27005 - Tesis de grado para optar como Ingeniera de sistemas, Proyecto curricular de ingeniería de sistemas, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

Orientación acerca del enfoque basado en procesos para los sistemas de gestión de la calidad. (Mayo 2001). Recuperado de http://www.iram.com.ar/Documentos/Certificacion/Sistemas/ISO9000_2000/procesos.pdf.

Una perspectiva de Silicon Valley-La Ciudad Tecnológica

MEDELLÍN, Guillermo

G. Medellín

Universidad Iberoamericana

P. Solares (eds.) Ciencias de los Sistemas de Información y Seguridad. Handbook T-I. -©ECORFAN, Ciudad de México, 2016.

Abstract

Silicon Valley is the result of an amalgam formed with elements from academia, the private sector and investment in research by the US government, to which is added a serial entrepreneurs population [1]. Currently in all aspects of social, economic and political life they can be affected by new information technologies and communication [2].

The new system that has transformed the new information society, has reshaped the conditions and characteristics of the groups that integrate and nurture culturally and economically, through a form of perception and action from Silicon Valley. This is the space where innovation associated with new technologies came with a unique intensity, so try in this article the benefits that gives the world have a place like Silicon Valley.

3 Introducción

Los países del mundo suspiran por tener más innovadores creadores de empresas como base del desarrollo económico y el empleo, por conseguir un Silicon Valley como el que se asienta en California junto a la Universidad de Stanford y constituido por un núcleo de grandes empresas de tecnología (como Apple, Google y otras). La combinación de universidades tecnológicas, incubadoras de empresas, inversionistas expertos en gerencia y, por supuesto, innovadores con una idea de un producto nuevo dispuestos a crear su empresa, ha resultado en el ejemplo del desarrollo económico cuantitativa y cualitativamente más importante en este siglo. [5]

Se puede decir que la zona, en la bahía de San Francisco en el norte de California, ha sido la capital mundial del emprendimiento, generando un flujo aparentemente infinito de distintas tecnologías, nuevas empresas y enorme riqueza.[3]. Silicon Valley es uno de esos lugares privilegiados de la innovación, donde la denominada sociedad del conocimiento ha expresado sus cualidades particulares, su capacidad para acumular creatividad, desarrollo tecnológico, dinamismo innovador y riqueza.[2]

La capacidad innovadora de las empresas, el uso flexible de nuevas tecnologías, la colaboración con otras empresas, la complementariedad de los trabajadores o las características generales de las ciudades son claves de la nueva organización productiva.[2]
Se convirtió en un medio de innovación por la convergencia en este sitio del nuevo conocimiento tecnológico, de un gran mercado de expertos ingenieros y científicos de las principales universidades de la zona, de financiamiento generoso [3].

Historia

Tras la Segunda Guerra Mundial, la Universidad de Stanford recibió una gran cantidad de subvenciones por parte del gobierno para el desarrollo de tecnologías militares. Con esta base, nació en la región una importante industria tecnológica de forma que poco a poco, y ayudándose del elevado crecimiento tecnológico que suponía la universidad, fueron surgiendo compañías en este sector. [7]

Pero la representación universitaria en el ámbito tecnológico en Silicon Valley no se limitó a la Universidad de Stanford; de esta forma, durante los años sesenta y setenta, la Univcersidad de Berkeley se convirtió en otro generador de innovaciones, llegando a mediados de los años setenta a lograr el mismo número de ingenieros electrónicos que Stanford y el Massachussets Institute of Technology (MIT).

Paralelamente, la Universidad de Stanford se fue centrando cada vez más en la relación con las empresas y la industria local, por encima de la relación con el gobierno. Estos vínculos con las empresas de la región se llevaron a cabo a través de varios instrumentos. Muestra de ellos son:

- El Stanford Research Institute (SRI), encargado de colaborar con empresas del sector en labores de investigación y desarrollo tecnológico [7].

- El Stanford Industrial Park, un parque industrial enfocado hacia el mercado tecnológico. [7]

- Los distintos cursos y seminarios para empresas realizados en el campus universitario. [7]

Posteriormente, otras instituciones como San José State University o la Foothill College de Los Angeles, fueron completando esta oferta universitaria hasta lograr convertir a Silicon Valley en la región más importante de estudios tecnológicos de los Estados Unidos. [7]

Como generar una compañía en Silicon Valley

Para que una compañía nazca en Silicon Valley se necesita [4]:

- Inspiración

- Empeño

- Formación de un equipo

- Concentración en la actividad

- Redacción del plan de la empresa

- Negociación de un acuerdo

- Arranque de la empresa

Sin embargo el alto índice de movilidad entre los profesionales de Silicon Valley se ve favorecido por la escasez de personal cualificado y con experiencia, otra razón de alta movidlidad es del deseo de obtener información técnica de la competencia, es decir, un ingeniero que deje una compañía para ir con otra, probablemente firmará un acuerdo para no revelar información secreta de su empresa, incluso cuando la haya dejado, sin embargo, el hecho de dejar una compañía no impide el retorno; tras seis meses o un año en una compañía competidora, un ingeniero puede ser contratado de nuevo por la compañía original, en parte para obtener información de la competencia. [4]

La transferencia de empleados clave de una firma a otra ayuda a producir una especie de “fertilización” en Silicon Valley. No existe un medio legal para borrar lo que hay en la cabeza de alguien. Si un empleado es verdaderamente valioso, su antiguo patrón puede demandarlo, pero esto es ante todo una manera de retenerlo por retrasar la contratación por la otra firma.[4]

Secreto de empresa

Una alternativa a la patente "es el secreto de empresa", estrategia mediante la que la innovación se mantiene a cubierto después de su desarrollo y antes de que se ponga en marcha su explotación comercial. Esencialmente un secreto de empresa de cualquier cosa que la compañía declare como tal. Los competidores de la empresa innovadora pueden tratar de develar el secreto a través de la "ingeniería inversa", práctica corriente que consiste en comprar un nuevo producto y desmontarlo para ver cómo está hecho.[4]

Una de las contra estrategias para proteger un secreto de empresa contra la ingeniería inversa, se conoce como "empaquetado" y consiste en empaquetar la innovación de tal manera que sea muy difícil abrir la carcasa sin destruir la innovación que hay dentro; ninguna técnica es completamente efectiva a largo plazo, pero permiten que una empresa consiga una corta ventaja, de unas semanas o meses. En una industria altamente competitiva, con innovaciones constantes, un periodo breve puede tener mucha importancia y hacer que valga la pena el costo de la ingeniería inversa. [4]

Capitalización

Los problemas de empresa resultantes de la insuficiente capitalización, no son exclusivos de Silicon Valley; en cualquier industria la falta de liquidez equivale a dificultades. Pero cuando la compañía es nueva y está implicado el capital-riesgo, la falta de dinero supone problemas y soluciones características. Las nueva empresas de Alta Tecnología suelen confiar en el capital-riesgo para su financiación inicial[4]. Cumplir los objetivos es importante para una empresa, justificando ante los inversionistas y asegurando la supervivencia durante algún tiempo. Se espera que el producto cause sensación en el mercado y se obtengan beneficios importantes, a veces sucede, pero más a menudo la esperanza se queda en eso, esperanza. La necesidad de disponer de más capital puede forzar a algunas firmas a salir al mercado de valores y animar a las compañías que ya coticen a aumentar su capital, emitiendo más acciones; los rumores de que una empresa va a salir a cotización o que va a realizar una emisión de acciones, son rumores importantes en Silicon Valley, que siguen muy de cerca los cazadores de fortunas.[4]

Para Silicon Valley no basta el trabajo y la plena dedicación, la meritocracia impera, y eso significa que tienes que saber lo que haces, no se trata de a quién conoces o quienes fueron tus padres, o donde fuiste a la escuela, o a que clubs perteneces, se trata de lo que sabes.[4]

La base del éxito de la estrategia llevada a cabo por las empresas de Silicon Valley se puede resumir en los siguientes puntos:

- Renovación de productos y servicios a través de una adaptación al máximo a las necesidades de los clientes, así como de una política de diferenciación más que de reducción de costos.

- Renovación de las estrategias de negocio, que significó una vuelta a la filosofía inicial de las empresas de Silicon Valley.

- Fuerte fragmentación del mercado.

- Uso de redes sociales y técnicas, información compartida, confianza entre clientes, proveedores, etcétera.

Esta estrategia, llevada a cabo por la mayor parte de las compañías de Silicon Valley, permitió una mayor flexibilidad y adaptabilidad al nuevo mercado, caracterizado por una gran competitividad; y por consiguiente, impulsó el éxito de la región.

Las redes e información

El intercambio de información es una característica dominante y distintiva en Silicon Valley. Puesto que la innovación trae consigo un alto grado de incertidumbre, tal innovación depende en gran medida de la información. La proximidad de las empresas facilita la libre circulación de información.[4]

Deberíamos pensar en Sillicon Valley no solo como un lugar , ni tampoco como varios cientos de empresas de alta tecnología, si no como un "entramado". EL poder de este entramado reside en que todos los participantes saben que existe. Todos sabemos que todos nosotros conocemos a mucha gente en el Valley. Esto debido principalmente a la alta tasa de movilidad en el empleo. La cantidad de rumores que circulan por Silicon Valley es sencillamente fenomenal. Reputaciones, éxitos, gente que abandona una empresa, nuevos productos. Una parte de ellos se debe a la proximidad de todas las empresas. Uno puede asomarse a la ventana de su despacho y ver la otra compañía.[4]

Asociaciones y redes empresariales

Desde sus inicios, Silicon Valley se caracterizó por la amplitud y fuerzas de las redes de cooperación formar e informal de las empresas, por un lado, trabajadores (especialmente directivos) por el otro. Aunque fuesen competidores, los directivos de las empresas de Silicon Valley mantenían grandes vínculos informales entre ellos, compartiendo información, técnicas de gestión, y experiencias, e incluso juntándoles tras las jornadas de trabajo para conversar en bares y cafeterías.[7]

Las redes de empresas ayudan a reducir las diferencias entre grandes y pequeñas compañías, dando mayor dinamismo al sector. Esto cobra especial importancia en un mercado como el tecnológico, caracterizado por los múltiples y rápidos cambios que representa; por ello, las empresas que operan en él, han de ser suficientemente flexibles y tener capacidad de adaptación para poder mantenerse en el mismo. En este sentido, las redes ayudan enormemente a que las compañías, tanto si dentro de red son proveedores como clientes, se especialicen en lo que mejor saben hacer, mostrando mayor capacidad de respuesta ante eventuales cambios del mercado.[7]

Así mismo, las relaciones personales entre los directivos de las compañías ayudan a mantener la confianza entre las sociedades. De este modo, los acuerdos de confidencialidad entre empresas resultan menos importantes al existir confianza mutua. En este sentido, la confianza contribuyó directamente a la mejor realización de los negocios entre compañías.[7]

La sociedad

Podemos afirmar que las tecnologías no son únicamente ciencia y máquinas, sino que también forman parte de la tecnología social y organizativa, principalmente si consideramos que los diferentes ámbitos de la sociedad son cada vez más interdependientes. Y que esto ha favorecido e Impulsado a las sociedades postindustriales a distinguirse por el cambio de bienes de producción hacia actividades encaminadas a los servicios, requeridas y favorecidas por los nuevos usuarios de la información.[2]

El papel de la sociedad en la Era de la Información es ser medios productores de innovación y de riqueza, capaces de integrar la tecnología, la sociedad y la calidad de vida en un sistema interactivo, que produzca un círculo ejemplar de mejora, no sólo de la economía y de la tecnología, sino de la sociedad y de la cultura. Las sociedades de la información que lo logren, ocuparían un lugar central en una nueva sociedad. Las que no puedan desarrollar medios sociales, económicos y tecnológicos innovadores, permanecerán en los márgenes.[2]

El planeta nunca había estado tan poblado como hoy. Nunca la técnica había permitido al ser humano interactuar con su entorno hasta el punto en que puede hacerlo ahora. Y, por supuesto, jamás había tenido acceso al cúmulo de información que hoy en día está al alcance de cualquiera. En suma, podría decirse que el ser humano nunca tuvo en sus manos tanta responsabilidad: garantizar que los extraordinarios conocimientos que ha llegado a poseer se utilicen para el bien. [2]

Usuarios sociedad de información

Quienes son los que están inmersos en las sociedades de información y para quienes es todo lo que se desarrolla en Silicon Valley, debemos comenzar por definir quiénes son realmente los usuarios de la Sociedad de la Información y hacer una clasificación de los mismos de acuerdo a su función principal. [6]

Los usuarios son los ciudadanos y organizaciones que participan de la Sociedad de la Información a través de la generación, uso y difusión de la información. Podemos identificar varios tipos de usuarios de acuerdo a su función en la Sociedad de la Información:

Ciudadanos. Todos aquellos que participan de la SI independientemente de su actividad profesional.

Empresas. Toda organización productora de bienes y servicios que incorporan las TIC para el desarrollo de su actividad empresarial.

Gobierno. Toda organización de la Administración Pública que desarrolla y administra servicios a los ciudadanos y de bienes públicos incorporando las TIC.

Centros Tecnológicos. Toda organización que trabaja directamente en el sector de las TIC, ya sea en la administración de las telecomunicaciones (Empresas de Telecomunicaciones) como el desarrollo de investigaciones y productos para el sector de las TIC.

Investigadores. Los investigadores que trabajan en el sector de las TIC generando una capacidad nacional de investigación y adaptación de las tecnologías a las exigencias propias de cada contexto para el desarrollo de la Sociedad de la Información, ya sean estos en áreas netamente tecnológicas como en áreas de desarrollo social.

Organizaciones sociales. Las organizaciones que trabajan en la difusión y en el uso de las TIC con impacto social, como ser ONG, grupos de ciudadanos organizados, grupos indígenas.[6]

Se puede considerar a Silicon Valley como un claro ejemplo de región que ha vivido un importante desarrollo en las últimas décadas, una de las principales causas de ese desarrollo ha sido el buen uso del capital social, tanto a través de políticas implantadas desde las instituciones locales, como de prácticas llevadas a cabo de manera informal por parte de los empleados de empresas.[7]

Política actual y futuro incierto

Ahora que la sorpresa por el triunfo de Donald Trump comienza a diluirse, es hora de analizar el potencial impacto de las propuestas de quien será el presidente de Estados Unidos.

Con Trump, el futuro está lleno de incertidumbre en numerosos ámbitos y en el mundo de la tecnología no se sienten una excepción. La Fundación para la Tecnología de la Información e Innovación (ITIF, por sus siglas en inglés) -una asociación sin fines de lucro con base en Estados Unidos- llevó a cabo una investigación sobre el asunto.

- Más seguridad y menos privacidad [8]

A raíz de los ataques de San Bernardino, California, el Buró Federal de Investigaciones de Estados Unidos (FBI, por sus siglas en inglés) le pidió a Apple que debilitara la encriptación de su iPhone para favorecer la investigación.

La empresa se negó, alegando que la privacidad de sus usuarios era más importante, una postura que fue respaldada por la mayoría de la comunidad tecnológica. Pero no por Donald Trump. La llamada al boicot de Apple surgió en un momento de acaloramiento. El asunto del boicot no se tomó muy en serio. Pero esas no fueron las únicas declaraciones de Trump en cuanto a la vigilancia de Estado.

Hablando sobre el controversial poder de la Agencia Nacional de Seguridad (NSA, por sus siglas en inglés) dijo lo siguiente:

"Yo asumo que cuando contesto al teléfono hay gente escuchando mis conversaciones. Es una observación muy triste, pero peco de exceso de seguridad".

En cualquier caso, afirmó que quiere restaurar la Ley Patriota, la cual se utilizó para dar a la NSA poderes para acceder a grandes volúmenes de datos, hasta que fue abolida por el Congreso. Al igual que con administraciones anteriores, podemos esperar que la guerra contra el terrorismo sea la principal justificación para que existan esos poderes.

En lo que respecta a encriptación, la disputa con Apple le dio a Trump la oportunidad de dejar claros sus puntos de vista. Y sus actitudes parecen estar firmemente asentadas en anteponer la seguridad a la privacidad.[8]

- Talento extranjero bajo el punto de mira [8]

Una de las cosas que preocupan a las firmas tecnológicas es el futuro de la visa de trabajo H1-B.

Este tipo de visado es considerado fundamental por las compañías tecnológicas que quieren llenar sus filas con desarrolladores e ingenieros especializados. Se trata de un permiso de residencia temporal, pero las empresas pueden optar por patrocinar a los empleados para que se queden en EE.UU. de forma indefinida.

Trump sostiene que la visa H1-B se está utilizando de forma abusiva para traer mano de obra más barata, y no personal cualificado.

Trump está a favor de la inmigración de trabajadores altamente cualificados, en especial cuando emigran para estudiar en las mejores escuelas y universidades estadounidenses.

Lo más probable es que modifique o anule la visa H1-B y trate de implantar una alternativa que restrinja lo que él ve como abusos del sistema actual. [8]

- Mayor disposición a ciberataques [8]

Los ciberataques son cada vez más frecuentes, potentes y peligrosos. Los analistas de la compañía de seguridad Forrester Research predijeron este miércoles que "en los 100 primeros días, el nuevo presidente se enfrentará a una crisis cibernética".

Y mientras gran parte del debate en el periodo previo a los comicios giró en torno al posible control de Trump sobre los códigos nucleares, hay preguntas en el aire sobre cómo manejará la creciente amenaza cibernética por parte de China, Rusia y grupos de hackers independientes.

Trump también se mostró reacio a seguir el ejemplo del FBI en culpar a Rusia por el hackeo de la Convención Nacional Demócrata (uno de los varios ciberataques que fue probablemente determinante en el triunfo de Trump).

En cualquier caso, Trump no será la primera persona en el poder que tiene una comprensión limitada sobre cómo funciona la tecnología, por eso fueron más importantes sus políticas en general que su experiencia.

A diferencia de las guerras tradicionales, en las cuales los aviones pueden ser vistos en el cielo o los tanques sobre el terreno, a la ciberguerra es mucho más difícil seguirle la pista.

Puede que nunca lleguemos a conocer las ideas concretas de Trump sobre las posibilidades de ataques cibernéticos de Estados Unidos, y podrían ser dictadas en secreto. La página web de su campaña proporciona descripciones vagas sobre lo que haría su administración, incluyendo una "revisión inmediata de todas las defensas y vulnerabilidades cibernéticas de EE.UU." También dijo que quería desarrollar las capacidades ofensivas para que el país pueda tomar represalias contra ciberataques. Esto no sería algo sin precedentes, pues EE.UU. ya utilizó armas cibernéticas en el pasado.[8]

- El fin de la neutralidad en internet [8]

Desde hace algún tiempo se sostiene un áspero debate sobre el control del tráfico de internet.

Los Proveedores de Servicios de Internet (ISP) solicitaron la capacidad de proporcionar lo que sería una vía rápida de internet para servicios que usan grandes cantidades de datos, como Netflix.

Los ISP cobrarían a las compañías que estuvieran en ese carril rápido, una medida descrita por la mayoría de la comunidad tecnológica como extremadamente anticompetitiva y contra el espíritu de la propia internet.

Hoy en día existe neutralidad en internet porque todo el tráfico de la red es tratado de manera igualitaria.

Trump, probablemente, no pasó mucho tiempo pensando en lo que significa la neutralidad en internet. Tiene sentido decir que no es su mayor preocupación ni está en su lista de prioridades.

Además, el sistema judicial estadounidense se ha pronunciado a favor de los principios de neutralidad. En cualquier caso, esta y otras cuestiones -como la tecnología energética- generan incertidumbre, frustración y una creciente fragilidad en la sede global de la innovación tecnológica.[8]

3.1 Conclusiones

Se puede decir que la tecnología no determina la organización social, sino que es la propia sociedad y el sistema económico vigente quienes se encargan de adaptar a las nuevas necesidades los avances tecnológicos que van surgiendo. Esta nueva tecnología ha tenido, está teniendo y tendrá un fuerte impacto en la sociedad, pero sus efectos varían en interacción con procesos políticos, sociales y culturales que determinan la producción y el uso de los nuevos medios tecnológicos.[2]

Descubriremos cada vez más que podemos adaptar los lugares existentes a las nuevas necesidades conectando de nuevo el equipamiento, modificando la informática y reorganizando las conexiones red, sin necesidad de demoler las estructuras físicas y construir otras nuevas.[2]

Podemos concluir que la filosofía que llevó al éxito económico de la industria tecnológica en Silicon Valley se basó en los tres siguientes factores:

- Alto nivel de competitividad entre las empresas.
- Alto nivel de confianza entre las empresas.
- Alto nivel de dependencia entre empresas.

Los pioneros de Silicon Valley lograron romper las tradicionales barreras que separan las relaciones laborales de las sociales, las empresas de los empleados, los directivos de los subordinados, y las empresas de las instituciones públicas locales. Este logro, y su mantenimiento a lo largo del tiempo, es el principal factor que, en un primer momento, impulsó el espectacular desarrollo económico de la región. [7]

Tal y como se llevó a cabo en Silicon Valley, este tipo de filosofía ha de estar respaldada desde las instituciones públicas a través de políticas que fomenten el desarrollo del capital social, de forma que, permitiendo un elevado grado de competencia entre compañías, éstas mantengan un alto grado de confianza e interdependencia. [7]

Dichas políticas son mucho más efectivas cuando se deciden y llevan a cabo desde la óptica regional, que cuando se hacen desde un ámbito nacional; por ello, para lograr una trayectoria adecuada de desarrollo económico, tan importante como las políticas macroeconómicas o sectorial, es la política regional que debería orientarse hacia ls construcción de sistemas industriales más descentralizados que potencien conjuntamente la competencia y la colaboración entre empresas a través del empleo e impulso del capital social. [7]

Para el tema de política actual, ciertamente, Trump no querrá pasar a la historia como el presidente que destruyó Silicon Valley, pero lo que preocupa es que las pocas políticas que han sido explicadas en detalle se contradicen.

Silicon Valley está en Estados Unidos, pero no es un sueño enteramente "estadounidense". Su éxito se forjó por ser un destino atractivo y progresista para los mejores cerebros del mundo.

Y a la industria le preocupa que pueda verse amenazado.[8]

3.2 Referencias

[1] Vint Cerf. Silicon Valley: cómo logró California hacerlo tan bien www.bbc.com

[2] Altamirano Martínez M. Silicon Valley: Cambio Elemental y Significativo en las Sociedades de la Información o Informacionales.

[3] Rogers, E. M., & Larsen, J. K. (1984). Silicon Valley fever: Growth of high-technology culture. Basic Books (AZ).

[4] Judith K. Larsen Everett M. Rogers.(1986) La fiebre del Silicon Valley

[5] Ogliastri, Enrique (2015) ChileconValley

[6] Pablo Valenti López. (2002) La Sociedad de la información en América Latina y el Caribe: TICs y un nuevo Marco Institucional

[7] Pablo Galaso. (2005) Capital Social y desarrollo económico. Los casos de Silicon Valley y Villa El Salvador.

[8] http://www.bbc.com/mundo/noticias-37937223

[9] http://www.redalyc.org/html/859/85902707/

La gestión de servicios de TI orientada al cliente

VELÁZQUEZ, Leonardo

L Velázquez

Universidad Iberoamericana

P. Solares (eds.) Ciencias de los Sistemas de Información y Seguridad. Handbook T-I. -©ECORFAN, Ciudad de México, 2016.

Abstract

The current business environment requires the services of Information Technology (IT) support and promote good practices to generate business value, not only for the development of products and/or services or technological issues , but also providing value to customers in the form of services. The capabilities of IT professionals are changing, communication and understanding with the business is demanding organizations, in addition to talking to interact with technology must reach all areas and change the paradigm to provide only infrastructure. Under this approach, this article proposes the ITIL framework reference that generate added value through a service management system, which enable strategically, knowledge management and innovation. To do this, we will review the basics of IT Service Management, IT Governance, the Lifecycle service and presentation of Practice ITSM study that aims to support initiatives related management services.

4 Introducción

La información dentro de las organizaciones se considera como el recurso intangible más importante [1], dado que permite apoyar la toma decisiones, bosquejar los horizontes del negocio y seleccionar las mejores alternativas para solucionar una necesidad particular. El apalancamiento de las Tecnologías de la Información y Comunicación -(TI)- es vital en el almacenamiento, gestión y análisis de este activo [2], en orden de lograr los objetivos en pro del mejoramiento continuo, lo que redunda en la generación de valor. La Gestión de Servicios TI no es solo un tema tecnológico; el mercado ha cambiado y se ha globalizado, por lo que hoy es un tema relacionado con el negocio de la empresa.

Sin embargo, para poder generar un valor diferenciador en cada uno de los interesados al usar las TI dentro y fuera de una organización, se requiere tener las metas estratégicas correctamente planificadas a través de estrategias de gobernanza claras, en las cuales todos los sectores de la empresa se sumen, incluyendo la alta dirección y los ejecutivos, así como actores externos que hayan sido previamente seleccionados para participar en las dinámicas de la organización [3].

El mundo moderno ha llevado a las empresas a ser cada vez más competitivas, volviendo al cliente el eje central de los procesos de comercialización, pero evidenciando la necesidad de tratar todas las actividades internas como clientes parciales en el proceso de entrega del producto o servicio a los consumidores finales. Un elemento necesario para asegurar un adecuado nivel de calidad a los clientes radica en la necesidad de gestionar adecuadamente los servicios requeridos en los procesos empresariales, donde la gestión de los servicios de tecnología se vuelve un imperativo en casi todas las empresas [4].

Una mejor práctica es una forma de hacer las cosas o una serie de principios generalmente aceptados en un ámbito profesional, y que sirven para aportar valor de negocio; en el caso de las TI, a través del manejo de la información. Pero antes de revisar un marco de referencia o mejor práctica es importante poner en contexto la importancia de la satisfacción del cliente siendo el reto a vencer por las áreas de tecnología. Los clientes satisfechos son la clave del éxito en todas las organizaciones de servicio, por lo cual las organizaciones deben de buscar métodos para lograr niveles de satisfacción mayores que su competencia. Y la única forma de hacerlo es teniendo fundamentos de que es lo que satisface al cliente y en base a esto diseñar tu servicio. Aunque muchas organizaciones saben que cumplir la satisfacción de sus clientes es la mejor forma de lograr el éxito, la mayoría fracasa, no por la falta de empeño en la calidad de sus servicio, si no por la mala planeación de esta.

La calidad en el servicio debe ser un acto planeado delicadamente en el cual la organizaciones deben asegurase que los objetivos estén estrechamente vinculados con los elementos que conforman su sistema de calidad, teniendo en cuenta que esto, es algo que nace de un profundo análisis de las necesidades del mercado y el conocimiento preciso de las expectativas de cada uno de sus clientes [5].

Considerando lo anterior, la alta dirección de una empresa en la actualidad espera que su departamento de sistemas y/o tecnologías de información responda con agilidad y de manera innovadora a nuevas oportunidades de negocio, para soportar entre otros aspectos, una gestión empresarial responsable, y con ello satisfacer las necesidades de información de sus clientes tanto externos como internos. En consecuencia, a medida que las organizaciones van ganado experiencia con metodologías orientadas a procesos de la gestión de servicios de TI, se ha hecho evidente la necesidad de incorporar marcos de mejores prácticas en la gestión de servicios de TI [6].

Cada día en mayor medida las organizaciones dependen de TI para cubrir las necesidades del negocio y crecer y/o, al menos, perdurar en su actividad. Esta dependencia requiere cada vez una mayor calidad de los servicios TI y se consigue mediante unas buenas directrices de Gestión de Servicios de las TI, políticas, principios, buenas prácticas y métodos que aplicados al unísono, faciliten la mejora continua de cualquier tipo de servicio [7].

Este artículo busca ser una referencia útil para las organizaciones que deseen incorporar el concepto de valor en la fase de identificación de necesidades en procesos de Gestión de Servicios de TI apoyándose en el control, el seguimiento, la gestión y la mejora continua de las actividades.

Gestión de servicios de TI

La Gestión de Servicios TI se conoce en principio como el planteamiento orientado al proceso y al servicio de los que fue una vez la Gestión de TI. El objetivo de los procesos de Gestión de Servicios TI es contribuir a la calidad de los servicios TI, buscando satisfacer una necesidad sin asumir directamente las capacidades y recursos necesarios para ello. La gestión de calidad y el control de procesos forman parte de la organización y sus políticas [8].

Una correcta gestión de servicios requiere:

- Conocer las necesidades del cliente
- Estimar la capacidad y recursos necesarios para la prestación del servicio
- Establecer los niveles de calidad del servicio
- Supervisar la prestación del servicio
- Establecer mecanismos de mejora y evolución del servicio

En la actualidad las áreas de TI que simplemente cumplen tareas específicas para la gestión y configuración de servidores, la red, soporte técnico, actualización de equipos, instalación y desarrollo aplicaciones, etc. son insuficientes para las organizaciones. Las demandas actuales de los mercados para la función de TI es cumplir con más requisitos: una gestión eficaz, el funcionamiento predecible y fiable, eficiente en términos de recursos (tiempo y dinero), con bien definidos y los procesos y funciones automatizadas y es evidente que las responsabilidades deben definirse.

El aumento de la utilización de modelos y estándares tienen planteado nuevos retos y nuevas exigencias, tales como: dar a conocer el propósito de la negocio y los beneficios de estos modelos, la ayuda en la toma de decisiones utilizando las mejores prácticas e integrando con ellos las políticas internas, procedimientos, la adaptación de los modelos y el nivel de los requisitos específicos de la organización [9].

La gobernanza en las TI se perfila como el medio para optimizar la creación de valor usando las TI. Esto por permitir minimizar los riesgos, maximización del uso de los recursos, y una visión holística desde la perspectiva organizacional [11].

Gobernanza de las TI

La Gobernanza se define como el sistema mediante el cual el uso presente y futuro de las TI es dirigido y controlado, el cual considera la evaluación y dirección de planes para su uso, en orden de apoyar los objetivos de la organización y monitorear su uso para ejecutar el plan, incluyendo estrategias y políticas transversales a la organización [12].

La alineación de las TI con la estrategia del negocio facilita la toma de decisiones, la asignación de roles proveedores de información relevante, el involucramiento de niveles directivos y operativos en procesos tan importantes como la mejora de procesos, entre otras ventajas [13]. De acuerdo a diferentes metodologías para aplicar el concepto de gobernanza TI, uno de los primeros pasos es la identificación y satisfacción de necesidades de los involucrados [14]. Existen multitud de definiciones y caracterizaciones de Gobierno de TI, entre las que destacan:

- COBIT 5: el gobierno de TI asegura que las necesidades, condiciones y opciones de las partes interesadas son evaluadas para determinar los objetivos de empresa acordados y equilibrados que han de ser alcanzados; establecer la dirección mediante la priorización y toma de decisiones; y supervisando el rendimiento y el cumplimiento respecto a la dirección y objetivos acordados [15].

- ITGI (IT Governance Institute): el gobierno de TI es responsabilidad del comité de dirección y de los ejecutivos. Es una parte integral del gobierno de la organización y consiste en el liderazgo y las estructuras y procesos organizativos que aseguran que las TI de la organización sostienen y extienden la estrategia y los objetivos de la organización (16).

- ISO 38500: el gobierno de TI es el sistema mediante el que se dirige y controla el uso actual y futuro de las TI [17].

El ciclo de vida del servicio y la gestión de servicios (ITSM)

ITIL es un marco de buenas prácticas y conceptos para la gestión y desarrollo de servicios de TI, brinda un esquema para la Gestión de Servicios enfocándose en la mejora continua de la calidad del servicio otorgado al cliente o usuario y del negocio. El Ciclo de Vida del Servicio es un aporte importante para gestión de las áreas de Tecnología poniendo énfasis en las 5 fases de ITIL que corresponden a los 5 libros: Estrategia, Diseño, Transición, Operación y Mejora Continua de los servicios proporcionados al negocio, mediante diferentes funciones para la gestión de los servicios a lo largo de su ciclo de vida con ello se intenta conseguir beneficios tales como establecer la integración de la estrategia del negocio con la de los servicios de TI. Este enfoque se ha convertido en el factor clave para el éxito de ITIL teniendo como objetivo ofrecer una visión global de la vida de un servicio [18].

La Gestión de Servicios o ITSM es una disciplina basada en procesos, enfocada a alinear los servicios de IT proporcionados, con las necesidades de la empresa, poniendo énfasis en los beneficios que puede obtener el cliente final. Supone dejar de centrarse en el aspecto tecnológico del negocio para dar un mayor peso a la calidad de los servicios ofrecidos y la relación con los clientes [19].

Los retos de la gestión de TI son coordinar y trabajar en alianza con el ámbito del negocio para poder ofrecer servicios de TI de alta calidad. Para ello debe adoptarse una posición más orientada al cliente y al negocio en la entrega de los servicios junto a una mayor optimización de costes. El principal objetivo de la Gestión de Servicios es asegurar que los servicios de TI están alineados con las necesidades de negocio y que las apoyan activamente. Los servicios de TI no sólo ofrecen la base de los proceso de negocio, sino que actúan cada vez más como un agente de cambio que facilita la transformación del negocio [20].

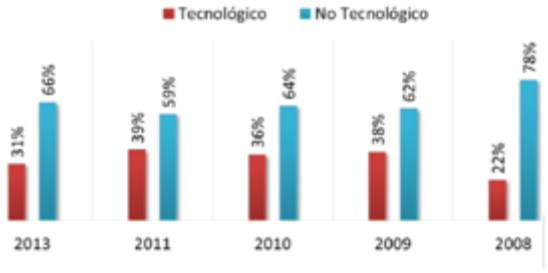
El Estado Actual de la Implementación de ITIL, "Prácticas de ITSM en México y Latinoamérica".

Para conocer el estado actual de utilización e implementación del marco de referencia ITIL, se analizaron los resultados obtenidos del estudio anual practicado en México y Latinoamérica por la firma Customer Care Associates (México), el Tecnológico de Monterrey (ITESM) y la Universidad Iberoamericana realizado con el objetivo de apoyar las iniciativas relacionadas con la gestión de servicios de T.I., denominado "Prácticas de ITSM en México y Latinoamérica" (PITSMLatam2014).

El estudio está basado en los datos obtenidos a través de una encuesta en línea aplicada desde el año 2008 hasta febrero de 2013; consta de 62 preguntas (tanto de tipo abierto como de tipo cerrado); el 76% de los participantes se encuentra vinculado con actividades en de T.I.; la encuesta cuenta con participación de los siguientes países: México, Colombia, Estados Unidos, Ecuador, República Dominicana, Canadá, España y Venezuela, en donde México es el país donde mayor participación se ha tenido -en promedio 91%- (Figura. 1); por tipo de industria a la que pertenecen (Figura. 4) la mayor participación se encuentra en las empresas del sector tipo no tecnológico con el 66% en promedio -Sector educación, gobierno y financiero [21].

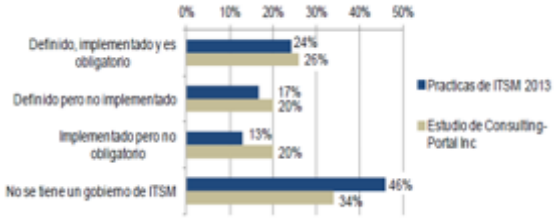
Figura 4 Porcentaje de países participantes en el estudio PITSMLatam2014

Figura 4.1 Tipo de industria a la que pertenecen las empresas participantes



En el estudio se destacan los resultados del estado en el que se encuentra el gobierno de ITSM dentro de las empresas encuestadas (gestión de servicios de TI) con los siguientes resultados: Solamente un 24% afirman tener un gobierno de ITSM que está definido, implementado y que es obligatorio, el 46% de los encuestados aún no tienen un gobierno de ITSM dentro de la gestión de servicios de TI (Figura.3). El estudio de Analysis 8th Annual ITSM Industry Survey of Consulting-Portal's Inc presenta un 34% en este sentido [21].

Figura 4.2 Estado actual del gobierno de ITSM



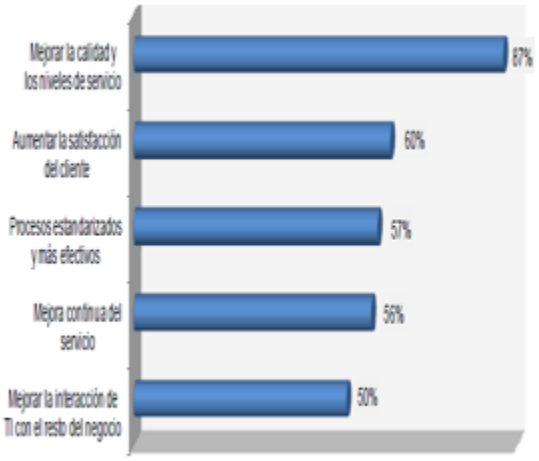
Por ello, como resultado evidente, al cuestionar el principal motivo que impulsó a la organización a implementar un marco de buenas prácticas como lo es ITIL, se destaca que la razón que prevalece en la encuesta más reciente (2013) es la de "mejorar la calidad en el servicio" con un 41%, seguida del incremento significativo a partir del 2010 (43 %) de la razón "mejorar la alineación estratégica entre T.I. y el negocio" [21].

Tabla 4 Principales razones para implementación de ITIL

Razones para implementar ITIL	2013	2011	2010	2009	2008
Mejorar la calidad en el servicio	**41%**	21%	22%	**33%**	**58%**
Mejorar a alineación estratégica entre T.I. y negocio	32%	**34%**	**43%**	10%	5%
Mejorar el desempeño de T.I.	16%	17%	12%	8%	20%
Incrementar la satisfacción del cliente/usuario	8%	18%	14%	17%	10%
Mejorar la productividad de T.I.	-	4%	8%	7%	7%
Otro	2%	5%	2%	26%	-

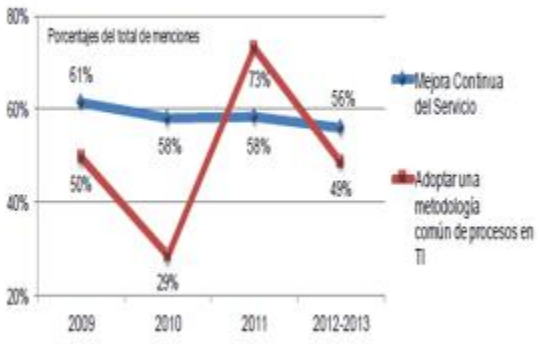
Los beneficios más importantes que consideran las empresas en la adopción de ITIL son: mejorar la calidad de los niveles de servicio (87%), aumentar la satisfacción del cliente (60%), tener procesos estandarizados y más efectivos (57%), mejora continua del servicio (56%), mejorar la interacción de TI con el resto del negocio (50%) ver (Fig.4.3).

Figura 4.3 Beneficios más importantes en la adopción de ITIL



En este mismo sentido en el estudio los encuestados manifestaron como uno de los beneficios de la adopción de ITIL que las empresas veían en el 2011 era adoptar una metodología común de procesos en TI, éste cambio a la mejora Continua del Servicio para el 2012 (Figura. 4.4).

Figura 4.4 Beneficios de la adopción de ITIL



Algunos de los beneficios de ITIL incluyen: incremento de la satisfacción del cliente/usuario con los servicios de TI; mejora la disponibilidad del servicio, que conduce directamente al aumento de los beneficios empresariales y los ingresos; ahorro financiero al reducir re-trabajo, pérdida de tiempo, mejora en la gestión y uso de los recursos; mejora el tiempo de salida al mercado de nuevos productos y servicios; mejorar la toma de decisiones y optimizar el riesgo [22].

4.1 Conclusiones

En consecuencia con los resultados del estudio y la información citada por los diferentes autores se pude ver la importancia de la Gestión del Servicio entre otros aspectos, como parte fundamental de la empresa y su alineación con el negocio que representará la capacidad organizacional y sostenible de gobernar y administrarse para la consecución de los objetivos. Las TI deben estar alineadas por una Gestión de Servicios en el cual se soporten, amplíen y desarrollen las estrategias y objetivos corporativos en el desarrollo de la creación de valor. Hay que dejar muy claro que las mejores prácticas son complementarias; ninguna por sí sola habilita o soluciona todos aspectos de TI. La Gestión de Servicios de TI requiere de una integración correcta de tres factores: personas, procesos y tecnología poniendo énfasis en los beneficios que puede percibir el cliente final.

4.2 Referencias

[1] Rojas, Y. (2004). Organización de la información: un factor determinante en la gestión empresarial. ACIMED, 12(2), 1-1.

[2] Gómez, A., & Suárez, C. (2005). Sistemas de información: herramientas prácticas para la gestión empresarial. Madrid: Ra-Ma Editorial.

[3] González, Mauricio, & González, Liliana. (2015). La co-creación como estrategia para abordar la gobernanza de TI en una organización. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (15), 01-16. https://dx.doi.org/10.17013/risti.15.1-16

[4] Gil-Gómez, Hermenegildo, Oltra-Badenes, Raúl, & Adarme-Jaimes, Wilson. (2014). Service quality management based on the application of the ITIL standard. DYNA, 81(186), 51-56. Retrieved February 05, 2016, from http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0012-73532014000400006&lng=en&tlng=en. 10.15446/dyna.v81n186.37953

[5] Berry, L. L. (2002). Un buen servicio yano basta 4 principios del servicio excepcional al cliente. Grupo Editorial Norma

[6] T Lucio-Nieto, RC Palacios, A Mora-Soto.(2012). Hacia una Oficina de Gestión de Servicios en el ámbito de ITIL

[7] Delgado, Agustín Prieto, & Velthuis, Mario Piattini. (2015). Propuesta de marco de mejora continua de gobierno TI en entidades financieras. RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação, (15), 51-67. https://dx.doi.org/10.17013/risti.15.51-67

[8] Van Haren Publishing (2007).Fundamentos de gestión de servicios TI: basado en ITIL

[9] Félix-Sánchez, A., & Calvo-Manzano, J. (2015). Comparison of models and standards for implementing IT service capacity management. Revista Facultad De Ingeniería, 1(74), 86-95

[10] Van Grembergen, W., & De Haes, S. (2009). Enterprise governance of information technology: achieving strategic alignment and value: Springer Science & Business Media.

[11]Grossi, L., & Calvo-Manzano, J. A. (2011). Análisis de decisiones en la selección de Proveedores de tecnologías de la información: una revisión sistemática. RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação,(8), 67-79.

[12] Calder, A. (2008). ISO/IEC 38500: the IT governance standard: IT Governance Ltd.

[13] De Haes et al., 2013; Zhang & Chulkov, 2011

[14] De Haes et al., 2013; Feltus, 2012; Zutshi, Creed, Wood, & Couchman, 2009

[15] ISACA (2012). COBIT 5 Implementación. Rolling Meadows, IL, EE.UU.

[16] ITGI (2002). IT Governance Executive Summary, IT Governance Institute

[17] ISO/IEC (2008). ISO 38500: 2008 ISO/IEC standard for corporate governance of information technology. Ginebra.

[18] Hoerbst, A., Hackl, W.O., Blomer, R. and Ammenwerth, E., The status of IT service management in health care - ITIL® in selected European countries. BMC Medical Informatics and Decission Makers. 11 (1), 76, 2011.

[19] Office of Government Commerce (OGC- UK) The Official Introduction to the ITIL Service Lifecycle.

[20] APMG (2008)."ITIL Service Management Practices: V3 Qualifications Scheme".

[21] Lucio-Nieto, T. & González-Bañales, D. L., Por publicar 2015. Prácticas de ITSM en México y Latinoamérica 2014 Estudios anuales 2008-2013. Universidad Iberoamericana

[22] Lucio-Nieto, Ricardo Colomo Palacios, Arturo Mora-Soto. Hacia una Oficina de Gestión de Servicios en el ámbito de ITIL. Instituto Tecnológico y de Estudios Superiores de Monterrey. 2012

El valor de contar con buen service desk

GONZÁLEZ, E.

E. González

Universidad Iberoamericana

P. Solares (eds.) Ciencias de los Sistemas de Información y Seguridad. Handbook T-I. -©ECORFAN, Ciudad de México, 2016.

Abstract

ITIL® provides the best practices and processes that enable technology areas manage and deliver better services and is used to meet the needs of customers and their priorities, more and more companies are implementing an IT service management model based on ITIL®. But even with the ITIL® methodology adopted in a large number of companies they can't improve their level of service management, so some factors become barriers to successful implementation of ITIL®, most companies invest in other ITIL® processes and neglect the value of the Service Desk. In this article, we review ITIL®, ITSM and Service Desk and identify the functions that are necessary today to give value to a Service Desk.

5 Introducción

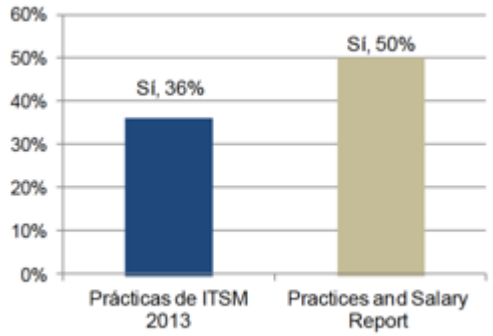
El valor es el núcleo del concepto de servicio. Desde la perspectiva del cliente valor consta de dos componentes principales utilidad y garantía. La utilidad es lo que el cliente recibe y la garantía es la forma en que se proporciona. Un servicio es un medio para entregar valor a los clientes facilitando los resultados que los clientes quieren lograr sin la participación de los costos o riesgos específicos [1]. ITIL® es una importante ventaja en las organizaciones orientadas a los procesos, por que éstos se pueden diseñar para facilitar una metodología orientada al cliente, lo que mejora considerablemente la alineación entre la organización de TI y los clientes [2].

Muchas veces se confunde lo qué es ITIL® [3];

Los términos de ITIL® e ITSM a menudo se intercambian, pero no son sinónimos. ITIL® es un conjunto de publicaciones que se enfoca en la optimización de los procesos para facilitar la gestión del desempeño y conseguir la optimización del servicio de TI. ITSM por su parte se refiere a la prestación de los servicios de TI que requiere el negocio y en última instancia se persigue la mejora del desempeño.

De acuerdo con el 5to estudio anual de prácticas de ITSM 2013 México Latinoamérica, 88% de los encuestados que conoce el término ITIL®, el 36% de las empresas implementan prácticas de ITIL® para sus procesos de gestión de servicios de TI [4].

Figura 5



El estudio Practices and Salary Report del HDI, 2013 registra un 51% en este sentido, 15% por arriba del registrado en el estudio Prácticas de ITSM 2013 como lo indica la Figura 5[4].

Existen 10 razones reales por las cuales fracasan las implementaciones de ITIL® las cuales se describen en la tabla 5 [5].

Tabla 5 Factores que afectan la implementación de ITIL

	Factor clave de fracaso en la implementación de ITIL
1	Insuficiente atención al Cambio Organizacional
2	Pobre relación con la prioridades del negocio
3	Falta de soporte por parte de la alta dirección
4	Gobierno, medición y planeación insuficientes
5	Perspectivas en desequilibrio
6	Se sobrepasa la capacidad de poder lograr el cambio organizacional
7	Comunicaciones deficientes
8	Poca agilidad
9	Selección de la herramienta en una etapa temprana
10	Gestión deficiente de proveedores y consultores

Después de revisar los principales factores clave del fracaso en la implementación de ITIL®, varios de ellos están directamente relacionados con Service Desk. El Service Desk como el único punto de contacto será muy útil para el cambio de cultura y así popularizar ITIL® a través del conocimiento. Por lo tanto un buen Service Desk es de gran valor para la implementación con éxito de ITIL® en la organización.

El Service Desk se centra en la gestión de incidencias del ciclo de vida y realiza las siguientes funciones primarias [6]:

- Interfaz del usuario para el registro y monitorización de cada incidente.
- Servicio de soporte requerido.
- Seguimiento del proceso escalado.
- Cierre del incidente y confirmación con el cliente.

El servicio de registro de incidentes es el principal punto de contacto para los clientes internos y externos. Una buena imagen de Service Desk puede ayudar al departamento de TI a obtener más apoyo económico para la implementación de ITSM y obtener mayor satisfacción de los clientes.

Hace no mucho un Service Desk sólo servía para resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida posible, generaba informes, comunicaba y manejaba peticiones, quejas y observaciones [7]. En la actualidad las instituciones necesitan un Service Desk con más funciones y capacidades más fuertes. En este artículo entregamos una revisión de ITIL®/ITSM y la importancia del Service Desk así como las nuevas funciones que debe tener en las Instituciones.

2.1 Reflexión

ITIL®

ITIL® es un marco de referencia de las mejores prácticas para la gestión de servicios de TI cuyo objetivo es proporcionar valor en la forma de servicios de TI [8].

Las fases, procesos y funciones se mencionan en la figura 5.1 [8];

Figura 5.1 Marco de referencia de ITIL

ITIL® ha evolucionado para satisfacer los problemas que enfrentan las organizaciones. Comenzó su vida en la década de 1980, cuando el Gobierno de Su Majestad en el Reino Unido estaba preocupado por la calidad del servicio de las tecnologías de información, encomendó a la Agencia Central de Informática y Telecomunicaciones el desarrollo de un marco para el uso eficiente y financieramente responsable de los recursos de TI. A medida que maduró se hizo evidente que ITIL® puede y debe existir por encima de los aspectos técnicos, la producción de una guía que no dependa de ninguna tecnología en particular. Desde su concepción ITIL® ha madurado y se ha desarrollado para satisfacer los desafíos que enfrenta la gestión del servicio.

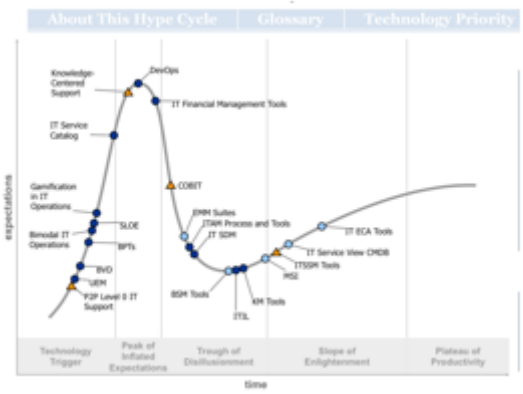
ITSM

ITSM es un marco de mejores prácticas, es un esfuerzo para mejorar la gestión y la eficiencia en TI [9].

Los proveedores de servicios de TI ya no pueden solo centrarse en la tecnología y en su organización interna, ahora tienen que considerar la calidad de los servicios que prestan y centrarse en la relación con los clientes. ITSM se centra en la mejora de calidad y la eficiencia con la que es compatible la infraestructura y la operación para los servicios de los usuarios finales [10].

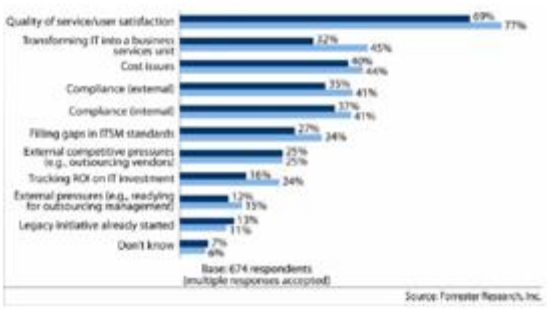
El trabajo de los líderes de TI es desarrollar las estrategias de ITSM y priorizar las inversiones en tecnología (ver Figura 5.2).

Figura 5.2 Estrategias y tendencias en TI



La calidad del servicio así como la satisfacción del usuario son aspectos importantes dentro de una institución y por esa razón es bueno invertir en gestión del servicio, ver Figura 5.3 [11].

Figura 5.3 Razones para invertir en la gestión del servicio



Service Desk según ITIL®

El Service Desk es el principal punto de contacto para los usuarios cuando existe una interrupción del servicio, para las solicitudes de servicio e incluso para algunas categorías de Solicitud de Cambio. El Centro de Servicio proporciona un punto de comunicación para los usuarios y un punto de coordinación para varios grupos de TI [12].

El Service Desk es un servicio que se pide en la gestión de servicios de TI (ITSM) tal como se define por ITIL®. Se tiene la intención de proporcionar un único punto de contacto para satisfacer las necesidades de comunicación de los usuarios y los empleados de TI, también para satisfacer a los clientes y los objetivos de los proveedores. El objetivo es implantar un Centro de Servicios cuyos objetivos se alineen con nuestros procesos de negocio, mejoren la satisfacción de nuestros clientes, optimicen la imagen externa de nuestra organización y nos sirva de plataforma para identificar nuevas oportunidades de negocio [13].

Actualmente los Service Desk no sólo desempeña un punto de contacto en la organización de servicios de TI, las instituciones esperan más ventajas y beneficios. Un buen Service Desk ofrece los siguientes beneficios a las empresas [14];

- Mejorar la percepción de servicio y la satisfacción del cliente.
- Mejorar la calidad y mejorar el tiempo de respuesta en las peticiones del cliente.
- Mejorar el trabajo en equipo y la comunicación.
- Mayor atención y un enfoque proactivo para la prestación de servicio.
- Reducir la Imagen negativa de las áreas de TI.
- Mejorar el uso de los recursos informáticos y el aumento de la productividad del personal de la empresa.
- Información más significativa para apoyar la toma de decisiones.

Funciones para dar valor en la actualidad al nuevo Service Desk

Con el desarrollo de la tecnología y los requerimientos del servicio, el Service Desk desempeña un papel importante en la operación del servicio.

El servicio de recepción no sólo necesita aceptar la solicitud de servicio de forma reactiva, sino también descubrir el problema de manera proactiva [15]. Las funciones para un nuevo Service Desk son;

- Filtrar y Clasificar las solicitudes de servicio.

El Service Desk acepta todas las solicitudes de los usuarios finales, dónde la mayoría de las solicitudes de servicio son sólo para solicitar información relacionada en resolver problemas sencillos, la mayor parte de la solicitud de servicio será resuelto y cerrado por un Centro de Servicio de primer contacto. Un 60% de las solicitudes de servicio son resueltos por el Service Desk directamente, después de eso se categorizan y se asignan a un segundo o tercer nivel, por lo que el Service Desk juega el papel más importante en el departamento de TI , ya que manejan la mayor parte de las peticiones de los usuarios finales[16].

- Responsable del proceso de administración de Incidentes

La gestión de incidentes puede ser definida como una interrupción no planificada de un Servicio de TI o una reducción de la calidad de un servicio de TI. El objetivo de la administración de incidentes es restaurar las operaciones normales tan pronto como sea posible con el menor impacto posible ya sea en el trabajo o el usuario, a un precio rentable [7].

El Service Desk debe ser el propietario del proceso de gestión de incidencias ya que son el punto de contacto principal para asegurar una pronta recuperación del sistema además de supervisar y dirigir los recursos internos o externos.

- Mantenimiento de la base de conocimientos

El Service Desk es el usuario clave de la Base de Conocimiento. En el trabajo diario, el Service Desk puede saber fácilmente qué artículo de la BC es útil, cuál está fuera de fecha y cuál tiene tasa muy baja de resolución. Con este tipo de registros de información el Service Desk debe mantener de forma proactiva la BC. Por ejemplo, pueden promover un artículo de BC debido a su alta tasa de resolución. Con un fuerte BC el Service Desk puede mejorar su eficiencia en el trabajo y resolver los problemas de forma más eficaz para los usuarios finales.

- Encuesta de Satisfacción del Cliente

En la actualidad, la mayor parte de las herramientas de ITSM tienen la función de llevar a cabo la encuesta de satisfacción del cliente de forma automática; esto se hace para ahorrar tiempo y mejorar la eficiencia. Sin embargo, el mismo cuestionario no puede recoger las diferentes voces de los usuarios finales. El Service Desk debe tener un proceso para recoger algunas solicitudes de servicio y devolver la llamada a los usuarios finales para conocer sus comentarios. Tal camino a seguir tan lineal es muy útil para entender las necesidades reales de nuestros clientes, que el departamento de TI deberá usar para mejorar su servicio [16].

5.3 Conclusión

¿Qué necesitamos hacer para contar con un magnifico Service Desk?

Obviamente, un Service Desk tradicional no puede satisfacer las nuevas necesidades de las empresas, por lo que debemos tener en cuenta que para contar con un magnifico Service Desk que realmente de valor a nuestra organización debemos considerar tres perspectivas diferentes, procesos, personas y herramientas.

– Procesos

Proceso es la parte más importante dentro del Service Desk, por que parte de su trabajo es asegurar que todos en la misma línea sigan y usen el mismo lenguaje. Al diseñar el proceso, hay que centrarse en la capacidad de proporcionar de manera eficiente a los clientes y usuarios finales, servicios que satisfagan sus expectativas, también se centra en los mecanismos para evaluar cuantitativamente en mantener y mejorar estos procesos para garantizar su funcionamiento eficaz y eficiente[16].

– Gente

Cumplir con los objetivos de disponibilidad y mejorar los niveles del mismo requiere una mano de obra debidamente capacitada y motivada. El Service Desk debe tener enfoques de gestión de personas que permitan a todo el personal cumplir eficaz y eficientemente sus funciones con servicios de calidad.

– Tecnología

La encuesta revela que el porcentaje de inversión en estrategias de ITSM u otras estrategias relacionadas es bajo, lo que posiciona a la obtención de recursos como un desafío prioritario (Figura 5.4); esto indica la falta de interés por la organización en invertir en ellas, a pesar de que la interrupción en los servicios de TI representa un elemento crítico (Lucio-Nieto & González-Bañales, Por publicar 2015).

Figura 5.4 Inversión en estrategia de TI

En la actualidad, muchos de los productos de Service Desk incluyen características para automatizar el proceso de incidentes. Estos productos también deben tener la capacidad de recoger información de incidentes en tiempo real, tales como datos de hora y fecha. Además, la herramienta debe enviar automáticamente notificaciones, asignar tareas y escalar a las personas adecuadas en función de los criterios de tipo de incidentes, prioridad, hora, estado y personalizados.

5.5 Referencias

Hanna, J. Windebank, S. Adams, J. Sowerby, S. Rance, and A. Cartlidge, ITIL® V3 Foundation Handbook. Norwich, UK: The Stationary Office, 2008. [1]

VAN BON, J. “Fundamentos de la Gestión de Servicios de TI basada en ITIL®® v3”. [2]

Spafford, George; Addy, Rob; Young, Colleen M. (2011). Maverick* Research: How to Avoid ITIL® Failure. Stamford, CT: Gartner, Inc. [3]

Lucio-Nieto, T. & González-Bañales, D. L., Por publicar 2015. Prácticas de ITSM en México y Latinoamérica 2014 Estudios anuales 2008-2013. p. 14. [4]

Head, Ian; Spafford, George. (2012). Successful ITIL® and Service Management Projects Avoid These 10 Common Failings. USA: Gartner, Inc. | G00231188. [5]

R. A. Steinberg, "ITIL® Service Operation," 2011 Edition, Randy A. Steinberg, Trafford, 2011. [6]

J. Van Bon, M. Picper and A. der Veen, "Foundations of IT Service Management Based on ITIL®," 2nd Edition, Van Haren Publishing, Zaltbommel, 2005.[7]

itSMF, "ITIL® COMO UN MODELO DE NEGOCIO" 2012. http://www.itsmfligcdmexico.org/evento7.html. [8]

Axelos Website, "IT Service Management," 2013. http://www.ITILofficialsite.com/home/home.aspx [9]

Gartner, Website, "Hype Cycle for ITSM 2.0, 201http://www.gartner.com/document/3096417?ref=solrAll&refval=165281392&qid=3c0d316e20551aea87efb3797e8a803f5.

Stephen Mann. (2007). ITIL® Global Adoption Rates, USA: Forrester Research.

Official-Site ITIL®, 2011. Official-Site ITIL®. [Online]Available at: https://www.axelos.com/store/book/ITIL®-service-operation.

Official-Site ITIL®.osiatis.es, "Service Desk,"2011. http://ITIL®.osiatis.es/Curso_ITIL®/Gestion_Servicios_TI/service_desk/introduccion_objetivos_service_desk/implementacion_service_desk.php

Official-Site IT SERVICE MANAGEMENT BOOKSHOP, "Service Desk,"2014. http://www.ITIL.org.uk/sm-cost.htm.

M. Toleman, A. Cater-Steel, B. Kissell, R. Chown and M. Thompson, "Improving ICT Governance: A Radical Re- structure Using Cobit and ITIL," In: A. Cater-Steel, Ed., Information Technology Governance and Service Management: Frameworks and Adaptations, Information Science Reference, Hershey, 2009, pp. 178-189.

A. Cater-Steel and W. Tan, "The Role of IT Service Management in Green IT," Australasian Journal of Information Systems, Vol. 17, No. 1, 2010, pp. 3-15.

El bienestar laboral y la felicidad como factores para la productividad y retención de los colaboradores de tecnologías de información en las organizaciones

RAMOS, Gerardo

G. Ramos

Universidad Iberoamericana

P. Solares (eds.) Ciencias de los Sistemas de Información y Seguridad. Handbook T-I. -©ECORFAN, Ciudad de México, 2016.

Abstract

This article describes how the interests, motivators, happiness and wellness of Information Technology collaborators are important factors in achieving the retention of these in the organization; and in this way also achieve collaboration and commitment to benefit the productivity of the organization.

6 Introducción

Las personas cada vez son más dinámicas que las organizaciones, y actualmente, donde el conocimiento de las personas es el más valioso, es un gran riesgo para las organizaciones el perder a sus empleados más valiosos. El que una persona desempeñe de forma exitosa una actividad, no significa que la disfrute y que esté satisfecha, en ese sentido es donde se ocasiona el cambio y la búsqueda de algo más. Para retener a los colaboradores de Tecnologías de Información, es necesario entenderlos, escucharlos y crear un vínculo en ambos sentidos que les permita estar satisfechos, no solo en el aspecto económico sino también en aspectos de interés personal, de desarrollo profesional y gozo de salud.

6.1 Desarrollo

Como se mencionaba en la introducción, el que una persona sea muy buena realizando una actividad, no significa que la esté disfrutando, en algunos casos, las personas no sabemos que es lo que queremos, o bien, no sabemos expresarlo con claridad. Algunas personas que tienen un buen trabajo, están dispuestas a escuchar nuevas ofertas laborales sin posibilidad de incrementar su ingreso económico, simplemente están abiertas a hacer algo distinto que les permitan estar bien consigo mismas.

Ante esta situación, las empresas no solo deben enfocarse a medir los parámetros de desempeño en: colaboración y compromiso, también deben cuestionarse y buscar acciones para conocer lo que el empleado quiere, cómo ofrecerle algo y cómo retenerlo.

Los estímulos económicos y las promociones de escalafón no siempre serán suficientes como motivadores y estrategias de retención de talento. Para retener a los colaboradores, también es necesario escucharlos, generar compromisos bidireccionales entre el colaborador y la empresa, y que esto tenga como resultado un plan de carrera.

Como inicio, es necesario implementar instrumentos o herramientas de diagnóstico, que tengan como objetivo identificar los intereses, habilidades y motivadores de cada persona, y la combinación de éstos que le permita lograr la máxima satisfacción tanto en lo personal como en lo profesional.

A continuación, se describen algunos de los factores relevantes que determinan la el bienestar laborar y la felicidad de los colaboradores.

Satisfacción laboral

Con base en lo mencionado por Diego y Olivar, 2001, el interés por la satisfacción laboral se enfoca en la capacidad para predecir la permanencia en el trabajo y la productividad laboral. Por esta razón, han surgido diferentes estudios e investigaciones las cuales se enfocan en analizar las causas de la satisfacción laboral.

En algunas bibliografías, (Peiró y Prieto 1996), se menciona que el pilar central se encuentra en estudiar las actitudes hacia el trabajo; es decir, la satisfacción laboral es una variable actitudinal que parece afectar el compromiso y la productividad en el trabajo, y a su vez se encuentra ligada a otros factores psicológicos como bienestar y satisfacción con la vida.

De esta forma, otros autores (Padgett y Baldwin, 1999) también han aportado en la estrecha relación entre la satisfacción laboral y la satisfacción de vida. De esta definición apunta la realización de una evaluación donde la persona examina los aspectos tangibles de su vida, lo bueno y lo malo, y lo compara con un criterio llegando a un juicio sobre su satisfacción de vida.

Felicidad en el trabajo

Algunos autores, han estudiado la felicidad en el trabajo en dos perspectivas, una basada en el ambiente: el puesto de trabajo y características de la organización, y la otra perspectiva centrada en la persona, es decir, los aspectos cognitivos; cada una tiene su valor, sin embargo, para determinar la felicidad en el trabajo hay que considerar ambas (Karasek, 1979).

Perspectiva ambiental

De acuerdo a este enfoque, se necesita entender la felicidad en el trabajo, con base a una adecuada clasificación de las características laborales.

A continuación, se identifican 12 características principales de un trabajo, asociadas a la felicidad de las personas.

Tabla 6 Características Laborales

	Características Laborales
1	Oportunidad en la toma de decisiones.
2	Oportunidad para aportar y adquirir de habilidades.
3	Metas ydesafíos.
4	Variedad en la actividades laborales.
5	Claridad en los objetivos laborales yel rol a desempeñar.
6	Relaciones sociales ytrabajo en equipo.
7	Disponibilidad de dinero.
8	Seguridad física.
9	Posición social valorada.
10	Apoyo de los supervisores yo jefes.
11	Desarrollo de carrera.
12	Equidad.

Perspectiva centrada en la persona

En este enfoque, el punto de partida es que la felicidad también se origina en uno mismo, y existen dos aspectos importantes: características a largo plazo y los procesos a corto plazo.

Características a largo plazo:

- Disposición personal.

- Aspectos poblacionales.

Procesos a corto plazo:

- Forma de afrontar una situación en el trabajo.

- Actitud y pensamiento para situaciones concretas.

Tabla 6.1 Procesos enfocados a la felicidad personal en el trabajo

	Tipo de Proceso
1	Comparaciones con otras personas.
2	Comparaciones con otras situaciones.
2.1	Situación esperada.
2.2	Situación hipotética.
3	Comparaciones con otra época.
3.1	Tendencia anterior.
3.2	Probable tendencia futura.
4	Evaluaciones de una situación relacionada con la autosuficiencia.
5	Evaluación de la innovación.
6	Evaluaciones de relevancia personal.

Emociones

Las emociones también son un factor relevante que no solamente pueden transformar a los individuos, sino que pueden actuar también a nivel organizativo; las emociones positivas individuales pueden contribuir a la transformación de las organizaciones y de las comunidades. Tal como indican algunos autores (Páez, Campos y Bilbao, 2008), existen por lo menos cinco estudios que muestran que hablar y compartir con otros una vivencia positiva refuerza la felicidad, más allá del impacto del hecho mismo. Este efecto, se da con mayor intensidad si las personas que escuchan la comunicación positiva responden de forma auténtica, validándola y aceptándola, sucediendo lo contrario si el entorno responde de forma pasiva o destructiva.

Otro autor, (Myers, 2000), menciona que cuando somos felices, estamos más disponibles para ayudar a los demás. Los psicólogos llaman a este hecho el fenómeno del sentirse bien, y hacer el bien. Otros estudios, (Fowler y Christakis, 2008) confirman esta intuición y muestran que la felicidad se puede extender, dentro de una red social, de unas personas a otras, llegando a la conclusión de que la felicidad de las personas depende de la felicidad de las personas con las que se relacionan, y que, por tanto, la felicidad tiene que considerarse como un fenómeno colectivo. La felicidad de una persona pone en marcha una reacción en cadena que beneficia no solo a sus amigos, sino a los amigos de sus amigos, y a los amigos de los amigos de sus amigos, hasta un tercer nivel.

Asimismo, existen otros factores claves que aportan a la permanencia y al bienestar de los colaboradores, las cuales se describen a continuación:

Optimismo: es una actitud que induce a las personas a confiar en que todo lo que ocurre es bueno y positivo. Como lo indica Peterson (2000), el optimismo es una actitud asociada al pensamiento de que el futuro conllevará a una situación que la persona considera como deseable y que le comportará unos placeres. El optimismo es la fuerza que mueve a la personas para alcanzar el objetivo propuesto, mientras que el pesimismo es la fuerza que nos impulsa a rendirnos.

Inteligencia Emocional: es la capacidad de reconocer nuestras propias emociones y las emociones de los de-más. Según Luthans (2012), la inteligencia emocional aplicada al trabajo es útil para la creación de una red de relaciones que se puede utilizar en los momentos de dificultad.

Salanova (2008), observa que los cambios de las sociedades determinan también un cambio rápido en las organizaciones. Los cambios organizacionales, a su vez, determinan cambios en los puestos de trabajo que pueden influir positiva o negativamente en la seguridad, la salud y el bienestar de los empleados. De manera que, si no se gestionan bien estos cambios, a la larga puede dar lugar a la aparición de organizaciones "enfermas" que se caracterizan por su incapacidad de adaptarse al entorno.

Adicionalmente, también señala que las organizaciones modernas esperan que sus empleados sean proactivos y muestren iniciativa personal, que colaboren con los demás, que sean responsables en su propio desarrollo de carrera y que se comprometan con la excelencia empresarial. Este objetivo empresarial no puede alcanzarse con una fuerza laboral saludable de forma tradicional: empleados satisfechos con sus trabajos, que no experimentan estrés laboral y que muestran bajos índices de absentismo. Se necesita algo más para poner en marcha toda la maquinaria organizacional y conseguir este objetivo. El concepto de organización saludable encaja perfectamente en esta perspectiva científica más positiva.

Sin embargo, Luthans y Youssef (Junio 2007) resaltan que las personas con actitudes positivas no necesariamente crean equipos positivos, ya que las cogniciones colectivas, las emociones y las acciones son legitimadas, promovidas y coordinadas por unos factores (valores, normas, políticas y prácticas empresariales) que tienen que existir en el contexto organizativo en el cual se manifiestan.

Medición de del bienestar en los empleados de tecnología de información

Con el objetivo de medir el bienestar de los empleados de tecnología de información, se realizó una encuesta (Lucio, 2016) a fin de conocer su grado de satisfacción en los siguientes factores:

a) Económico

b) Emocional

c) Espiritual

d) Relación

e) Felicidad

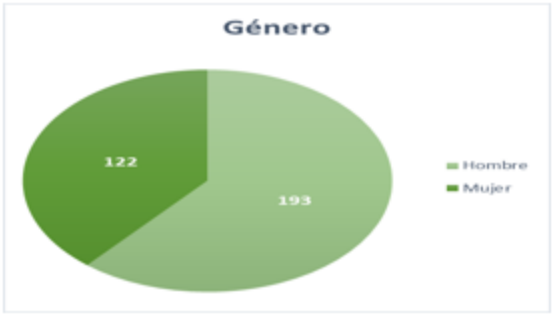
f) Físico

g) Profesional

h) Sexual

La encuesta fue aplicada a 315 personas dedicadas al ramo de Tecnologías de Información, la cual fue respondida por 122 mujeres y 193 hombres.

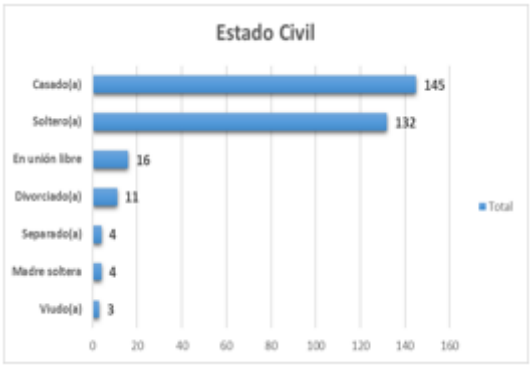
Gráfica 6 Género



Fueron considerados los datos de estado civil, edad, ingreso salarial mensual y nivel de estudios, los cuales fueron agrupados por ciertos criterios, para poder tener una mayor claridad de las tendencias de satisfacción y bienestar.

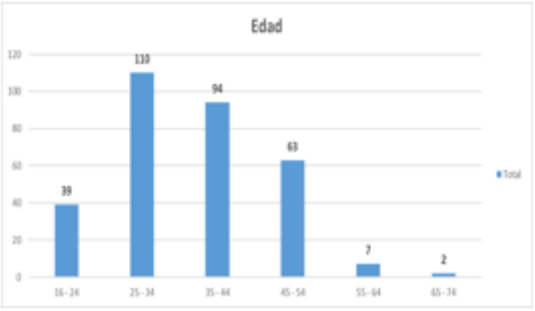
Estado Civil

Gráfica 6.1 Estado Civil



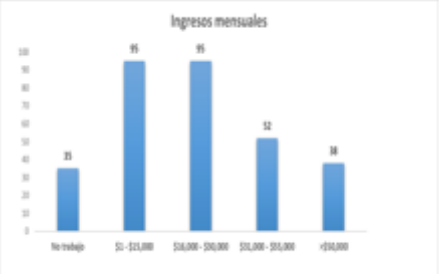
Edad

Gráfica 6.2 Edad



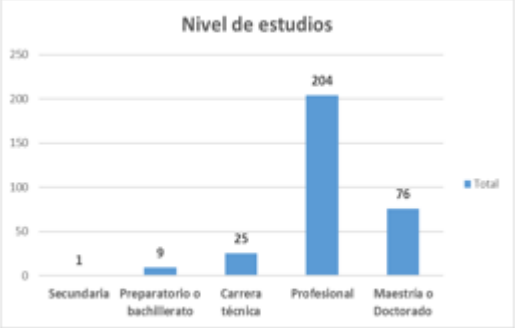
Ingreso Salarial

Gráfica 6.3 Ingreso Salarial



Nivel de Estudios

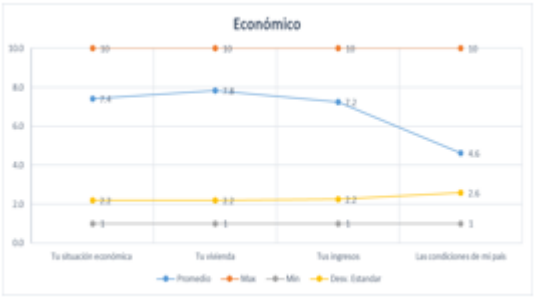
Gráfica 6.4 Nivel de Estudios



El método utilizado para generar esta evaluación, fue basado en una escala de 1 a 10, dónde 1 es la calificación más baja en cuanto al grado de satisfacción y 10 la calificación más alta de satisfacción.

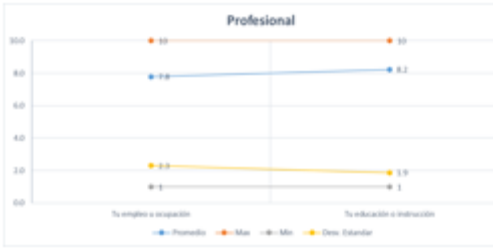
En la parte económica, las personas se encuentran mediamente conformes con su situación económica, de vivienda e ingresos, sin embargo, están preocupados por las condiciones económicas de su país.

Gráfica 6.5 Aspecto Económico



En la parte profesional, existe una ligera conformidad con su ocupación, y están más conformes con su educación y la formación que recibieron.

Gráfica 6.6 Aspecto Profesional

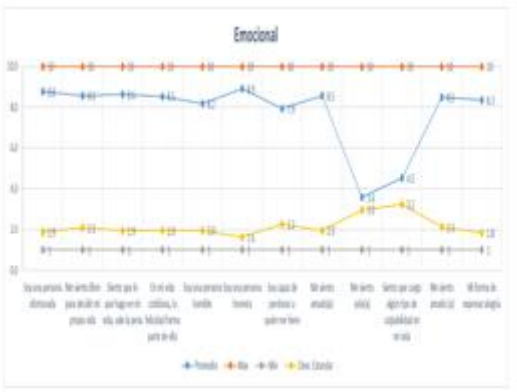


Los resultados de esta encuesta arrojaron que a nivel felicidad, con una escala de 1 a 10, donde 1 es el punto más bajo y 10 el más alto, las personas son felices en un promedio de 8 puntos.

Gráfica 6.7 Resultados de Felicidad

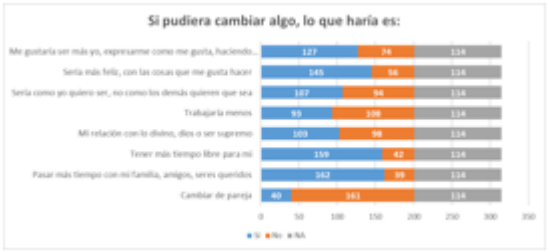
En el aspecto emocional, existen dos aspectos relevantes donde los colaboradores de Tecnología de Información sienten soledad y algún tipo de culpabilidad en su vida. En los demás aspectos, el promedio es de 8 puntos.

Gráfica 6.8 Resultado de aspectos emocionales



Adicionalmente, cuestionando los aspectos que les gustaría cambiar, se refleja en mayor cantidad el pasar mayor tiempo con la familia, amigos y seres queridos, así como tener más tiempo libre para sí mismo.

Gráfica 6.9 Aspectos a cambiar



6.2 Conclusiones

Las empresas están conscientes que su recurso más importante es la energía y la lealtad de sus colaboradores, el capital intelectual, que a diferencia de los demás activos físicos: maquinaría e infraestructura, pueden renunciar y buscar otras oportunidades para ejercer el intelecto en otras compañías.

Normalmente los colaboradores con alto potencial son los que tienden a buscar nuevos retos y tienen expectativas superiores para continuar desarrollándose, pues es un compromiso con ellos mismo, además de que han desarrollado aprendizajes y habilidades de adaptación a diferentes situaciones, que las hace tener mayor experiencias y ser más competitivos.

Es importante que las empresas generen mecanismos de medición, que vayan mas allá de solo medir el desempeño de los colaboradores. Deben implementar mecanismos obtengan información respecto a qué tan feliz es el colaborador y qué grado de bienestar está viviendo, tanto laboral como personal.

Con esta encuesta, se observa que los colaboradores de TI están a gusto con su trabajo y su formación, económicamente también están conformes, en el aspecto de felicidad también se encuentran satisfechos, sin embargo, si expresan la necesidad de tener mayor tiempo para sí mismos y para sus relaciones personales, por lo que la empresas podrían tomar decisiones en afán de apoyar a que los colaboradores de TI satisfagan esa necesidad y asimismo generen mayor productividad y compromiso en la organización.

6.3 Referencias

Lizana Lizana, José, Castillo Guevara, Ramón, Moyano Díaz, Emilio, Trabajo informal: motivos, bienestar subjetivo, salud, y felicidad en vendedores ambulantes Psicologia em Estudo [en linea] 2008, 13 (Diciembre-Sin mes) : [Fecha de consulta: 28 de noviembre de 2016] Disponible en:<http://www.redalyc.org/articulo.oa?id=287122111007> ISSN 1413-7372

Lucio T., 2016, Encuesta de Felicidad y Bienestar.

Moccia, Salvatore, FELICIDAD EN EL TRABAJO, Papeles del Psicólogo [en linea] 2016, 37 (Mayo-Agosto): [Fecha de consulta: 28 de noviembre de 2016] Disponible en:<http://revele.com.veywww.redalyc.org/articulo.oa?id=77846055007> ISSN 0214-7823

Moyano-Díaz, E., Gutiérrez, D. P., Zúñiga K. C., & Cornejo, F. A. (2013).

Warr, Peter; (2013). Fuentes de felicidad e infelicidad en el trabajo: una perspectiva combinada. Revista de Psicología del Trabajo y de las Organizaciones, Diciembre-Sin mes, 99-106.

HERNÁNDEZ, B. Y VALERA, S. (2001). Psicología Social Aplicada e Intervención Psicosocial. España: Ed. Resma.

SGSI en las sociedades de información crediticia

CÁRDENAS, Federico, SOLARES-SOTO, Pedro F.

F. Cárdenas y P. Solares

Universidad Iberoamericana

P. Solares (eds.) Ciencias de los Sistemas de Información y Seguridad. Handbook T-I. -©ECORFAN, Ciudad de México, 2016.

Abstract

The implementation of an Information Security Management System is very useful for organizations of all kinds, however, it is indispensable for those whose operation relies on the safeguarding of sensitive and confidential information. For this, it is convenient to follow a methodology that describes the implementation process adhering to the ISO / IEC 27001 standard and above all, that exists a commitment on the part of the management in order to maintain a process of continuous improvement to the system.

This work intends to take as an example the implantation of an ISMS in an organization such as a Credit Information Society whose characteristics conform to the previously described requirements.

7 Introducción

Los riesgos a los que se enfrentan cada día las organizaciones para conservar la integridad y valor de sus activos requiere que tomen medidas importantes con el propósito de contar con esquemas de seguridad lo suficientemente confiables para que personas internas o externas a la organización vulneren su información. La implantación de un Sistema de Gestión para la Seguridad de la Información se vuelve más crítico conforme aumenta el impacto de una vulnerabilidad a los datos manipulados y resguardados por la empresa.

A continuación, se describirá un modelo de implantación de un SGSI, exponiendo los pasos requeridos a través de un hilo conductor que permita exponer la secuencia derivada de todo sistema basado en un esquema PHVA.

Seguridad de la información

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Indica que esto se logra implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y de hardware. Ya en 1992, el Consejo de la Organización para la Cooperación y el Desarrollo Económico (OCDE), emitió una recomendación relacionada a las directrices de seguridad que deberían adoptar las organizaciones respecto a sus sistemas de información: La seguridad de los sistemas de información tiene por objetivo proteger los intereses de los que cuentan con sistemas de información contra los perjuicios imputables a defectos de disponibilidad, de confidencialidad y de integridad.

La norma ISO/IEC 27001:2013 establece las siguientes definiciones al respecto:

- Confidencialidad: la propiedad por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.
- Integridad: la propiedad de salvaguardar la exactitud y completitud de los activos.
- Disponibilidad: la propiedad de ser accesible y utilizable por una entidad autorizada.

Adicionalmente, la norma ISO/IEC 27002:2009 sugiere que la seguridad en la información debe tomar en consideración la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Sistemas de Gestión de la Seguridad en la Información

Un Sistema de Gestión de la Seguridad en la Información (SGSI) proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección a activos de información para lograr los objetivos de negocio conforme a una revisión del riesgo y la aceptación a los niveles de riesgo de la organización diseñados para el tratamiento y gestión de riesgos. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

El propósito de un sistema de gestión de la seguridad de la información no es garantizar que la organización contará con una protección total a las distintas amenazas ni reducir a cero sus vulnerabilidades, sino garantizar que los riesgos relacionados a la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

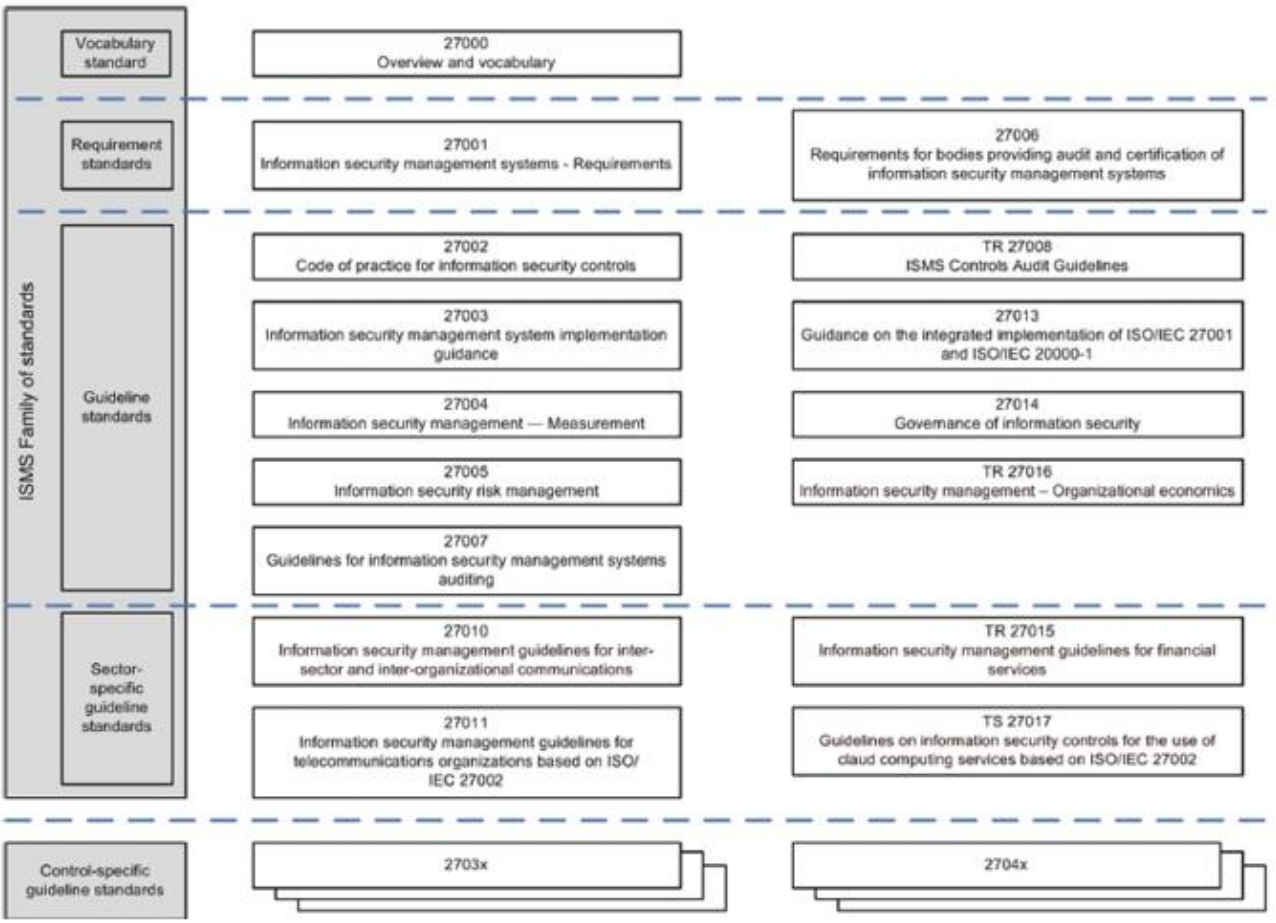
Familia ISO/IEC 27000 y norma ISO/IEC 27001:2013

La familia de normas ISO 27000 corresponden a estándares de seguridad publicadas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Dicha serie ayuda a las organizaciones a mantener seguros sus activos de información, tales como información financiera, propiedad intelectual, detalles de sus empleados o información de terceras personas bajo resguardo. ISO/IEC 27001 es el estándar en la familiar que proporciona los requerimientos que debe cubrir un sistema de gestión de seguridad de la información (SGSI). A continuación, se describen las normas que conforman esta familia:

- ISO/IEC 27000, Information security management systems — Overview and vocabulary
- ISO/IEC 27001, Information security management systems — Requirements
- ISO/IEC 27002, Code of practice for information security controls
- ISO/IEC 27003, Information security management system implementation guidance
- ISO/IEC 27004, Information security management — Measurement
- ISO/IEC 27005, Information security risk management
- ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007, Guidelines for information security management systems auditing
- ISO/IEC TR 27008, Guidelines for auditors on information security controls
- ISO/IEC 27009, Sector-specific application of ISO/IEC 27001 — Requirements
- ISO/IEC 27010, Information security management for inter-sector and inter-organizational communications

- ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014, Governance of information security
- ISO/IEC TR 27015, Information security management guidelines for financial services
- ISO/IEC TR 27016, Information security management — Organizational economics
- ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27019, Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

Figura 7 Familia de estándares para el Sistema de Gestión de la Seguridad en la Información



Para el caso del modelo planteado por ISO/IEC 27001:2013, el sistema de gestión corresponde al PHVA/PDCA (Planear, Hacer, Verificar, Actuar). A continuación, se hace una asociación entre los puntos de la norma y su correspondiente función dentro del PHVA:

Tabla 7 Relación PHVA y puntos de la norma

PHVA	Requisito General	Punto de la norma
PHVA	La organización	Todos, especialmente en el 5 por la responsabilidad de la dirección
P	Crear	4.2.1, el detalle de las actividades de creación está en la definición del alcance, política y análisis de riesgos que figuran más adelante
H	Implementar y operar	4.2.2
V	Supervisar y crear	4.2.3 y 6 y 7
A	antener y mejorar	4.2.4 y 8
PHVA	SAGSI documentado	4.3
P	Actividades empresariales	4.2.1.a y 4.2.1.b
P	Riesgos que esta afronta	4.2.1.c-j

Implementación de un Sistema de Gestión de Seguridad de la Información

Como propone Gomez5, un proyecto para la implantación de un SGSI puede desarrollarse en base a una serie de fases, que se incluyen en la figura 2 y que se describen a continuación.

Lanzamiento y análisis del contexto de la organización. Se deben conocer las circunstancias de la organización, su funcionamiento, las implicaciones, dependencias y requisitos internos y externos y las motivaciones para la implantación de un SGSI.

Definición del alcance. Se determina que elementos formarán parte del SGSI, generalmente identificando procesos de negocio sobre los que se aplicará el sistema.

Definición de los objetivos y la política de seguridad. Además de fijar un marco organizativo, determinando funciones y responsabilidades para la gestión de la seguridad de la información, debe cubrir de manera general todos los aspectos de la seguridad: seguridad física, seguridad lógica, seguridad del personal, y adecuarse a las necesidades y recursos de la organización.

Evaluar los riesgos de la organización. Uno de los métodos para la realización de la evaluación de riesgos es el tradicionalmente seguido de identificar activos, amenazas y vulnerabilidades, de acuerdo a lo siguiente:

- Desarrollar el inventario de activos de información. Se deben identificar los activos que dan soporte a los procesos de negocio en el alcance del SGSI y cuantificar su valor en términos de confidencialidad, integridad y disponibilidad.

- Identificar y valorar amenazas. Se deben identificar todas aquellas amenazas que, en función de la naturaleza del activo, podrían afectarle y asignarles un valor de probabilidad de ocurrencia y de degradación del activo en caso de materialización de la misma, para cada una de las dimensiones.

- Calcular el impacto. Para cada activo y para cada una de las dimensiones de seguridad, se calcula el impacto de la materialización de las amenazas identificadas. Este impacto será una función del valor del activo y de la degradación que produce la amenaza.

- Calcular el riesgo. Para cada activo se calcula el riesgo, que será una función del impacto, calculado en el punto anterior, y de la probabilidad de ocurrencia de la amenaza.

- Identificar a los propietarios de los riesgos. Para los riesgos identificados se debe determinar a la persona o personas responsables de tomar la decisión de la opción de tratamiento de riesgo y de aprobar los planes para la mitigación de los mismos.

- Tratamiento de los riesgos. En este punto se determinan las estrategias a aplicar sobre los riesgos identificados.

- Determinar las medidas de seguridad a implementar. Para gestionar los riesgos será necesario establecer una serie de controles organizativos y técnicos que permitan reducirlos a un nivel aceptable. En el proceso de selección de controles, deben considerarse los beneficios que aportarán y el coste de implantación y mantenimiento de los mismos.

- Evaluar los riesgos residuales. Tras la selección de los controles que permitirán a la organización reducir los riesgos a un nivel aceptable, se deberá calcular cuál será el riesgo que quede tras su implantación, ya que este nunca será cero. El propietario del riesgo tiene que conocer que este riesgo existe y aceptarlo.

- Plan de tratamiento de riesgos. Detallará las actividades necesarias para la implantación de las medidas seleccionadas, incluyendo información sobre plazos, recursos, responsables, etc.

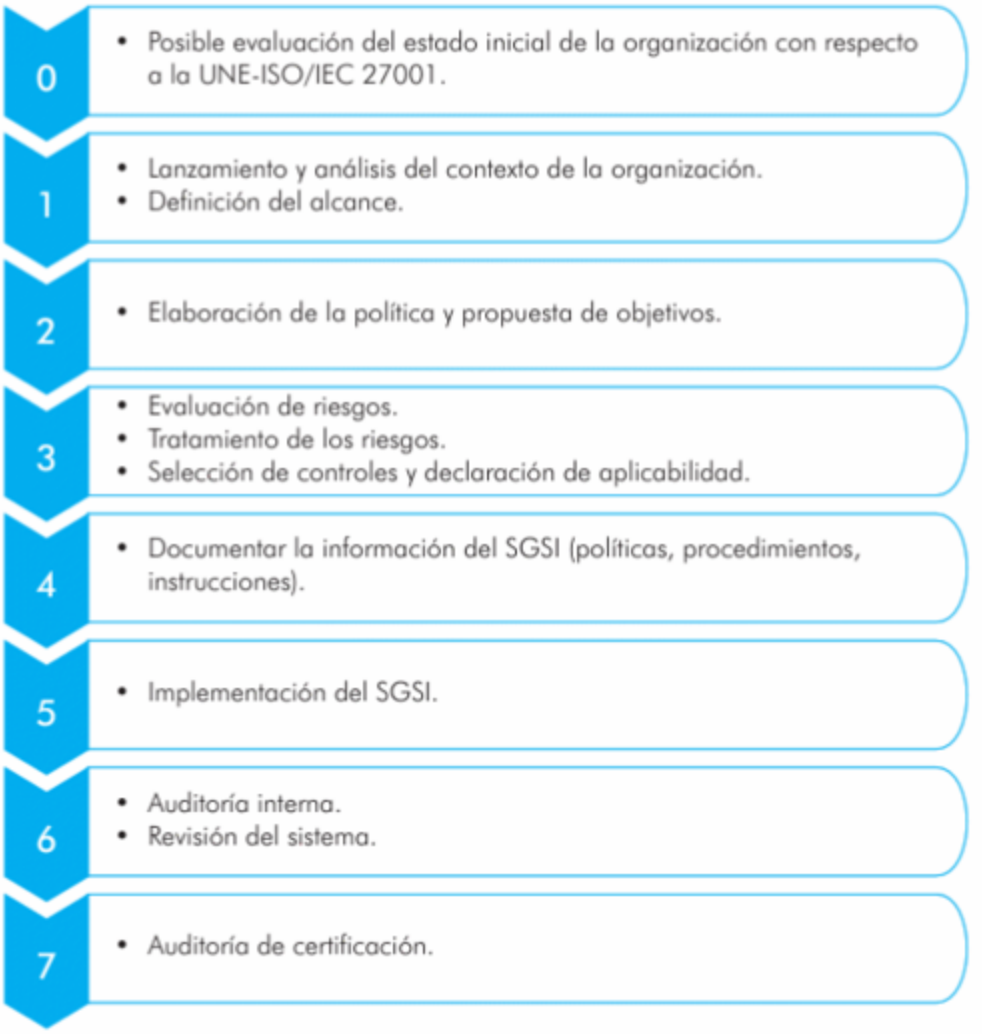
- Elaborar la información documentada necesaria para implementar las medidas seleccionadas. Los procedimientos son la manera de plasmar la implementación de los controles de seguridad y las tareas de administración del SGSI. Un procedimiento debe reflejar fielmente los pasos a seguir para la realización de las tareas, pero debe ser conciso y claro para que no se cometan errores.

- Implementación de los controles y los procedimientos. De una manera planificada y organizada se irán implantando los controles y procesos definidos. Puede ser conveniente comenzar la implantación por aquellas acciones que con un menor esfuerzo aporten un gran valor a la organización (conocidos como Quick Wins).

- Formar y concienciar al personal. Para que la implantación de los procedimientos sea efectiva, es necesario concienciar y formar a todas las personas implicadas. La formación y capacitación de cada usuario deberá ser acorde con las funciones que desempeñe.

- Realizar la auditoría interna y la revisión del SGSI por la dirección. Esto permitirá comprobar el grado de ajuste el SGSI a los requisitos de la norma y determinar si está alineado con los objetivos de la organización.

Figura 7.1 Fases del proyecto de implementación de un SGSI



Para poder implantar un Sistema de Gestión de Seguridad de la Información en una institución, es fundamental tener un conocimiento amplio de la misma, incluyendo sus objetivos de negocio, así como los diferentes actores que giran en torno a ella y que puedan influir en sus fortalezas y debilidades. Esto es importante ya que como se ha mencionado, uno de los propósitos de un SGSI es coadyuvar a que las organizaciones cumplan con los objetivos que se han planteado.

Contexto de la organización. Las Sociedades de Información Crediticia

A continuación, se describe de forma breve la naturaleza de las Sociedades de Información Crediticia.

Los Burós de Crédito son instituciones financieras, autorizadas por la SHCP, previa opinión del Banco de México y de la CNBV. Oficialmente, este tipo de entidades es conocida como Sociedades de Información Crediticia (en adelante, SIC), y son organizaciones que proporcionan servicios de recopilación, manejo y entrega o envío de información relativa al historial crediticio de personas físicas y morales.

Su objetivo es contribuir al desarrollo económico del país ofreciendo servicios que promueven minimizar el riesgo crediticio, al proporcionar información que ayuda a conocer la experiencia de pago de empresas y personas físicas, lo que a su vez, contribuye a formar la cultura del crédito entre la población, al tiempo de promover un sano consumo interno.

En 1996 surge la primera Sociedad de Información Crediticia en México autorizada por la SHCP, con el fin de proporcionar información del comportamiento crediticio de personas físicas. Tiene como socios a la Banca Comercial, a Trans Union Co. (buró crediticio con experiencia en manejo de registros de crédito) y Fair Isaac Co. (empresa con experiencia en modelos de análisis de riesgo).

En 1998 se incorpora el Buró de Personas Morales, con el fin de proporcionar información sobre el comportamiento crediticio de personas morales, y físicas con actividad empresarial. Tiene como socios a la banca comercial, a Trans Union Co. y a Dun & Bradstreet Co., con experiencia a nivel mundial en la evaluación de empresas. En 2005 surge la tercera Sociedad de Información Crediticia en el país contando como socios a Banco Afirme, Coppel, Grupo Chedraui, dos inversionistas privados y Grupo Elektra.

La información que tienen las Sociedades de Información Crediticia reduce los siguientes problemas en la asignación de los créditos:

1. Información asimétrica entre prestamistas y prestatarios, debido a que al haber información crediticia los prestamistas pueden conocer la calidad crediticia de los deudores;

2. Selección adversa, debido a que al haber mayor información se evita el que se considere un posible deudor, de alto riesgo, como de bajo riesgo;

3. Riesgo moral, debido a que se generan incentivos a los acreditados para ser puntuales en su pago, al saber que cualquier incumplimiento afectará su historial crediticio y la posibilidad de obtener créditos en el futuro, y

4. Racionamiento de crédito, debido a que al haber información se evita el que los prestamistas limiten la oferta del crédito a los que demandan créditos, quienes están dispuestos a pagarlo a la tasa de interés a la que se ofrece el crédito.

Las SICs cumplen con los siguientes objetivos:

1. Permite una evaluación completa del desempeño crediticio de los deudores;

2. Facilita el acceso al crédito de los deudores cumplidos con buen historial crediticio;

3. Incrementan la competencia entre instituciones financieras y no financieras que otorgan créditos, al tener acceso a la misma información de las personas;

4. Al haber mayor información sobre la calidad crediticia, permite a las personas con buen historial crediticio el obtener créditos a tasas más bajas;

5. Se reduce la cartera vencida debido a los incentivos que se generan entre los deudores para evitar un mal historial crediticio;

6. Incrementa la movilidad de los clientes debido a que un buen historial crediticio facilita el que se establezca una nueva relación con una institución de crédito;

7. Evita el sobreendeudamiento de los clientes al poder analizarse la capacidad de pago de los clientes, y

8. Se incrementa la posibilidad de que la gente con menores recursos obtenga créditos.

Marco Legal

En julio de 1993 se publicaron enmiendas a la Ley Para la Regulación de Grupos Financieros en el Diario Oficial de la Federación. Entre ellas, la reforma del artículo 33, y la adición de los artículos 33-A y 33-B, con el objeto de crear un nuevo tipo de entidad llamada "sociedad de información crediticia" (buró de crédito). El propósito de dichas reformas fue regular las actividades de reporte de crédito, lo cual hasta ese momento únicamente se había realizado a través del SENICREB del Banco de México.

En enero de 2002, la Ley para Regular las Sociedades de Información Crediticia fue promulgada y se enmendó en 2004, 2008, 2009, 2010 y 2014. Esta ley regula las actividades de los burós de crédito privados. Las provisiones de esta ley son suplementadas por las Reglas Generales a las que Deberán Sujetarse las Operaciones y Actividades de las Sociedades de Información Crediticia y sus Usuarios emitidas por el Banco de México en 2002.

La ley y las reglas antes mencionadas buscan mejorar la veracidad y consecuente credibilidad de los registros de crédito al fortalecer sus normas operacionales. Algunos de los elementos más importantes de dichas regulaciones incluyen mecanismos para proteger los derechos del consumidor. Dichas provisiones establecen requerimientos de consentimiento para la distribución de los reportes de crédito, el derecho de los individuos y empresas a tener acceso a su reporte de crédito completo en los burós de crédito, y procedimientos rápidos y de bajo costo para disputar y corregir la información errónea.

Otras leyes federales que apoyan a los sujetos de los reportes de crédito en sus interacciones con las compañías de reportes de crédito son la Ley de Protección y Defensa al Usuario de Servicios Financieros de 2000, que le provee asistencia al consumidor de enfrentarse a problemas con la misma empresa de reportes de crédito o con un acreedor financiero (bancario o no bancario) y la Ley Federal de Protección al Consumidor de 1992, enmendada en 2004, la cual, entre muchos otros asuntos, es aplicable en casos donde los consumidores experimenten problemas con un acreedor no-financiero.

Marco Regulatorio

Las autoridades que regulan las actividades de las SICs son:

- Secretaría de Hacienda y Crédito Público.

- Banco de México.

- Comisión Nacional Bancaria y de Valores.

- Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros.

Cumplimiento regulatorio referente a seguridad

Existen varias provisiones que exige la Ley para Regular las Sociedades de Información Crediticia requiere como cumplimiento a las SICs en relación a la seguridad de la información:

Artículo 7. Indica que la solicitud para constituirse y operar como Sociedad debe incluir las medidas de seguridad y control a fin de evitar el manejo indebido de la información;

Artículo 19. La Secretaría de Crédito y Crédito Público podrá revocar la autorización otorgada a la Sociedad cuando comenta de manera grave o reiterada violaciones al Secreto Financiero o altere, modifique o elimine reiteradamente algún registro de su base de datos, salvo los supuestos previstos en la ley;

Artículo 22. Exige que la Sociedad adopte las medidas de seguridad y control que resulten necesarias para evitar el manejo indebido de la información, entendiéndose esto último como cualquier acto u omisión que cause daño en su patrimonio al sujeto del que posea información, así como cualquier acción que se traduzca en un beneficio patrimonial a favor de los funcionarios y empleados de la Sociedad o de esta última, siempre y cuando no se derive de la realización propia de su objeto;

Artículo 27. Las Sociedades, al proporcionar información sobre operaciones crediticias y otras de naturaleza análoga, deberán guardar secreto respecto de la identidad de los acreedores, salvo en el supuesto a que se refiere el artículo 39 de la ley, en cuyo caso, informarán directamente a los Clientes el nombre de los acreedores que correspondan;

Artículo 28. Se entenderá que violan las disposiciones relativas al Secreto Financiero tanto la Sociedad, como sus empleados o funcionarios que participen en alguna consulta a sabiendas de que no se ha recabado la autorización correspondiente. Se considerará que los Usuarios, así como sus empleados o funcionarios involucrados, han violado las disposiciones relativas al Secreto Financiero, cuando realicen consultas o divulguen información en contravención a lo establecido en los artículos mencionados en la ley. Las Sociedades, sus empleados y funcionarios tendrán prohibido proporcionar información relativa a datos personales de los Clientes para comercialización de productos o servicios que pretendan ofrecer los Usuarios o cualquier tercero, salvo para la realización de consultas relativas al historial crediticio. Quien proporcione información en contravención a lo establecido en este párrafo, incurrirá en el delito de revelación de secretos a que se refiere el artículo 210 del Código Penal Federal.

Artículo 33. La Sociedad deberá contar con sistemas y procesos para verificar la identidad del Usuario o del Cliente mediante el proceso de autenticación que ésta determine, el cual deberá ser aprobado previamente por el consejo de administración de la Sociedad, a fin de salvaguardar la confidencialidad de la información en los términos de las disposiciones legales aplicables,

Artículo 37. Las Sociedades deberán presentar a la Comisión manuales que establezcan las medidas mínimas de seguridad, mismas que incluirán el transporte de la información, así como la seguridad física, logística y en las comunicaciones. Dichos manuales deberán contener, en su caso, las medidas necesarias para la seguridad del procesamiento externo de datos;

Artículo 38. Los Usuarios de los servicios proporcionados por la Sociedades y cualquier otra persona distinta del Cliente que tenga acceso a sus Reportes de Crédito o Reportes de Crédito Especiales, así como funcionarios, empleados y prestadores de servicios de dichos Usuarios y personas, deberán guardar confidencialidad sobre la información contenida en los referidos reportes y no utilizarla en forma diferente a la autorizada.

Artículo 51. Las Sociedades responderán por los daños que causen a los Clientes al proporcionar información cuando exista culpa grave, dolo o mala fe en el manejo de la base de datos;

En relación a las multas que la CHCP podrá aplicar por incumplimiento, se indica lo siguiente:

- Artículo 60. Sanción con multa de 300 a 5,000 veces el salario mínimo general diario vigente en la CDMX, cuando
- La Sociedad, sus empleados o funcionarios proporcionen a los Usuarios información que incluya la identidad de los acreedores, en contravención a lo previsto por el artículo 27;
- La Sociedad no cuente con los sistemas y procesos previstos en el artículo 33, o no hayan sido aprobados por su consejo de administración;
- Artículo 62. La Comisión sancionará con multa de 2,000 a 20,000 veces el salario mínimo generar diario vigente en la CDMX cuando:
- La Sociedad o Entidad Financiera haga uso o manejo indebido de la información en términos del artículo 22;
- La Sociedad, la Entidad Financiera, o sus funcionarios, empleados o prestadores de servicios incurran en violación al Secreto Financiero o en el delito de revelación de secretos en cualquier forma de las previstas en los artículos 28 y 38;
- Artículo 66. El Banco de México sancionará con multa de 1,000 a 15,000 veces el salario mínimo general vigente en la CDMX, a las Sociedades cuando:
- Omitan sujetarse a lo que el Banco de México les señale en relación con el manejo y control de su base de datos, cuando se acuerde su disolución y liquidación

Alcance del Sistema

Otro aspecto fundamental dentro del proceso de implementación de un SGSI es la identificación de su alcance y límites. Para ello es necesario conocer los procesos que manejan información que deberá ser gestionada en términos de seguridad. En caso de que la organización cuente con el estándar ISO/IEC 90000, se puede tomar el manual de calidad como referencia para la identificación de tales procesos. Una vez realizado esto, es necesario hacer un inventario de activos su origen y destino, así como su clasificación y la tecnología que los soporta.

El inventario de activos debe recoger la siguiente información:

- El nombre del activo, por ejemplo: equipo de usuario, router 014, proyecto, expediente, etc.
- La descripción del activo.
- Categoría a la que pertenece, por ejemplo: equipo, aplicación, servicio, etc.
- Ubicación: el lugar físico en el que se encuentra dentro de la organización.
- Propietario: entendiendo por tal al responsable del activo.

Identificados los activos de información se les debe valorar de acuerdo a su importancia para la empresa. Esta apreciación será lo más objetiva posible, ya que con ella se determinará sobre qué activos se realizará el análisis de riesgos. Por supuesto, se puede hacer una estimación de todos los activos, pero si son muchos, los recursos limitados, o ambas cosas, lo razonable es elegir un grupo de activos reducido para que el análisis de riesgos no sea inabarcable. Por ejemplo, se puede escoger analizar los activos que están por encima de un valor. Para valorar los activos se considerarán los parámetros de confidencialidad, disponibilidad e integridad de los activos, determinándose la importancia que tienen para la organización en una escala de valores predefinida7.

La delimitación del alcance del SGSI es una actividad fundamental, ya que marca la pauta para el resto de las actividades y podrá implicar cambios respecto a la forma en la cual se viene manejando la información dentro de la institución. Más aún, resulta imprescindible que estos cambios se mantengan y mejoren a lo largo del tiempo como parte del proceso de mejora continua del sistema de gestión. Un aspecto importante a considerar es que la norma no requiere aplicarse a toda la organización completa, sino a las partes que más beneficios presenten en relación a los recursos que serán destinados para la implantación del sistema.

Política de Seguridad

Las Políticas de Gestión de la Seguridad de la Información están constituidas por el conjunto de normas reguladoras, procedimientos, reglas y buenas prácticas que determinan el modo en que todos los activos y recursos, incluyendo la información, son gestionados, protegidos y distribuidos dentro de una organización6. Gómez7 menciona que la política de seguridad recogerá las líneas generales de actuación de la organización en una declaración que estará firmada por la dirección, en la que se compromete a velar por la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos de información. Además, como parte de este documento o en otro distinto, se debe documentar:

El alcance del sistema, es decir, qué partes de la organización van a estar protegidas por el SGSI. Puede ser la organización entera o una parte relevante de la misma: departamento, servicio o proceso. La recomendación a la hora de decidir el alcance es escoger uno que sea realmente abordable por la empresa. Si es demasiado amplio y no se cuenta con los recursos necesarios para llevar a cabo un SGSI de esa dimensión, el proyecto se alargará y llegará un momento en que se parará, puesto que no hay personal o presupuesto para continuar con él, con la consiguiente frustración de los implicados y la pérdida de tiempo y dinero de la organización.

La estructura de la empresa, un organigrama de las distintas áreas y responsables de la organización, y sus relaciones internas.

Las diferentes responsabilidades de cada parte de la organización: el responsable de seguridad, la dirección, el responsable de sistemas, el personal, etc.

La topología de la red, de manera que se muestren los principales sistemas de información y comunicación que se emplean.

La clasificación de la información, utilizando la nomenclatura de la organización y explicando los criterios de clasificación.

El enfoque y la metodología del análisis de riesgos. Así cualquiera puede verificar los resultados del análisis, ajustándose al razonamiento que se ha seguido para llevarlo a cabo.

Las normas generales de uso de los activos. Estas normas deben existir para evitar incidentes no deseados y utilizaciones indebidas de los activos. Serán hechas públicas, e incluso pueden ser objeto de una entrega formal a los empleados o terceras partes implicadas, de modo que se hagan responsables de las infracciones. Es fundamental establecer unas pautas mínimas en temas como el empleo de las contraseñas y el de las comunicaciones, fuente de numerosas incidencias. Estas normas de uso son un elemento importante en la concienciación del personal, ya que establecen unas pautas de comportamiento, que aunque sean de sentido común y no marquen límites demasiado estrictos, sí indican que la empresa se preocupa al respecto y que los empleados deberían hacer lo mismo.

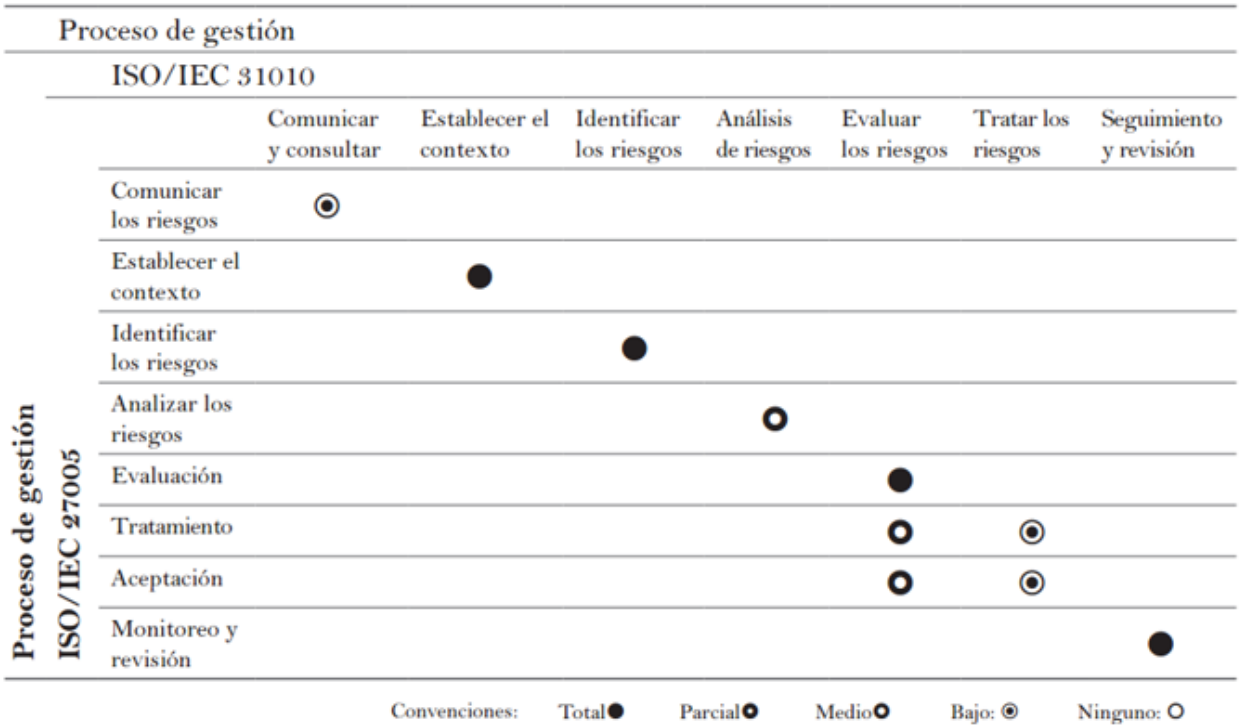
Los objetivos de seguridad que se pretenden alcanzar. Puede ser difícil establecer unos objetivos claros y útiles sin tener datos de partida, pero al menos se deberá intentar expresar qué nivel de seguridad se desea alcanzar. Se puede comenzar por estimar qué metas se quieren lograr en términos de confidencialidad, disponibilidad e integridad. Por ejemplo, para verificar las mejoras en confidencialidad puede utilizarse como métrica el número de incidencias relativas a la confidencialidad, y decidir que el objetivo para este año va a ser tener tres o menos incidencias de este tipo. Con los resultados que se vayan obteniendo, se irá revisando dicho objetivo para ajustarlo a la realidad. Si sistemáticamente obtenemos un valor mucho más elevado, puede que el objetivo no sea realista y haya que revisarlo a la baja.

Gestión del riesgo

Dentro de la familia de normas ISO/IEC 27000 revisada anteriormente se encuentra la norma ISO/IEC 27005, la cual es el estándar internacional que proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en la norma ISO/ IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de elementos que permitan garantizar la seguridad de la información basada en un enfoque de gestión de riesgos. Es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que podrían comprometer la seguridad de su información8.

Esta norma tiene aspectos comunes con la norma ISO/IEC 31000, Gestión de riesgos – Principios y guías, así como la ISO/IEC 31010 Gestión de riesgos – Técnicas de evaluación de riesgos. Como muestra el estudio de Medina (2015), la diferencia básica entre ambas normas, es que la ISO/IEC 31000 se enfoca en la Gestión de riesgos de manera integral y genérica, mientras que la ISO/IEC 27005 lo hace de forma específica en la Gestión de Riesgos en la Seguridad de la Información. Sin embargo, existe similitud en muchos de los procesos y en la terminología utilizada al definir sus conceptos10.

Figura 7.2 Relación entre los modelos y normas de gestión de riesgos ISO/IEC 27005 e ISO/IEC 31010



Con el propósito de gestionar los riesgos de la organización, se propone emplear la metodología sugerida por Devia, G. A. V., & Pardo (2015), resultante de contrastar los diferentes modelos de riesgos de TI existentes:

Identificar el contexto de la organización. Proporcionando los parámetros básicos para la gestión de riesgo teniendo en cuenta el alcance y los criterios que se van a utilizar durante el proceso. Incluye la consideración de parámetros internos y externos relevantes para la organización, en su conjunto, así como los antecedentes de los riesgos particulares que se están evaluando. Al establecer el contexto, se determinan: el programa de evaluación de los riesgos, los objetivos de la evaluación de riesgos y los criterios del riesgo.

Definir los roles y las responsabilidades del personal relacionado con TI. Determinar los actores que intervienen, llevando un manual de funciones que permita tener claro el papel de cada uno en la organización, de manera que cuando ocurra un riesgo se puedan determinar las posibles fallas por donde se originó el riesgo.

Identificar los activos tecnológicos de la organización. Un activo es algo que tiene valor o utilidad para la organización teniendo en cuenta la continuidad de sus operaciones comerciales; es por eso que un activo necesita protección, para garantizar las operaciones comerciales y la continuidad del negocio.

Identificar los riesgos, amenazas y vulnerabilidades. Los riesgos deben ser identificados de manera que se puedan entender antes de ser analizados y gestionados correctamente. Esta identificación debe tener un enfoque detallado que permita abarcar todos los eventos posibles, de modo que se clasifiquen los riesgos en las categorías definidas en la estrategia de gestión del riesgo, de tal manera que los riesgos formen una línea base para el inicio de actividades en la gestión de riesgo.

Los riesgos deben ser revisados periódicamente para reexaminar las posibles fuentes de riesgo y revisar las condiciones cambiantes, revisando los riesgos que se pasaron por alto o aquellos que no existían en la última revisión.

Analizar los riesgos. El análisis de riesgos implica su identificación a partir de fuentes internas y externas; cada riesgo es evaluado para determinar su probabilidad y sus consecuencias. Los riesgos se categorizan con base en la evaluación establecida en la estrategia de gestión de riesgos, proporcionando información suficiente para su manejo, estableciendo un nivel de análisis con base en lo que es apropiado y razonable.

Evaluar los riesgos, determinando el nivel de riesgo. Este es el proceso donde se consolida la identificación, el análisis y la evaluación de los riesgos, es en este punto donde se determina su prioridad para el tratamiento adecuado.

Tratar los riesgos, definir e implementar los planes de mitigación. Terminada la evaluación del riesgo, se ejecutan las medidas correctivas, se escoge una serie de opciones para mitigar el riesgo; este es un proceso repetitivo que tiene como fin determinar su tolerabilidad en contra de los criterios establecidos, con el fin de decidir si se requiere un tratamiento posterior. Los riesgos son monitoreados cuando superan los umbrales establecidos, los planes de mitigación de riesgos se despliegan para devolver el esfuerzo afectado a un nivel de riesgo aceptable. Si el riesgo no puede ser mitigado, se puede invocar un plan de contingencia.

Aceptar el riesgo. En este punto del proceso, toma parte la alta dirección de la organización que es la encargada de determinar el nivel de impacto del riesgo y de decidir si se acepta o no, teniendo en cuenta sus consecuencias. Aceptar el riesgo incluye asumir las responsabilidades frente a las insuficiencias encontradas luego de haber tratado el riesgo (si ha quedado algún riesgo residual).

Llevar un control de seguimiento y monitoreo del riesgo tratado. Como parte del proceso de gestión, los riesgos y los controles deben ser monitoreados y revisados periódicamente para verificar que las hipótesis sobre los riesgos sigan siendo válidas.

Registrar el proceso de gestión de riesgos. Se debe llevar un histórico de todos los incidentes, que permita llevar una auditoría independiente en la gestión de riesgos con el fin de garantizar que se ha realizado una buena gerencia de riesgos8.

Información documentada sobre procesos

Como parte de la implantación del SGSI, es necesario documentar la forma en la cual operará el sistema. Para ello se deberá recurrir a las políticas, normas, procedimientos e instrucciones técnicas que soporten el modelo.

Implementación del SGSI

Para poner en marcha el SGSI la dirección tiene que aprobar la documentación desarrollada en las actividades detalladas en el punto anterior y proveer los recursos necesarios para ejecutar las actividades. Para ello es necesario contar con el plan de tratamiento del riesgo el cual deberá incluir los controles necesarios para atender los riesgos conforme a la tolerancia aprobada por la dirección.

Supervisión y verificación del sistema

Como parte de la implementación del sistema, es necesario contar con un mecanismo que permita verificar que el plan de tratamiento a los riesgos cumple su cometido, así como validar que los objetivos de seguridad se han cumplido de manera eficaz y que las incidencias están siendo atendidas conforme los procedimientos previstos. Para llevar a cabo esta fase se realizan una serie de acciones: las revisiones periódicas, las auditorías internas y la revisión del sistema por la dirección5.

Revisiones periódicas

La organización requiere contar con un conjunto de revisiones que permitan verificar que el sistema cumple con sus objetivos definidos y documentarlos correctamente. Lo anterior permitirá validar el progreso de las actividades programadas que se emplearán para el cumplimento de los objetos.

Auditoría interna

El propósito de las auditorías internas es poder detectar y documentar de forma veraz e imparcial las vulnerabilidades que presenta una organización que cuenta con el SGSI, a fin de garantizar que tal sistema está cumpliendo con los requisitos de la norma por medio de sus objetivos de control, controles, procesos y procedimientos existentes.

La documentación que deberá revisarse dentro de las auditorías internas es la siguiente:

- Política, objetivos y alcance.
- Procedimientos y mecanismos de control de soporte.
- Metodología de evaluación de riesgos.
- Informe de evaluación de riesgos.
- Plan de tratamiento de riesgos.
- Procedimientos específicos para la planificación, operación y control de los procesos de seguridad de la información, así como los relacionados con la medición de la eficacia de los controles.
- Otros registros exigidos por la norma ISO 27001.
- Declaración de aplicabilidad de los controles.

Revisión del sistema por la dirección

Otro aspecto importante dentro de la supervisión del sistema es la validación que realiza la dirección a fin de corroborar que las acciones están encaminadas de forma correcta y alineadas de forma adecuada a sus expectativas.

Mejora del sistema

Este punto concreta el ciclo PHVA, al tomar las medidas necesarias a fin de corregir los hallazgos detectados durante la fase de supervisión y validación. De esta forma, el proceso de mejora continua se mantiene durante cada iteración al poner en marcha las acciones preventivas y correctivas necesarias.

7.2 Conclusiones

Para las Sociedades de Información Crediticia es indispensable contar con un sistema de gestión de seguridad de la información que permita identificar y controlar los diferentes riesgos que puedan comprometer la información que resguardan y, por ende, el secreto financiero asociado. Asimismo, se tiene el beneficio adicional de reforzar el sistema de gestión de riesgos que pudiera tener implementada la empresa (tal como ISO/IEC 31000:2009), al contar con una visibilidad más detallada en las amenazas que pudieran comprometer aspectos específicos de seguridad de la organización y robustecer la continuidad y disponibilidad del negocio. De esta forma es posible dar cumplimiento y conformidad a la regulación a la que están sujetas. Como beneficio complementario, permite generar credibilidad y confianza a sus clientes, socios y proveedores al contar con una certificación emitida por un tercero, alineada a las mejores prácticas internacionales.

Para lograr lo anterior, es imprescindible que la empresa cuente con el compromiso de la Alta Dirección, tener un gobierno corporativo maduro y una cadena de responsabilidades claramente definida, así como sensibilizar a la toda la organización respecto a la importancia de la seguridad y la gestión de riesgos a fin de hacerlos partícipes de este esfuerzo de mejora continua que se busca en el sistema.

Como pudo mostrarse en el desarrollo del contexto de la empresa, son varios los aspectos que deben ser atendidos por una Sociedad de Información Crediticia en términos de cumplimiento por la legislación actual, los cuales pueden atender su conformidad por medio de la norma ISO/IEC 27001. Al momento, las SICs existentes en México se encuentran certificadas en el sistema de gestión mencionado y mantienen el ciclo de mejora continua dentro de sus procesos.

7.3 Referencias

Gil Hubert, J. (2004). The Mexican Credit Reporting Industry Reform: A Case Study.

CNBV, “Ley para Regular las Sociedades de Información Crediticia”. Enero 2014, Disponible en: http://www.cnbv.gob.mx/Paginas/NORMATIVIDAD.aspx

Mundial, B. (2005). Sistemas de reporte de préstamos bancarios y créditos en México. México: Centro de Estudios Monetarios Latinoamericanos, Banco Mundial y First Initiative.

Gómez Fernández, Luis, and Fernández Rivero, Pedro Pablo. Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad. Madrid, ES: AENOR - Asociación Española de Normalización y Certificación, 2015.

Fernández Sánchez, Carlos Manuel, Piattini Velthuis, Mario. Modelo para el gobierno de las TIC basado en las normas ISO. Madrid, ES: AENOR - Asociación Española de Normalización y Certificación, 2012

Gómez Vieites, Álvaro. Seguridad en equipos informáticos. Madrid, ES: RA-MA Editorial, 2014. ProQuest ebrary. Web. 5 November 2016.

Gómez Fernández, Luis, and Andrés Álvarez, Ana. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Madrid, ES: AENOR - Asociación Española de Normalización y Certificación, 2012.

Devia, G. A. V., & Pardo, C. J. (2014). Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT. Sistemas & Telemática, 12(30), 35-48.

Castro, A. R., & Bayona, Z. O. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. Ingeniería, 16(2), 56-66.

Medina Tapia, M. A. (2015). Estudio analítico de la compatibilidad e integración de las normas ISO/IEC 31000 e ISO/IEC 27005 referente a riesgos en la seguridad de información (Doctoral dissertation, Universidad de las Fuerzas Armadas ESPE. Carrera de Ingeniería en Sistemas e Informática.).

Apéndice A. Consejo Editor ECORFAN

9 786078 324859
ISBN 978-607-8324-85-9