Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

GESTIÓN DE ACCESO A LA INFORMACIÓN EN LAS PEQUEÑAS Y MEDIANAS EMPRESAS DE GUATEMALA, UTILIZANDO ESTÁNDARES INTERNACIONALES

Rodrigo Esteban Azurdia Muñoz
Asesorado por el Ing. Gustavo Adolfo Alvarado Villatoro

Guatemala, marzo de 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

GESTIÓN DE ACCESO A LA INFORMACIÓN EN LAS PEQUEÑAS Y MEDIANAS EMPRESAS DE GUATEMALA, UTILIZANDO ESTÁNDARES INTERNACIONALES

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

RODRIGO ESTEBAN AZURDIA MUÑOZ
ASESORADO POR EL ING. GUSTAVO ADOLFO ALVARADO VILLATORO

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, MARZO DE 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Luis Pedro Ortiz de León
VOCAL V	P.A. José Alfredo Ortiz Herincx
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADORA	Inga. Virginia Victoria Tala Ayerdi
EXAMINADOR	Ing. Edgar Eduardo Santos Sutuj
EXAMINADOR	Ing. Ludwin Federico Altán Sac
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

GESTIÓN DE ACCESO A LA INFORMACIÓN EN LAS PEQUEÑAS Y MEDIANAS EMPRESAS DE GUATEMALA, UTILIZANDO ESTÁNDARES INTERNACIONALES

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha septiembre de 2010.

Rodrigo Esteban Azurdia Muñoz

ACTO QUE DEDICO A:

Dios Por ser el creador de todo y haberme dado la sabiduría de finalizar este proyecto. “Gracias por permitir cumplir este sueño” Mateo 7:7-8.

Mis padres Ernesto Azurdia Arriola, por ser un padre como ningún otro y tener la paciencia y ejemplo que me hace estar orgulloso de ser su hijo. Gracias papá, lo logramos.

Mercedes Elisa Muñoz de Azurdia, por haberme guiado y escuchado mis penas, darme consejos a lo largo de la vida, una mujer ejemplar que me enseñó a trabajar duro para lograr metas. Tu ayuda incondicional mamá, me da las fuerzas de cada día.

Mi abuelo Benjamín Azurdia Mendoza (q.d.e.p.), por su entusiasmo y espíritu emprendedor. Guilo, sus anécdotas me inyectaron lo que soy, sé que lo veré pronto.

Mis hermanos Ernesto Rabindranath Azurdia Muñoz, por su orientación y ejemplo para nunca rendirme.

Mauricio Andrés Azurdia Muñoz, por los pequeños pero valiosos consejos en mi trayectoria de vida.

Mis tíos Elsa de Quiñónez (q.d.e.p.)**,** Antonio Azurdia (q.d.e.p.), Beatriz, Estuardo y Miriam Azurdia. Por el apoyo que me han brindado en cada etapa de la vida.

AGRADECIMIENTOS A:

Dios Por haberme otorgado la vida necesaria para alcanzar esta meta.

Mis padres Por haberme brindado todo lo que necesité, su amor y guía me hacen sentir orgulloso de tenerlos a mi lado.

Mis profesores Susan Bryan, Blanca Álvarez, Ligia Ortiz, Francisco Quiñónez y Miriam Peralta, por ser pilares fundamentales en mi educación.

Mi asesor Gustavo Alvarado Villatoro, por su amistad, compromiso, consejos y ayuda para culminar la meta.

Mis amigos William Yon, Ariel Valdez, Luis Ángel Grijalva, Juan Paulo Vaides, Melvyn Ramos, Nisdem Arenales, Luis Quiñónez, Jonathan Quiacain, Víctor Hernández, Juan Pablo Caballeros, Karen García, Raúl del Cid, Miguel Lemus, Antonio Meoño, Oscar Miranda, Marlon Castillo, Arelis González, Félix Medrano, Jorge Dávila, Mauro Ortega, Marco Hernández, Fabiola González y Leslie García. Les agradezco su apoyo en cada etapa de mi vida, tanto personal como profesional.

Universidad de San Carlos de Guatemala Por abrirme las puertas de la sabiduría intelectual.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Activos Conjunto de bienes tangibles o intangibles que posee una empresa. Se consideran activos aquellos bienes que tienen alta probabilidad de generar un beneficio económico a futuro. Los activos de un negocio varían de acuerdo a la naturaleza de la empresa.

Benchmarking Evaluación comparativa que establece un punto de referencia a partir del cual se comparan de manera sistemática los productos, servicios y métodos de una empresa respecto a sus competidores.

CEO C*hief executive officer*. Director ejecutivo también conocido como ejecutivo delegado, jefe ejecutivo, presidente ejecutivo y principal oficial ejecutivo.

CIO *Chief Information Officer*. Director ejecutivo en info-tecnología, director ejecutivo en informática, director ejecutivo en sistemas de información, ejecutivo principal en toda el área tecnológica.

Cloud Computing La computación en nube, del inglés *cloud computing*, es un paradigma que permite ofrecer servicios de computación a través de Internet.

COBIT	Conjunto de mejores prácticas (marco) para la tecnología de la información (TI), creado por la Comisión de Auditoría de Sistemas de Información y Asociación de Control (ISACA) y el *IT Governance Institute* (*ITGI*) en 1996.
Confidencialidad	Garantizar que la información es accesible sólo para entes autorizados.
Disponibilidad	Acceso a la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a disponer de los recursos protegidos y capacidades asociadas.
Firewall	Un muro de fuego (*firewall* en inglés), parte de un sistema o una red diseñada para bloquear el acceso no autorizado, permitiendo únicamente comunicaciones autorizadas.
GDAI	Grupo de acceso a la información. Personas, entidades o dispositivos que tienen acceso a un determinado fragmento de información que comparten para un bien en común.
Gestión	Proceso que desarrolla actividades productivas con el fin de generar rendimientos de los factores que en él intervienen.

Hacker	Experto en redes y seguridad que accede a sistemas a los que no tiene autorización sin ánimo de causar daño, generalmente para aprender más y superarse a sí mismo.
Información	Conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que lo recibe. Desde el punto de vista de la teoría general de sistemas, cualquier señal o *input* capaz de cambiar el estado de un sistema constituye un pedazo de información.
Integridad	Seguridad de que una información no ha sido alterada, borrada, reordenada, o copiada, durante el proceso de transmisión o envío, en su propio equipo u origen.
Interface	Lugar de la interacción, el espacio donde se desarrollan los intercambios.
ISM3	Marco para la Seguridad de la Información Sistemas de Gestión. Vela por la definición de niveles de seguridad adecuada a la misión de negocio y que representen un alto retorno de la inversión. Permite la mejora continua de los sistemas ISM utilizando métricas.
ISO	Organización Internacional para la Estandarización.
IT	Tecnología de la Información, en inglés *Information Technology.*

ITIL	Del inglés *Information Technology Infrastructure Library*, marco de trabajo para buenas prácticas destinadas a facilitar la entrega de servicios en tecnología de la información (TI). Resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones.
Outsourcing	Subcontratación, proceso económico en el que una empresa mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato.
PDA	Del inglés *Personal Digital Assistant* (Asistente Digital Personal), computador de mano, originalmente diseñado como agenda electrónica.
Phising	Término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas.
Postmortem	Después de la muerte.
Prince2	Método basado en procesos para la gestión eficaz de los proyectos.
PYME	Pequeñas y medianas empresas.
Riesgo	Vulnerabilidad de bienes ante un posible o potencial perjuicio o daño.

SaaS	Por sus siglas en inglés, *Software as a Service,* ejecuta un servicio que no se encuentra en un servidor físico sino virtual dentro de la nube.
Sistema	Conjunto de elementos organizados y relacionados que interactúan entre en sí, para llegar a un mismo objetivo y beneficio en común.
SGS	Sistema de Gestión de la Seguridad. Parte de un sistema general de gestión establecido por una organización que incluye la estructura organizativa, planificación de las actividades, responsabilidades, prácticas, procedimientos, procesos y recursos para desarrollar, implantar, llevar a efecto, revisar y mantener al día.
SGSI	Sistema de Gestión de la Seguridad de la Información. Parte del sistema gerencial general, basada en un enfoque de riesgo comercial para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
Sniffer	Programa de captura de las tramas de red.
Staff	Grupo de empleados dentro de la compañía que vela por alcanzar los compromisos adquiridos en cada Departamento y monitorea el seguimiento y finalización exitosa de un proyecto.

Stakeholders	Quienes pueden afectar o son afectados por las actividades de una empresa.
TICS	Tecnologías de la información y de la comunicación.
TGS	Teoría General de Sistemas (TGS) o enfoque sistémico. Esfuerzo de estudio interdisciplinario que trata de encontrar las propiedades comunes de entidades llamadas sistemas.
VOIP	Voz sobre Protocolo de Internet, también llamado Voz IP, VozIP.
VPN	Red en la que algunas partes se conectan usando internet público, los datos enviados por esa vía se cifran, de manera que toda la red es virtualmente privada.
Wrapper	Componente que incluye el sistema para mostrar otro sitio *Web* o una URL en el propio sitio *Web*.

RESUMEN

Recopilar información en una compañía puede dificultarse, pero es más difícil mantenerla a salvo, esto conlleva altos costos y tiempo, lo que reduce las ganancias haciendo a la empresa menos productiva por fallas o incidentes que no se pueden solucionar de manera inmediata, debido a que con frecuencia se carece de un plan de acción al respecto.

Las empresas buscan mantener control de los activos de información que les permita manejarla más ordenadamente, creando sinergia en cada área laboral, procurando que su manipulación y el acceso a ella sea más efectiva. Contar con un panorama que incluya los puntos que se deben considerar antes de comenzar a realizar cambios en la administración y acceso de la información, es de suma importancia. Manejar adecuadamente la información no solamente facilita a cada una de las empresas mantener sus activos resguardados, sino que además ayuda a contar con documentación fidedigna permitiendo llevar un control de toda la gestión de acceso a la información, a través de la implementación de estándares que velan por la calidad.

La utilización de estándares internacionales asegura crear un orden relacionado con la gestión de acceso a la información, sin embargo es responsabilidad de la compañía darle el debido seguimiento para que esta práctica se convierta en una mejora permanente. Con mayor frecuencia las empresas buscan certificarse observando estándares que les permitan competir

con entidades extranjeras; esto conlleva muchas ventajas de las cuales cabe mencionar competir en contratos internacionales, adjudicación de servicios, manejo adecuado de incidentes y gestionar la información de manera continua, entre otros.

Esos estándares implementan bitácoras para el registro de acontecimientos y datos relevantes lo que representa, no únicamente, valor agregado sino que mantiene ordenada la información para tenerla al alcance del personal. Esto brinda también respaldo y fiabilidad para los clientes, asegurando que sus datos son tratados adecuadamente, de manera física y virtual.

Los estándares que actualmente se implementan son: *ITIL*, ISO/IEC 27000 y *COBIT*, se aconseja utilizar las mejores prácticas de cada uno dependiendo del área en que se aplican; cabe recalcar que también existen certificaciones que ayudan a mejorar su implementación. La meta a alcanzar es llegar a crear un Gobierno de TI que pueda mantener una visión completa de toda la empresa, el encaminamiento más próximo es por medio de ISO/IEC 38500:2008 el cual guía la dirección de las organizaciones y se utiliza además, para monitorear el uso de tecnologías de información.

Para ayudar a la Pequeña y Mediana Empresa –PYME- se creó una guía práctica que puede utilizarse en la certificación de estándares internacionales, con base en el análisis realizado por medio de una encuesta, dirigida a personal relacionado con tecnología de la información en el sector privado.

OBJETIVOS

GENERAL

Contribuir con el sector empresarial guatemalteco a brindar seguridad en la información, a través de una adecuada gestión de acceso que garantice integridad, confidencialidad y disponibilidad mediante lineamientos y seguimiento de buenas prácticas en la organización.

Específicos

1. Contribuir a expandir el conocimiento respecto a la gestión de la información por medio de una herramienta que mitigará la distribución no autorizada de la misma.
2. Incidir en el sector empresarial para la utilización de estándares internacionales en gestión de acceso a la información.
3. Aprovechar los estándares internacionales en gestión de acceso a la información, para obtener reconocimiento y apertura a mercados globalizados.
4. Ofrecer lineamientos para el diagnóstico de la empresa, referente a la gestión de acceso a la información.
5. Orientar el uso de medidas y lineamientos para que puedan implementarse estándares internacionales en gestión de acceso a la información en la compañía.

INTRODUCCIÓN

Conservar la información segura es un punto importante en la empresa u organización, lo deben tomar en cuenta al momento de realizar un análisis que encierra las políticas de seguridad dentro de la misma. Manejar la seguridad de la información es vital para evitar ataques físicos y virtuales de los datos, información confidencial de clientes y proveedores, investigaciones, estrategias de mercado y demás partes.

El presente trabajo de graduación tiene como alcance brindar recopilaciones fidedignas sobre las instituciones, normas y reglas que involucra la organización utilizando la gestión de acceso la información en las pequeñas y medianas empresas en Guatemala. Realizar un análisis de las consecuencias y buenas prácticas, le permitirá guiar a la organización en el proceso de implementar y utilizar las herramientas adecuadas.

Ampliar los detalles sobre el acceso a la información en las normas ISO/IEC 27000, *ITIL*, *COBIT*, permite un manejo adecuado y constante de los estándares internacionales de seguridad aplicados en la industria actualmente y trasladar mayor seguridad en los activos de información de la organización.

1. GESTIÓN DE ACCESO A LA INFORMACIÓN

1.1. La administración del conocimiento

Concepto que se refiere a transmitir dentro de una organización la información y la experiencia de cada uno de los miembros para lograr reutilizar o mejorar la calidad de información. Recopilar la información puede resultar sumamente difícil y mucho más poder transmitir este conocimiento a nuevas generaciones, el proceso debe ser respaldado por técnicas de captura, organización y almacenamiento de la actividad de cada uno de los colaboradores. El desarrollo de esta estrategia se ha realizado por medio de TICS que nos permiten obtener una ventaja competitiva para aprender de los éxitos y fracasos que pueden ocurrir dentro de la compañía.

Se menciona que conocimiento es “El capital intelectual y todo aquel pensamiento que se puede convertirse en valor”[1] esta definición se cumple y más cuando existe tanta información que solamente conocen los colaboradores dentro de la empresa; si ellos emigran, se pierde un gran valor que es difícil recuperar al no existir ciertas herramientas o técnicas para recopilación del conocimiento.

[1] Tomada de Leif Edvinsson, Daniel Ochoa, 2000.

[2] Tomás Bradanovic, Asesoría y Proyectos, 2010.

1.2. Gestión de acceso a la información

Incluye la realización de procedimientos que pueden abarcar uno o más pasos para desarrollar actividades productivas, se llevan a cabo para realizar una tarea específica o generar rendimientos de los factores que en ellas intervienen. Se siguen lineamientos bien definidos para que el trabajo se realice con éxito o satisfacción de una meta.

Un conjunto de datos sin procesar tiene poca importancia dentro de una compañía, pero que al transformarlo y clasificarlo adquiere significado e importancia conociéndole como “información”, ésta tiene vigencia, validez y valor que se puede transformar con el paso del tiempo. La información puede estar restringida para ser utilizada solo por un determinado grupo de personas quienes acceden a ella pudiéndola examinar, analizar, manipular y operar con base en sus datos. Las personas, entidades o dispositivos que tienen acceso a un determinado fragmento de información que comparten para un bien en común, se denominan “Grupo de acceso a la información” –GDAI-.

El uso de la información, dentro de una organización, es sumamente extenso debido a la cantidad de datos que pueden recopilarse y dependiendo del área de trabajo. Para ejemplificar se puede mencionar una Fábrica de Calzado, ésta realiza varios procedimientos y está integrada por departamentos que se relacionan entre sí para lograr el resultado final que es la fabricación y envío de zapatos a los clientes.

Lógicamente la fábrica debe llevar un manejo de las campañas de mercado y ventas realizadas, registro de los catálogos de diseño, colores y calidad del cuero que se utiliza como materia prima; además se lleva un control de hormas y moldes para la suela y los ornamentos adicionales como cintas, telas de cubierta, encerado, espuma de plantillas, entre otros.

Estos registros originan información vital para la compañía, agregando lo relacionado con los diseños originales realizados en cada temporada, los procesos de trabajo por cada familia de calzado, tiempos de producción, además, pedidos que se realicen a los diferentes proveedores, la fecha de entrega, logística, departamento legal y otros.

Esta información es vital para la compañía por lo que debe mantenerla almacenada y con fácil acceso para diferentes áreas de trabajo, convirtiéndose en confidencial. Cada equipo de un área involucrada puede considerarse un GDAI que mantiene contacto con la información que le corresponde debiendo cuidarla de intrusos previendo que los datos estén resguardados en computadores y dispositivos móviles seguros de robo de *mails*, ideas y alcances que la misma empresa tenga proyectada a futuro.

La información como se observa es de vital importancia para el GDAI, sin embargo, si llegara a ser utilizada por personas o dispositivos ajenos sería sumamente peligroso para la organización. Es por ello que la gestión de acceso a la información, se basa en la administración de los procedimientos y procesos que conlleven a utilizar la información de manera segura y confiable en un momento determinado para lograr un beneficio en común dentro de la

organización, además debe comprenderse que a la información solamente pueden acceder los miembros y dispositivos que tengan autorización.

Muchas empresas se preguntan:

- ¿Cómo puedo mantener la información importante en manos de las personas adecuadas y que esta se mantenga de manera confidencial?
- ¿Cómo puedo otorgar el acceso de información al personal, de manera efectiva?
- ¿Qué impacto tiene sobre la organización el robo de información de ventas, estrategia de mercado, proveedores, clientes y análisis financieros?
- ¿Cómo tener acceso a toda la información y validar que cada área pueda visualizar solamente lo que le corresponde?
- ¿Qué metodología o tecnología existe para implementar seguridad de información dentro de la organización?

Para responder a esas interrogantes se echa mano de la gestión de acceso a la información que incluye la administración de los procedimientos que mantienen la información segura por medio de procesos categóricos y seguros que permiten la regencia utilizando estándares y reglas de su fácil manejo.

Lo que se logra dentro de la compañía es el cumplimiento de estándares de seguridad, gestión de solicitudes de acceso, seguimiento y validación de las mismas ya sea de forma física o digital a un GDAI. Dentro de la gestión de acceso a la información se deben considerar cinco aspectos importantes:

confidencialidad, integridad, disponibilidad de activos de información, riesgos de seguridad y un sistema de gestión de la seguridad. Esta es una tendencia que cada vez más las organizaciones están adoptando y utilizando en sesiones laborales.

1.2.1. Confidencialidad

La externalización de información cada vez es más común dentro de las organizaciones en donde se le da el control a un equipo de trabajo ajeno a la empresa, las áreas que se externalizan suele ser Recursos Humanos, Asesoría Legal, Contabilidad entre otros.

El término confidencialidad se refiere a la propiedad de la información, garantiza que la accesibilidad será otorgada a personal autorizado. Esta debe incluir a todas las organizaciones, departamentos, individuos y dispositivos electrónicos que estén incluidos para acceder a la información que les corresponda .

La información puede corroborarse si es confidencial y sensible dentro de la compañía al momento de divulgarlo a cierto grupo de individuos y que conlleva estas acciones positivas o negativas. Es útil resaltar que la confidencialidad es una forma de llevar también un control de qué información es relevante para la compañía y cómo ésta puede asegurarse utilizando subprocesos garantizados.

1.2.2. Integridad

La integridad se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada o copiada durante el proceso de transmisión. Este aspecto es indispensable debido a que constituye una fuente valiosa para la toma de decisiones dentro de la empresa[2].

Existen diferentes tipos de integridad: personal, datos, mensaje, referencial y moral, están amarrados a un mismo fin que es proveer información fidedigna y correcta en cualquier momento. La precisión que se maneje en cada parte de la integridad es muy importante. Se considera que deberán existir diferentes niveles de integridad desde el básico operacional hasta el gerencial. Asimismo, se debe tomar en cuenta la parte que ocupa la informática para mantener íntegros los datos al momento de utilizarlos.

1.2.3. Disponibilidad de activos de información

La disponibilidad se refiere a contar con la información cuando ésta es requerida para el proceso de negocio ahora y en el futuro, también está relacionada con en salvaguardar los recursos necesarios[3].

Los activos de información incluyen un conjunto de bienes dentro de una compañía. Se pueden definir como todos los bienes tangibles o intangibles que

[2] Tomás Bradanovic, Asesoría y Proyectos, 2010.
[3] Objetivos de Control para la Información y Tecnologías Relacionadas, Gobierno de Mendoza, Argentina 2005.

utilizan un determinado GDAI para generar beneficio económico en la organización. Esta disponibilidad permite mantener y consultar todos los activos importantes para la organización, deben estar en cualquier momento, a disposición del GDAI y ser almacenados de forma adecuada para usos futuros.

Lo relativo a la disposición de activos de información dentro de una organización se puede ejemplificar en una compañía que se dedique al aseguramiento de vehículos. Deberá contar con una base de datos adecuada para el manejo de las empresas a las cuales presta servicio y adicionalmente llevar el control de pagos mensuales, quincenales o anuales que la compañía cobra. Toda esta información debe estar a disposición de los empleados que laboran por si llegara a ocurrir algún accidente y se requiera la información de inmediato para realizar el procedimiento establecido, respecto al seguro.

Esta información puede llamarse activos de información debido a que maneja datos que a su vez se convierten en beneficios no solo para la compañía de seguros sino también para los beneficiarios que necesitan ese apoyo para cubrir sus necesidades.

El no disponer a tiempo o de manera correcta de la información, podría invalidar el pago del seguro o el actuar en un asunto legal. Otro aspecto importante que se puede ejemplificar es el cobro de seguro en las empresas, si la disponibilidad de las fechas de corte no son correctas podrían dañarse los compromisos que la compañía de seguros tenga pactados.

1.2.4. Riesgos de la seguridad

Se define por riesgo como lo que representa una vulnerabilidad para la información y como ésta puede ser manipulada en contra de la empresa. Debe tenerse claro que riesgo es distinto a amenaza, la amenaza consta de actos dirigidos o deliberados (terrorismo, *hackers,* entre otros) y aleatorios o impredecibles (terremoto o rayos) los cuales pueden afectar de manera significativa la información.

El riesgo de la seguridad exige una práctica de mitigación sobre las posibles amenazas que pueden ocurrir y que en efecto podrían afectar la información, no verlo solamente como una responsabilidad más de resguardar los datos sino considerarlo activo necesario.

Los riesgos en una compañía pueden ser muchos, primero que nada se debe identificar prematuramente o idear un plan en donde resulte fácil observar situaciones que se puede volcar a ser un riesgo por medio de la detección e identificación de riesgos. Una vez se tiene claro que la compañía tiene algunos riesgos, se debe trazar una estrategia clara y concreta, y una vez definida se debe comunicar la estrategia de una forma clara y contundente a la entidad.

Se debe dimensionar la estructura que se necesitará para realizar la estrategia y valorar el número de recursos necesarios. Una vez que tengamos identificados los recursos necesarios también se debe asignar e identificar los

roles de trabajo y una vez claro los recursos y lo roles hay que definir las responsabilidades de cada rol dentro de la estrategia[4].

La organización debe efectuar un seguimiento de estos pasos para que sea satisfactorio mitigar los riesgos de seguridad. A continuación se detallan los riesgos que existen en la informática de los negocios:

- Riesgo de Integridad. Incluye los riesgos asociados con la autorización, totalidad y exactitud de la entrada además del procesamiento de las aplicaciones. Se manifiesta en múltiples lugares y momentos y en los componentes de los sistemas (interface de usuario, procesamiento de errores, interface, administración de cambios);

- Riesgo de relación. Se refiere al uso oportuno de la información creada por una aplicación, se basa directamente en la toma de decisiones (información y datos correctos de persona/proceso/sistema, en el tiempo preciso, permiten tomar decisiones correctas);

- Riesgo de acceso. Inadecuado acceso a sistemas, datos e información. Abarca separación inapropiada de trabajo como colocar la información en grupos de trabajo que no necesariamente la necesitan, acceso a base de datos y en paralelo con la confidencialidad que esto conlleva. Dentro de los niveles donde puede ocurrir este riesgo se encuentran el proceso de

[4] Norman Castro, Gestión del riesgo. Archivos de la temática gestión del riesgo, 2010.

negocio, aplicaciones, administración de la información, entorno de procesamiento, redes y nivel físico;

- Riesgo en la planeación e infraestructura. Se encuentra al momento que las organizaciones presentan debilidades por no poseer información tecnológica efectiva para soportar adecuadamente las necesidades presentes y futuras de los negocios, con un costo eficiente. Los riesgos se ven reflejados en la planeación organizacional, definición de aplicaciones, administración de seguridad, operaciones de red y computacionales, administración de sistemas de base de datos y en general afectan toda la información y el negocio;

- Riesgo de seguridad en general. Todo riesgo físico que se transforma en inseguridad de la información, de los empleados y de toda la organización como lo es el riesgo de choque eléctrico, incendio, niveles inadecuados de energía, radiaciones, riesgos mecánicos, inundaciones y riesgos de edificaciones[5].

1.2.5. Sistema de gestión de la seguridad (SGS)

Permite un conjunto de políticas y administración correcta de los procesos involucrados para llevar de manera organizada la información para que soporte cualquier cambio dentro de la compañía.

[5] La Alianza Empresarial para el Comercio Seguro, Riesgos Informáticos. Costa Rica, 2010.

Se incluye la estructura organizativa, la planificación de actividades, responsabilidades, las prácticas, los procedimientos y los recursos para desarrollar, implementar, llevar a cabo, revisar y mantener un seguimiento diario.

El SGS maneja los elementos de organización, personal, evaluación e identificación de los riesgos de accidentes, control, adaptación a modificaciones, planificación ante situaciones de emergencia, seguimiento de objetivos fijados y por último pero no menos importante, las auditorías.

El Sistema de Seguridad de la Información –SGSI- se utiliza para gestionar efectivamente la accesibilidad de la información, es un conjunto de políticas de administración directamente utilizado por la ISO/IEC: 27001 que busca asegurar la confidencialidad, integridad y disponibilidad de los activos de la información, minimizando a su vez el riesgo de seguridad de la información y manteniendo un vínculo de responsabilidad en todos los miembros que lo utilicen.

Existen modelos de SGSI que se especializan en mejorar o poder complementar lo mencionado por el modelo que van de la mano con metodologías como *ITIL*, *COBIT*, ISO/IEC 27001 o ISM3, que en lugar de centrarse en los controles, se centra en los procesos comunes de seguridad de información que se comparten en cierta medida en las organizaciones, estos se maneja formalmente a través reforzar, priorizar y optimizar la seguridad dentro de la organización, incluye las métricas del proceso.

Existen organizaciones que permiten realizar un benchmarking y la misma identificación de buenas prácticas en seguridad de la información como es ISF -*Information Security Forum*- basadas en “El estándar de las buenas prácticas para la seguridad de información”, el estándar se actualiza regularmente probando buenas prácticas y direcciones, estimulando a los miembros a ver una buena imagen de sus organizaciones y su desempeño en todos los aspectos de seguridad de la información.

Otros marcos de trabajo dirigidos por organizaciones como *COBIT*, *ITIL* o *PRINCE*2 los cuales abarcan lo conversado sobre el SGSI. Estos manejan metodologías similares validándolas dentro del marco de referencia que se cita en capítulos posteriores, relacionados con cada uno de ellos. El SGSI permite a la empresa administrar toda la información de forma metódica, esto se logra por medio de conocer, gestionar y minimizar los riesgos.

Dentro de las recomendaciones al implementar un SGSI están:

- Tener un fuerte compromiso por parte de la Alta Dirección, realizando un Comité de Seguridad
- Definir un modelo que abarque a toda la organización, no solamente la implantación y administración del SGSI
- El enfoque que se desee tomar fundamental (tecnológico u orientado a procesos, el alcance y ámbito de la aplicación, la metodología del análisis de riesgo)
- Identificación de los activos de la información y empezar a trabajar en un plan piloto sobre un proceso

- Selección de una aplicación que soporte el SGSI y que cumpla con la flexibilidad, adaptabilidad, implantación y administración del modelo

1.3. Áreas de aplicación

El área de aplicación para la gestión de acceso a la información dentro de una compañía es muy amplia, que se depende mucho de si ésta determina poner para su utilización; las áreas donde se recomienda utilizar inicialmente la gestión de acceso a la información las podemos dividir en generales y específicas.

Como generales podemos denominar las que están dentro de cada área de trabajo que son:

- Interna, manejo de la información por departamento involucrado
- Dirección, dirigentes de la organización
- Usuarios, directamente ligados con la compañía
- Seguridad, a nivel de la organización

Las específicas son las relacionadas directamente con una aplicación o un GDAI que opera la información en la compañía:

- Desarrollo de proyectos
- Sistemas implementados
- Comunicaciones dentro y fuera de la compañía
- Seguridad de acceso físico o digital

Las áreas serán diferentes en cada organización ya que las necesidades que cada una debe cubrir al inicio de implementar la gestión de acceso a la información dependerán de los estudios iniciales y de la identificación de necesidades primordiales.

Como ejemplo se menciona que para una entidad bancaria su mayor preocupación es resguardar la información de los clientes, manejo de transacciones, accesos de seguridad en bóvedas o departamentos de manejo de información sensible y la gerencial sobre el patrimonio, acciones y estrategias con planes a futuro. Por otro lado, en una institución hospitalaria, prevalecerá la información de sus pacientes y su historial médico, el manejo de la planilla de pagos de la entidad, el control de cobro a tratamientos a largo plazo y sobre todo, mantener en resguardo el acceso a los medicamentos, equipo y recursos adicionales del hospital.

Cualquier empresa puede tener la necesidad de realizar en un área específica la gestión del acceso a la información, todo depende de las áreas que desee abordar y los GDAI más críticos donde inicie.

Como recomendación deberá enfocarse en conocer que áreas son más vulnerables y necesitan mayor cuidado, además que sean las áreas donde se desee comenzar a realizar la gestión de la información y minimizar los riesgos.

1.3.1. Evaluación de sistemas y Departamentos dentro de una compañía

La evaluación de sistemas consiste en realizar un monitoreo constante que utiliza una empresa en una o más áreas que sirven para comunicar y relacionar la información de manera simultánea. Esta manera de llevar el control permite que los sistemas funcionen adecuadamente y que cada cierto tiempo se le valide que esté respondiendo a las necesidades del negocio proveyendo información fidedigna y en el momento preciso a la compañía y partes interesadas.

Cada departamento podrá estar regido por uno o más sistemas que se mantengan a la disposición de la compañía, también puede existir la posibilidad de utilizar un sistema, especialmente para cada área específica. La forma de evaluar los sistemas dependerá del equipo responsable, es necesario contar con una persona que conozca a profundidad cada uno de los sistemas o procesos que se manejen en las áreas involucradas; adicionalmente que exista una encargada, en la misma área, de explicar el funcionamiento del proceso de trabajo y cómo ingresan los datos al sistema para posteriormente, convertirlos en información.

Cabe resaltar que se deberá mantener un orden al momento de realizar este tipo de evaluaciones y el período del año en que se realizarán también, debido a que existen fechas críticas (cierre mensual, cierre anual, auditorías internas y externas, vacaciones, congresos y otros).

Aspecto importante es que se localice a la mayoría de empleados que conforman el área y al funcionario crítico del área disponible al momento de realizar estas evaluaciones, considerando una planificación y horas específicas de visita.

Las evaluaciones como se menciona, deben ser constantes y planificadas, validadas por la Alta Dirección permitiendo el total acceso a la información y procedimientos, dando un diagnóstico de cómo se encuentra actualmente el área revisada incluyendo fortalezas y debilidades del diagnóstico. Este informe debe ser dirigido tanto a la Alta Dirección como al área específica para que pueda realizar las correcciones necesarias en el sitio.

1.3.2. Control de proyectos

Los proyectos se consideran planificaciones que incluyen un conjunto de actividades interrelacionadas y coordinadas de manera correcta, para cumplir un objetivo en un tiempo estimado. Es necesario realizar proyectos para poder alcanzar objetivos dentro de un límite de presupuesto, calidades específicas y un lapso de tiempo previamente establecido. Se realiza inicialmente la idea del proyecto a ejecutar, el diseño y en conjunto un estudio de pre-factibilidad, ejecución y evaluación.

Dentro de un proyecto se cuida de manera muy minuciosa cada una de las etapas debido a que en cualquier momento se manifiestan riesgos o no

conformidades que ponen en peligro los compromisos que realice al inicio del proyecto. El tiempo, coste y alcance son primordiales para que no ocurra ningún contratiempo.

Existen factores externos que interviene en el control de proyectos, como los que a continuación se citan:

- El ambiente general que incluye todos los agentes externos que afectan de manera directa o indirecta como la economía, regulaciones de gobierno, normativas internacionales, costos de inflación, entre otros que se toman en cuenta al inicio de la planificación del proyecto;

- Las normas y códigos aplicables representan un conjunto de reglas y políticas que definen orden, lineamientos y pautas a seguir para el establecimiento de estándares sobre los cuales se deben regir las actividades planificadas. Pueden utilizarse normas como las de instituciones citadas a continuación: la Organización Internacional de normalización –ISO- por sus siglas en inglés, Sociedad Americana de Ingenieros Mecánicos -ASME- siglas en inglés, *ASTM International*, Administración de Servicios de Tecnología (*ITIL* por sus siglas en inglés), Marco Integrado de control interno –*COSO*- sus siglas en inglés, por mencionar algunas;

- Nuevas tecnologías se toman en cuenta al momento de realizar un proyecto, ya que la economía mundial sigue en cambio constante y el

fenómeno de globalización ha representado un reto grande para cualquier organización; en la planificación y sobre todo en la inversión, se debe tomar muy en cuenta la tecnología que desea utilizar la compañía, lo cual puede llegar a reducir el tiempo, cumplimiento de los objetivos, mejorar la calidad del producto o los servicios a brindar.

Para tener éxito en el proyecto deberá considerarse el entorno donde se desarrollará, los riesgos ambientales, el cumplimiento de entregas a tiempo, las condiciones que demanda el contrato, los papeles que se ponen en juego dentro en la comunidad y otros. Esto debe estar validado dentro del alcance y los objetivos previstos en las etapas iniciales y en el transcurso de la ejecución.

La determinación de los recursos es importante ya que también puede representar riesgos al momento de selección; se toma en cuenta que existen tres tipos de recursos: humanos, materiales y económicos. Cada uno puede significar el éxito o fracaso del proyecto, sumándose al desembolso de un capital innecesario o la interrupción de las acciones en cualquier etapa.

1.3.3. Seguridad física

Se refiere a las prácticas de la seguridad de la información dentro de las instalaciones donde se encuentra almacenada. Para resguardarla deben existir ciertas medidas a adoptar por todo el personal para que se cumplan y a la vez educar constantemente en la utilización de dichos procedimientos tratando que

esta práctica se convierta en una situación cotidiana dentro del manejo de las operaciones e información.

Cabe mencionar que el responsable de todo este procedimiento siempre es el Encargado de Informática quien asegura que todo esté correcto para un buen funcionamiento manteniendo segura la información, es la persona que propone el plan y garantiza que en cada uno de los puntos se manifieste su validez y mejoramiento.

La protección de oficinas, recintos e instalaciones es básica para el inicio de la seguridad física. Se deberá seleccionar un diseño y una área de trabajo en donde se puedan mitigar los daños ocasionados por un incendio, inundación, explosión, agitación civil, terremoto y otras formas de desastres naturales y sobre todo, validarlo en la región donde se planifican construcciones, esto es vital principalmente si la empresa desea relocalizar sus oficinas.

Si las oficinas ya están ubicadas, se deberán evaluar los riesgos que corre la información dentro de la misma y la implementación de medidas de seguridad de acuerdo a lo citado en el párrafo anterior. Al momento de evaluar la situación si esta área no cumple con los requerimientos planteados, se deberá cambiar asumiendo un plan de traslado del lugar.

Considerar lo que implica un lugar físico seguro y la protección de oficinas, recintos e instalaciones, se muestra la tabla a continuación:

Tabla 1. **Consideraciones de protección física.**

Almacenamiento de materiales peligrosos o combustibles en lugares seguros y a una distancia prudencial.
Almacenamiento de los *backups* o resguardos en un sitio seguro y distante del procesamiento.
Definición del área de recepción y/o entrega de información o implementación de procedimiento de acceso de personal autorizado, al centro de procesamiento.
Ubicación de los *backups* fuera de las oficinas, el traslado de dicha información debe ser un procedimiento establecido y previamente autorizado por la dirección y el encargado de informática.
El suministro de energía debe estar protegido de posibles fallas para evitar incendios; las medidas que se adopten deben ser revisadas por un experto y dejar documentada dicha información.
Cada equipo de cómputo debe tener una fuente ininterrumpida de poder (conocida como *UPS*), dependiendo del tamaño de su capacidad puede contener a uno o más equipos.
El generador eléctrico debe ser considerado si la necesidad de duración de la energía eléctrica es prolongada.
El cableado de energía eléctrica y comunicaciones debe quedar separado del de comunicación para evitar interferencia. Las canaletas deben resguardar cada uno de los cableados.
El mantenimiento de los equipos de trabajo debe ser programado por medio de un plan que integre la limpieza, resguardo y actualización de cada uno de ellos sin repercutir en el funcionamiento diario de la compañía. Realizarlo fuera del horario de oficina y por personal calificado y certificado, avalado por un proveedor si no pudiera realizarlo personal propio de la empresa.
Manejar la información confidencial dentro de los equipos por medio de la eliminación o respaldo, antes de realizar algún procedimiento.
En el inventario se detallará el tipo de equipo con que se cuenta por medio del registro respectivo, además el estado del mismo, área a la que pertenece y alguna observación importante que se desee registrar.
El resguardo de papeles y equipamiento consiste en mantener bajo llave cualquier documento confidencial o en una caja fuerte la cual debe ser a prueba de incendios o medidas extremas. Eliminar cualquier información digital del equipo que este duplicada.

Fuente: elaboración propia.

Realizar periódicamente revisión de cada una de las normas de seguridad establecidas y especificar que se continúen cumpliendo; si existiera alguna anomalía o falla debe modificarse ya que es invalidada por los cambios dentro de las políticas de seguridad.

1.3.4. Seguridad lógica

La seguridad lógica se debe manejar de manera confidencial, consiste en asegurar los recursos de los sistemas de información que puede ser material informático o programas diseñados dentro o fuera de la empresa para que sean utilizados de forma adecuada y con los propósitos correctos.

A diferencia de la seguridad física, consiste en la “concentración” de barreras y procedimientos que resguarden el acceso a los datos y que solamente puedan acceder las personas autorizadas. Entre los procesos que abarca debe existir una Gestión de Comunicaciones y Operaciones que permite mantener segura la información en todo momento y el acceso correcto a las personas responsables.

Debe regirse por procedimientos y responsabilidades operativas asignadas a encargados dentro de las distintas áreas y que sean ellos lo que administren la información. Las personas involucradas deben conocer la documentación para cada uno de los procedimientos operativos involucrados. El responsable del área de informática debe asistir en cada uno de los procedimientos, si éstos no son requeridos dentro de los dispositivos de la organización (por haberlos remplazado), adicionalmente deberá existir previa autorización. Es importante almacenar todos los medios en un ambiente seguro y adecuado siguiendo las indicaciones de los proveedores o de requerimientos que se hayan establecido dentro de la misma área de informática.

Los procedimientos de manejo de la información se incluyen a todos los documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicación de voz en general, multimedia, servicios postales, máquinas de fax, o cualquier otro dispositivo que se necesite protección. Cada protección es diferente y debe realizarse un plan para los distintos dispositivos mencionados y la forma de enfrentarla, si existiera alguna amenaza. Éste es el primer punto a tratar para mantener seguridad lógica dentro de la compañía.

Al momento de ocurrir cualquier problema dentro de la compañía, el procedimiento de manejo de la información para cada una de las unidades es vital, asimismo las instrucciones para el abordaje de errores excepcionales. Tener a mano un listado de los contactos de soporte de proveedores que pudiera necesitar la empresa en caso de algún imprevisto que no pueda ser resuelto por el área de informática y adicionalmente el reinicio de los sistemas si fuera necesario debido a fallas en el *software*, es necesario mantenerlo al alcance del personal involucrado quien debe tener acceso al cuarto de servidores y poder reiniciar las aplicaciones, sistemas o los comandos de acceso y de esa manera activar las bases de datos e información relevante y no afectar la operación diaria de los usuarios.

Se debe preparar la documentación sobre actividades que necesitan un procedimiento determinado como:

- Instalación y mantenimiento de equipos
- Instalación y mantenimiento de plataformas de procesamiento
- Monitoreo de procesamiento y comunicaciones

- Inicio y finalización en la ejecución de sistemas
- Programación y ejecución de procesos
- Gestión de servicios
- Resguardo de la información
- Reemplazo de componentes en las comunicaciones
- Utilización de correo electrónico

Esto no solamente permite mantener en un manual el procedimiento que mayor éxito pudiera generar al surgir alguna eventualidad sino que adicionalmente, le permite a todo el personal resolver en cualquier momento, si no se encontrara disponible el representante de informática.

Si volviera a darse algún suceso similar se maneja como un incidente a través de pasos al igual que un procedimiento, con la variante de que no solamente se debe actuar en base a los procedimientos ya establecidos sino buscando la causa que genera la eventualidad. Los problemas que mayormente ocurren son: fallas operativas, código malicioso, intrusiones, fraude informático, falla en comunicaciones, errores humanos y catástrofes naturales. Para cada uno de los incidentes debe mantenerse un Manual de Procedimientos y notificar a las líneas de mando jerárquico correctas para poder recibir apoyo en ejecución y aprobación del plan. Esto es necesario para que la Alta Dirección esté al tanto de lo ocurrido y conozca los riesgos y consecuencias que pudieran existir si no se actúa a tiempo.

Las acciones necesarias al momento de restablecer los sistemas, se citan a continuación:

- Definición de las medidas implementar
- Análisis e identificación del incidente
- Planificación de medidas que hagan que no vuelva a ocurrir este incidente
- Comunicación con las personas afectadas o involucradas con la recuperación del incidente
- Notificación a la organización

Al registrar los rastros por medio de una auditoría se evidencia lo recopilado al momento de la amenaza o riesgo, por medio de un análisis interno y revisión de posibles violaciones contractuales o de normativas se pueden llegar a un proceso judicial. En un punto más adelante se hablará de cómo dar seguimiento más profundo por medio de la auditoría forense de la información.

Como se mencionó se deberá de comunicar esto a la organización haciendo un plan de concienciación si fuera necesario para que las partes involucradas puedan prever este tipo de situaciones y que los incidentes se disminuyan, gran parte de los incidentes ocurren debido a la falta de comunicación para informar cómo se puede solucionar algún problema.

Esta información que se registra con cada incidente y como fue solucionado debe irse agregando al Manual de Procedimientos que se crea para cada dispositivo logrando que funcione como retroalimentación para toda la organización.

Una de las mejoras que se realiza dentro de un Departamento de Informática es la separación de instalaciones. Por mencionar un ejemplo podemos hablar de una compañía farmacéutica que maneja una base de datos de proveedores; el sistema se desea migrar o actualizar con módulos que harán más eficaz la información, lamentablemente se realizan dentro del mismo sistema, creando tablas en la base de datos en tiempo real y haciendo ajustes a los módulos al mismo momento que funcionan con usuarios finales.

Lo anterior trae como consecuencia que los usuarios perciban que el sistema no se comporte correctamente desconfiando de su buen funcionamiento, adicionalmente pudiera conllevar pérdida de captura de información vital para la compañía.

Estas previsiones benefician no solamente a los usuarios finales sino a los mismos desarrolladores que pueden ejecutar, modificar y crear información de pruebas sin ningún problema; la separación de entornos diferentes permite que la creatividad del mismo desarrollador esté enfocado al mejoramiento completo. Si este procedimiento se realiza en un determinado momento, es necesario mantener restringido el acceso a dichos editores de compilación dentro del sistema de desarrollo y cuando éste ya no sea necesario, bloquearlo. Algo importante es mantener los perfiles de acceso a las modificaciones dentro de los mismos sistemas y que éstos sean diferentes tanto para el sistema de desarrollo como para el operación o producción, estas interfaces permiten controlar a qué sistema se está accediendo.

La planificación y aprobación de sistemas es algo que se debe realizar en la seguridad lógica, dicha aprobación deberá realizarla el responsable del área informática y el de seguridad, solicitando las pruebas necesarias que permitan el aseguramiento del sistema a implementar. Dichas pruebas deberán ser diseñadas para realizar test con los usuarios finales involucrados que permitan evaluar el funcionamiento y la jerarquización, en base al acceso de la información que cada uno de ellos pudiera tener. Los test deberán ser llenados y certificados con los encargados de cada área.

Otro aspecto a cuidar es la protección contra el *software* malicioso, el responsable de seguridad informática define controles de detección y prevención. Dentro de los controles se pueden mencionar: Prohibición de uso de *software* ajeno a lo solicitado en la organización, redacción de procedimientos para transferencia de *software* e información, utilización y actualización de *antivirus*, actualizaciones de los sistemas operativos y aplicaciones, revisiones periódicas a los equipos de los usuarios, envió de boletines al personal para enfrentarse a códigos maliciosos o virus, concienciar al personal de la importancia de que cada uno pueda evitar riesgos que comprometan a toda la compañía.

El mantenimiento pretende conservar y lo que se consigue es mantener la información de manera segura por medio de resguardos en lugares apropiados siguiendo, como anteriormente se explica, el uso de procedimientos. Otro aspecto es el registro de actividades por parte del personal operativo llevando un control de tiempos de inicio y fin de los sistemas, errores y medidas correctivas, intentos de acceso, ejecución de operaciones críticas y modificaciones en la información de este tipo; llevando una bitácora de lo

ocurrido, la empresa al momento de enfrentar alguna amenaza, falla o riesgo cuenta con información para que se pueda solucionar de manera más eficiente el problema.

La administración de la red de comunicación dentro de una compañía es primordial, se maneja como seguridad lógica debido a que es un valor intangible que viaja a través de los departamentos y transporta toda la información vital. Esto reclama procedimientos para manejar tanto la administración dentro de la compañía y también de manera remota, estableciendo controles especiales para mantener la confidencialidad e integridad de los datos que atraviesan redes públicas o privadas, manteniendo la disponibilidad de la comunicación y servicios de red. Cada uno de los controles implementados deberá ser aplicado de igual manera a cada área, creando uniformidad en las comunicaciones de la empresa.

La restricción al acceso para asegurar que solamente pueda ingresar el personal autorizado a los dispositivos, manteniendo un registro de los usuarios que han accedido, por medio de una bitácora que almacene fecha y hora de ingreso. Se debe garantizar datos de entrada ingresen completos y que las salidas de información, como por ejemplo servicios *web*, envío postal y de fax se reenvíe una confirmación para saber que llegó correctamente la información ya sea por otro servicio web, una llamada telefónica o correo de recepción correcta.

Se debe tomar en cuenta la protección de todos los datos o información que se envíe por esta vía y que se mantengan en espera hasta llegar a su

destino; esto se debe evitar, de no ser posible se deberá mantener un monitoreo constante de la información ya sea por medio del sistema respectivo o por cortafuegos para evitar ingreso de intrusos.

El intercambio de información entre las organizaciones puede ser demasiado sensible para la información que se recopila en cada empresa, por ello se debe evaluar minuciosamente la seguridad y la información que se enviará hacia el otro lado del puente de información. Tomar en cuenta los siguientes aspectos:

- Responsabilidades gerenciales para las trasmisiones, recepciones y envíos de información
- Procedimiento de comunicación
- Normas de empaquetamiento, encriptamiento de los datos
- Responsabilidades definidas ante pérdida de datos
- Realización de convenio pactado por las dos partes interesadas, sobre la confidencialidad de la información
- Procedimientos de comunicación documentados y entregados a cada una de las partes interesadas
- Condiciones de uso de la información brindada

La seguridad del gobierno electrónico, es un aspecto que las instituciones utilizan para la comunicación de información vital y que permite realizar transacciones con las organizaciones. Los puntos que se deben validar son:

a) La autenticidad que valida el nivel de confianza sobre la identidad del usuario y el organismo
b) Niveles de autorización para emitir o firmar documentos
c) Procedimientos de oferta y contratación pública en donde se evalúe la confidencialidad de la información que se está enviando y no repudio de los contratos licitados
d) Trámites en línea que evalúa todos los datos suministrados con respecto a trámites y prestaciones ante el estado
e) Verificación que la información brindada por los usuarios, sea correcta
f) Cierre de transacciones para evitar posibles fraudes
g) Protección de la duplicidad en las transacciones
h) No repudio, manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió
i) Criptografía de la comunicación con el sistema de gobierno
j) Términos y condiciones de las responsabilidades tanto de la organización que se comunica como de la entidad de gobierno que actúa

La seguridad en el correo electrónico permite controlar toda la información que ingresa a la compañía, por medio de las bandejas de entrada de cada usuario. Para realizar un seguimiento se debe comunicar al personal sobre los posibles mensajes maliciosos que pudieran recibir y cómo actuar en esos casos. Otro aspecto a evaluar es el acceso remoto de las cuentas de correo, lo que implica enviar fuera de la compañía los listados de correos que pertenecen al personal y cómo afecta la misma confidencialidad al público. Todo lo citado en esta sección permite visualizar los posibles aspectos que debe abarcar la seguridad lógica dentro de la compañía.

1.3.5. Seguridad en la utilización del equipo

Es necesario mantener el aseguramiento del equipo lo más posible, como se pudo destacar en la seguridad física y lógica, se debe hacer énfasis en el equipo que almacena la información.

Para mejorar la seguridad del equipo y sobre todo en el que se utiliza de forma remota como equipo de oficina, servidores y cualquier otro dispositivo debemos considerar:

- Utilización de contraseñas: dentro del equipo o áreas específicas, éstas deben ser utilizadas al momento de ingresar al sistema, en correos electrónicos, apertura de archivos confidenciales, en compresión/descompresión de los mismos, ingreso a sistemas dentro y fuera de la empresa, acceso a base de datos, a dispositivos móviles, utilización de telefonía IP, claves en las fotocopiadoras e impresoras, ingreso a áreas restringidas. Cada una de estas medidas de seguridad deberán ser implementada, lo ideal es contar con una contraseña de 6 a 8 caracteres combinado con letras mayúsculas y minúsculas, números y signos; es aconsejable cambiar contraseña periódicamente para mayor protección;

- Encriptación de datos: la información se encuentra disponible en ordenadores que pueden estar dentro de la compañía o en computadores portátiles o dispositivos móviles que pueden ser utilizados fuera del recinto, para ello es necesario proteger los datos a través de métodos que

no los pongan en riesgo. En los usuarios que utilizan internet es fundamental implementarlo incluyendo la realización de compras electrónicas, el ingreso de tarjetas de crédito, publicación de información confidencial para que usuarios habilitados puedan acceder a ella, el ingreso a sitios *web* de antecedentes personales, o los datos que están dentro de un portátil o teléfono multifuncional, son solamente algunos ejemplos de contenido sensible que debe contar con las medidas de seguridad adecuadas para evitar problemas y no perder privacidad y confianza;

- Desconectar ordenadores o computadores cuando no se utilicen: esta medida permite mantener la información resguardada contra cualquier ataque debido a que no se puede acceder a ella si el computador no está conectado, adicionalmente reduce el riesgo de incendio accidental y el costo de por consumo eléctrico;

- Utilización de programas legales: básico en cualquier empresa debido al problema legal que puede conllevar, debe hacerse conciencia en la alta gerencia para mantener el licenciamiento de cada sistema al día y evitar así pérdidas de información por no tener actualizados los datos o utilizar claves de las que no se conoce su procedencia, esto no solamente fomenta estabilidad y seguridad dentro de la compañía sino que también fortalece los vínculos de las buenas prácticas en todos los trabajadores;

- *Antivirus y firewall* (cortafuego): la utilización de *antivirus* dentro y fuera de la organización garantiza que los sistemas se comporten debidamente manteniendo seguridad en la información, además que se detecte a tiempo cualquier ataque de virus o persona externa a la organización. Este

es un método preventivo necesario de mantenerse actualizado monitoreando la red contra cualquier posible ataque;

- Utilización de certificados digitales: le ayudan a la compañía a mantener la identidad de las personas y servidores involucrados dentro de una comunicación, garantizando la integridad de los datos que se transmiten, de modo que nadie puede alterarlos. Se gana confidencialidad y privacidad asegurando el origen de la información de modo que se puede verificar la identidad de la persona que la envía;

- Realización de *backups*: es necesario mantener periódicamente un plan para formalizar *backups* a los equipos de la empresa o bien mantener *backups* automáticos sincronizando la información, almacenándola dentro de un servidor de *backups*. Es prudente mantener por lo menos una semana antes la información y si fuera necesario restaurarla debido a robo, pérdida del equipo, accidente o falla del mismo equipo.[6]

1.3.6. Auditoría forense

Como recalcamos en el apartado de seguridad lógica y física, las amenazas y riesgos pueden existir en cualquier momento, pero se debe tomar en cuenta la eliminación de estos factores. De suceder hecho, es necesario dar un seguimiento lo más minucioso posible para saber cuáles son los factores que están afectando la seguridad y cómo se deben emplear técnicas para el seguimiento del acontecimiento, esto se logra por medio de un análisis forense. "La Auditoría forense en la actualidad es reconocida internacionalmente como

[6] La seguridad informática también es cosa tuya, Universidad Carlos III, Madrid, 2010.

un conjunto de técnicas efectivas para la prevención e identificación de actos irregulares de fraude y corrupción"[7].

Una auditoria forense es la actividad de un equipo multidisciplinario, a través de un proceso estructurado, donde intervienen contadores, auditores, abogados, investigadores, informáticos y otros, de acuerdo al tipo de empresa, sus dimensiones y diversidad de operaciones. Se puede requerir la participación de otros especialistas como ingenieros de sistemas, agrónomos, forestales, metalúrgicos, químicos, etc. que de la mano y bajo la conducción del Auditor Forense realizan la investigación. Para el área de informática se necesitan informáticos especializados y acreditados como auditores forenses que manejen el seguimiento de los acontecimientos y pistas de fuga de la información conllevando al por qué sucedió el hecho delictivo para realizar un plan de seguridad y prevención sobre este y otros posibles casos que puedan ocurrir.

El auditor debe ir más allá de la evidencia que se tiene dentro de la organización, debe estar abierto a interrogarse sobre la "buena fe" o "mala fe" de las personas que incurrieron en dicho problema. Los campos de acción del auditor deben guiarse por objetivos precisos respecto debido a las áreas que se ven involucradas.

Este especialista reclama estar certificado debido a los múltiples delitos que puedan ocurrir como enriquecimiento ilícito, soborno, malversación de

[7] Pablo Fudim, Contador Público (Universidad de Buenos Aires), Certified Internal Audit. (C.I.A.), Evaluador de Calidad (Q.A.).

fondos, conflicto de intereses, estafas entre otros. Un auditor forense no está limitado al sector público, puede actuar dentro del sector privado, manteniendo con la Alta Dirección y sus departamentos una comunicación abierta debido a que puede resultar incómodo y también sospechoso, no dar toda la información posible y que puedan implicarlo dentro en el delito.

Cabe mencionar que un auditor forense es imparcial debe velar porque el trabajo que realiza conlleve al cumplimiento o esclarecimiento del delito para que se encuentren si es posible, los culpables del hecho. Para cumplir con esto deben observarse los siguientes pasos:

a) Planificación: se obtiene toda la información necesaria, analizar los indicadores de fraude, evaluación del control interno, investigación a fondo para realizar el informe inicial y definir un programa de auditoría forense, debido a que ciertos delitos ya están catalogados con objetivos y procedimientos a seguir;
b) Trabajo de campo: es el trabajo necesario para llegar para llegar a las áreas involucradas, aquí es donde se necesita la participación de todo el personal interno (empleados) y externo (policía, ejército entre otros), debe siempre ser asesorado por un abogado si esto fuera necesario dentro del proceso judicial;
c) Comunicación y resultados: comunicación parcial o total de lo encontrado en el hallazgo, este debe ser un paso prudente y con información completamente revisada;
d) Monitoreo del caso: validar que al o los culpables se les dé el seguimiento adecuado para que este acto delictivo no vuelva ocurrir dentro de la organización.

La auditoría de la seguridad informática, comprende directamente el análisis y gestión de sistemas para identificación de fallas y posteriormente implementar correcciones en las vulnerabilidades que puedan existir dentro de las redes de comunicación, equipos de cómputo, enlace con proveedores o clientes externos dentro de los servidores.

Los métodos en las auditorías de seguridad informática se pueden realizar por medio de:

- Auditoría de seguridad interna: centrada en la seguridad y privacidad a nivel de las redes locales y corporativas;

- Auditoría de seguridad perimetral: permite revisión de un perímetro de la red local o corporativa y el grado de seguridad que se observa en las entradas de comunicación que esta posea;

- Test de intrusión: revisa cualquier intromisión por parte de terceros y se realiza por medio de intentar acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada;

- Análisis forense: revisión posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperatividad del sistema, el análisis se denomina análisis postmortem;

- Auditoría de páginas *web*: análisis externo de la *web*, comprobando vulnerabilidades como la inyección de código, verificación de existencia y anulación de posibilidades de *Cross Site Scripting* (*XSS*), saturación de peticiones al servidor web, entre otros;

- Auditoría de código de aplicaciones: análisis del código tanto de aplicaciones páginas web como de cualquier tipo de aplicación, independientemente del lenguaje empleado.

2. ESTÁNDARES INTERNACIONALES

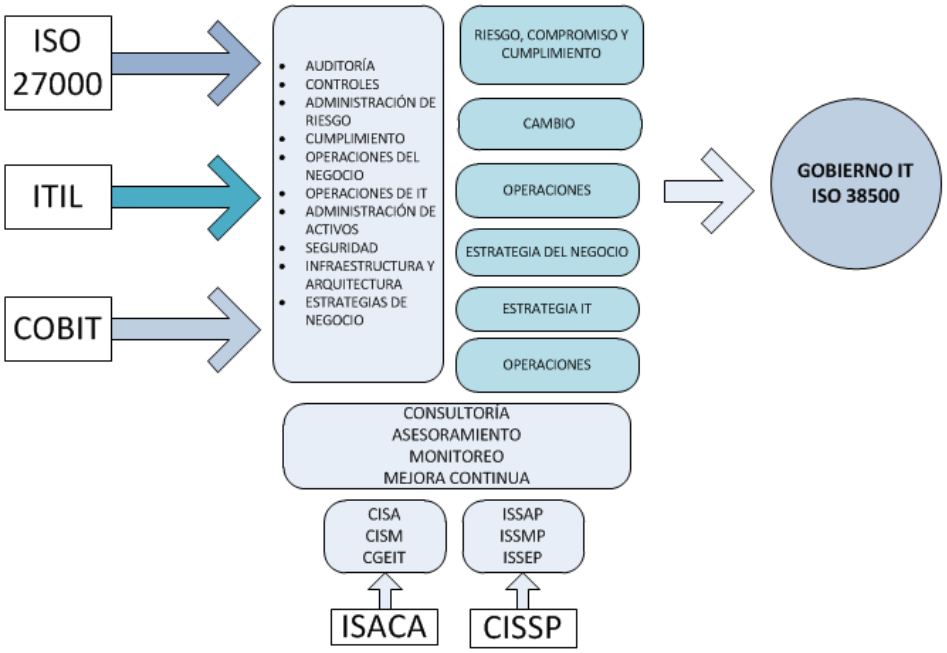
Los estándares son producto de diferentes organizaciones que en conjunto emiten determinado número de reglas y políticas para uso dentro de una o varias organizaciones. Su propósito es establecer normas que ayuden a uniformar las situaciones diversas que puede enfrentar una compañía, cada estándar puede estar enfocado a un determinado sector de mercado o industria para mejorar la calidad de la misma compañía y permita competir para lograr niveles de excelencia.

En el capítulo 3 se abarcará el análisis detallado de las tres instituciones certificadoras que engloban el marco mundial a nivel de seguridad en acceso a la información, basándose directamente en las secciones ISO *IEC* 27000 en conjunto con *COBIT* e *ITILv3*.

Los estándares por lo general suelen regirse a nivel internacional y son una manera de prevenir o superar un problema. A continuación se presenta un resumen de los diferentes tipos de estándares de políticas que existen en el mundo, que ayudan a realizar una gestión del acceso a la información de manera adecuada y que han sido catalogados como normas internacionales en las cuales una empresa se debe basar permitiendo la integración de la información de manera correcta. La idea fundamental es que estos estándares se orienten a un Gobierno de TI mediante el cual se dirige y controla el uso actual y futuro de las tecnologías de información. El estándar ISO 38500

encierra este concepto y ayuda a dirigir correctamente el encaminamiento de las normas que se plantean dentro de la organización. Para tener un idea más amplia de qué abarca el conocimiento de cada estándar cómo interviene, se puede incluye la siguiente Ilustración.

Figura 1. **Gobierno TI**



Fuente: elaboración propia.

2.1. ISO/IEC 27000

Conjunto de estándares desarrollados por la Organización de Estandarización Internacional, por sus siglas en inglés ISO y la Comisión internacional electromecánica por sus siglas en inglés IEC, proporcionan un marco de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Sus raíces están

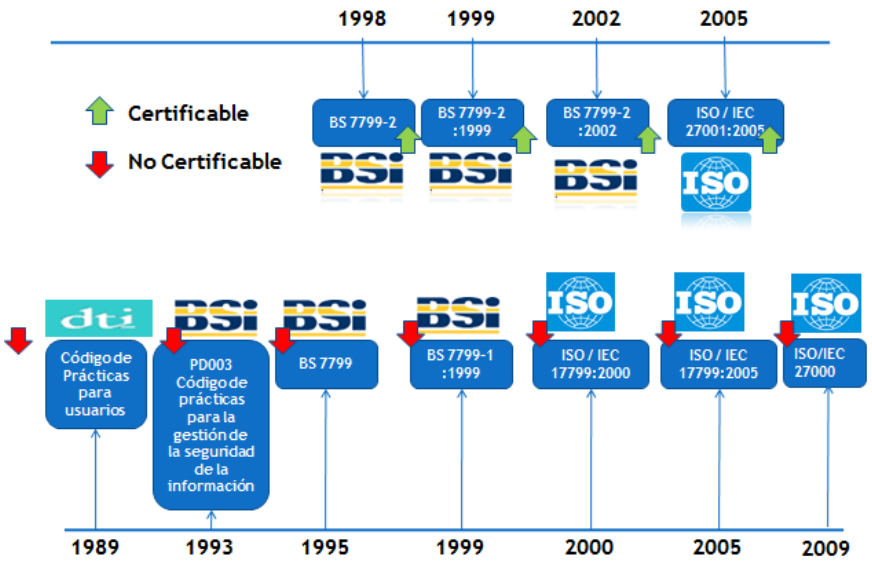
cimentadas por el Departamento de Información de Tecnología, por sus siglas en inglés -DTI- , la Institución de Estándares Británicos que por sus siglas en inglés -BSI- los cuales fueron la base fundamental para convertir lo que hoy es ISO 27000 y sus ramificaciones.

Para la adecuada gestión de la seguridad de la información es necesario implantar un sistema que aborde esta tarea de forma metódica, documentada y con base en objetivos claros de seguridad, evaluando los riesgos a los que está sometida la información de la organización. La utilización del estándar provee al establecimiento de una metodología de gestión de la seguridad clara y estructurada e implica una reducción del riesgo de pérdida, robo o corrupción. Los clientes mantienen acceso a la información a través de medidas de seguridad y los riesgos y sus controles son continuamente revisados.

Esto da como resultado el incremento de la confianza entre los clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial y operativa. Las auditorías externas que se realizan periódicamente ayudan a identificar las debilidades del sistema y las áreas a mejorar. Adicionalmente este estándar también puede integrarse con otros sistemas como ISO 9001, ISO 14001, OHSAS. El sistema permite operaciones necesarias de negocio tras incidentes de gravedad y la conformidad con la legislación vigente sobre información personal, propiedad intelectual, esto da como resultado que la empresa concurse a nivel internacional y exista un elemento diferenciador con la competencia, adicionalmente agregue confianza y reglas claras para las personas que dirigen la organización.

La reducción de costes y una mejora continua en los procesos y servicio, brindan adicionalmente aumento de motivación y satisfacción de todo el personal, realizando una evaluación de riesgos adecuada para la organización. El ISO 27001 asegura que el SGSI cumpla con los requerimientos dentro de la certificación, en el siguiente capítulo se realizará un análisis sobre las ventajas que el estándar posee. La siguiente figura muestra la ISO 27000 y la ISO 27001:2005 y su evolución.

Figura 2. **Evolución ISO/IEC 27000 y 27001:2005**



Fuente: elaboración propia.

2.2. *COBIT*

Por sus siglas en inglés *The Control Objectives for Information and related Technology* se refiere a los objetivos de control para la información y tecnologías relacionadas. Es un elemento crítico para el éxito y la supervivencia de las organizaciones, significa la administración efectiva de la información y de

la tecnología de la información (TI). Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar, comprenden y administran los riesgos asociados con la implementación de nueva tecnología, por lo tanto la administración debe tener una valoración y un entendimiento básico de los posibles riesgos que pueden ocurrir además de las limitantes de tecnología. En lo que ayuda *COBIT* es a salvaguardar estas brechas existentes entre el riesgo del negocio, necesidades de control y por supuesto, aspectos técnicos. Todo este conjunto de prácticas que utiliza permite a la empresa mantener habilidades sanas que ayudan a optimizar la inversión en información, pero lo más importante, representan aquello sobre lo que podrá ser juzgada si las cosas salen mal.

Todas las organizaciones por medio de *COBIT* deben cumplir con requerimientos de calidad, reportes de seguridad para la información como para sus activos. Para cumplir con toda esta responsabilidad debe mantenerse control interno por medio de un sistema o marco teórico que es el que brinda *COBIT*, con esto se logra que el impacto en los recursos de TI sea enfatizado en el Marco Referencial respectivo adicional a los requerimientos de información del negocio que deben ser alcanzados creando efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. El control que incluye políticas, prácticas y procedimientos organizacionales, es responsabilidad de la administración.

La administración mediante este Gobierno Corporativo, debe asegurar que la actividad sea ejercitada por todos los individuos involucrados en la administración, empleo, diseño, desarrollo, mantenimiento u operación de sistemas de información.

La orientación a negocios es el tema principal de *COBIT*. Está diseñada no solo para ser utilizada por usuarios y auditores. Sino por los propietarios a través de una lista de verificación, en inglés *Checklist*. La idea de esto es implementar empoderamiento o *empowerment* en los dueños de los procesos para que se les otorguen todas las responsabilidades y que por medio del marco referencial que ofrece *COBIT* pueda controlarse cada uno de los procesos del negocio que facilitan el cumplimiento de esta responsabilidad.

COBIT en cada inicio mantiene una premisa idéntica, en conjunto con 34 objetivos de alto nivel uno para cada proceso de TI que los agrupa en cuatro dominios:

- Planeación & Organización
- Adquisición &Implementación
- Entrega (de servicio)
- Monitoreo

El Marco Referencial *COBIT* otorga especial importancia al impacto sobre los recursos de TI, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. Además, el Marco Referencial proporciona definiciones para los requerimientos del negocio que son derivados de objetivos de control superiores en lo referente a calidad, seguridad y reportes fiduciarios en tanto se relacionen con Tecnología de Información.

La administración de una empresa requiere de prácticas generalmente aplicables y aceptadas de control y gobierno en TI para medir en forma comparativa conocida como *benchmark* tanto el ambiente de TI existente, como el planeado. *COBIT* es una herramienta que permite a los gerentes comunicarse y salvar la brecha existente entre los requerimientos de control, aspectos técnicos y riesgos de negocio.

Habilita el desarrollo de una política clara y de buenas prácticas de control de TI a través de organizaciones, a nivel mundial. El objetivo es proporcionar estos objetivos de control, dentro del marco referencial definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. Está orientado directamente a ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de riesgos asociados con tecnología de información y otras relacionadas dentro de la organización.

2.3. *ITIL*

ITIL es el método ampliamente aceptado para la gestión de servicios en el mundo, proporciona un conjunto coherente de mejores prácticas, extraídas de los sectores público y privado a nivel internacional. La biblioteca de Infraestructura de Tecnologías de la Información o más conocido como su acrónimo *ITIL*, se ha convertido ya en un estándar internacional dentro de la gestión de servicios informáticos; inició a finales del 1980 y servía como una guía para el gobierno de Inglaterra, esta misma estructura ha demostrado ser

útil para organizaciones en todos los sectores, base para la administración, educación y soporte de herramientas de informática.

Fué desarrollado al reconocer que las organizaciones tienen un vínculo cada vez más estrecho con la informática la cual utilizan para alcanzar cualquier meta corporativa. Esto como consecuencia, ha dado cada vez mayor énfasis a servicios personalizados y con un nivel de informática de mejor calidad que corresponda con los objetivos del negocio. Actualmente *ITIL* está utilizando la versión 3, de acuerdo a esta nueva versión se espera que *ITIL V3* pueda mostrar de mejor manera las inversiones en TI, asimismo integrar el negocio con el valor de TI y permitir un portafolio dirigido a los servicios.

Este deberá incluir un *ROI* (*Return On Investment*) o retorno de la inversión para hacer proyectos más viables enfocados en TI. También la adaptación ágil y modelos de servicio flexibles además de un rendimiento alineado con el negocio, validando todos los activos de servicios del mismo. *ITIL V3* introduce el concepto de servicios como activos, considera que un servicio es un activo para el consumidor y que éste se compone de dos entidades: utilidad y garantía.

La utilidad es el servicio en sí, suministrado por una combinación de personas, procesos y tecnología. Como ejemplos podríamos citar un servicio de introducción de pedidos y suscripción en línea de un establecimiento comercial o un plan de seguro de salud de una compañía.

La garantía es la seguridad de que la utilidad se ejecutará dentro de los niveles esperados. Por ejemplo, la citada herramienta de introducción de pedidos en línea podría garantizar factores tales como informar sobre la existencia de *stock* y el plazo de entrega[8].

2.4. ISACA

Sus comienzos fueron a través de grupos de personas que comprendían trabajos similares como auditoría de controles en los sistemas de computación y que cada vez se hacían más críticos para las operaciones de sus respectivas organizaciones. Luego se conoció como Asociación de Auditores de procesamiento Electrónico de Datos o por sus siglas en inglés *EDP Auditors Association*.

Las certificaciones que existen para ISACA son:

- CISA. Basado en la auditoría de sistemas y control interno;

- CISM. Administrador Certificado en Seguridad de los Sistemas de Información, es la certificación de ISACA dirigida específicamente a profesionales experimentados en la seguridad de la información. Está orientada a la gerencia de riesgos y seguridad de la información, así como al diseño y manejo de aspectos técnicos de la seguridad de la información a un nivel conceptual. Los profesionales con experiencia en temas de seguridad de información han encontrado en esta certificación una herramienta de gran valor;

[8] Sharon Taylor y Ken Turbitt, *Informe sobre mejores prácticas de gestión de TI*, BMC *software*. 2010.

- CGEIT. La certificación de Gobernabilidad TI reconoce un amplio rango de profesionales por su conocimiento y aplicación de las prácticas y principios de gobierno TI, al momento, más de 200 certificados CGEIT han sido otorgados. Esta certificación está diseñada para los profesionales que gestionan, administran, asesoran o tienen responsabilidades de aseguramiento con actividades relacionadas y conocimiento alrededor del tema de gobierno TI. Obteniendo este nombramiento, un profesional puede responder a la demanda creciente de las compañías en establecer un programa comprensible de gobierno TI que establezca responsabilidades e importancia a nivel empresarial.

ISACA se basa en principios de *COBIT* y otras certificaciones para poder enriquecer su conocimiento, investigaciones de TI, información de "*The IT Governance Institute*", *benchmarking* sobre las herramientas efectivas a cada uno de los profesionales que se certifican.

2.5. CISSP

Es una entidad que permite realizar certificaciones de información de la seguridad por el consorcio de certificación internacional de seguridad de sistemas de información por sus siglas en inglés (*ISC)2*, directamente está enfocada en la seguridad de la información la cual es relevante para los profesionales involucrados en este tópico. Este ha realizado un cuadro de términos y principios de seguridad de la información.

Las áreas de interés dentro de CISSP encierran:

- Acceso de control
- Aplicaciones de desarrollo de seguridad
- Continuidad de negocios y planificación de la recuperación de desastres
- Criptografía
- Administración de la información de seguridad y gestión de riesgos.
- Legales, reglamentos, investigaciones y cumplimiento
- Seguridad en las operaciones
- Seguridad física (ambiente)
- Seguridad en la arquitectura y diseño
- Telecomunicaciones y seguridad de la red

Cada área es un estudio que está conformado de forma detallada para comprender las técnicas y mejores prácticas de seguridad que pueden utilizarse en cada sección. Son consideradas como buen modelo para llevar a cabo la certificación.

CISSP está regulado directamente para una fuente común de conocimiento en el campo de seguridad de sistemas de información, proveyendo certificación para los profesionales y personas que deseen ponerlo en práctica. No es una guía sino más bien un certificado que acredita al que lo realiza, una forma de tener un conocimiento más amplio y con ayuda de la experiencia que éste posee, lograr mejorar la seguridad dentro de la compañía.

Luego de finalizar la certificación, el profesional puede tomar tres vías para especialización que son:

- Arquitectura de sistemas de información de seguridad profesional –ISSAP. Los puntos clave son la metodología para el acceso de sistemas de control, criptografía, integración de seguridad física, estándares de seguridad y toma de requerimiento y análisis, criterio, tecnología basada en aspectos de planeación continua dentro del negocio, planeación de recuperación por desastres y seguridad en telecomunicaciones;

- Sistemas de información de gestión de seguridad profesional –ISSMP-. Enfocado en la administración de políticas de seguridad, prácticas, principios y procedimientos. Clave en la cobertura de dominio donde se incluye la administración de prácticas de seguridad, visualización a lo largo de todo el sistema que engloba la empresa, leyes, investigaciones, auditoría forense y ética. Ser experto en la compañía y cumplimiento de medidas de seguridad;

- Ingeniería de sistemas de información de seguridad profesional –ISSEP-. Orientado para los profesionales que diseñen e ingenien seguridad de *hardware* o *software*, sistemas de información, componentes o aplicaciones. Los dominios cubren la certificación y acreditación, sistemas de seguridad, administración técnica, que se apegue a regulaciones de gobierno.

3. VENTAJAS Y BENEFICIOS DE LA GESTIÓN DE ACCESO DE LA INFORMACIÓN

El acceso de la información se implementa por una serie de procedimientos que se realizan a través por un conjunto de restricciones y excepciones de determinada compañía, éste es la base de todo sistema de informática y de otros sistemas integrados para accesar a la información. Un conjunto de procedimientos brinda mayor control de acceso al personal, garantizando seguridad y restricción a la información confidencial dentro de un área específica, adicionalmente monitorea su uso adecuado.

La gestión de acceso de la información deberá ser constantemente actualizada debido a las diferentes amenazas o riesgos que existen dentro de una compañía. La capacitación constante en cada área y la validación de las vulnerabilidades para mantener una retroalimentación y reforzamiento de los procedimientos es vital, si fuera necesario desechar uno de ellos para sustituir por otro que se acomode a las nuevas necesidades. Debe tomarse en cuenta que no es lo mismo tener la seguridad de una empresa donde hayan transcurrido 5 años que tenerla en los próximos años.

La gestión del acceso a la información, contribuye a la unidad de equipos y áreas de trabajo, manejando la comunicación en todas las vías de una manera más eficiente, adicionalmente mejora el comportamiento de los trabajadores de acuerdo a manuales y capacitaciones constantes. Esta

comunicación permite mantener control y orden a cada área, incluyendo la Alta Dirección. Otro aspecto importante es que permite mantener un nivel de confianza interno y externo que no solo eleva la percepción de excelencia en quienes colaboran con la empresa, sino que promueve que los mismos interesados conozcan el compromiso que se tiene y los estándares de manejo de la información que los hace fiables para realización de operaciones.

3.1. Análisis FODA de estándares actuales.

La manera de visualizar este análisis es manejando una alineación en cada estándar y subrayar los beneficios que cada uno ofrece, dentro de ellos destacan los de ISO/IEC 27000, *ITIL* y *COBIT*. Este análisis centrará directamente a la gestión de acceso a la información en cada uno de los estándares a revisar y le dará a la compañía una mejor visión de lo necesario para comenzar la gestión de acceso a la información.

Utilizando el documento ***Aligning COBIT4.1, ITIL V3 and ISO/IEC 270002 for Business Benefit*** de la institución *IT Governance Institute* y la Oficina de Comercio de Gobierno por sus siglas en inglés -OGC-, se realiza un análisis de cada una de las fortalezas, oportunidades, debilidades y amenazas que puede presentar cada estándar.

3.1.1 Requerimiento comercial para el control del acceso

Tabla 2. **Requerimiento comercial para el control del acceso**

ISO/IEC 27002:2005		***COBIT* 4.1 Objetivos de control**		**Referencia *ITIL V3***	
A 11.1.1	Políticas de control de acceso	PO2.2	Diccionarios de datos de la empresa y reglas de sintaxis de los datos	SD 4.6.4	Políticas, principios y conceptos básicos
		PO2.3	Esquema de clasificación de los datos	SD 4.6.5.1	Control de seguridad (cubre a alto-nivel, no a detalle)
		PO6.2	Riesgo corporativo y marco de referencia de control interno de TI	SD 5.2	Administración de datos e información
		DS5.2	Plan de seguridad de TI	SD 7	Consideraciones de tecnología
		DS5.3	Dirección de identificación	SO 4.5	Dirección de acceso
		DS5.4	dirección de cuentas de usuarios	SO 4.5.5.1	Petición de acceso
				SO 4.5.5.2	Verificación
				SO 4.5.5.4	Supervisión de identidad de estado
				SO 4.5.5.6	Eliminación o restricción de acceso

Fuente: ***Aligning COBIT4.1, ITIL V3 and ISO/IEC 270002 for Business Benefit*, Pag.111**

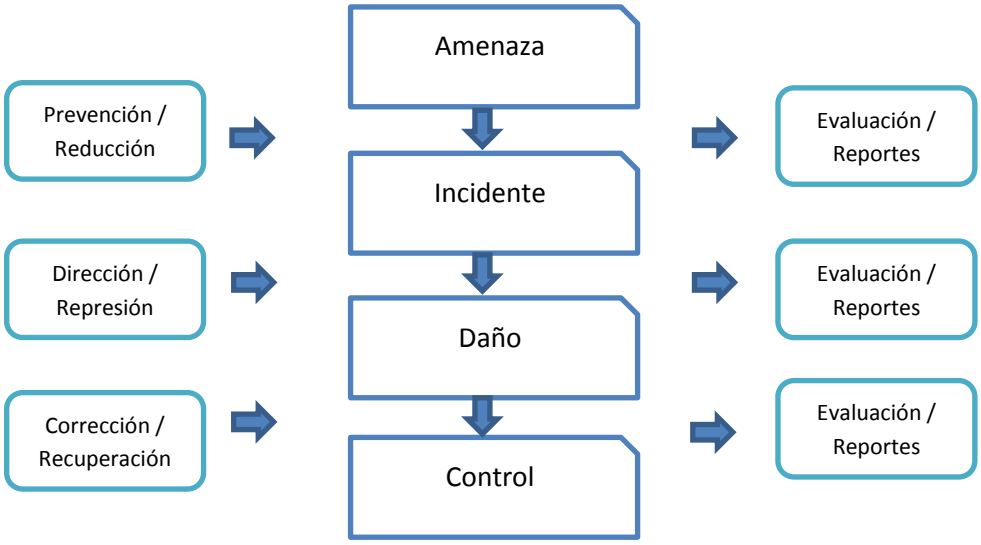
Las políticas nos dan un enfoque gerencial hacia los riesgos y control que no se deben perder de vista para alinearlo con la política de TI, insumo que debe incluir un marco de trabajo que sea comprendido por la Alta Dirección y que vele por cada una de las áreas. Si bien es cierto que se nos mencionan que el control de acceso en base a la seguridad y requerimientos comerciales son importantes, debemos enfocarnos en cubrir las necesidades básicas que empiezan desde la planificación. Durante la implementación, evaluación,

control y supervisión debe mantenerse vigilancia constante teniendo en consideración el tipo de infraestructura y la cultura de seguridad del personal. La comunicación es un aspecto vital, en cualquier momento todo cambio, principalmente de nuevas instrucciones, se debe notificar al personal monitoreando que estos procedimientos se cumplan, de acuerdo a la norma establecida.

Para que los nuevos procedimientos y reglas tengan una mejor aceptación, el manejo de términos y abreviaturas reclama la creación de un diccionario de datos que los incluya y que sea de fácil referencia para los usuarios de cada área. Como recomendación se puede restringir acceso privilegiado a ciertos usuarios a términos o procedimientos confidenciales o propios de un área de trabajo.

La administración de seguridad de la información es un punto clave que debe manejarse en ciclos de vida de los servicios y ser parte integral de los sistemas manteniendo en curso las necesidades que constantemente se pueden presentar, como podemos observar en la ilustración 3. La seguridad mide el estado de prevención y abordaje de incidentes, su manejo correcto conduce a reducir la mayor cantidad de problemas, detectándolos a tiempo, poder actuar ante cualquier situación importante que surja.

Figura 3. **Controles de seguridad para amenazas e incidentes**



Fuente: elaboración propia.

Durante la implementación se debe tratar de no modificar procesos que se adapten a la herramienta de trabajo correctamente, ya que esto podría ocasionar retrasos que no se tienen programados; esto cambia solamente si es estrictamente necesario, normalmente una organización piensa que con cambiar de herramienta ha solucionado los problemas pero esto depende de los procesos, las funciones y sobre todo del personal del proyecto.

3.1.2 Gestión del acceso al usuario

Tabla 3. **Gestión del acceso al usuario**

ISO/IEC 27002:2005		***COBIT* 4.1 Objetivos de control**		**Referencia *ITIL V3***	
11.2.1	Inscripción del usuario	DS5.4	Gestión de la cuenta del usuario	SO 4.5	Gestión de acceso
				SO 4.5.5.1	Solicitud de acceso
				SO 4.5.5.2	Verificación
				SO 4.5.5.3	Proveyendo privilegios
				SO 4.5.5.4	Monitoreo de acceso a la identidad
				SO 4.5.5.5	*Login* y seguimiento de acceso
				SO 4.5.5.6	Eliminación o restricción de acceso
A 11.2.2	Gestión de privilegios	DS5.4	Administración de cuentas del usuario	SO 4.5	Gestión de acceso
				SO 4.5.5.1	Solicitud de acceso
				SO 4.5.5.2	Verificación
				SO 4.5.5.3	Proveyendo privilegios
				SO 4.5.5.4	Monitoreo de acceso a la identidad
				SO 4.5.5.5	*Login* y seguimiento de acceso
				SO 4.5.5.6	Eliminación o restricción de acceso
A 11.2.3	Gestión de la clave del usuario	DS5.3	Administración de identidad	SO 4.5	Gestión de acceso
				SO 4.5.5.1	Solicitud de acceso
				SO 4.5.5.2	Verificación
				SO 4.5.5.3	Proveyendo privilegios
				SO 4.5.5.4	Monitoreo de acceso a la identidad
				SO 4.5.5.5	*Login* y seguimiento de acceso
				SO 4.5.5.6	Eliminación o restricción de acceso
				SO 5.4	Administración de servicio y apoyo

Continuación de tabla 3. ***Gestión del acceso al usuario***

A 11.2.4	Revisión de los derechos de acceso del usuario	DS5.4	Administración de cuentas del usuario	SO 4.5	Gestión de acceso
				SO 4.5.5.1	Solicitud de acceso
				SO 4.5.5.2	Verificación
				SO 4.5.5.3	Proveyendo privilegios
				SO 4.5.5.4	Monitoreo de acceso a la identidad
				SO 4.5.5.5	*Login* y seguimiento de acceso
				SO 4.5.5.6	Eliminación o restricción de acceso

Fuente: ***Aligning COBIT4.1, ITIL V3 and ISO/IEC 270002 for Business Benefit*****, Pag.111**

No se debe tomar a la ligera modificar el acceso de la información para los usuarios finales (internos, externos o temporales), sino que se debe revisar en un plan a detalle que integre cada una de las áreas de trabajo y permiso a contener, con el fin de no dejar espacio donde se pueda acceder con permisos no autorizados. Esto se obtiene al realizar un trabajo correcto en el manejo y administración del acceso a la información.

Para comprender el proceso, se debe conocer el inicio de la contratación del usuario en la empresa por medio de recursos humanos -RRHH-, este es un procedimiento muy importante por definir debido a que es el origen para permitir acceso a diferentes áreas de acuerdo al trabajo que se realizará, el alcance depende del grado de madurez en que se encuentre la compañía y que también desee la Alta Dirección y el Departamento de TI, por medio de una solicitud de cumplimiento.

Se debe tener en cuenta que un usuario puede poseer un perfil y funciones que lo identificarán dentro de la compañía, cada uno de los nombres puede variar de acuerdo a las herramientas o términos que el Departamento de TI utilice. Otorgar los permisos correctos, permite a cada Departamento obtener un mejor enfoque en el trabajo de su equipo, facilitar la información al iniciar labores, conocer las funciones de un integrante, mantener a detalle los accesos y con ello poder pedir actualizaciones mucho más sencillas.

El procedimiento general incluye el llenado de una hoja de solicitud que integre todos los permisos y la autorización del Departamento en donde laborará, esto se deberá desarrollar por cada sistema en el cual se vea involucrado el usuario, la validación de estos permisos es necesario realizarla en el Departamento de TI por medio de una notificación a RRHH y realizando cualquier ajuste que se requiera por cambios de actividades como se visualiza a continuación.

Figura 4. **Restricciones de acceso a la información**

Fuente: elaboración propia.

Las restricciones pueden ser momentáneas o definitivas, estas se darán de acuerdo a los reglamentos establecidos. La finalización se debe tomar como definitiva ya que para que vuelva a ingresar al sistema deberá de crearse un nuevo contrato y que no exista pérdida de información si se decide involucrar al proveedor o usuario. Cuando se labora dentro de una empresa un despido, muerte o retiro pueden ser motivos para eliminar todo acceso posible del usuario.

La construcción de este procedimiento podría llegar a ser tedioso, sin embargo es muy útil para validar cada uno de los sistemas y llevar un control de los perfiles y accesos que se tienen registrados. La definición de esta sección ahorrará tiempo y para otorgar acceso a nuevos usuarios se debe tener cierto grado de control de la información que ingresa cada uno de ellos, ayudarlo a eliminar acceso de una manera eficiente, auditar a futuro o presentar estadísticas de utilización y manejo de cada uno de los sistemas en la compañía.

Es importante recibir la información de RRHH para otorgar accesos así como recibir una solicitud de cumplimiento en donde se lleve la baja, modificación o promoción del usuario, avalada por ellos. Esto juega un papel importante al momento de llevar control de las personas que solicitan dichos cambios. En ciertas ocasiones RRHH es solamente un vínculo para el proceso, esto está relacionado con la definición de los perfiles de cada Departamento de acuerdo a las funciones que el usuario tendrá para cumplir sus asignaciones, se recomienda dejarlo documentado para evitar malos entendidos.

3.1.3 Responsabilidades del usuario

Tabla 4. **Responsabilidades del usuario**

ISO/IEC 27002:2005		***COBIT* 4.1 Objetivos de control**		**Referencia *ITIL V3***	
A 11.3.1	Uso de clave	PO6.2	Riesgo corporativo y marco de referencia de control interno de TI		
		DS5.4	Administración de cuentas del usuario		
A 11.3.2	Equipo de usuario desatendido	PO6.2	Riesgo corporativo y marco de referencia de control interno de TI	SO 5.4	Administración de servicio y apoyo
		DS5.7	Protección de la tecnología de seguridad		
A 11.3.3	Política de pantalla y escritorio limpio	PO6.2	Riesgo corporativo y marco de referencia de control interno de TI	SO 5.4	Administración de servicio y apoyo
		DS5.7	Protección de la tecnología de seguridad		

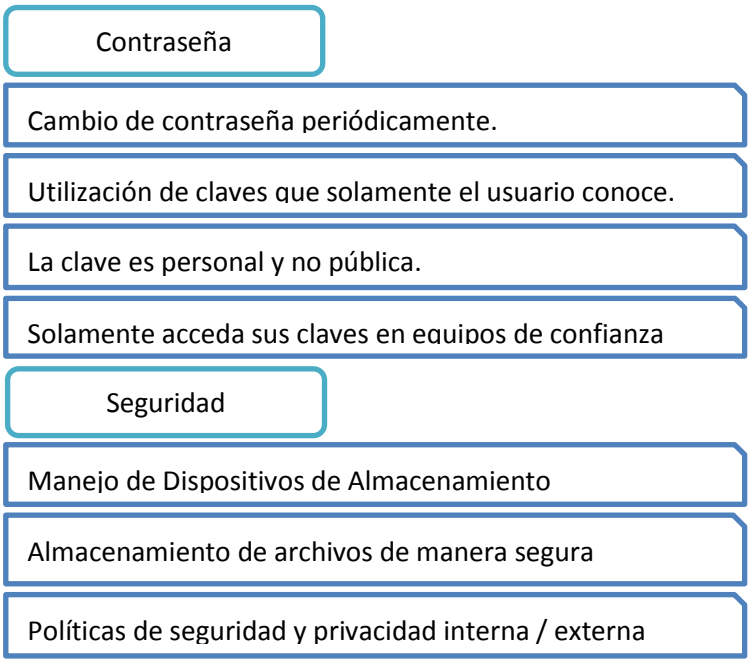
Fuente: ***Aligning COBIT4.1, ITIL V3 and ISO/IEC 270002 for Business Benefit*, Pag.112**

La educación de acceso a la información sobre el uso de seguridad en cada usuario depende mucho de la comunicación que el Departamento de TI otorgue a los Departamentos dentro de la organización, para ello es necesario mantener una comunicación constante sobre los sistemas y la utilización de ellos de manera correcta y efectiva.

Esto debe realizarse por medio de comunicados escritos o electrónicos así como constantes capacitaciones respecto a la utilización correcta de claves,

medios de acceso, políticas de almacenamiento dentro de la compañía que ayuden a no poseer información redundante en los servidores, manejo adecuado de carpetas y grupos de trabajo, información pública y privada por Departamento y utilización correcta de las claves de acceso. Se observa en la figura 5.

Figura 5. **Seguridad y almacenamiento**



Fuente: elaboración propia.

La contribución del Departamento de TI es mantener, como indica *ITILV3,* un uso adecuado de la administración de los servidores y soporte de ellos; la mayoría de organizaciones proporciona servicio de acceso a aplicaciones, *hosting*, base de datos, ejecución de servicios por medio del servidor, almacenamiento, impresión, administración de archivos, correo electrónico. En sí es una responsabilidad de TI mantener en buen funcionamiento disponible la información integra y segura. Observar Figura 6.

Figura 6. **Restricciones de acceso a la información**

Fuente: elaboración propia.

3.1.4 Control de acceso a redes

Tabla 5. **Control de acceso a redes**

ISO/IEC 27002:2005		***COBIT* 4.1 Objetivos de control**		**Referencia *ITIL V3***	
A 11.4.1	Política sobre el uso de servicios en red	DS5.9	Prevención, detección y corrección de *software* malicioso	SO 5.5	Administración de red
A 11.4.2	Autenticación del usuario para conexiones externas	DS5.9	Prevención, detección y corrección de *software* malicioso	SO 5.5	Administración de red
		DS5.11	Intercambio de datos sensitivos		
A 11.4.3	Identificación del equipo en red	DS5.7	Protección de la tecnología de seguridad	SO 5.4	Administración de servicio y apoyo
		DS5.9	Prevención, detección y corrección de *software* malicioso	SO 5.5	Administración de red

Continuación de tabla 5. ***Gestión del acceso al usuario***

		DS5.11	Intercambio de datos sensitivos	ST 4.1.5.2	Preparación para la transición de servicios
		DS9.2	Identificación y mantenimiento de elementos de configuración	ST 4.3.5.3	Identificación de configuración
				ST 4.3.5.4	Control de la configuración
				ST 4.3.5.5	Estado de contabilidad y presentación de informes
A 11.4.4	Protección del puerto de diagnóstico remoto	DS5.7	Protección de la tecnología de seguridad	SO 5.4	Administración de servicio y apoyo
		DS5.9	Prevención, detección y corrección de *software* malicioso	SO 5.5	Administración de red
		DS5.11	Intercambio de datos sensitivos		
A 11.4.5	Segregación en redes	DS5.9	Prevención, detección y corrección de *software* malicioso	SO 5.5	Administración de red
		DS5.11	Intercambio de datos sensitivos		
A 11.4.6	Control de conexión de redes	DS5.9	Prevención, detección y corrección de *software* malicioso	SO 5.5	Administración de red
		DS5.11	Intercambio de datos sensitivos		
A 11.4.7	Control de *routing*	DS5.9	Prevención, detección y corrección de *software* malicioso	SO 5.5	Administración de red
		DS5.11	Intercambio de datos sensitivos		

Fuente: ***Aligning COBIT4.1, ITIL V3 and ISO/IEC 270002 for Business Benefit*****, Pag.112**

ISO muestra una validación sobre el acceso que los usuarios de la compañía deberán mantener, la red dentro de la compañía habrá de ser lo suficientemente segura para resguardar cualquier acceso a intrusos, iniciando con la validación del acceso correcto de los usuarios, los cuales solamente deben acceder a los sistemas o rutas que se han determinado en su área de trabajo.

Es importante recalcar que actualmente se utilizan redes internas, externas y compartidas para poder comunicarse. El acceso y protección que se dé en la autenticación de usuarios es vital al momento de permitir su acceso ya sea localmente o de manera remota. Se recomienda validar todas las formas de comunicación, ya que actualmente las violaciones que existen permiten fácilmente ingresar a un intruso o *sniffer* dentro de la red que pueda obtener paquetes de información privada, robo de contraseñas, intercepción de mensajes electrónicos y conversaciones, entre otros.

Utilizar adecuadamente las herramientas de acceso a sistemas permite que esto no ocurra, una manera de lograrlo es haciendo coincidir la arquitectura manejada dentro de la compañía y compatibilizándola con los dispositivos que los usuarios utilicen, por ejemplo computadores personales, *tablet PC*, computadores de escritorio, móviles. Esto es importante tomarlo en cuenta al momento de adquirir o utilizar un servicio, actualización del *software* y *hardware* que se necesite para montar el proyecto.

La configuración de la red y las direcciones públicas y privadas son un factor que se debe tomar en cuenta al momento de realizar las conexiones en la

compañía tanto como de *software*. La configuración debe permitir privacidad y crecimiento de cada área.

3.1.5 Control de acceso al sistema de operación

Tabla 6. **Control de acceso al sistema de operación**

ISO/IEC 27002:2005		***COBIT* 4.1 Objetivos de Control**		**Referencia *ITIL V3***	
A 11.5.1	Procedimientos de registro en el terminal	DS5.4	Administración de cuentas del usuario	SO 4.5	Gestión de acceso
		DS5.7	Protección de la tecnología de seguridad	SO 4.5.5.1	Solicitud de acceso
				SO 4.5.5.2	Verificación
				SO 4.5.5.3	Proveyendo privilegios
				SO 4.5.5.4	Monitoreo de acceso a la identidad
				SO 4.5.5.5	*Login* y seguimiento de acceso
				SO 4.5.5.6	Eliminación o restricción de acceso
				SO 5.4	Administración de servicio y apoyo
A 11.5.2	Identificación y autenticación del usuario	DS5.3	Administración de identidad	SO 4.5	Gestión de acceso
				SO 4.5.5.1	Solicitud de acceso
				SO 4.5.5.2	Verificación
				SO 4.5.5.3	Proveyendo privilegios
				SO 4.5.5.4	Monitoreo de acceso a la identidad
				SO 4.5.5.5	*Login* y seguimiento de acceso
				SO 4.5.5.6	Eliminación o restricción de acceso
				SO 5.4	Administración de servicio y apoyo

Continuación de tabla 6. ***Gestión del acceso al usuario***

A 11.5.3	Sistema de gestión de claves	DS5.4	Administración de cuentas del usuario	SO 4.5	Gestión de acceso
				SO 4.5.5.1	Solicitud de acceso
				SO 4.5.5.2	Verificación
				SO 4.5.5.3	Proveyendo privilegios
				SO 4.5.5.4	Monitoreo de acceso a la identidad
				SO 4.5.5.5	*Login* y seguimiento de acceso
				SO 4.5.5.6	Eliminación o restricción de acceso
A 11.5.4	Uso de utilidades del sistema	AI6.3	Cambios de emergencia	ST 4.2.6.9	Cambios de emergencia
				SO 5.4	Administración de servicio y apoyo
A 11.5.5	Sesión inactiva	DS5.7	Protección de la tecnología de seguridad	SO 5.4	Administración de servicio y apoyo
A 11.5.6	Limitación de tiempo de conexión	DS5.7	Protección de la tecnología de seguridad	SO 5.4	Administración de servicio y apoyo

Fuente: ***Aligning COBIT4.1, ITIL V3 and ISO/IEC 270002 for Business Benefit*****, Pag.114**

ISO presenta una temática directamente relacionada con la utilización de sistemas seguros para acceder a cuentas de usuarios, acceso a sistemas de forma local o remota utilizando autenticación de conexión y periodo de tiempo que deberá estar conectado. Esta tecnología actualmente se maneja por medio de sistemas biométricos, estos no solamente permiten autenticar a un usuario de manera más eficiente que una tarjeta o controles remotos sino que adicionalmente permite al sistema reconocer la hora y fecha en que éste ha ingresado a su cuenta, dirección IP validando su ubicación y si pertenece a una red pública o privada.

Los sistemas biométricos más utilizados actualmente han sido desarrollados por medio de las huellas digitales, iris de los ojos y facciones del rostro, estos sistemas se encuentran ya disponibles en *hardware* en conjunto con los computadores y firmas de fabricantes de teléfonos o *PDA's* inteligentes que traen reconocimiento dactilar o de iris.

Es básico mantener una acceso correcto que sea contabilizado sobre el tiempo de conexión, para ello se debe contar con un sistema que valide el tiempo de conexión y si existe actividad en la cuenta abierta. *ITIL* no solamente recalca esta validación sino adicionalmente menciona que debe llevarse una notificación de manera escrita si este fuera un acceso a nuevo usuario y un procedimiento documentado como por ejemplo, la solicitud de cambios (también denominado en inglés *Request For Changes –RFC-*).

ITIL y *COBIT* mencionan que debe regularse por medio de administración correcta de acceso a usuarios utilizando mecanismos de seguridad que lo brinden, no solamente de manera normal sino que sean efectivos en cambios de emergencia que puedan suscitarse, siendo validados por un administrador de cambios que estará a la cabeza de la junta de consulta prevista en una compañía. La junta consultiva es la reunión del grupo de interesados para manejar todo tipo de cambios, dentro de la funcionalidad de la compañía.

Los proyectos como tal deben validarse si son complejos, de alto impacto o alto riesgo. Los cambios de emergencia directamente validados en TI deben ser mínimos y estar ligados a un grupo de técnicos que validen la construcción

del cambio, pruebas y su aplicación. Debe preverse y ser tomado a consideración en la junta consultiva que si sale mal el cambio este puede representar mayor impacto para la empresa, se debe medir el riesgo que esto involucra.

Para que el impacto sea menor, las preguntas que se deben hacer la junta y los encargados son:

- ¿El error fue identificado, analizado y diagnosticado correctamente?
- ¿La solución al problema ha sido probada de forma adecuada?
- ¿La solución fue correctamente implementada?

Al no realizar los debidos pasos suele empeorar la situación y poner en riesgo la calidad de los datos, el acceso de usuarios, descontrol en el manejo de procesos, entre otros; por ello, aunque la urgencia sea crítica, no debe apresurarse y caer en presión de externos que puedan entorpecer el éxito de las acciones.

Una recomendación adicional es que dentro del lapso de tiempo en que ocurren los cambios de urgencia, deben documentarse. Sin embargo, en este momento de tensión normalmente se documenta fuera de horario de trabajo recomendando que se realice en el menor tiempo posible y notificar que está ya se encuentra dentro de los registros debidamente almacenada.

3.1.6 Control de acceso a la aplicación e información

Tabla 7. **Control de acceso a la aplicación e información**

ISO/IEC 27002:2005		***COBIT* 4.1 Objetivos de control**		**Referencia *ITIL V3***	
A 11.6.1	Restricción al acceso a la información	DS5.4	Administración de cuentas del usuario	SO 4.5	Gestión de acceso
				SO 4.5.5.1	Solicitud de acceso
				SO 4.5.5.2	Verificación
				SO 4.5.5.3	Proveyendo privilegios
				SO 4.5.5.4	Monitoreo de acceso a la identidad
				SO 4.5.5.5	*Login* y seguimiento de acceso
				SO 4.5.5.6	Eliminación o restricción de acceso
A 11.6.2	Aislamiento del sistema sensible	AI1.2	Reporte de análisis de riesgos	SD 2.4.2	Ámbito de aplicación
		AI2.4	Seguridad y disponibilidad de las aplicaciones	SD 3.6	Diseño de los aspectos
		DS5.7	Protección de la tecnología de seguridad	SD 3.6.1	Diseño de soluciones de servicio
		DS5.10	Seguridad de la red	SD 4.5.5.2	Requerimientos y estrategia
		DS5.11	Intercambio de datos sensitivos	SO 4.4.5.11	Los errores detectados en el entorno de desarrollo
				SO 5.4	Administración de servicio y apoyo
				SO 5.5	Administración de redes

Fuente: ***Aligning COBIT4.1, ITIL V3 and ISO/IEC 270002 for Business Benefit*, Pag.115**

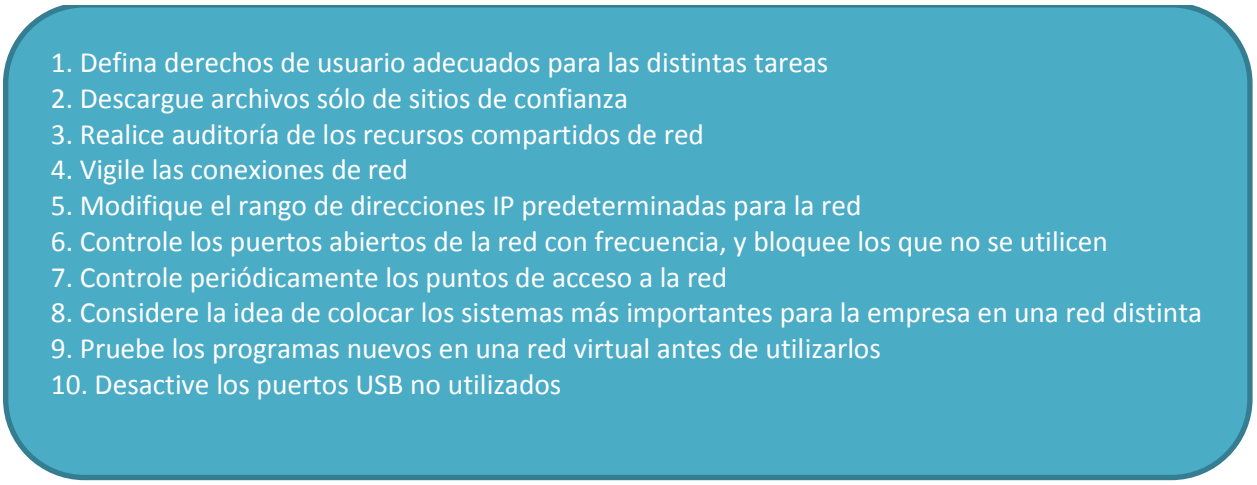
La manera más simple para restringir la información es no permitir acceder a ella, ya sea de forma física o de manera digital. Para ello ISO menciona restringir toda información sensible a la compañía, aislándola de cualquier contacto del personal. Entiéndase, en una construcción adecuada para el almacenamiento de los servidores de información, administración de correo electrónico, base de datos, servidores de aplicaciones y toda la infraestructura para la distribución de la información.

Esta es una forma eficiente de mantener resguardados los datos y de permitir solamente acceso autorizado al personal, manteniendo también un control de las personas externas que ingresan al área para realizar actualizaciones, cambio de equipo y respaldo de seguridad. El área delimitada puede utilizar sistemas biométricos para el ingreso, vigilancia constante del área por medio de un circuito cerrado de cámaras y alarmas, manejo de medidas de seguridad como alarmas contra incendios, monitoreo constante del voltaje y de la ventilación del mismo.

COBIT menciona adicionalmente que la documentación de cómo está distribuida la seguridad dentro del área es primordial, manteniendo una guía de planos de la infraestructura y dispositivos instalados en el área. Esto es importante, sin embargo la documentación deberá abarcar también la seguridad de la red interna que brinda acceso a los datos del área hacia la compañía, la utilización de técnicas de seguridad y procedimientos asociados (como por ejemplo *firewalls*, dispositivos de seguridad, segmentación de redes y detección de intrusos) para autorizar acceso y controlar flujos de información desde y hacia todas las redes. Muy importante de mencionar es que la arquitectura empleada debe ser compatible para los dispositivos que se utilicen.

La autenticación de las fuentes que solicitan información es necesaria debido a que normalmente los datos sensibles se manejan directamente en el envió de información dentro de la red. A continuación se presentan diez consejos básicos para administración de la red.

Figura 7. **Diez consejos para la administración de la red**



Fuente: elaboración propia.

ITIL maneja el acceso a la aplicación e información, por medio de un ciclo de vida diseñado con cambios directamente requeridos por el negocio, para ello el logro de *ITIL* es utilizar el diseño de servicio. Para mantener un portafolio de servicios en donde básicamente son analizados, documentados y aprobados para su pronta ejecución; si la arquitectura o tecnología no se acopla adecuadamente al cambio que se desea realizar será necesario revisarlo, también los procesos involucrados en la implementación. Adicionalmente a ello las métricas de los métodos que se miden en el proceso deberán evaluarse si el nuevo servicio permite acoplarse a las métricas actuales, de lo contrario es necesario tomar en cuenta mejorar las mediciones de calidad, niveles de seguridad u objetivos trazados en el negocio.

3.1.7 Computación móvil y tele-trabajo

Tabla 8. **Computación móvil y teletrabajo**

ISO/IEC 27002:2005		***COBIT* 4.1 Objetivos de control**		**Referencia *ITIL V3***	
A 11.7.1	Computación móvil y comunicaciones	PO6.2	Riesgo corporativo y marco de referencia de control interno de TI	SD 4.6.4	Políticas, principios, conceptos básicos
		DS5.2	Plan de seguridad de TI	SD 4.6.5.1	Controles de seguridad (cobertura de alto nivel, no en detalle)
		DS5.3	Administración de identidad	SO 5.4	Administración de servicio y apoyo
		DS5.7	Protección de la tecnología de seguridad		
A 11.7.2	Teletrabajo	PO3.4	Estándares tecnológicos	SD 4.6.4	Políticas, principios, conceptos básicos
		PO6.2	Riesgo corporativo y marco de referencia de control interno de TI	SD 4.6.5.1	Controles de seguridad (cobertura de alto nivel, no en detalle)
		PO5.2	Prioridades dentro del presupuesto de TI	SO 5.4	Administración de servicio y apoyo
		DS5.3	Administración de identidad		
		DS5.7	Protección de la tecnología de seguridad		

Fuente: ***Aligning COBIT4.1, ITIL V3 and ISO/IEC 270002 for Business Benefit*, Pag.115**

ISO menciona el trabajo a distancia realizado por el personal de la compañía fuera de oficinas que es siempre un riesgo ya que para empezar es necesario que utilicen una red de internet para poder acceder a aplicaciones o información interna de la empresa. Sabiendo manejar adecuadamente las Tecnologías de Información y la comunicación pueden ser un medio muy

seguro para conectarse de manera remota, sin embargo se deben tomar en consideración las condiciones y equipo que el trabajador o usuario necesitará:

- Computador personal
- Línea telefónica o *VOIP* (voz sobre *IP*)
- Acceso a internet
- Equipos de interfaces (r*outers*, *modems*)
- Impresora
- *Scanner*
- *Webcam*
- Energía eléctrica
- Dispositivos biométricos

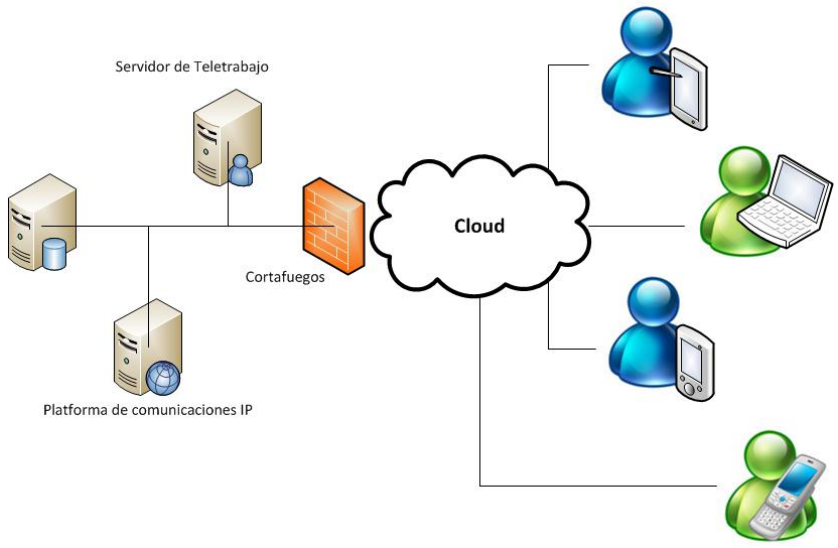
En el listado se observa que esto no solamente pide una infraestructura dentro del hogar sino que adicionalmente se debe tener un sistema de acceso eficiente. El teletrabajo se debe manejar con un plan que no solamente incluya a los trabajadores sino a la Gerencia en donde se creará un plan sobre los accesos que cada uno deberá tener desde su casa y verificar que éstos se cumplan a cabalidad. Las políticas que se generen servirán para crear la guía correcta de controles de seguridad que deberán monitorearse de manera constante en cada punto de acceso.

Las redes VPN utilizadas deberán contar con un sistema encriptado de ingreso y documentar los permisos otorgados llevando un control de las personas que tienen o no acceso por medio de esta vía. La fuga de información es relevante, por ello es necesario contar con políticas de seguridad en redes y acceso a las mismas.

ITIL como *COBIT* mencionan que debe velarse por disminuir el riesgo a nivel corporativo sobre estas prácticas, manejándolo dentro del plan ideado por TI, que debe ser revisado minuciosamente al momento de decidir realizar este tipo de práctica dentro de la empresa, antes de hacerlo marchar. Las principales líneas de protección que debe contar un trabajador dentro del punto externo a la compañía son:

- Traducción de direcciones de red (*NAT*)
- Cortafuegos/*Routers* para la conexión *ADSL* o cable
- Utilizar cortafuegos personales en cada sistema
- Verificación automática de puertos abiertos
- *Software antivirus*
- Verificación de vulnerabilidades
- Respaldo de seguridad[9]

Figura 8. Diseño de teletrabajo



Fuente: elaboración propia.

[9] Taringa usuario ps981, Seguridad Informática Teletrabajo, 2010.

A continuación se resume el FODA para cada uno de los estándares.

Tabla 9. **FODA *ITIL V3***

Fortalezas	Oportunidades	Debilidades	Amenazas
Administración de los datos y activos. La granularidad que se detalla permite un mejor manejo de cada activo de información dentro de la compañía. Gestión del acceso a usuarios de manera detallada. Administración correcta de la red. En este caso mejora el monitoreo constante y estructuración correcta del sistema de red que se implementa en la compañía	Aprovechar la mejora en la comunicación de los clientes de manera más específica. Podría mejorar la adaptabilidad en los servicios. Cubrir un fortalecimiento del seguimiento en el *log* de los usuarios. Este puede convertirse a ser más específico.	No permite atacar debilidades del usuario. Es compleja y costosa la implementación del estándar. No existe administración de control de cambio de forma detallada. Esto hace vulnerable al estándar el no tener controlado algún ataque o manipulación de datos que podría ser corregido si existieran políticas de control de versionamiento o sobre los cambios realizados en un periodo de tiempo. Existe poco enfoque al teletrabajo	Contratación de *outsourcing* para mantener la operación, podría provocar fugas de información o falta de conocimiento de la lógica del negocio. La administración de la red no penetra las prevenciones o detecciones de manera profunda

Fuente: elaboración propia.

Tabla 10. **FODA *COBIT***

Fortalezas	Oportunidades	Debilidades	Amenazas
La información detallada en clasificación, permite un seguimiento de los activos, utilización de diccionarios y explicaciones detalladas hacen que sea fácil su búsqueda por cualquier eventualidad. Ver al usuario más que una persona que utiliza y manipula la información. Este realiza una gestión de riesgo corporativo de formato 360. Protección y prevención de datos y red sensibles al negocio. Incorporación de análisis de riesgos dentro de cada área.	Podría contar con agentes certificadores dentro de la compañía que posean un aval y faciliten y especialicen su implementación. Se podría ampliar a manejar un seguimiento detallado en cambios de emergencia que requiera la empresa.	La falta de documentación en base a mediciones o *SLA's* que respalden la información hacen que no se permita llevar un control como los demás estándares. El tiempo para implementar las condiciones planteadas necesita mucho apoyo local y *Outsourcing*.	Pueden existir riesgos externos debido a la falta de mediciones continuas dentro de cada departamento que provoquen fallas o aseguramiento de la calidad de la información.

Fuente: elaboración propia.

Tabla 11. **FODA ISO/IEC 27000:2005**

Fortalezas	Oportunidades	Debilidades	Amenazas
Fortalecimiento en las políticas de acceso de control Buenas prácticas para guiar al usuario en sus responsabilidades, hacen que cada área pueda lograr direccionar a su equipo de una manera más eficiente y alcanzar los objetivos trazados. El buen diagnóstico de la red que recalca el estándar, permite un constante monitoreo y seguridad dentro de cada área. Posee protecciones de Red y control detallado que permiten detectar cualquier intrusión o amenaza latente. Cuenta con una familia de estándares que permiten a la empresa utilizarlos y encaminarse a tener varias certificaciones que no solamente abarcan la gestión de acceso a la información.	Podría contar con certificadores dentro de la compañía que faciliten la implementación del estándar.	No se toma en cuenta el control y toma de decisiones No existe una Inscripción del usuario de manera individualizada. No se realiza algún procedimiento de cambios de emergencia de manera detallada. Falta de manejo de usuarios a detalle, se puede caer en el problema de no conocer las actividades que cada usuario debiera tener activas y cuales restringidas.	La falta de detalle dentro del estándar puede hacer tender a utilizar otros estándares que estén mejor especificados para esta área.

Fuente: elaboración propia.

La información recopilada se basa en el acceso de acuerdo a las necesidades que la compañía puede necesitar en cierto momento. No importa qué sección de estándar utilice, siempre se podrá mejorar y/o necesitar unificar fortalezas de otro estándar que complemente o integre la idea que se desea implementar en un área específica.

4. GESTIÓN DE ACCESO DE LA INFORMACIÓN EN EL SECTOR PRIVADO DE GUATEMALA

4.1. Cuándo y por qué es necesario en la empresa

La necesidad de mantener asegurado los activos de la empresa es vital para el funcionamiento de la misma, cualquier momento se recomienda para comenzar a resguardar la información de una manera correcta o validar las vías actuales de almacenamiento y acceso a la misma.

Por qué es necesario realizarse una gestión de acceso a la información dentro de la compañía es una pregunta que se hace cada gerente debido a que no solo es implementar la solución sino que conlleva una serie de pasos los cuales requieren esfuerzo, tiempo y recursos monetarios para llevarse a cabo. Normalmente, las empresas jóvenes son reactivas a cualquier suceso de seguridad o pérdida de información lo cual las lleva a enfrentar mayor grado de emergencias que en una empresa consolidada, debido a la misma experiencia que las grandes empresas han forjado durante su trayectoria. Esta experiencia la han formado de diferentes maneras como son los hechos fortuitos, descuidos o la misma negligencia que ha conllevado a crear una serie de planes para mejorado de forma significativa su proyección al trabajo y la misma seguridad que deberían tener los empleados y los Departamentos dentro de la empresa.

La evaluación del diseño del programa de seguridad que estará dirigida por los Departamentos involucrados, acorta el tiempo de reacción. Muchas pequeñas y medianas empresas poseen medidas de seguridad preventivas pero resulta crítico tener un plan para afrontar las potenciales amenazas y la habilidad para evaluar estratégicamente áreas con debilidades, que es donde se deberá aplicar una evaluación de todo el programa de seguridad.

Estas evaluaciones permiten conocer los riesgos para tomar medidas y mirar la capacidad de la organización en implementar controles adicionales. El resultado de una evaluación destaca las áreas en las que una empresa puede administrar su riesgo en costes, de una manera efectiva.

Las necesidades de realizar un plan y evaluarlo realmente corresponden a medir en costos las emergencias, por lo tanto prevenir un alto costo y poderlo evitar significa menos dinero debido a que se puede designar un monto mensual sobre el gasto, teniendo el tiempo necesario para que expertos ayuden a realizar la mejor solución y planes de contingencia, en comparación con un acontecimiento que no se tiene contemplado y requiere un esfuerzo mayor en cuestión monetaria el cual puede obligar a recurrir a proveedores menos confiables y con mayor costo; todo ello se prevé al planificar o realizar cierto procedimiento y es ahí el por qué no es una condición sino una necesidad alta para la misma empresa.

4.2. Áreas de impacto directo en la compañía

Las áreas de una compañía son vulnerables a cualquier ataque, intruso o pérdida de información en cualquier momento; cada área es una pieza fundamental, sin embargo existen áreas mucho más vulnerables que otras, para determinarlo se debe realizar la siguiente pregunta.

Qué información dentro de la compañía corre más riesgo y qué Departamentos o áreas de trabajo se ven involucradas, de acuerdo al estudio de Tendencias de Mercado de IBM en octubre del 2010:

- Ordenadores
- Celulares y *PDA's*
- Acceso a la red
- Acceso a página *web*
- Códigos fuentes
- Manuales y libros
- Mercadería prototipo
- Estados financieros
- Planillas de pago
- Correspondencias
- Patentes y/o fórmulas
- Estrategias y estudios de mercado
- Planes del negocio
- Cuentas bancarias

Las áreas que se catalogan más vulnerables son:

- Gerencia
- Contabilidad
- RRHH
- Informática
- Producción
- Mercadeo

4.3. Está preparada la compañía para involucrar el estándar

El estar preparado para implementar una serie de estándares o políticas de seguridad dependerá mucho del involucramiento de la Alta Dirección y la iniciativa o propuesta que se plantee directamente para realizarla.

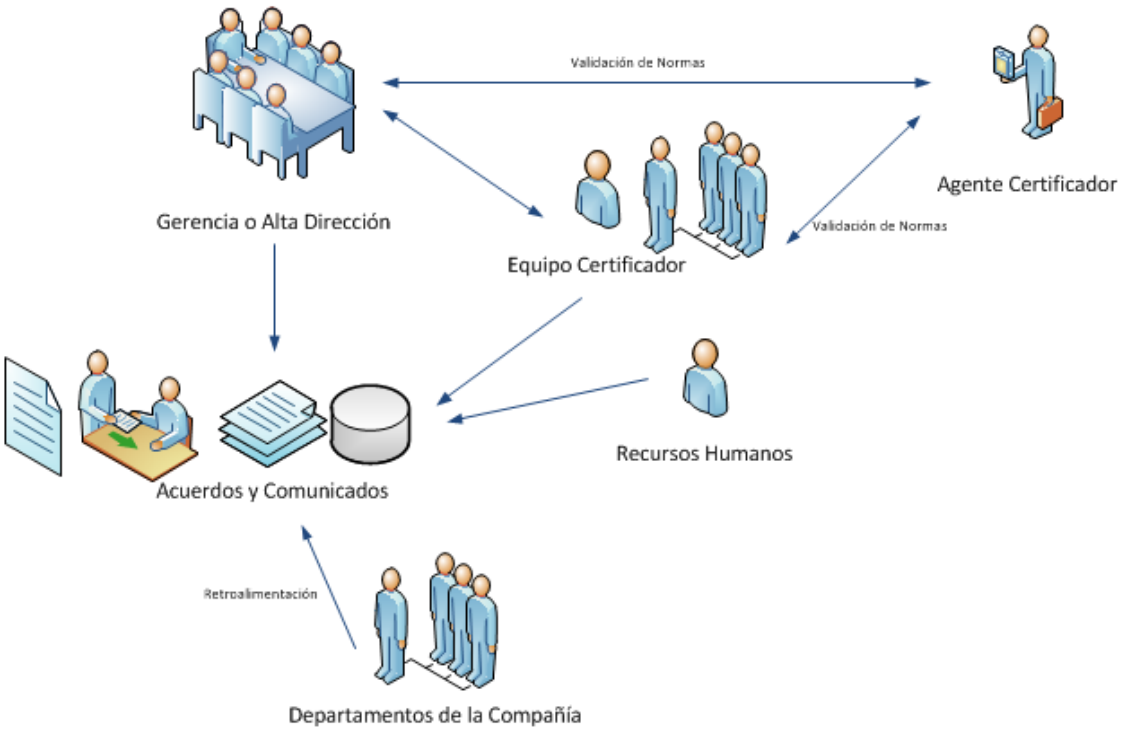
No importa si la empresa es grande o pequeña, lo importante es tener el ánimo de llevarlo a cabo, de hecho los problemas que pueden existir en una empresa pequeña o mediana pueden ser menores a los que ocurren dentro de una empresa de grandes proporciones. Se plantea las siguientes interrogantes al involucrar a la empresa:

- ¿La Gerencia o Alta Dirección, avala el proyecto y gestión de acceso?
- ¿Se puede implementar procedimientos en paralelo?
- ¿Está dispuesta la compañía a integrar y automatizar procesos en un mediano plazo?

- ¿La comunicación estará gestionada de forma integral para cada área o Departamento de la compañía, brindando avances sobre la certificación, noticias o avisos importantes para el conocimiento general?

Al obtener un “si” en cada una de las preguntas, se afirma el compromiso real que debe existir para formalizar el arranque del proyecto.

Figura 9. **Interacción para poner en marcha el estándar dentro de la compañía**



Fuente: elaboración propia.

4.4. Qué análisis de factibilidad debe realizar la compañía antes de implementar el estándar

La evaluación para que un proyecto sea viable realizarlo es primordial que se realice al inicio de comenzar cualquier tipo de proyecto. Mediante este proceso se valoran cualitativa y cuantitativamente las ventajas y desventajas de destinar recursos para las acciones. De la correcta evaluación que se realice de un proyecto de inversión, depende que las acciones a ejecutar contribuyan al desarrollo a mediano o largo plazo de una empresa en específico y en general de la economía de un país.

La evaluación de proyectos de inversión es un análisis que se lleva a cabo mediante un proceso de varias aproximaciones en las que intervienen técnicos, financistas y administradores. Las tres etapas que se deben considerar al evaluar un proyecto de inversión son:

- Etapa de pre inversión
- Etapa de maduración
- Etapa de funcionamiento

El análisis de factibilidad es parte de la etapa de pre inversión dentro de la evaluación de proyectos de inversión. La aprobación o visto bueno de parte de la compañía se denomina “viabilidad”. Esta se debe realizar considerando el tiempo que dura el proyecto. Cualquier evaluación no viable o existencia de una inconformidad grave hará que el proyecto no resulte. En pocas palabras la predisposición de la Alta Gerencia y los Departamentos deberá reflejarse de

forma paralela y colaborativa para no generar inconformidades antes de iniciar el proyecto.

El objetivo central se d obedeciendo que cada inversión que se optimice al cien por ciento y que ésta se encuentre debidamente documentada y fundamentada, donde las soluciones a emplear estén avaladas por la compañía y los responsables. Los planes de ejecución deben apegarse a las leyes nacionales y adicionalmente le servirán para una recopilación de datos relevantes sobre el desarrollo del proyecto y en base a ellos el grupo que dirige la operación y gerencia podrá elegir la mejor solución.

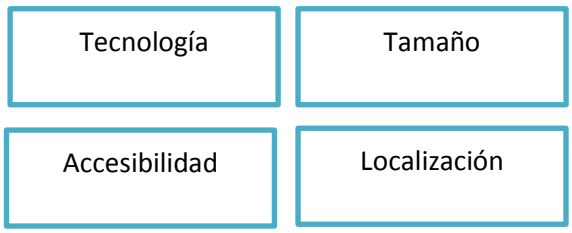
4.4.1. Factibilidad técnica

Algunas de las preguntas que se pueden realizar al momento de empezar el estudio de factibilidad:

- ¿Existe o se puede adquirir la tecnología necesaria para realizar lo que se pide?
- ¿El equipo propuesto tiene la capacidad técnica para soportar todos los datos requeridos a usar en el nuevo sistema?
- ¿El sistema propuesto ofrecerá respuestas adecuadas a las peticiones sin importar el número y ubicación de los usuarios?
- Si se desarrolla el sistema, ¿se puede crecer con facilidad?
- ¿Existen garantías técnicas de exactitud, confiabilidad, facilidad de acceso y seguridad de los datos?

Se debe tomar en cuenta dentro de la factibilidad técnica las variables incluidas a continuación.

Figura 10. **Variables para la factibilidad técnica**



Fuente: elaboración propia.

También es necesario realizar un análisis correcto del lugar y el tamaño del área donde se ubicará el mismo, pensar a futuro es crítico para poder elegir correctamente; así mismo sucede con la accesibilidad de la información dentro de la compañía y la tecnología que se utilizará. Si bien es cierto que no se sabe el comportamiento económico externo, podemos tomar como fundamento los pronósticos actuales o tendencias de infraestructura, regiones comerciales, materiales de vanguardia, sectores sociales, importaciones y exportaciones, índices de seguridad por región, actualizaciones de tecnología, información sobre la misma seguridad violada en términos empresariales. Todo esto puede ayudar a tomar una mejor decisión y hacer una propuesta de la factibilidad técnica adecuada.

Al momento de elegir la tecnología adecuada dentro del proyecto, se debe realizar una lluvia de lluvia de ideas en donde se rechacen todas las que no son posibles técnicamente.

Luego se realizará los involucrados un análisis más detallado de todas las áreas que se cubrirán, priorizando cada una de ellas de acuerdo a la tecnología a utilizar al momento de realizar la gestión de acceso a la seguridad. Una interrogante alta se refiere a la facilidad de obtener la tecnología para cubrir las necesidades, la disponibilidad de proveedores y subcontratistas que nos ayuden a completarla en el tiempo exacto. Un error frecuente que puede cometerse es delegar toda la responsabilidad a terceros, esto no es aconsejable, se recomienda que el grupo encargado de la certificación y factibilidad tenga conocimiento al menos general o incluido del personal confianza para que pueda opinar sobre la planificación.

La selección correcta, implica elegir una combinación de factores provechosos para convertirlos en activos para nuestra organización. Es aquí donde se pueden mencionar las reglas para toma de decisiones en la viabilidad técnica:

- Relación entre demanda y capacidad
- Características y disponibilidad de la mano de obra
- Características y disponibilidad de materiales
- Personal calificado subcontratado o interno de la compañía
- Disponibilidad financiera
- Tamaño de la tecnología a instalar

El espacio debe ser adecuado para el buen desempeño de la compañía, es necesario contar con áreas de trabajo administrativo, operativo, almacenamiento de mercancía, distribución de productos o servicios, recreación, estacionamiento, entre otros.

Dentro de una ciudad o región debe considerarse el lugar idóneo para la localización de la empresa o fábrica, si se estuviera iniciando desde cero es primordial; de igual manera si se estuviera coordinando una remodelación o ampliación, siempre es necesario considerar las siguientes variantes:

- Materiales y estándares de construcción
- Dispositivos de seguridad
- Planeación y diseño del área
- Contratistas y empleados calificados
- Espacio para otras actividades

El tamaño no adecuado implica altos costos de remodelación, ampliación e incluso cambio de localización por no haberlo previsto.

La accesibilidad es un tema importante para la compañía ya que permite llegar más rápido y en menor tiempo a sus clientes, proveedores y empleados. No solamente se refiere a un espacio físico sino también a acceso virtual. Esta permite una forma ágil corregir errores, comunicarnos de manera simultánea con nuestros clientes o proveedores, acceder a información correcta en el

tiempo indicado, poder acceder de forma remota a la información. Debe considerarse lo siguiente:

- Planeación y diseño del área (seguridad y fácil acceso)
- Canales de distribución
- Seguridad de materiales
- Canales de comunicación (física o virtual)

Es importante recalcar que la accesibilidad será pieza fundamental en la seguridad de la información dentro y fuera de la compañía, se deberá realizar un análisis detallado de los posibles proveedores que entren a participar en la estructuración de la seguridad de la compañía.

La conectividad debe ser brindada por parte de un proveedor de internet y comunicación certificado que tenga amplia experiencia en el tema y mantenga respaldo o plan de contingencia para evitar fallos. Manejar estándares de instalación de circuitos cerrados de transmisión permite mantener visibilidad dentro de la empresa así mismo mantener estándares en la instalación de redes, cableado eléctrico, telefonía, tuberías de agua potable, aguas servidas o gas, entre otros.

El lugar donde se ubique la empresa al igual que sus sucursales es necesario validarlo desde el inicio. Este debe ser céntrico para las operaciones diarias, así mismo se debe cumplir con los requisitos que la municipalidad o región exigen. Tomar en cuenta:

- Estudio de localización idónea (empleados, materiales, clientes, seguridad entre otros)
- Zona de seguridad
- Impacto ambiental
- Tipo de zona de industria (industrial, administrativa, producción, entre otras)
- Agentes inmobiliarios y papelería en orden

Una buena ubicación permite no solamente ahorrar tiempo, sino tener tener mucho más tráfico de personas y más información. Se debe considerar contar con la papelería y estándares controlados por parte de la comunidad, esto ahorrará muchos trámites molestos o retrasos para comenzar el proyecto.

4.4.2. Factibilidad económica

El objetivo esencial de la evaluación económico financiera es apreciar la inversión a partir de criterios cuantitativos y cualitativos, empleando los modelos más representativos usados para tomar decisiones de inversión. El modelo permite al analista experimentar con diferentes hipótesis y escenarios, sin poner en riesgo el negocio. La simulación financiera implica la cuantificación del impacto probable de las decisiones sobre los resultados, el balance general de la compañía.

Las premisas que se deben considerar son:

- ¿Están definidos los procesos o políticas a implementar?
- ¿En qué costo incurrirá cada una de ellas?
- ¿Se debe contratar nuevo personal para la implementación y cuál será el costo?
- ¿Qué se obtendrá de todo esto?
- ¿Habrá costos ocultos mientras se ejecuta la gestión?
- ¿Cuál es la ganancia a obtener?
- ¿Existe un análisis detallado de las ganancias por medio de la inversión que se deberá presentar a las partes interesadas?

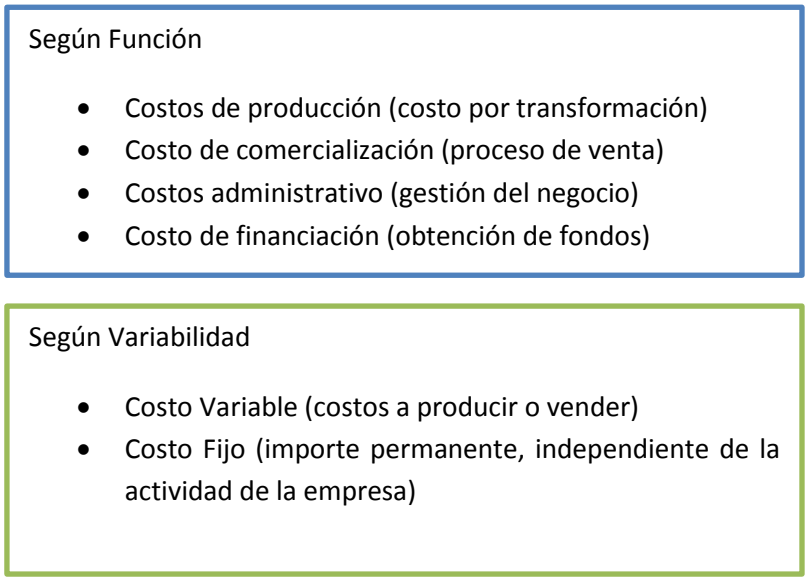
El análisis costo y beneficio verifica que la inversión sea económicamente viable. El beneficio contable representa el exceso de ingresos sobre los gastos, dichos ingresos y gastos no son necesariamente entradas y salidas de efectivo sino el resultado de dos ejercicios contable. Permite establecer un proceso de valoración económica de los costos evitados como beneficios o de los beneficios no percibidos como costo en un proyecto. Es primordial que el valor de las ganancias sea a corto plazo, sin embargo no necesariamente esto evitaría una quiebra, entonces se debe validar que el beneficio sea también a largo plazo el cual muestra la disposición de fondos suficientes para el pago de obligaciones durante el proyecto. Por esto es necesario tener criterios de evaluación de inversiones ya que éstos influyen en el estimado del proyecto, en términos monetarios.

El costo de realización del proyecto es un valor sacrificado para obtener el rendimiento total, la gerencia se enfrenta a la selección de diferentes

decisiones mientras se ejecuta el proyecto. La información que se brinde acerca de los costos incurridos y el comportamiento de ellos es vital para la toma de una decisión efectiva.

Este es un análisis que se debe llevar a profundidad considerando que un costo puede contener otros los cuales podemos desglosar como aparece en la figura 11.

Figura 11. **Costos según función y variabilidad**



Fuente: elaboración propia.

Si el costo beneficio no se cumple, se tendrá una pérdida para el proyecto o empresa. Para el proyecto de gestión de acceso a la seguridad es necesario realizar este análisis, presentarlo en conjunto a Gerencia y que se tome en cuenta para la viabilidad del proyecto.

El análisis temporal de proyectos de inversión permite realizar estadísticas y tomar varios criterios para evaluar la inversión, normalmente se podrán tomar valores promedio de rentabilidad o una validación del periodo de recuperación simple. Estas no son muy fiables debido a que mantienen intacto durante todos los años el flujo de efectivo. Se deben utilizar técnicas que consideren el dinero en el tiempo y que éste se verá afectado por la operación de descuento y capitalización, éstos son más confiables aunque su utilización resulta más compleja. Se enumera las técnicas a utilizar:

- Período de recuperación descontado (PERd)
- Tasa interna de rentabilidad (TIR)
- Tasa verdadera de rentabilidad (TVR)
- Plazo financiero medio (PFM)
- Valor actual o presente neto (VAN)
- Razón beneficio costo (B/C)
- Valor futuro neto (VFN)
- Costo total actualizado (CTA)
- Costo anual equivalente (CAE)

El flujo de efectivo neto es el reflejo de los cobros y pagos durante el periodo que dura el proyecto de inversión. Los costos de inversión son un punto esencial para empezar el proyecto, es ahí donde surgirán los desembolsos para la adquisición de activos que sustenten la realización de la inversión, debemos incluir dentro de este costo el de previsiones que puedan ocurrir en el transcurso del mismo, a medida que el proyecto avance se verán incrementadas estas previsiones y al final del proyecto disminuirán. Se considera necesario agregar un margen del 10% de costo de inversión para las contingencias.

Se debe identificar el período de inversión, esto no solamente es un dato que la Alta Dirección pedirá sino que si éste no se cumple, la inversión del proyecto pueden ser superada por no contemplar costos adicionales por retraso, hacerlo no viable y por ende su fracaso.

Es de suma importancia para la empresa conocer sus flujos de efectivo (entradas y salidas) ya que una compañía puede tener problemas en este sentido, aun siendo rentable. Por otra parte hay que considerar que son fundamentales para analizar la viabilidad de proyectos de inversión, pues son la base de criterios importantes de cálculo como VAN, la TIR y del PER, además para medir la rentabilidad o crecimiento de un negocio.

Se debe detallar cada uno de los componentes que se utilizara a lo largo del proyecto e ir agregándolo a los costos reales del proyecto, con ello podremos hacer un estimado de cada área involucrada y el financiamiento necesario para volver realidad la gestión de acceso a la información. Es vital involucrar al administrador financiero para que evalúe y esté atento a todos los costos incluidos en el presupuesto.

4.4.3. Factibilidad operativa

Se refiere a que debe existir personal capacitado para llevar a cabo el proyecto y usuarios finales dispuestos a emplear los productos o servicios generados por el mismo.

Las preguntas que se pueden plantear para definir la factibilidad operativa son:

- ¿Existe apoyo para el proyecto por parte de la administración?
- ¿Y por parte de los usuarios?
- ¿Son aceptados por los usuarios?
- ¿Los usuarios han participado en la planeación y desarrollo del proyecto?
- ¿El sistema propuesto causará algún tipo de daño?
- ¿Producirá resultados pobres en alguna área?
- ¿Se perderá control en alguna área específica?
- ¿Se perderá la facilidad de acceso a la información?
- ¿La productividad de los empleados será menor después de instalado el sistema?
- ¿Los clientes se verán afectados por la implantación?[10]

La garantía de una operación correcta está relacionada con el personal a cargo ya que el compromiso que cada uno tiene para realizar el proyecto, es primordial. Sin embargo, se deben tomar en cuenta las premisas que se presentan. Cada una de ellas explica que el proceso no es fácil, es necesario contar con un lineamiento sobre cada área involucrada. El orden que se debe seguir para que la operación funcione es:

- Gerencia
- Usuarios clave
- Proveedores y subcontratistas de las herramientas

[10] Gobierno de Hidalgo, <http://www.scribd.com/doc/28111897/FACTIBILIDAD-OPERACIONAL>, consulta diciembre 2010.

- Ejecutores y realización de pruebas
- Capacitadores y comunicadores
- Monitoreo de cada proceso involucrado
- Clientes

Cada uno de los puntos enumerados es requerido para que la gestión tenga éxito, esto debe estar presente en cada una de las etapas en que se encuentre la gestión de acceso a la información.

El mayor reto de esta factibilidad es que los usuarios finales estén dispuestos a enfrentar este cambio y como lo pondrán en práctica en su diaria ejecución. Es un reto grande ya que la mayoría de personas están acostumbradas a trabajar en una forma secuencial y con un orden específico. La gestión de acceso a información no solamente hace un cambio significativo sino que requiere nuevas políticas para acceso, tendiendo a generar en algún momento, cierto tipo de burocracia. La forma en que se desarrolle dentro de la empresa la gestión, estará de la mano en la comunicación abierta que exista para explicar y hacer comprender las nuevas ideas en los trabajadores.

Otro grupo importante y que no debe descuidarse son los clientes leales a la compañía, la gestión de acceso a la información por ningún motivo debe entorpecer esta vía con el mayor activo como son los clientes. Las líneas de acceso deben facilitar el proceso, por ello que es necesario hacer un excelente análisis de cada área para que esto no ocurra al momento de ejecutar cualquier gestión.

La forma de implantar cualquier cambio, debe estar avalado y supervisada a conciencia pues es un tema delicado para con las personas que están fuera del sistema, y más serio para las personas que pueden llegar a sentir frustración por no tener respuesta en un momento dado.

4.5. Plan de acción para elegir áreas claves de compañía

Elegir la estrategia correcta para implementar el SGSI requiere una planificación que cubra los puntos claves, sin embargo para lograrlo se debe investigar las áreas de la compañía que sean críticas, La elección dependerá de la disposición y conocimiento de las áreas que se cubran y los puntos clave que la gerencia y el equipo integrador SGSI necesiten abarcar.

4.5.1. Cómo prepararse para el cambio e implementación SGSI

No importa qué certificación se esté implementando, siempre deben seguirse lineamientos, no se debe tomar a la ligera sino como un gran proyecto que cambiará la forma de llevar la gestión dentro de la empresa para beneficio de todo el personal involucrado; debe estar claro que este proyecto no se realizará de manera ágil, sin el trabajo en equipo. Para implementar un proyecto de tal magnitud debemos tener claro, como se había mencionado antes con un consentimiento de la Alta Dirección, debe ser un compromiso concreto, si es posible por escrito que alimente una sinergia para poder hacer realidad las acciones.

El alcance debe visualizarse desde el inicio del proyecto pensando en implementarlo por partes si es una organización de gran magnitud, hasta cubrir todas las áreas. El alcance no debe ser tan detallado, ya que lo que se pretende es conocer los límites del proyecto.

Un buen control en la documentación, desde el inicio, es esencial para llevar un orden cronológico de cada reunión con los acuerdos y compromisos de cada una de las partes involucradas. Es importante que archivar los documentos de cada reunión, minutas, memos o acuerdos y que éstos se comuniquen al equipo de una manera simple como por ejemplo creando un grupo de usuarios dentro del correo electrónico o un repositorio de datos a donde solamente los interesados puedan ingresar.

Debe seleccionarse minuciosamente cada uno de los miembros que conformarán el equipo certificador de la implementación de SGSI, éstos no solamente se deben elegir sino entrenarse y capacitarse en el proceso. Es necesario apoyarse en un ente certificador que pueda ayudar a capacitar al personal.

El liderazgo es un factor clave para enfrentar la implementación, es necesario saber guiar y hacer comunicar cualquier procedimiento nuevo, escuchar al personal y las necesidades que cada uno de ellos tiene, la mayoría de la gestión de acceso a la información implementada puede ser producto del intercambio de ideas del área involucrada y el equipo implementador. Se debe observar y analizar cada detalle.

4.5.2. Documentación necesaria

La documentación es necesaria al iniciar y preparase para el cambio, todo debe quedar registrado por medio de una bitácora que incluirá cualquier apunte o recordatorio necesario para implementación, hay que cerciorarse que cada uno de los puntos evaluados dentro del SGSI estén cubiertos.

No solamente se trata de realizar mejoras y documentarlas, se trata de direccionar cada una de las metas hacia el objetivo planteado. Este se puede derivar en objetivos iniciales de Alta Dirección, servicios prestados a cada área, control de riesgos para acceso a la información. Es un conjunto de mejoras que harán que la gestión al acceso de la información sea correcta y segura.

Debe definirse una metodología de evaluación de riesgos, en ella se identifican los activos, que en este caso será la información o cualquier vínculo que esté relacionado con ella. Asimismo las vulnerabilidades actuales, amenazas dentro y fuera de la compañía y las probabilidades, siempre utilizando una medida de riesgo que es tolerable. Las reglas o controles deben quedar estrictamente definidas, de no ser así podrían obtenerse datos que no son correctos y apuntar hacia un proyecto inalcanzable en cuestión de recursos y no viable. Se debe ser realista en cuestión de saber hasta dónde puede perfeccionarse la gestión de acceso a la información, si es posible manejarla por fases lo cual representa mejora continua.

La metodología a utilizar para reducir el riesgo en el acceso a la información se puede otorgar por medio de una empresa certificadora, también puede hacerse a través de la búsqueda de una metodología dentro del internet localizando una herramienta que puede adquirirse para no crear desde cero un sistema tal vez ya creado por terceros. La metodología deberá poder identificar los activos, amenazas, vulnerabilidades, probabilidades, un método matemático para cálculo de riesgos y definición de niveles aceptables del mismo. El sistema como tal debe contener catálogos de vulnerabilidades y amenazas, previamente identificadas.

Todo lo planteado en la evaluación de riesgos, en algún momento se pondrá en práctica, debe recordarse que esto tomará cierto tiempo lo que reclama un orden de los pasos y la documentación para no pasarlo por alto. El objetivo de este documento es tratar cada riesgo o amenaza en un rango aceptable, se utilizarán algunos controles definidos por el equipo certificador o por la herramienta seleccionada.

Cada vez que se realice una mejora para el riesgo seleccionado, debe documentarse el proceso que conllevó mitigar el riesgo como mejor práctica o en lo posible, llegarlo a mantener en un rango aceptable definido por el equipo. Debe existir una aprobación por parte del mismo Departamento que mantiene este riesgo y cómo el equipo intervino para lograr el objetivo.

Los pasos que se deben seguir en la documentación de riesgos son:

a) Definir la metodología a utilizar

b) Identificar los activos
c) Organización de entrevistas con los propietarios de activos
d) Revisión completa de los activos
e) Consolidación de datos (activos), evaluar cada uno y sus riesgos
f) Cada riesgo debe contener controles para poderlo mitigar

Se debe tener presente que crear todos los controles y la documentación son pilares para la gestión del acceso a la información, pero no significa que sea complicado.

4.5.3. Cómo iniciar la transición

La transición para iniciar el proceso debe ser manejada por medio de una comunicación constante con el personal, estableciendo lineamientos para manejarlo de manera gerencial sobre todo con los empleados y clientes.

Es aconsejable que se realice por fases, lo que permitirá conocer cada etapa y la implementación en una determinada área para luego evaluar si la conducción del proyecto, va por buen camino. Dicha división de fases se debe plantear al inicio de la documentación en donde se establecen las prioridades al igual como se mencionó con los objetivos y metas a alcanzar. Este proceso va de la mano con las metas a mediano y largo plazo, en cada meta se ve involucrado no solamente el equipo de *staff* sino el área de mejora, clientes, proveedores, materiales, comunicación y monitoreo.

Para comenzar se debe utilizar el cuadro de riesgos y áreas priorizando el área más vulnerable y los riesgos que cada una presenta en cuanto a:

- Líneas de comunicación
- Introducción a tecnología
- Manejo de personal
- Papeleo y trámites legales
- Capacitación
- Prueba de programas piloto
- Lanzamiento el proyecto
- Monitoreo y supervisión
- Cierre

Cada uno de los puntos citados es necesario validarlos y para conocer las áreas de mayor y menor disposición. Se recomienda elegir para comenzar áreas críticas y que presenten mejor disponibilidad para realizarlo, esto podrá ayudar a dar una buena imagen del cambio que se desea realizar y contribuye a lograr el visto bueno de las áreas de trabajo en donde deba implementarse posteriormente.

La interacción entre Departamentos o áreas puede presentar cierto conflicto, por eso es necesaria la comunicación, el apoyo de Gerencia y la compresión de los jefes. El agente comunicador y la supervisión son piezas de éxito.

Otro tema a considerar se refiere que los *stakeholders* estén disponibles al momento de realizar la transición. “¿Y esto por qué?”, normalmente los procedimientos o accesos son de conocimiento de una persona específica, la cual brinda experiencia y soluciones a cualquier situación que se presente, amplia la visión del mismo equipo de *staff* de cómo resolver de manera ágil cierto atraso que pudiera ocurrir. Si esto no fuera posible es considerado tener una línea de comunicación abierta de manera remota con el *stakeholder*.

La papelería y trámites legales deben tomarse en cuenta ya que cualquier atraso podría afectar de manera significativa la entrega del proyecto, se debe revisar minuciosamente con un asesor legal cada término o acuerdo en cuestión, como por ejemplo:

- Licencia de uso de suelo. Escrituración, certificado de libertad de gravamen, impacto ambiental;
- Requisitos legales de un proyecto que involucra licencia de construcción, contratos de proveedores, contratos de arrendadores, licencia de restricciones naturales.

Cabe mencionar que cada trámite se debe hacer oportuna y adecuadamente para evitar clausuras que repercutan en multas, retrasos y costos extra.

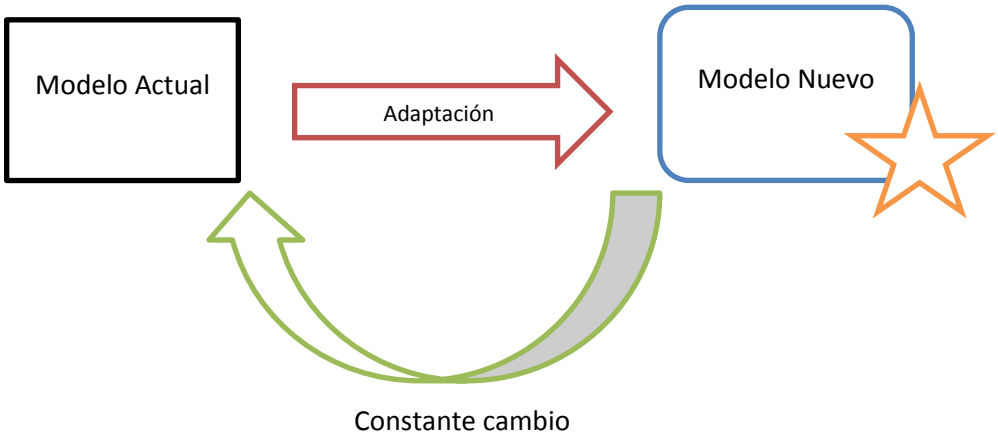
4.5.4. Modelo de negocio actual y adaptación

Las empresas más exitosas a nivel mundial son aquellas que pueden adaptarse a los cambios de una manera rápida y eficiente, reevaluando y rediseñando los modelos de negocio que manejan, la gestión de acceso a la información no es la excepción para realizarlo, es más bien un pilar y una necesidad para que los modelos a crear prevalezcan y no existan hurtos de información confidencial.

El aprendizaje que la empresa brinda a los empleados es necesario para lograr las metas establecidas. Los cambios constantes que surgen deben ser absorbidos por la empresa, mejorando el conocimiento de cada área y manteniendo una constante capacitación de los mismos.

Para ser eficaz y cambiar el modelo actual por el modelo nuevo dentro de la empresa, se debe retroalimentar al área involucrada, las políticas y medidas de seguridad, periódicamente, como se muestra en la figura 12.

Figura 12. **Cambio del modelo actual al nuevo**



Fuente: elaboración propia.

La mayoría de *CEOs* prevén una complejidad en el futuro y más de la mitad no están seguros de cómo manejar dicha complejidad. Los cambios siempre existirán sin embargo es necesario adaptar dichos cambios en conjunto con el equipo para que la dirección y solución se dé sin ocasionar nuevos problemas.

Las organizaciones normalmente utilizan métodos diferentes para crear nuevas oportunidades y vencer los retos, la gestión al acceso de la información no es la excepción. La creatividad es un factor importante a tomar en cuenta en donde se anima a las organizaciones a experimentar y llevar a cabo estrategias. Se estima que la creatividad puede llegar a superar el liderazgo dentro de las empresas debido a un mundo ahora más complejo que al inicio de la era de la información.

La complejidad puede llegar a asfixiar a los mejores elementos del equipo y reducir las respuestas positivas o acertadas para realizar el trabajo correcto o poder cubrir una emergencia de cualquier índole. Se enumeran los pasos a realizar para llegar a cubrir esta necesidad:

- Incorporar un liderazgo creativo aceptando el nuevo ambiente de trabajo
- Afianzar relaciones con clientes y empleados, este es un punto clave que puede aprovecharse en el beneficio de la empresa
- Desarrollar una habilidad operativa, simplificando el trabajo y administrando la complejidad

4.5.5. Resistencia al cambio

La peor debilidad dentro de un equipo puede encontrarse al tratar de incorporar la gestión de acceso a la información en la resistencia que ocurre a cualquier nivel. Lo primero que debe hacerse es quebrantar dicha resistencia desde la cabeza pues ellos son los que deben dar el primer paso y transmitirlo hacia toda la compañía.

Se observa que existe aún un poco de resistencia al cambio tanto en los mandos medios como en alta gerencia dentro de las empresas de Guatemala, esto se debe a que las ideas que promovidas aún no son bien vistas por la gerencia y también existen resistencia al cambio por parte de los empleados.

Atacar este problema de raíz se logra cambiando la manera de actuar dentro de la compañía, esto se podría invitando al personal a participar abiertamente en actividades que promuevan lazos de unión entre Departamentos. Las actividades pueden ser reuniones generales, capacitaciones, mesas de diálogo y sugerencias, concursos que promuevan soluciones de seguridad dentro de la compañía entre otros, las posibilidades son infinitas.

Cabe destacar que depende mucho del ambiente que se viva dentro de la compañía, en algunos casos podría requerirse ayuda profesional para lograr el objetivo, ya que si no se rompe la barrera de resistencia al cambio el proyecto puede llegar a fracasar por el mismo sabotaje o mala disposición del personal.

4.6. Impacto de privacidad de información en el sector privado de Guatemala

En el transcurso de los años se han visto múltiples vulnerabilidades dentro de cada organización, tanto como entidades privadas como gubernamentales tienen una intrusión en sus sistemas. Por ejemplo el de robo y el acceso a información confidencial de gobiernos mundiales mostraron la fragilidad de un sistema como le puede suceder a cualquier compañía nacional o multinacional, por ello que se debe enseñar a los usuarios y empleados de la compañía a mantener la información de manera segura, manejándose bajo las políticas establecidas.

Actualmente Guatemala posee una infraestructura de servicios y comunicaciones lo suficientemente robusta para abastecer servicio a muchas personas sobre todo en la ciudad capital; existen redes públicas o privadas a lo largo de centros comerciales, edificios, restaurantes y residencias, puede ser víctima de espionaje o robo de información.

El impacto virtual se podría comenzar con robo de contraseñas e información confidencial del usuario o que pertenezca a la empresa al navegar en una red insegura o desconocida y hasta más grave de eliminación de archivos, acceso a cuentas bancarias y traslado de fondos de una planilla de trabajo, robo de material o de las cuentas bancarias, estrategias de mercado o documentos confidenciales que ponen en riesgo la integridad de la compañía. Al momento que suceden estos hechos delictivos, no solamente está afectándose a un empleado sino a la misma empresa pudiendo afectar a clientes y proveedores. Otro impacto es dejar sin servicio a los usuarios y gran cantidad de transacciones o ventas podrían perderse en un periodo corto de tiempo que el sitio esté bloqueado.

El impacto de seguridad también puede suceder dentro de la empresa, el acceso a la información valiosa puede ser hurtada y violados los accesos respectivos; sin equipo que pueda detectar a los intrusos, códigos de acceso y personal calificado que vele por la seguridad del mismo es difícil capturar a los delincuentes, lo que puede significar pérdida de quetzales. Así mismo cualquier emergencia física o efecto climatológico, si no se tiene un plan de contingencia, puede ocasionar pérdidas de información virtual o física que no podrán recuperarse con facilidad. Por medio de una gestión adecuada pueden llegarse

a minimizar estos sucesos, dar un seguimiento adecuado y encontrar las causas para tomar medidas de una manera más eficiente y eficaz.

4.6.1. Enfoque de privacidad de información a una organización

El sentido de mantener resguarda la información dentro de una organización asegura los activos y a los empleados de la compañía, manteniendo el foco en las actividades diarias y siendo mucho más productivos en el área que desempeñan. La privacidad de la información permite que solamente los interesados puedan acceder a ella y realizando una gestión de acceso a la información correcta, se logran mantener los indicadores de seguridad establecidos en un parámetro normal, sin perder el enfoque de monitorear constantemente cada una de las áreas que puedan ser corrompidas por personas ajenas a la organización.

Las políticas que se desea implementar dentro de una organización ayudan a maximizar el enfoque de privacidad de cada empleado y permiten llevar un seguimiento y mejora continua de cada área, adelantándose a acontecimientos que puedan suscitarse en periodos futuros. Este enfoque ayuda a que la misma organización vele por su cumplimiento y transmita este sentimiento a cada empleado.

4.6.2. Encuesta sobre seguridad e información

Para conocer cómo se maneja en algunas empresas la seguridad de información, se realizó una encuesta del 29 de diciembre del 2010 al 3 de enero del 2011 con empleados que laboran en TI, aplicando un formulario de 14 preguntas clave que encierran la gestión del acceso a la información y elementos que se utilizan para llevarla a cabo. El formulario se adjunta en el anexo I.

Los criterios para la encuesta fueron:

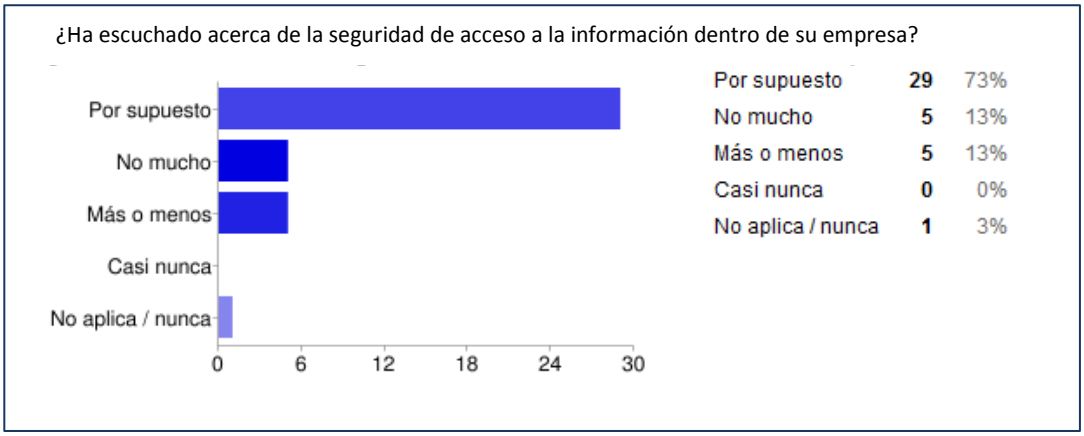
- Selección de la muestra, realizada a 40 personas.
- Sexos masculino y femenino
- Desempeño dentro del sector guatemalteco en área de TI
- 12 preguntas con 5 opciones para cada respuesta
- 2 preguntas con más de 5 opciones
- Utilización de *Google Docs*. para captura de datos

La encuesta se enfocó en la participación de la alta gerencia y la comunicación que esta sostiene con la empresa para enfrentar cambios de procedimientos y manejo del personal llegando a realizar un análisis sobre los temas expuestos y las posibles soluciones que se adjuntan en el apéndice I.

4.6.2.1 Análisis de resultados

Análisis de resultado obtenido en la encuesta a 40 empleados de TI en Guatemala.

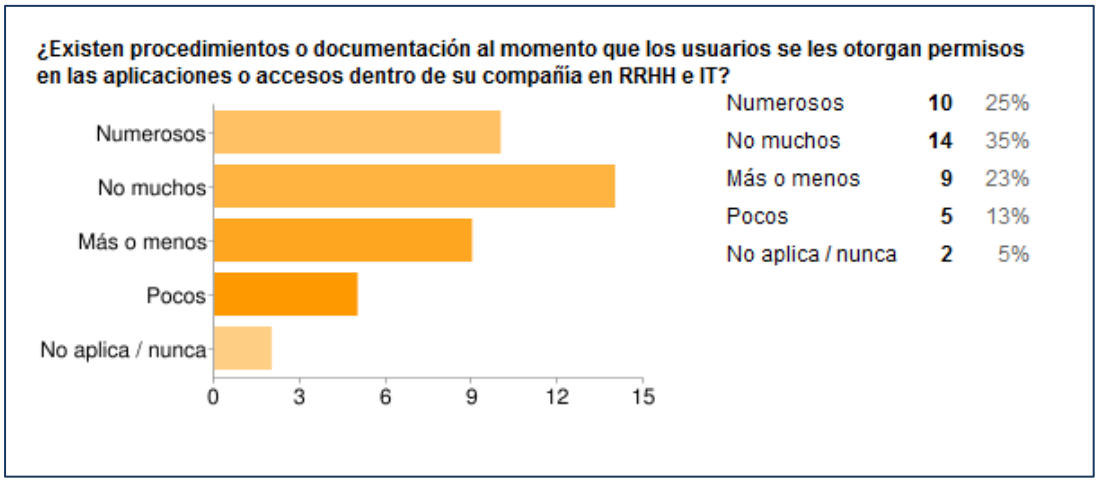
Figura 13. **Pregunta 1**



Fuente: elaboración propia.

Un 73% de la muestra menciona que ha escuchado sobre el término, sin embargo 26% que no ha escuchado, a pesar de que la mayoría ha podido escuchar del término, es necesario que se realice dentro de cada empresa una mayor divulgación sobre la seguridad del acceso a la información.

Figura 14. **Pregunta 2**



Fuente: elaboración propia.

Cuando se menciona un procedimiento o documentación se abarca cualquier tipo de gestión realizada al momento de contratar nuevo personal; como se vio en el capítulo 3 es necesario que exista no solamente una hoja de control sino un registro de cambios y fechas de modificación sin embargo únicamente 25% de la muestra respondió afirmativamente al respecto.

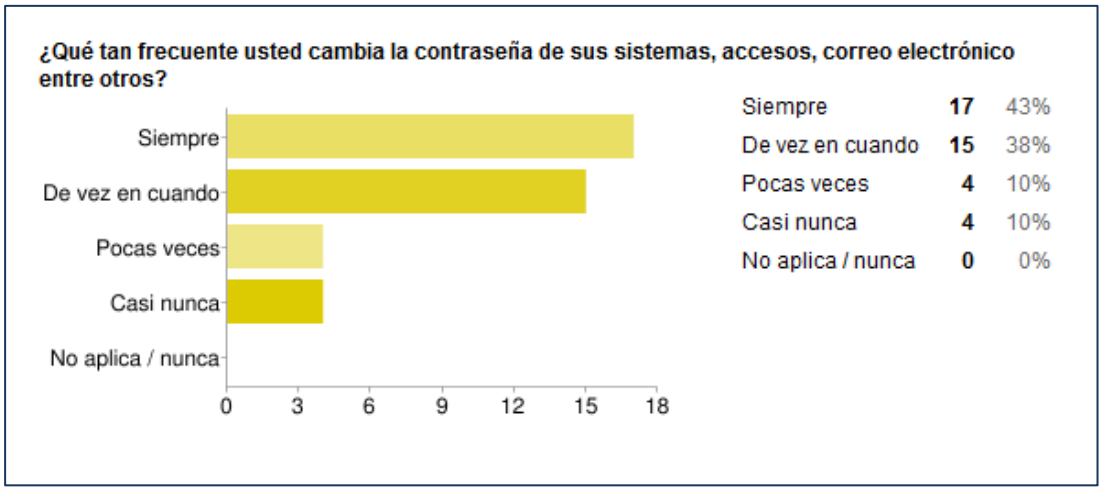
Figura 15. **Pregunta 3**

Fuente: elaboración propia.

Esto recalca el cuestionamiento de la pregunta anterior, vemos que la mayoría de empleados cuenta con una jerarquización llegando a 73%, embargo existen algunas deficiencias de 18% no cuentan con una jerarquía clara al momento de acceder a herramientas del sistema. Es preocupante no tener clara la jerarquización de la empresa ya que esto provoca que exista dualidad de permisos, líneas de mando inestables en los sistemas y acceso indebido, entre otros.

La información debe ser más estricta al momento de otorgar acceso, esto se logra realizando gestión de la documentación necesaria antes y después de que el empleado éste laborando dentro y fuera de la empresa.

Figura 16. **Pregunta 4**

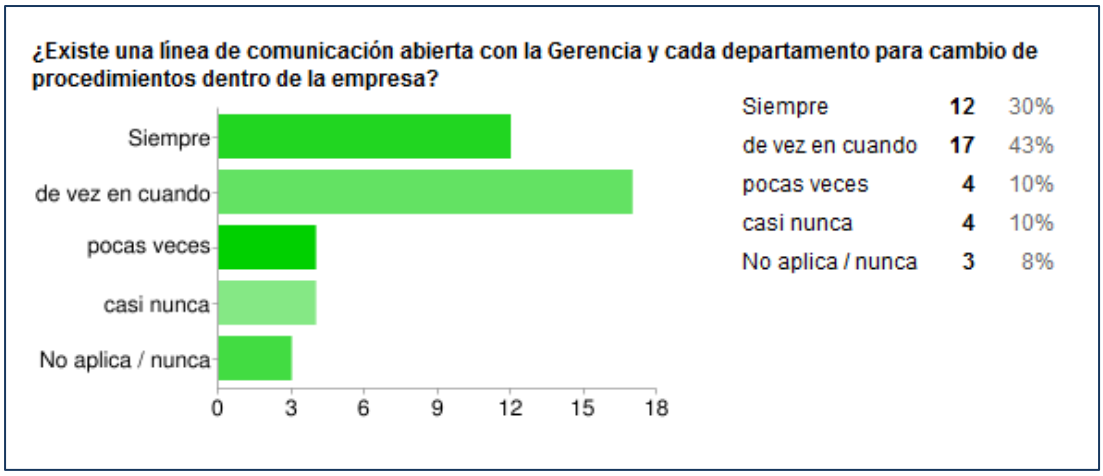


Fuente: elaboración propia.

Esta pregunta responde a la típica forma en que una compañía emplea responsabilidad y confianza dentro de los empleados, debido a que normalmente lo que sucede es que los sistemas otorgan una contraseña y esta no es cambiada hasta que el empleado lo solicita. 43% respondió que siempre.

Llevar un estricto control del período de tiempo válido para un contraseña es vital para la gestión de acceso a la información, esto ayuda a mejorar el control de fechas en que el empleado tuvo acceso y también permite verificar si una persona ajena a la compañía comience a utilizarla, llegando un momento en que no se puede acceder, evitando pérdidas de información vital.

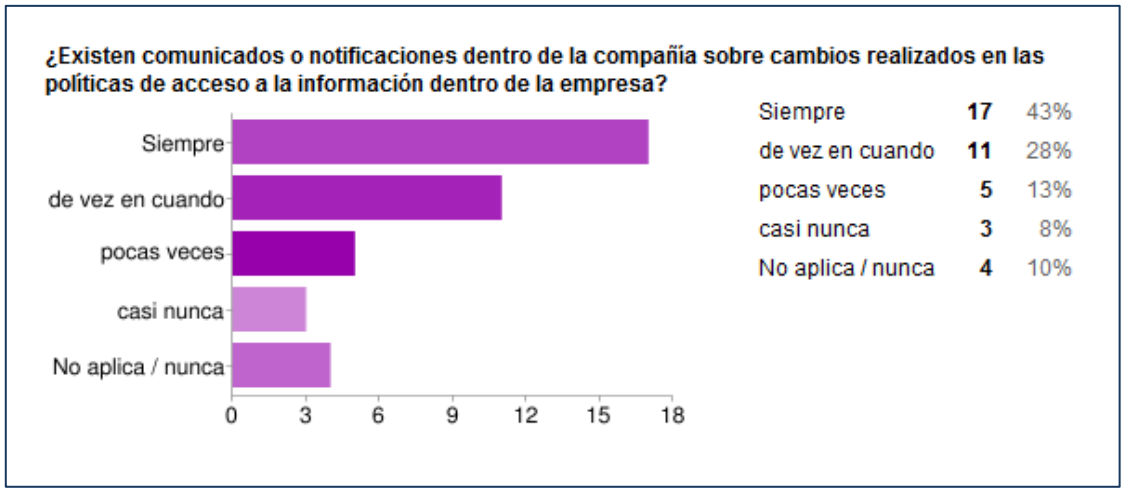
Figura 17. **Pregunta 5**



Fuente: elaboración propia.

La comunicación en cualquier empresa es clave de éxito para poder llegar a cumplir objetivos, pero mucho más importante es que el personal pueda crear objetivos o metas y que éstos lleguen a gerencia para poner en marcha un plan de acción para llevarlo a cabo. Vemos que el 43% opina que de vez en cuando existe una línea de comunicación y 28% (pocas veces, casi nunca y nunca). Es altamente preocupante que solamente exista un 30% de la muestra con línea de comunicación correcta, este factor es clave de éxito para la puesta en marcha de una gestión de acceso a la información.

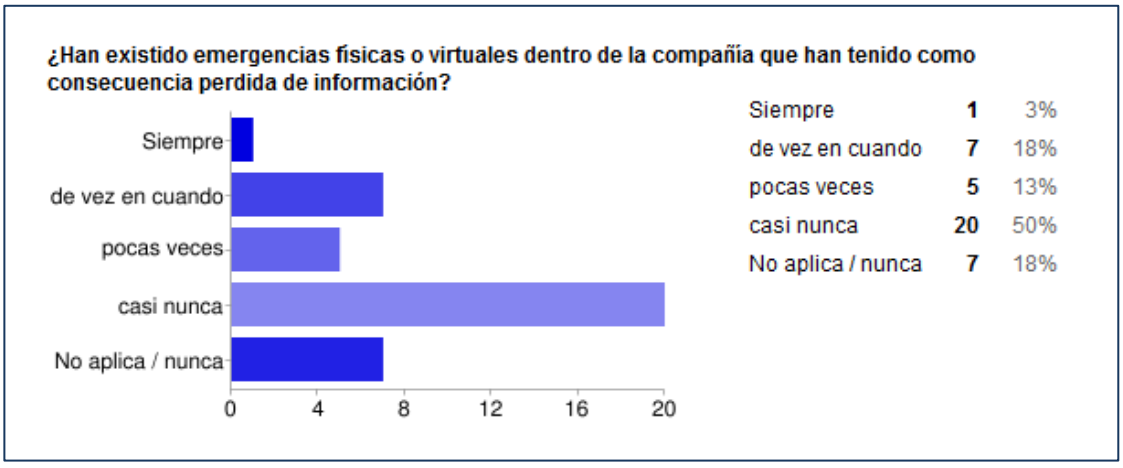
Figura 18. **Pregunta 6**



Fuente: elaboración propia.

La comunicación va de la mano con los cambios que ocurren dentro de la compañía, vemos que a pesar que no existe una gran comunicación con la gerencia, esta disminuye cuando hablamos a nivel general. Siempre respondió un 43%; 28% de la muestra, de vez en cuando y 31% que casi nunca tienen notificación.

Figura 19. **Pregunta 7**



Fuente: elaboración propia.

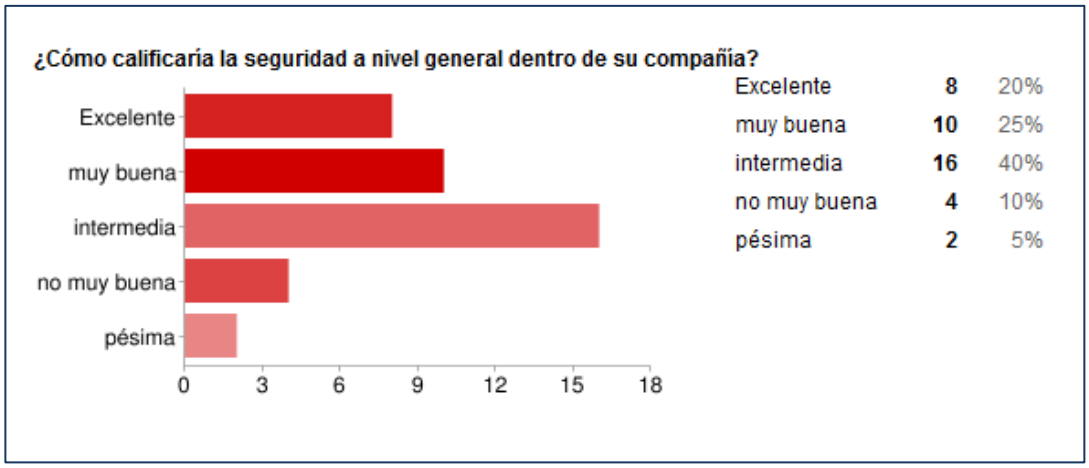
No es alentador ver que solamente un 18% no ha sufrido emergencias, el 81% si ha tenido problemas tanto físicos o virtuales, algo muy curioso es que 3% de la muestra que respondió que siempre existen. Debe tomarse en cuenta la información de empleados y ver cómo ellos perciben la situación de la compañía en este aspecto.

Figura 20. **Pregunta 8**

Fuente: elaboración propia.

Dando un seguimiento a la pregunta anterior vemos aquí que la mayoría de compañías le dan un seguimiento a problemas internos, en este caso de los 33 entrevistados que ha tenido problemas solamente 12 mencionan que sí pudieron solucionarlo, un 10 mencionó que de vez en cuando, cualquier motivo de emergencia debe ser remediado de manera inmediata. 11 personas mencionan que pocas veces, casi nunca e inclusive nunca resuelven el problema.

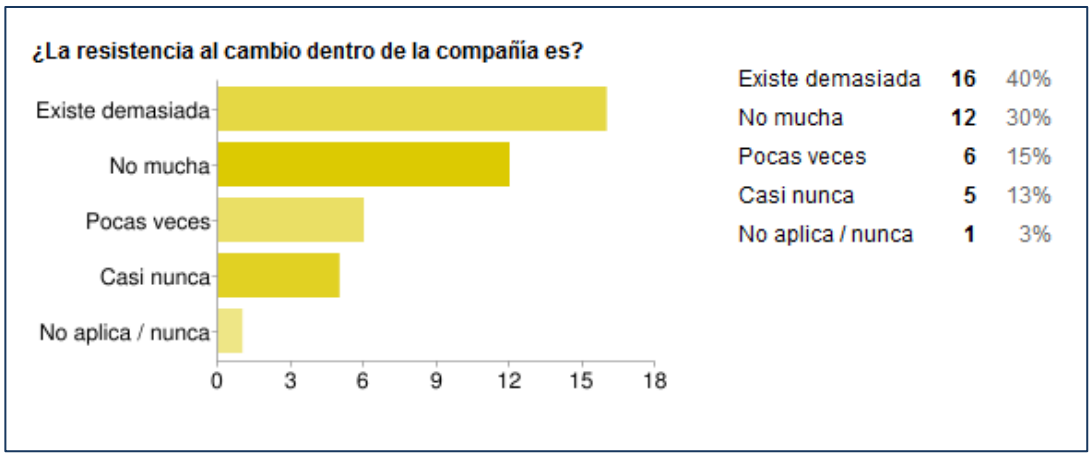
Figura 21. **Pregunta 9**



Fuente: elaboración propia.

Se ve que la mayoría de empleados no considera que la seguridad sea primordial dentro de la compañía se ve reflejado en 40% de la muestra que menciona que es intermedia. El 15% está por debajo de la media y un 45% dice que la compañía es muy buena tendiendo a excelente. Si el personal no está completamente seguro dentro de las instalaciones su productividad se ve afectada.

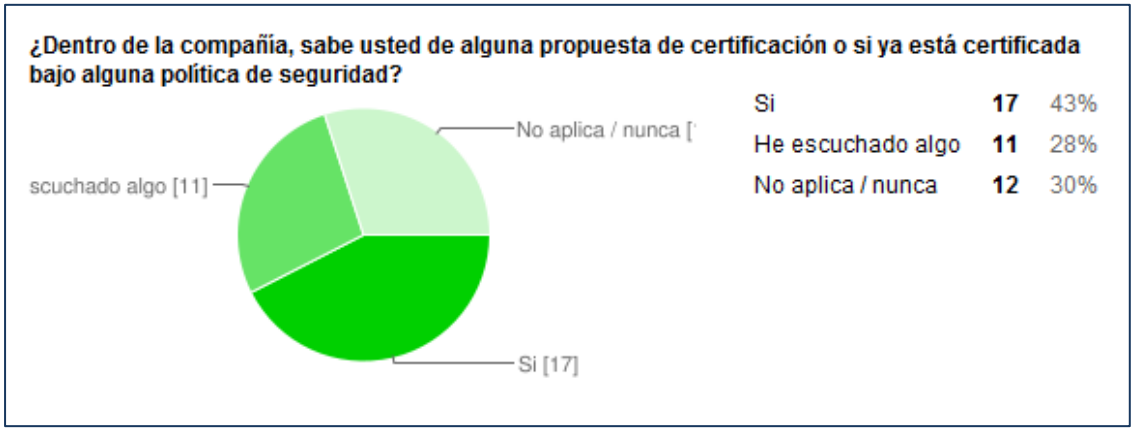
Figura 22. **Pregunta 10**



Fuente: elaboración propia.

Un factor clave para cambiar la mentalidad de las personas es la resistencia al cambio y como éste se maneja dentro de la empresa. La mayoría coincide que existe demasiada resistencia 40%, no mucha y pocas veces 45% en conjunto y por último y siendo optimistas vemos que solamente un 16% en conjunto con casi nunca y nunca tienen resistencia al cambio. Éste último es el valor que debemos de buscar dentro de la compañía, lo que refleja voluntad, para hacer cambios y mejoras. La gestión de acceso a la información puede ser mucho más fácil de introducir en ambientes donde este aspecto es nulo.

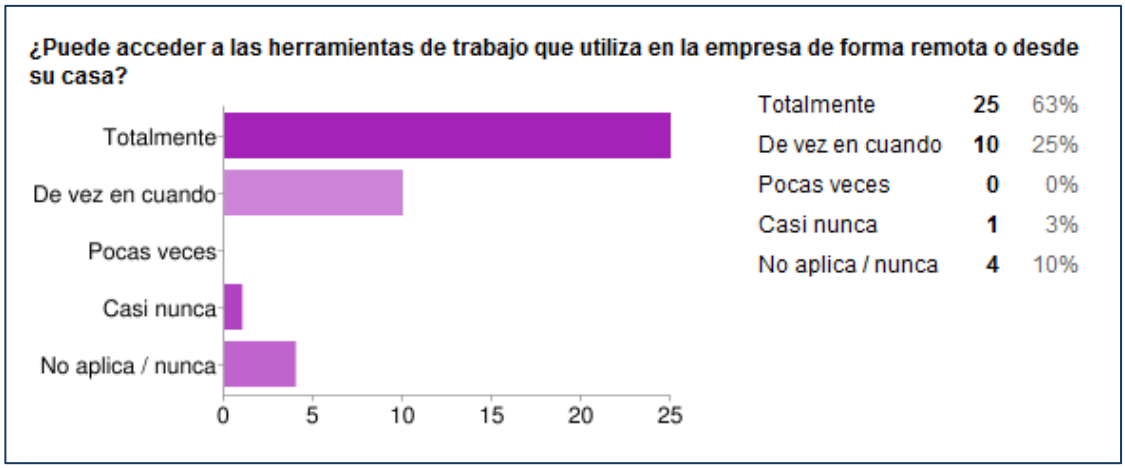
Figura 23. **Pregunta 11**



Fuente: elaboración propia.

El 43% de la muestra menciona que sí y posiblemente se implemente o exista alguna documentación preliminar, un 30% nunca y 28% menciona que si ha escuchado en alguna ocasión dicha información.

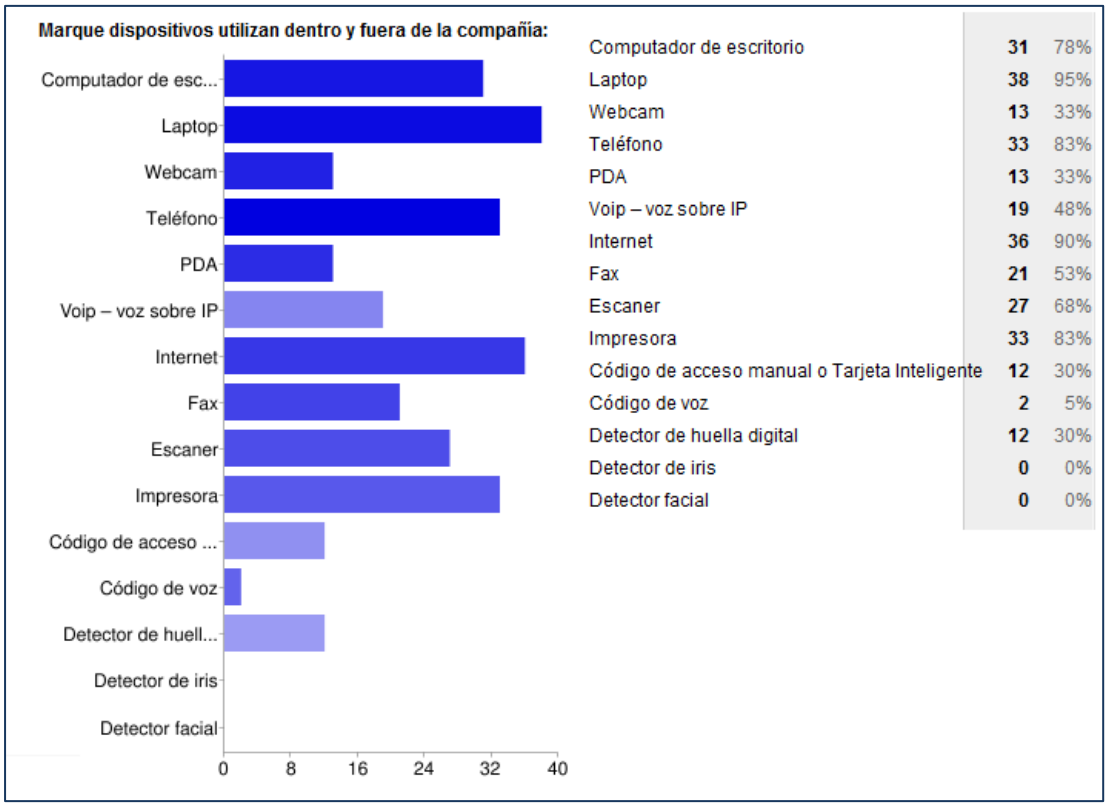
Figura 24. **Pregunta 12**



Fuente: elaboración propia.

La accesibilidad es importante para la seguridad de la información, 63% de entrevistados de TI tienen un acceso total, 25% menciona que de vez en cuando y 13% que casi nunca o nunca puede acceder. Debemos tomar en cuenta que un acceso remoto hoy en día es sumamente necesario para cualquier área de trabajo.

Figura 25. **Pregunta 13**



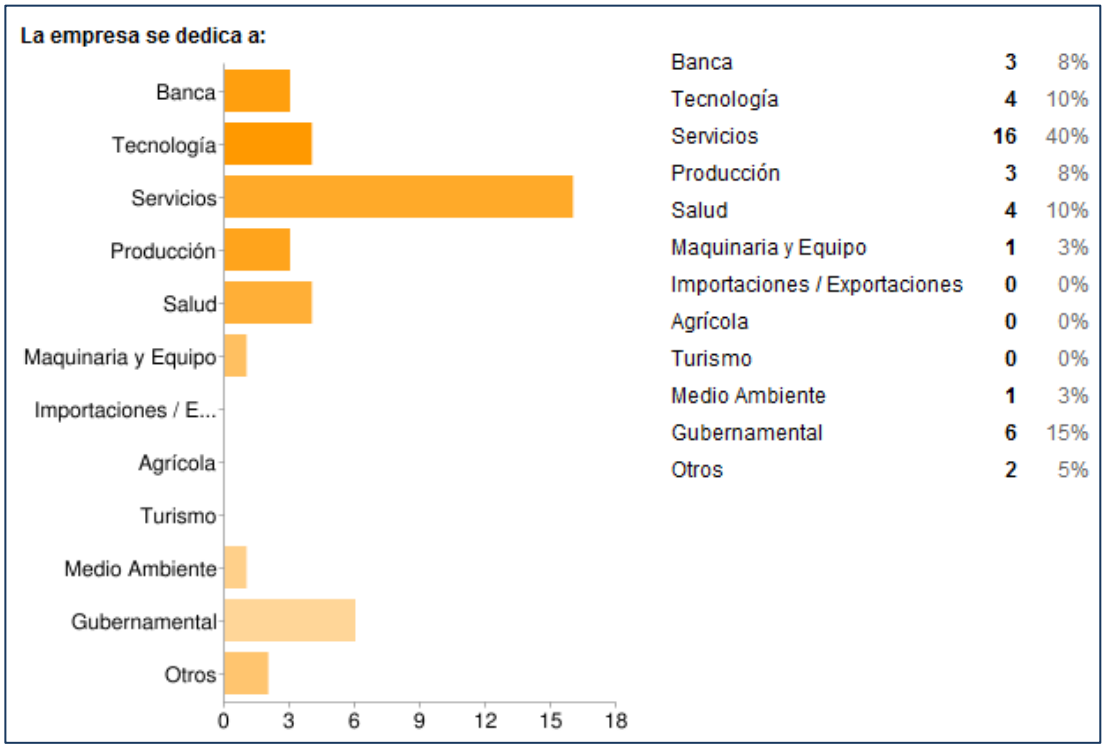
Fuente: elaboración propia.

Los 40 entrevistados 95% utilizan laptop, 78% utilizan además computadores de escritorio también.

Para comunicación vemos que un 83% tienen teléfono, sin embargo Voip está ganando terreno y 48% lo utilizan, 90% usan internet. El método de acceso por seguridad vemos que está parejo con el acceso manual y con el de utilización de huella digital, 30% para cada uno, por debajo está el comando de voz.

Se observa que siguen liderando la laptop, el internet, impresora y teléfono como los más influyentes medios de transmisión de información dentro de TI.

Figura 26. **Pregunta 14**



Fuente: elaboración propia.

La mayoría de personas entrevistadas están en el área de servicios con 40%, luego tenemos gubernamental con 15%, salud 10% y tecnología también 10%.

4.6.2.2 Gestión del acceso del usuario y responsabilidades que éste conlleva.

Como se puede observar en la encuesta realizada el acceso a la información no siempre es bien realizada dentro de una organización, una simple responsabilidad de seguridad que se le puede confiar a un usuario como es el acceso secreto que solamente él debe poseer normalmente es quebrantado otorgándolo a empleados de la misma área o entregada a personas ajenas a la organización provocando fuga de información ya sea física o virtual.

Las responsabilidades que un usuario tenga en cuestión de seguridad dependerán de las autoridades respectivas dentro de la organización que otorguen a cada usuario. Los usuarios normalmente son empleados que acatan órdenes de los altos mandos y mandos medios. Los altos mandos y mandos medios son los encargados de solicitar y otorgar hacia el usuario final. Esto se logra por medio de procedimientos previamente establecidos dentro de la alta gerencia, RRHH y el Departamento de TI.

La seguridad para que se cumpla a cabalidad dependerá de los sistemas de monitoreo que la compañía proporcione y el seguimiento adecuado para validar que se esté utilizando correctamente. Este sistema deberá ser validado por los jefes inmediatos en períodos de tiempo que se realicen por un acuerdo entre las partes o según políticas ya establecidas dentro de la compañía.

El otorgar mayores o menores permisos a los usuarios dependerá de una gestión que también debe ser coordinada por los mismos encargados y llevando un historial por cada usuario en donde se validará que efectivamente es necesario el acceso o de negación al área solicitada. Es importante mantener dentro de la compañía una jerarquización de permisos y estos también destinados a cada puesto, los cuales se pueden identificar por roles y funciones que deben de otorgársele a un usuario.

4.6.2.3 Acceso a redes e infraestructura

La encuesta revela que las compañías guatemaltecas en alguna ocasión han sufrido emergencias físicas o virtuales y cabe destacar que existe un 3% de la muestra que experimenta siempre este tipo de problemas.

La seguridad de la red es paradójicamente hablando, como la llave de la casa de una familia en donde se da acceso a cualquier habitación para utilizar, tomar por prestado, ver información privada, robar cualquier objeto dentro de ella. Para que esto no suceda es ideal solamente darle llaves a personas conocidas, en este caso a los miembros de la familia. Si existe alguna intromisión a la casa o se viola la puerta, esta se debe cambiar la cerradura o de preferencia se tiene una alarma contra robos y lleguen las autoridades respectivas, de esta manera la misma familia se mantiene a salvo así como sus objetos más valiosos.

Así como se menciona el hogar de una familia, así mismo funciona una red dentro de la empresa, en donde ciertos empleados tendrán acceso a determinados sistemas y ciertas áreas, pero solo algunos podrán acceder a administrar por completo un sistema o poder validar cuentas bancarias dentro de la misma. Las redes deberán tener dispositivos de seguridad que aseguren la detección de cualquier tipo de violación ya sea física o virtual, esto se logra por medio de programas de *hardware*, *software* o sensores colocados dentro del mismo centro de datos donde se almacenan las conexiones de la red.

Las redes se dividirán en locales, públicas o privadas para este caso debido a que dentro de la compañía se podrían presentar estas opciones. Se deberá tener un personal calificado que pueda ayudar a configurar las entradas y salidas de cada acceso; así mismo utilizar materiales y dispositivos estándar dentro del mercado es importante para que cualquier dispositivo que se adquiera tenga respaldo de un proveedor local en el mejor de los casos. La segmentación de la red debe estar acompañada por un mapa o canales de distribución que ayuden a corregir cualquier anomalía o falla dentro de la misma.

La seguridad virtual también es importante, se debe contar con el *software* adecuado y realizar constantemente las actualizaciones necesarias dentro del sistema, es obligado a realizar monitoreo constante de las vulnerabilidades que puedan existir de manera física como virtual. El manejo de redes VPN, comunicación VOIP, actualizaciones, telefonía celular y red inalámbrica dentro del diseño de la red se deben de representar

Pero mucho más importante que realizar todo lo anterior es realizar una planificación de validaciones clave dentro de la red e infraestructura que cubran:

- Períodos de monitoreo
- Fechas de mantenimiento del equipo y notificaciones a la compañía
- Actualizaciones críticas
- Actualizaciones realizadas por terceros
- Capacitación del personal
- Comunicados de mejoras realizadas a la red
- Mantenerse informado de los acontecimientos de ataques

La seguridad de la red e infraestructura deberá de garantizar:

- La Disponibilidad de los sistemas de información en cualquier punto de la red
- La Recuperación rápida y completa de los sistemas de información
- La Integridad de la información
- La Confidencialidad de la información

4.6.2.4 Acceso a sistemas operativos y aplicaciones de *software*

La diversidad de sistemas operativos y aplicaciones dentro de las ofertas del mercado son muy amplias, sin embargo, se debe elegir un sistema que tenga cumpla con los siguientes criterios:

- Buen desempeño
- Cubre las necesidades del área y si permite crecimiento
- Bajo impacto de utilización en el personal
- Capacidad de procesamiento masivo
- Escalabilidad comprobada
- Soporte y asistencia del proveedor local o internacional
- Actualización del *software*
- Bajo costo y consumo de energía
- Menor vulnerabilidad de acuerdo a estudios o *benchmarking* realizados con sistemas similares
- Manuales técnicos y de usuario
- Validación de sistema abierto y configurable
- Especificaciones técnicas de mantenimiento y ambiente adecuado del equipo de *hardware* donde se almacenará

Las necesidades de un buen sistema son muy propias de cada empresa, así como existen compañías que deciden realizar sus sistemas a la medida, existen empresas que utilizan sistemas de terceros que garantizan un funcionamiento formidable, la gran mayoría utiliza sistemas híbridos que han

sido diseñados para la compañía utilizando sistemas que traen especificaciones de caja.

Se debe considerar si las aplicaciones serán para utilización interna o si serán para usarse por medio de internet y la interoperabilidad que estas conllevan. Es de suma importancia escoger el *software* adecuado para el buen funcionamiento y el resguardo de la información, más si este será el de los datos de toda la corporación. El mantenimiento es vital y los sistemas de seguridad para el buen manejo del sistema maestro.

Los sistemas de seguridad deben monitorearse constantemente con tal de revisar que no se encuentren notificaciones de intrusos, archivos no deseados, o pérdida de información significativa. Nadie en la era digital que se vive actualmente puede decir que nunca sufrirá algún ataque, sin embargo se puede llegar a minimizarlo utilizando sistemas adecuados que brinden estabilidad y adicionalmente teniendo planes de contingencia.

La información debe estar segura no solamente de forma digital sino físicamente y esto se logra utilizando “sistemas que vigilen sistemas”. Generalmente en las empresas se manejan códigos de seguridad los que se administran por medio de un sistema centralizado que permite el acceso a cada área, los intrusos pueden llegar por vías físicas o virtuales. Si llegan por vías virtuales el sistema notificará las anomalías y manteniendo alerta a la empresa. Si las amenazas o intrusos son físicos, la compañía debería tener integrado el sistema de alarma directamente con autoridades o un proveedor externo que

pueda notificar lo que sucede al equipo encargado de seguridad dentro de la compañía.

Los sistemas que actualmente se utilizan son:

- Sistemas de detección de intrusos: se centran en la realización de bitácoras de ingreso en busca de patrones de comportamiento validando cualquier evento sospechoso, normalmente se les denomina “monitores”;

- Sistemas orientados a conexión de red: monitorean las conexiones de red validando las vías de conexión y los dispositivos que están dentro de la compañía, pudiendo ser capaces de detectar el origen y el destino de la información, aquí podemos localizar los *Wrappers* o *Firewalls*;

- Sistemas de análisis de vulnerabilidades: buscan debilidades dentro de los mismos sistemas de la empresa, estos no solamente los pueden utilizar los empleados sino también intrusos;

- Sistemas de protección a la integridad de la información: utilizan criptografía para asegurase que la información no o ha sido violada;

- Sistemas de protección a la privacidad de la información: criptografía para que solamente los verdaderos usuarios puedan visualizar la información;

- Sistemas de respaldo de información: son necesarios en cualquier ataque que ocurra, estos pueden ser programados para que vayan almacenando la información de cada equipo importante dentro de la compañía.

4.6.2.5 Computación móvil y teletrabajo

Actualmente la tendencia de trabajo directamente remoto y sin supervisión está siendo una realidad con el fin de reducir costos fijos dentro de la organización. Sin embargo, existe aún un control adecuado para llevar a cabo esta actividad y no abusar de forma inadecuada por parte de la empresa hacia el empleado y viceversa.

Los problemas más comunes que se dan son:

- Aumento de trabajo laboral de acuerdo al horario establecido
- Ausencias por parte del trabajador y sustituidas por otro día no laboral
- Interrupción de comunicación y no fidedigna
- Fallos técnicos (computador y dispositivos, energía eléctrica, telefonía, internet)
- Falta de supervisión y calidad del trabajo realizado por parte de los jefes
- Vulnerabilidad de parte del empleado por compartir información hacia terceros sin supervisión de la empresa
- Falta del equipo adecuado para poder realizar el trabajo correctamente
- Problemas de acceso seguro hacia los sistemas de la empresa

De acuerdo a la encuesta realizada vemos que la mayoría puede acceder de forma eficaz a la información y de hecho, con mayor razón debe darse prioridad al riesgo que se corre en compartir la información de esta manera. Llevar un control más estricto en los perfiles que maneja la compañía,

procedimiento de gestión de usuarios hacia la compañía y registro de cada uno de las modificaciones, es primordial.

El control debe ser bastante medible para saber hasta qué punto se puede proteger la información dentro de los objetivos del negocio. Los sistemas a implementar deben acoplarse adecuadamente para que no ocurran fallos, hacer el test correcto antes de realizar el paso a producción de una aplicación evitará varios dolores de cabeza. A pesar que los sistemas biométricos no son un dispositivo aún que se utiliza dentro de las empresas guatemaltecas, se observa la tendencia actual de protección de datos. Es muy probable que la utilización de teletrabajo requiera como norma ciertos métodos biométricos disponibles en el mercado y que sean utilizados por medio de un dispositivo por separado o integrado dentro del computador.

5. TENDENCIAS DE LA GESTIÓN DE ACCESO DE LA INFORMACIÓN

El mundo se transforma constantemente. Es importante comprender que los mercados no mantienen una dirección constante y esa dirección constituye la tendencia del mercado. La tendencia actual que se maneja para la gestión de acceso a la información la resumen explícitamente las organizaciones al abordar cómo debe trasladarse este conocimiento y plasmarlo dentro de la compañía. Para ello existe el termino TICs que agrupa los elementos y técnicas utilizadas en el tratamiento y la transmisión de información. Existen diversas organizaciones enfocadas y especializadas en el acceso de la información, sin embargo debe determinarse la ruta que más le conviene a la compañía. Dentro del análisis que se ha realizado durante los capítulos anteriores se validada que cada uno tiene sus puntos fuertes para mejorar la gestión de acceso a la información. Cada organización incorpora series de pasos que conllevan a lograrlo, sin embargo la organización pudiera necesitar un detalle más profundo o una ágil transición en algunas áreas específicas.

Se ha visto a lo largo de los últimos 10 años cómo ha evolucionado la seguridad de acceso a la información de manera sorprendente; cómo ha mejorado la comunicación no solamente local sino remota, cómo esto ha mejorado la calidad de información que podemos obtener en un corto periodo de tiempo; la forma de almacenamiento ha cambiado desde los discos duros y computadores de gran poder, pasando por los discos duros, *cd's*, *dvd's bluray's*, memorias de almacenamiento *usb*, proveedores de *cloud computing* entre

otros, pero existe una contra parte nos muestra cómo el mundo ha tenido que enfrentar problemas de seguridad en base a terrorismo, robos, manejo inadecuado de cuentas, accesos no deseados, información altamente confidencial, ha provocado mejorar constantemente los métodos de almacenamiento físico y virtual. Quiere decir que dentro de 10 años nos enfrentaremos a otros tipos de problemas de seguridad y para ello se debe estar preparado para poder llegar a mitigarlos.

5.1. Tendencias actuales

Los gestores de acceso a la información cada vez se enfocan en el servicio debido a que actualmente existe una necesidad de descubrir la información directa de los servicios y un autodescubrimiento y gestión de activos más populares.

El análisis forense en este momento es un tema que está directamente dentro de la gestión de incidentes que pueden ocurrir, este análisis incluye un cibercrimen de búsqueda de responsables por medio de pistas o evidencias que los mismos intrusos haber dejado, realizando una documentación detallada de los hechos, investigación de sospechosos y testigos y proseguir con un proceso legal que condene a los responsables.

Los cambios resultan en ciertas ocasiones abrumadores y más cuando se trata de la protección de los datos personales y de la compañía; sin

embargo, hay que recalcar que las vulnerabilidades actuales que se presentan fuera y dentro de la compañía son:

- Acceso a la información
- Denegación de servicio
- Manipulación de datos
- Obtener información
- Eludir seguridad
- Obtener privilegios
- Manipulación de archivos
- Avanzada amenaza persistente (termino de profesionales en busca de dinero dentro de la red)
- Desastres naturales y cambios climáticos
- Violencia e inseguridad nacional

La colaboración entre Departamentos es primordial, las tareas deben volverse mucho más sociales incrementando cada vez más participantes para poder gestionar mejores soluciones o políticas; los sistemas o herramientas deben permitir gestión de la información de manera colaborativa.

La creación de un catálogo de servicios que mejore el entendimiento de la cartera que se utilice dentro de la organización y asegurando que el diseño y la implantación del Catálogo de Servicios proporcionará un beneficio para el negocio y los clientes.

5.2. Tendencias a largo plazo

Las directrices que se inician a utilizar en el marco en la gestión de acceso a la información, se observa:

- Publicaciones de revistas, emails o documentos online o como en se comparta la información dentro de los próximos años
- Existe el etiquetado semántico o lenguaje natural en la gestión de servicios de TI
- Los servicios tradicionales pueden ser modificados
- Redes sociales pueden obtener información de los empleados e información de la compañía
- Ataques en los dispositivos de telecomunicación y teléfonos inteligentes que deben cubrirse en nuevas reglas por parte de los estándares actuales.
- Adopción de modo *SaaS* en soluciones en la gestión de servicios de TI
- Apoyo organizativo para la gestión de servicios de TI en continuo crecimiento
- Se presta más atención a los procesos orientados al cliente como la gestión de niveles de servicio y la gestión del catálogo de servicio
- Redes neurológicas que permiten aprender a lo que se denomina “redes inteligentes”
- Validación en el *outsourcing*

5.3. Por qué certificarse o encaminarse a tener estándares de acuerdo a la norma.

Las razones son muchas, sin embargo se mencionarán las que más peso tienen en este momento:

- Una imagen internacional donde se cumplen estándares directamente avalados y reconocidos por instituciones que velan por la gestión del acceso a la información y muchas áreas adicionales. Esto genera confianza entre los clientes y proveedores que están ligados de la empresa y en algunos casos hace que la comunicación mejore debido a que ellos mismos se ven involucrados dentro de las mejoras del proceso;

- Al momento de certificarse le puede servir para medir la evaluación de nuevos proveedores, selección de materiales, dispositivos de *hardware* y *software* o contratistas y que al momento de elegirlos cumplan con los requisitos establecidos por las normas;

- Las certificaciones permiten asegurar que los bienes y servicios cumplen con los requisitos obligatorios relacionados con el sector empresarial en que se labora, en este caso el acceso a la información es viable dentro de la organización y para resguardo de información o bienes valiosos de los clientes;

- Por medio de la certificación se obtiene una visión más detallada de la situación en cuanto a gestión de acceso a la información, ya que es un proceso que involucra a cada área de la empresa y las mejoras, permitiendo dar un panorama de cómo son manejados los procesos de

acceso a la información, cómo se resuelven y cuáles son los planes de contingencia si llegara a ocurrir una emergencia;

- Permite medir por medio de acuerdos de seguridad, impuestos directamente con la norma para verificar que cada área es segura y que se encuentra dentro de los estándares previstos por la propia compañía y la certificadora;

- Actualmente una ventaja competitiva es que las empresas poseen ciertas certificaciones ya que el mercado guatemalteco aún la mayoría no las posee, esto puede ser beneficioso para contratos a nivel internacional en donde se toma muy en cuenta.

5.4. Qué importancia tiene un SGSI dentro de la organización.

En Guatemala las compañías normalmente se manejan medidas de seguridad que ayudan a mejorar el desempeño de la compañía, sin embargo si estas se trabajan por separado solamente se constituyen controles técnicos pero que no crean una sinergia y por ende no pueden ayudar a mejorar los controles. Un SGSI permite tener una explicación del por qué se deben utilizar ciertos controles para obtener seguridad dentro de la información que se gestiona, involucra criterios de evaluación, métricas e implica estudios sobre los riesgos a que está sometida la información, generando soluciones en caso de existir alguna emergencia.

Permite garantizar que los riesgos que la compañía correrá serán menores a los que alcanzaría si no fuera avalada por ninguna gestión en

seguridad de la información. Es común observar en la cultura guatemalteca decide esperar a que ocurra algún incidente para luego mitigar la emergencia. SGSI permite prevenir y preparar a cada área para los imprevistos mencionados. Se agrega en el apéndice II una guía práctica para implementar la gestión de acceso a la información.

Esto es necesario cambiarlo ya que la cantidad de tiempo y recursos utilizados pueden llevar a retrasos y generar desconfianza hacia la misma compañía. La organización debe valorar que la prevención hace que la compañía sobresalga, genere oportunidades a nivel nacional y sobrepase los estándares y seguridad en el extranjero.

CONCLUSIONES

1. Implementar un sistema de gestión de acceso a la información no es tarea sencilla; sin embargo resulta necesario y beneficioso promulgar una serie de políticas que ayuden a reducir los posibles ataques o robos de información confidencial a intrusos que puedan lucrar con ello y utilizar de forma indebida.

2. Independientemente del sector que se está desarrollando, la empresa debe velar porque la información y sus empleados se encuentren seguros, manteniendo una constante capacitación e involucrándolos en dicha acción.

3. Existen muchos estándares de acceso a la información a implementar pero no necesariamente es obligatorio certificarse en alguno de ellos, lo importante es que la empresa utilice ciertas características de cada uno de ellos para establecer mayor seguridad al acceder a su información.

4. Las buenas prácticas que se utilicen en seguridad de la información serán recompensadas al final de la implementación, encaminándose a realizar una certificación en corto o mediano plazo.

5. La resistencia al cambio dentro de una compañía, puede entorpecer el proceso de aseguramiento de la información y la certificación, es prudente manejar las asperezas que pueden existir en cualquier área de trabajo y conocer cada una de ellas antes de comenzar el proyecto, es de suma importancia el involucramiento de la Alta Dirección de la empresa y el Departamento de TI manteniendo siempre alineados sus objetivos para lograr sinergia, entusiasmo y compromiso en todo el personal.

6. De acuerdo a la encuesta realizada en este estudio se observa un alto índice de personal de TI que conoce acerca de la seguridad de acceso a la información dentro de la compañía; sin embargo ésta se ve empobrecida debido a que existen incidentes intermedios que entorpecen las acciones como falta de comunicación con los altos mandos.

7. Los dispositivos de seguridad pueden contribuir a mejorarla cuando se utilizan los mecanismos correctamente. Las personas que se entrevistaron no poseen un acceso seguro debido a la jerarquización de permisos y documentación para la creación de los mismos, otro posible obstáculo son los dispositivos electrónicos que no siempre son los ideales.

RECOMENDACIONES

1. Se debe reclutar personal altamente calificado validando sus credenciales de trabajo antes de iniciar un proyecto de gestión de acceso a la información, esto permitirá contar con un respaldo y profesionalismo para la toma de decisiones, análisis de riesgo, criterios de solución y reducción en el tiempo de certificación de la compañía.

2. Implementar los estándares de seguridad en la gestión de acceso a la información guiándose por el documento *Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for business benefit*, el cual presenta un resumen completo para estudiar cada área y elegir el estándar que mejor se acople a las necesidades del negocio.

3. Para cumplir con el Gobierno TI, se sugiere a las empresas integrar, a mediano plazo la norma ISO 38000 que incluye cada uno de los estándares de certificación.

4. Fomentar el seguimiento e investigación iniciado en esta tesis, realizando un estudio más profundo desligado de cada estándar y revisando alternativas y políticas al respecto.

5. Es aconsejable mantener el sistema y no desestabilizarlo utilizando recursos poco confiables, ya que se corre el riesgo de sufrir vulnerabilidades de seguridad. Lo ideal es realizar las pruebas y test con el tiempo necesario para posteriormente trasladarlas al ambiente de producción e instalar los dispositivos correctos.

BIBLIOGRAFÍA

1. TORREGROSA, Aroa. *Introducción a la Gerencia de R.R.H.H. y glosario de términos*. España: Universidad Politécnica de Valencia, 2002. 20p.

2. IT Governance Institute & Office of Government Commerce, *Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for business benefit*. Estados Unidos: Crown, 2008. 130 p.

3. AGSA, *Auditoría de controles y gestión basados en un SGSI*. Guatemala: Agsa, 2010. 77p.

4. AGSA, *Estándares de clase mundial para la auditoría informática*. Guatemala: Agsa, 2010. 46 p.

5. *IT GOVERNANCE INSTITUTE*. *COBIT* 4.1 *versión español.* Estados Unidos. *IT Governance Institute,* 2007. 211 p.

6. GOBIERNO DE MENDOZA. *Objetivos de control para la información y tecnologías relacionadas resumen ejecutivo*. Argentina: Tipografía de Mendoza, 2004. 20 p.

7. *OFFICE OF GOVERMENT COMMERCE*. *ITIL*3 *Continual Service Improvement.* Inglaterra: The Stationery office, 2007. 233 p.

8. *OFFICE OF GOVERMENT COMMERCE*. *ITIL*3 *The official Introduction to the ITIL Service Lifecycle*. Inglaterra: The Stationery office, 2007. 252p.

9. *OFFICE OF GOVERMENT COMMERCE*. *ITIL3 service design*. Inglaterra: The Stationery office, 2007. 346 p.

10. *OFFICE OF GOVERMENT COMMERCE*. *ITIL*3 *service operation.* Inglaterra: The Stationery office, 2007. 276 p.

11. *OFFICE OF GOVERMENT COMMERCE*. *ITIL*3 *service strategy*. Inglaterra: The Stationery office, 2007. 276 p.

12. *OFFICE OF GOVERMENT COMMERCE*. *ITIL*3 *service transition*. Inglaterra: The Stationery office, 2007. 274 p.

13. PRICEWATERHOUSECOOPERS*. Findings from the 2011 Global State of Information Security Survey*. Estados Unidos: Pricewater-house-Coopers LLP. 2010. 58 p.

14. PRICEWATERHOUSECOOPERS. *The Global State Of Information Security 2007*. Estados Unidos: CXO Media, 2007. 11 p.

15. CANO, Jeimy J. *Seguridad informática en Colombia tendencias 2008*. Colombia: Segurinfo, 2008. 23 p.

16. *IBM X-FORCE*. 2010 *Mid-Year trend and risk report. IBM global business services*. Estados Unidos, IBM, 2010. 112 p.

17. *GLOBAL CHIEF EXECUTIVE OFFICER STUDY*. Liderar en la Complejidad. Estados Unidos: IBM Global Business Services, 2010. 8 p.

18. *GLOBAL CHIEF EXECUTIVE OFFICER STUDY*. El nuevo integrador de valor. Estados Unidos: IBM Global Business Services, 2010. 8 p.

19. ISO, Estándar internacional ISO/IEC 27001. Ginebra: Organización Internacional para Estandarización, 2005. 41 p.

20. RUIZ, Javier S., LÓPEZ Agustín N. ISO 27000. España: ISO27000.es, 2008. 19 p.

APÉNDICE I

Guía de consejos e ideas prácticas al inicio, en la implementación y el seguimiento en la gestión de acceso a la información

1. La mejora continua es el mejor aliado dentro de la empresa, contribuye a eliminar las no conformidades, permita buscar una solución adecuada, documenta cada uno de los pasos que necesite ser resueltos y que sirva de apoyo para mitigar acontecimientos a futuro.

2. Recopilar las sugerencias de empleados son valiosas, ellos mejor que cualquier persona conocen el sistema, fallas y vulnerabilidades. Cuando se realice la toma de requerimiento es útil el conocimiento que ellos han adquirido. Si en el departamento el especialista no está disponible, consulte información en internet, información a colegas que tengan la experiencia del mismo problema, un consultor experto, pero sobre todo consulte una segunda opinión antes de implementar cualquier solución o mejora.

3. Solicitar a los empleados medir los riesgos dentro del departamento podría resultar complejo, debido a que ellos viven sumergidos dentro del área y a veces es difícil localizar los puntos débiles, se aconseja pedir ayudar al equipo de *staff* para realizarlo en conjunto o tener a un agente externo que pueda cuestionar los riesgos que ocurran e identificarlos para dar la mejor solución.

APÉNDICE II

Guía para implementar la gestión del acceso a la información en PYMES

La información generada a partir de la gestión de acceso a la información permite llevar control adecuado durante la realización del proyecto completo, se presenta una guía que ayude a cada pequeña y mediana empresa a realizar de manera detallada al inicio, durante y al finalizar el proyecto.

Antes de iniciar el proyecto

1. Comunicar la gestión del acceso a la información.
2. Consultar los estándares y actualizaciones recientes.
3. Elaborar un listado de las instituciones que brindan certificación, consultoría y capacitación. Indagar compañías dentro de Guatemala o si existe presencia de ellas en el país.
4. Realizar análisis de la situación actual de la compañía, se debe validar el estándar adecuado a implementar y validar si existe una empresa de consultoría correcta.
5. Elaborar un análisis de factibilidad, evaluando los activos, recursos humanos y relaciones con los clientes.
6. Efectuar la reunión inicial con gerencia y plantear los lineamientos iniciales del proceso y el involucramiento de la compañía. Indicar las ventajas y beneficios que se obtendrán del proyecto.
7. Seleccionar el estándar que mejor se acople a las áreas de trabajo.

8. Realizar una reunión con la empresa que ayudará al proceso de certificación, además iniciar un plan estratégico integrando gerencia y las áreas que mayor relevancia tendrán.
9. La comunicación de todas las áreas es importante, sobre todo la participación e involucramiento de cada miembro y el beneficio que se obtendrá al finalizar el proyecto.

Durante el proyecto

1. Realizar un plan de trabajo inicial, donde se seleccionen las áreas involucradas.
2. Cumplir el plan detallado de las áreas a implementar la gestión y realizar una reunión con el equipo.
3. Documentar cada una de las tareas y listado de procedimientos que se realizan y validar con el estándar que se tenga seleccionado y que cumpla con los requisitos del mismo.
4. Las modificaciones necesarias deben ser implementadas y buscar la mejor solución, de forma interna o externa. Las personas ajenas a la compañía deben ser debidamente calificadas.
5. Llevar la bitácora de procesos, procedimientos, cambio de gestiones, actualizaciones de equipos y aplicaciones. Cada uno debe tener la fecha de la implementación, costo, tiempo invertido, personal involucrado.
6. Elaborar manuales, diagramas, cuadros de acuerdos de niveles de seguridad, flujos, boletines informativos, comunicación en general, para que cada uno de los involucrados esté pendiente de cada una de las
7. Las sugerencias y mejoras que desee proponer el departamento o miembro del equipo deben ser bien vistas y se deben evaluar antes de poner en marcha la solución.

8. Reuniones de seguimiento detallando el avance del proyecto a gerencia y comunicando cualquier atraso o adelanto del mismo resulta productivo. La comunicación debe ser obligatoria notificarla a la compañía.
9. Obtener pruebas constantes o validar los resultados antes de iniciar la migración de información hacia el repositorio destino.

Finalizando cada fase o el proyecto

1. Al finalizar cada área deberá de asegurarse de cumplir cada uno de los puntos que pide el estándar, si tiene alguna duda comuníquese al agente certificador y pídale el asesoramiento adecuado.
2. Monitorear que cada procedimiento o proceso se cumpla.
3. Monitorear los equipos o aplicaciones instaladas dentro de la gestión del acceso a la información.
4. Supervisar que la sinergia del equipo, verificando que las mejoras dentro del área se conserven.
5. Inspeccionar que los colaboradores y departamentos conozcan la importancia de las modificaciones y nuevos procedimientos.
6. Celebrar que el proyecto o fase se ha finalizado con éxito, esto no solamente permite dar a conocer el esfuerzo del equipo sino que ayuda a crear mayor confianza en el proyecto y una imagen positiva hacia los departamentos que están a punto de iniciar el cambio hacia la certificación.

La empresa debe seleccionar el estándar que mejor se acople y las necesidades que esta desee, tener en cuenta el costo, tiempo y recursos disponibles.

Si la decisión es solamente validar puntos débiles de la compañía y agregar una gestión de acceso a la información, deberá de tomar seriamente cuando implemente las reglas y políticas de un estándar, ya que los lineamientos deben quedar claros y completamente válidos si decide en un mediano plazo continuar la certificación, esto le ahorrará tiempo en llegar cumplir el estándar.

La capacitación y lectura de nuevos documentos sobre los estándares es constante, no puede decidir implementar un estándar sin llegar a actualizar o llevar un monitoreo de la operación dentro de las áreas por un largo tiempo. Es responsabilidad del equipo validar, actualizarse y verificar nuevas formas de controlar la gestión de acceso a la información.

Por último y como se ha recalcado durante todo el proyecto, la comunicación que se tenga con el equipo *staff*, entes certificadores, alta gerencia y clientes pueden lograr hacer de este proyecto un fracaso o un rotundo éxito, depende mucho de éste eslabón que permita y se encamine hacia la ruta seleccionada.

ANEXO I

Seguridad de acceso a la información dentro de su compañía

Encuesta: por favor responda con la escala de 1-5, califique cada una de las preguntas, donde (*) es requerida.

¿Ha escuchado acerca de la seguridad de acceso a la Información dentro de su empresa? *

La seguridad es a nivel general y no solamente dentro de IT

- Por supuesto
- No mucho
- Más o menos
- Casi nunca
- No aplica / nunca

¿Existen procedimientos o documentación al momento que los usuarios se les otorgan permisos en las aplicaciones o accesos dentro de su compañía en RRHH e *IT*? *

Al momento de existir una contratación o cambio de puesto

- Numerosos
- No muchos
- Más o menos
- Pocos

- No aplica / nunca

¿Se manejan jerarquías de privilegios en las herramientas para cada empleado dentro de la compañía? *

Los permisos a cada aplicación o área son diferentes para cada usuario

- Si
- No muchos
- Más o menos
- Pocos
- No aplica / nunca

¿Qué tan frecuente usted cambia la contraseña de sus sistemas, accesos, correo electrónico entre otros? *

La clave de sistemas o acceso a áreas restringidas, bóvedas si las hubiera

- Siempre
- De vez en cuando
- Pocas veces
- Casi nunca
- No aplica / nunca

¿Existe una línea de comunicación abierta con la Gerencia y cada departamento para cambio de procedimientos dentro de la empresa? *

Existe la disponibilidad por ambas partes por escuchar las propuestas o mejoras

- Siempre
- de vez en cuando
- pocas veces
- casi nunca
- No aplica / nunca

¿Existen comunicados o notificaciones dentro de la compañía sobre cambios realizados en las políticas de acceso a la información dentro de la empresa? *

Por medio de correos electrónicos, memos, carteleras entre otros

- Siempre
- de vez en cuando
- pocas veces
- casi nunca
- No aplica / nunca

¿Han existido emergencias físicas o virtuales dentro de la compañía que han tenido como consecuencia perdida de información? *

Incendios, virus, intrusos, robos, accidentes ambientales

- Siempre
- de vez en cuando
- pocas veces
- casi nunca
- No aplica / nunca

¿Si han existido, se han corregido las faltas y han sido comunicadas al personal? *

Por medio de avisos, mejora de seguridad, precauciones, métodos de mitigación

- Siempre
- de vez en cuando
- pocas veces
- casi nunca
- No aplica / nunca

¿Cómo calificaría la seguridad a nivel general dentro de su compañía? *

Seguridad a nivel general y no solamente a nivel IT

- Excelente
- muy buena
- intermedia
- no muy buena
- pésima

¿La resistencia al cambio dentro de la compañía es? *

Los empleados normalmente no se acostumbran a nuevos procedimientos

- Existe demasiada
- No mucha
- Pocas veces
- Casi nunca
- No aplica / nunca

¿Dentro de la compañía, sabe usted de alguna propuesta de certificación o si ya está certificada bajo alguna política de seguridad? *

Las certificaciones como ISO 27000, COBIT, ITIL o alguna otra creada por la misma empresa

- Si
- He escuchado algo
- No aplica / nunca

¿Puede acceder a las herramientas de trabajo que utiliza en la empresa de forma remota o desde su casa? *

Trabajo en diferentes ciudades, home office, ingreso directo en las oficinas de los clientes

- Totalmente

- De vez en cuando
- Pocas veces
- Casi nunca
- No aplica / nunca

Marque dispositivos utilizan dentro y fuera de la compañía: *

- Computador de escritorio
- Laptop
- Webcam
- Teléfono
- PDA
- Voip – voz sobre IP
- Internet
- Fax
- Escáner
- Impresora
- Código de acceso manual o tarjeta Inteligente
- Código de voz
- Detector de huella digital
- Detector de iris
- Detector facial

La empresa se dedica a: *

Por favor si es más de una, indique las opciones

- Banca
- Tecnología
- Servicios
- Producción

- Salud
- Maquinaria y equipo
- Importaciones / exportaciones
- Agrícola
- Turismo
- Medio ambiente
- Gubernamental
- Otros

ANEXO II

Acrónimos dentro del documento que puede ayudarle a enriquecer el significado del documento.

- A - Control de acceso ISO
- PO- Planear y Organizar *COBIT*
- DS - Entregar y Dar Soporte *COBIT*
- SD - Diseño de Servicio *ITIL*
- SO - Operación de Servicio *ITIL*
- *RFC ITIL* – Petición para el cambio, en inglés *request for change*
- SLA - Service Level Agreement