UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

PROPUESTA DE METODOLOGÍA DE EVALUACIÓN DE SEGURIDAD INFORMÁTICA, APLICADA A PROVEEDORES DE SERVICIOS DE PEQUEÑAS Y MEDIANAS EMPRESAS (PYME), QUE ACCEDAN A INFORMACIÓN DE PERSONAS FÍSICAS EN EL MUNICIPIO DE TOLUCA, ESTADO DE MÉXICO.

TRABAJO TERMINAL DE GRADO

QUE PARA OBTENER EL GRADO DE

MAESTRO EN ALTA DIRECCIÓN EN SISTEMAS DE INFORMACIÓN

(Administración de Proyectos)

PRESENTA

DANIEL DAVID PÁEZ GONZÁLEZ

DRA. EN C. ED. ARACELI ROMERO ROMERO
TUTOR ACADÉMICO

MARZO, 2017

Agradecimientos.

A mis padres, personas excepcionales que con su ejemplo de fortaleza y perseverancia me han enseñado a luchar por lo que quiero, que con todo su amor y esfuerzo han formado a la persona que soy y que, sin su apoyo incondicional, no hubiera sido posible la culminación de este trabajo, gracias por todo, con su cariño ha sido mucho más fácil.

A mi tutora la Dra. en C de Ed. Araceli Romero Romero por su colaboración en cada momento de consulta y soporte en este trabajo de investigación.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

CAPITULO I

MARCO TEÓRICO CONCEPTUAL

1 Introducción a la Seguridad Informática.

Desde el surgimiento de la raza humana en el planeta, la información estuvo presente bajo diversas formas y técnicas. El hombre buscaba representar sus hábitos, costumbres e intenciones en diversos medios que pudiesen ser utilizados por él y por otras personas, además de la posibilidad de ser llevados de un lugar a otro. La información valiosa era registrada en objetos preciosos y sofisticados, pinturas magníficas, entre otros, que se almacenaban con mucho cuidado en locales de difícil acceso, a cuya forma y contenido sólo tenían acceso quienes estuvieran autorizados o listos para interpretarla.

En la actualidad la información es considerada uno de los objetos de mayor valor para las empresas. El progreso de la informática y de las redes de comunicación presentan un nuevo escenario, donde los objetos del mundo real están representados por bits y bytes, que ocupan lugar en otra dimensión y poseen formas diferentes de las originales, no dejando de tener el mismo valor que sus objetos reales y en muchos casos, llegando a tener un valor superior (Academia Latinoamericana de Seguridad Informática, 2003).

Por esto y otros motivos, la seguridad de la información es un asunto tan importante para todos, ya que afecta directamente a los negocios de una empresa o de un individuo.

La seguridad de la información tiene como propósito proteger la información registrada, independientemente del lugar en que se localice: impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que la conocen.

Una de las preocupaciones de la seguridad de la información es proteger los elementos que forman parte de la comunicación. En la siguiente figura (Figura 1.1.) se identifican los elementos que la seguridad de la información busca proteger:

- La información.
- Los equipos que la soportan.
- Las personas que la utilizan.

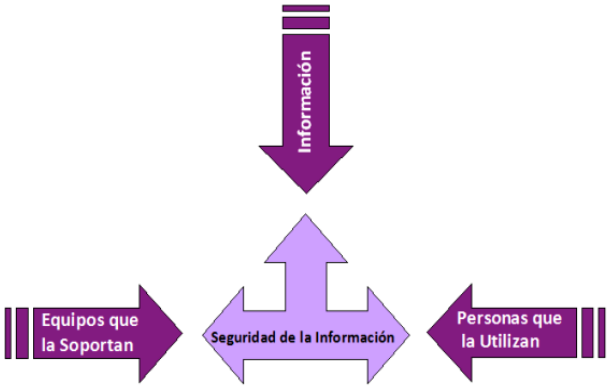


Figura 1.1 Elementos de la Seguridad de la Información (Academia Latinoamericana de Seguridad Informática, 2009)

1.1 Conceptos Básicos.

La Seguridad de la información. - es el conjunto de estándares, procesos, procedimientos, estrategias, recursos informáticos, recursos educativos y recursos humanos integrados para proveer toda la protección debida y requerida a la información y a los recursos informáticos de

una empresa, institución o agencia gubernamental (Escuela Colombiana de Ingeniería Julio Garabito, 2008).

Seguridad informática. - se entiende como el conjunto de procedimientos, estrategias y herramientas que permiten garantizar la integridad, la disponibilidad y la confidencialidad de la información de una entidad. Es el estado de cualquier sistema (informático o no) que indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo (Universidad Nacional del Nordeste Argentina U.N.N.E, 2001).

La seguridad de la información es la protección de información de una gama amplia de amenazas para asegurar la continuidad comercial, minimizar el riesgo comercial, y aumentar al máximo el retorno en las inversiones y las oportunidades de negocios, se logra implementando un conjunto conveniente de controles, incluyendo, políticas, procesos, procedimientos y funciones del hardware y software. Estos controles deben ser establecidos, implementados, supervisados, revisados y mejorados, en conjunto con los procesos de negocio para asegurar la seguridad específica y los objetivos de la organización (Escuela Colombiana de Ingeniería Julio Garabito, 2008).

Una vez que se conoce el concepto de Seguridad de la Información, se profundizará en los principios básicos que ayudarán a proteger el activo de más valor en los negocios modernos: la información, representados en la figura (Figura 1.2.).

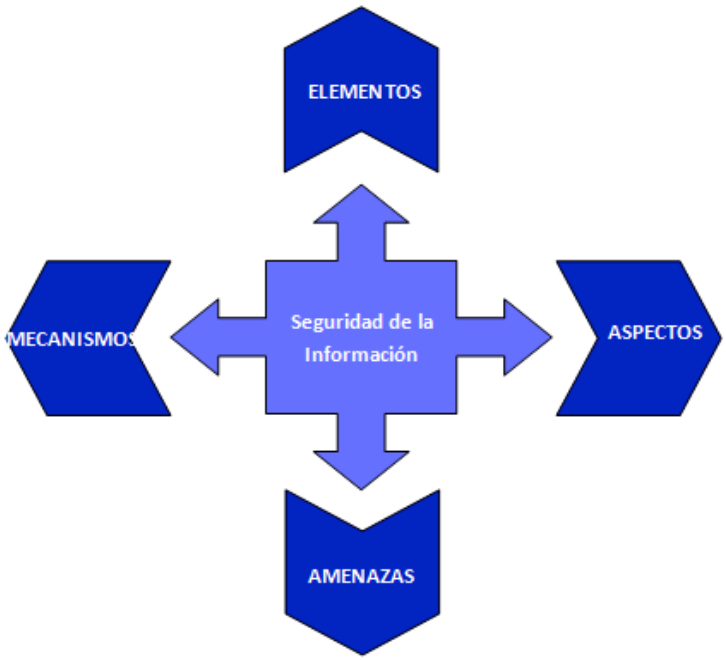


Figura 1.2 Principios Básicos

1.2 Aspectos de la Seguridad Informática.

Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener cuatro características (Empresa Oficial de Servicios Públicos de Yumbo Colombia, 2010):

Integridad: La información sólo puede ser modificada por quien está autorizado. Es necesario asegurar que los datos no sufran cambios no autorizados, la pérdida de integridad puede acabar en fraudes, decisiones erróneas o como paso a otros ataques. El sistema contiene información que debe ser protegida de modificaciones imprevistas, no autorizadas o accidentales, como información de censo o sistemas de transacciones financieras.

Confidencialidad: La información sólo debe ser legible para los autorizados. Se refiere a la protección de datos frente a la difusión no autorizada, la pérdida de confidencialidad puede resultar en problemas legales, pérdida del negocio o de credibilidad. El sistema contiene información que necesita protección contra la divulgación no autorizada, como información parcial de informes, información personal o información comercial patentada.

Disponibilidad: Debe estar disponible cuando se necesita. Se refiere a la continuidad operativa de la entidad, la pérdida de disponibilidad puede implicar, la pérdida de productividad o de credibilidad de la entidad. El sistema contiene información o proporciona servicios que deben estar disponibles a tiempo para satisfacer requisitos o evitar pérdidas importantes, como sistemas esenciales de seguridad y protección de la vida.

Irrefutabilidad: (No-Rechazo o No Repudio) Que no se pueda negar la autoría.

1.3 Elementos de la Seguridad Informática.

Un activo es todo aquel elemento que compone el proceso de la comunicación, partiendo desde la información, su emisor, el medio por el cual se transmite, hasta su receptor (Poder Judicial Republica de Honduras, 2003).

Los activos son elementos que la seguridad de la información busca proteger. Los activos poseen valor para las empresas y como consecuencia de ello, necesitan recibir una protección adecuada para que sus negocios no sean perjudicados.

Son tres elementos que conforman lo que se denominan activos:

- Información: En este grupo están los elementos que contienen información registrada, en medio electrónico o físico, dentro de los más importantes tenemos: documentos, informes, manuales, información de mercado, código de programación, reportes financieros, planillas de sueldos de empleados, plan de negocios de una empresa, etc.

- Equipos que la soportan: Entendemos como equipos que soportan la información, cualquier componente disponible para, sustentar, almacenar y procesar información sustancial para los procesos de negocio de una entidad o procesos de negocio.

- Software: Este grupo de activos contiene todos los programas de computadora que se utilizan para la automatización de procesos, es decir, acceso, lectura, tránsito y almacenamiento de la información. Entre ellos se citan: las aplicaciones comerciales, programas institucionales, sistemas operativos, etc.

La seguridad de la información busca evaluar la forma en que se desarrollan las aplicaciones y la forma de cómo son utilizadas por los usuarios y por otros sistemas, para detectar y corregir problemas existentes en la comunicación entre ellos.

Las aplicaciones deberán estar protegidas para que la comunicación entre las bases de datos, otras aplicaciones y los usuarios se realice de forma segura, atendiendo a los principios básicos de la seguridad de la información (Integridad, Confidencialidad, Disponibilidad e Irrefutabilidad).

- Hardware: Estos activos representan toda la infraestructura tecnológica que brinda soporte a la información durante su uso, tránsito y almacenamiento. Los activos que pertenecen a este grupo son: cualquier equipo en el cual se almacene, procese o transmita la información de la empresa; computadoras, servidores, mainframes, medios de almacenamiento, equipos de conectividad (enrutadores, switches) y cualquier otro elemento de una red de computadoras por donde transita la información.

- Organización: En este grupo se incluyen los aspectos que componen la estructura física (ubicación física de los servidores y armarios donde están localizados los documentos) y organizativa (estructura departamental y funcional) de las empresas.

- Usuarios: El grupo usuarios se refiere a los individuos que utilizan la estructura tecnológica y de comunicación de la empresa y que manejan la información.

El enfoque de la seguridad en los usuarios, está orientado hacia la toma de conciencia de formación del hábito de la seguridad por parte de todos los empleados de una empresa.

1.4 Amenazas de la Seguridad Informática.

1.4.1 Tipos

Los elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Contra cualquiera de los elementos mencionados anteriormente (pero principalmente sobre los datos) se puede realizar una multitud de ataques o, dicho de otra forma,

están expuestos a diferentes amenazas. Generalmente, la taxonomía más elemental de estas amenazas las divide en cuatro grandes grupos, como se muestra en la siguiente figura (Figura 1.3.) (Universidad de las Américas Puebla, 2000):

Interrupción. - Si se hace que un objeto del sistema se pierda, quede inutilizable o no disponible.

Interceptación. - Si un elemento no autorizado consigue un acceso a un determinado objeto del sistema.

Modificación. - Si además de conseguir el acceso consigue modificar el objeto.

Destrucción. - Modificación que inutiliza el objeto afectado.

Fabricación. - Se trata de una modificación destinada a conseguir un objeto similar al atacado de manera que sea difícil distinguir entre el objeto original y el "fabricado".

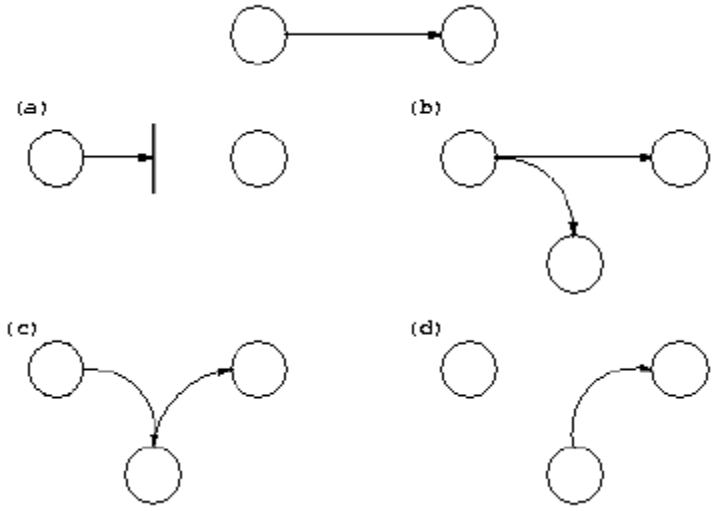


Figura 1.3 Flujo normal de información entre emisor y receptor y posibles amenazas a) interrupción, b) interceptación, c) modificación y d) fabricación

1.4.1.1 Amenazas Lógicas

Entendemos como amenazas lógicas, todo tipo de programas que de una forma u otra pueden dañar un sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros) (Simson Garfinkel and Eugene H. Spafford, 1996).

Los protocolos de comunicación utilizados en la actualidad carecen (en su mayoría) de seguridad o esta ha sido implementada en forma de "parche" tiempo después de su creación (Seguridad de la Información Segu-Info, 2005).

- Existen agujeros de seguridad en los sistemas operativos.
- Existen agujeros de seguridad en las aplicaciones.
- Existen errores en las configuraciones de los sistemas.
- Los usuarios carecen de información respecto al tema.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un Sistema Informático.

1.4.1.2 Acceso - Uso - Autorización

Podemos considerar acceso no autorizado cuando una persona que no tiene permiso para acceder o utilizar un sistema, entra de manera no autorizada o deseada.

Específicamente "Acceso" y "Hacer Uso" no son el mismo concepto cuando se estudian desde el punto de vista de un usuario y de un intruso. Por ejemplo:

-Cuando un usuario tiene acceso autorizado, implica que tiene autorizado el uso de un recurso.

-Cuando un atacante tiene acceso desautorizado está haciendo uso desautorizado del sistema.

-Pero, cuando un atacante hace uso desautorizado de un sistema, esto implica que el acceso fue autorizado (simulación de usuario). Luego un Ataque será un intento de acceso, o uso desautorizado de un recurso, sea satisfactorio o no. Un Incidente envuelve un conjunto de ataques que pueden ser distinguidos de otro grupo por las características del mismo (grado, similitud, técnicas utilizadas, tiempos, etc.).

John D. Howard [9] en su tesis estudia la cantidad de ataques que puede tener un incidente. Al concluir dicho estudio y basado en su experiencia en los laboratorios del CERT afirma que esta cantidad varía entre 10 y 1.000 y estima que un número razonable para estudios es de 100 ataques por incidentes.

1.4.1.3 Detección de Intrusos

La detección de intrusiones es un tipo de sistema de gestión de la seguridad para las computadoras y redes. Un sistema de identificación se reúne y analiza la información de diferentes áreas dentro de une quipo o una red para identificar posibles violaciones de seguridad, que incluye las intrusiones (ataques desde fuera de la organización) y el mal uso (ataques desde dentro de la organización), es una tecnología desarrollada para evaluar la seguridad de un sistema informático o red.

A finales de 1996, Dan Farmer (creador de una de las herramientas más útiles en la detección de intrusos: SATAN) realizó un estudio sobre seguridad analizando 2.203 sistemas de sitios en Internet. Los sistemas objeto del estudio fueron Web Sites orientados al comercio y con contenidos específicos, además de un conjunto de sistemas informáticos aleatorios con los que realizar comparaciones.

1.4.2 Identificación

La identificación de amenazas requiere conocer los tipos de ataques, el tipo de acceso, la forma operacional y los objetivos del atacante.

Las consecuencias de los ataques se podrían clasificar en:

-Data Corruption: la información que no contenía defectos pasa a tenerlos.

-Denial of Service (DoS): servicios que deberían estar disponibles no lo están.

-Leakage: los datos llegan a destinos a los que no deberían llegar.

Una vez conocidos los riesgos, los recursos que se deben proteger y como su daño o falta pueden influir en la organización es necesario identificar cada una de las amenazas y vulnerabilidades que pueden causar estas bajas en los recursos. Se suele dividir las amenazas existentes según su ámbito de acción:

-Desastre del entorno (Seguridad Física).

-Amenazas del sistema (Seguridad Lógica).

-Amenazas en la red (Comunicaciones).

-Amenazas de personas (Insiders-Outsiders).

Se debería disponer de una lista de amenazas (actualizadas) para ayudar a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar. Es importante que los Administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan de forma continua.

1.4.3 Origen

Aunque todas las amenazas tienen la característica de ser las posibles causantes de destrucción a los sistemas, las amenazas pueden tener diferentes orígenes. Existen varias categorías de amenazas, para esta investigación se clasificarán por su origen, las cuales son: amenazas humanas, amenazas lógicas y desastres naturales (David Luis de la Red Martínez 2001).

- Amenazas Humanas

Existen diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas. Generalmente se dividen en dos grandes grupos: los atacantes pasivos, aquellos que acceden al sistema, pero no lo modifican o destruyen y los activos, aquellos que dañan o modifican el objetivo a su favor.

Atacantes Pasivos.

Personal- Aunque los ataques pueden ser intencionados lo normal es que más que de ataques se trate de accidentes causados por un error o por desconocimiento de las normas básicas de seguridad.

Atacantes Activos.

Ex-empleados- Personas descontentas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente para dañarlo como venganza por algún hecho que no consideran justo.

Terroristas- Cualquier persona que ataca al sistema simplemente por causar algún tipo de daño en él.

Intrusos Remunerados- Personas con gran experiencia en seguridad y un amplio conocimiento del sistema, que son pagados para robar secretos o simplemente para dañar la imagen de la entidad afectada.

- Amenazas Lógicas

Todo tipo de programas que de una forma u otra puedan dañar a los sistemas, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros).

- Desastres Naturales

Las catástrofes (naturales o artificiales) son la amenaza menos probable contra los entornos habituales: terremotos, inundaciones, incendios, humo o atentados de baja magnitud.

1.5 Mecanismos de Seguridad Informática.

Los mecanismos de la Seguridad Informática son técnicas o herramientas que se utilizan para fortalecer los principios básicos de la seguridad de la información ya antes mencionados, y según su función se clasifican en (Universidad de las Américas Puebla, 2000):

- Preventivos

Los mecanismos de prevención son un conjunto de pasos predefinidos que deben seguirse para evitar ataques antes de que ocurran. Entre estos pasos se incluye observar cómo podrían afectar o dañar el sistema, y los puntos vulnerables. Los pasos para seguir un mecanismo de prevención son:

-Determinar el daño que causará el ataque: Los daños pueden oscilar entre pequeños fallos del equipo y la pérdida de los datos.

-Establecer los puntos vulnerables y debilidades que explotará el ataque: La determinación del tipo de ataque, amenaza y método facilita el descubrimiento de los puntos vulnerables existentes.

-Reducir los puntos vulnerables y las debilidades que se han determinado: La reducción de los puntos vulnerables y las debilidades, es el primer paso para desarrollar directivas y controles de seguridad eficaces.

- Detectivos

Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema, se caracterizan por enviar un aviso y registrar la incidencia.

- Recuperación

Se implementa cuando ha fallado el mecanismo de prevención y define los pasos que deben adoptarse después o durante un ataque, ayuda a identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, a determinar pro que tuvo lugar, a reparar el daño que causo y a implementar un plan de contingencia si existe. Tanto la estrategia de Prevención como la de Recuperación funcionan para desarrollar directivas y controles de seguridad con el fin de reducir los ataques y el daño que pudieran ser causados.

2 Importancia de la Seguridad Informática.

La seguridad hoy en día es uno de los principales problemas encontrados en el área informática, cuando se habla de seguridad por lo general se piensa en un término de privacidad de la información en el cual se pueden incluir aspectos tales como: contraseñas, accesos a la información, mensajes cifrados y, en definitiva, todo lo relacionado con la protección y confiabilidad de los datos.

2.1 Funciones de la Seguridad informática

Las funciones de la seguridad informática tienen mucho que ver con "donde se emplean". Dentro de las funciones que se refieren a la seguridad informática se consideran (Omar Alejandro Herrera Reyna, 2007):

Función centralizada. - La función centralizada permite un mejor control y desempeño de las funciones de seguridad informática, sin embargo, este esquema también suele generar algunos roces con otras áreas de la empresa particularmente con el área de Sistemas.

Función Distribuida. - Para algunas organizaciones hace más sentido distribuir la función de la seguridad ya que esto permite tener un mejor desempeño operativo a costa de menor control y desempeño en la seguridad informática.

La información es un recurso o activo que, como otros recursos importantes del negocio, es esencial en una organización y en su operación, por consiguiente, necesita ser protegida adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta interconectividad creciente, la información se expone a una variedad más amplia de amenazas y vulnerabilidades.

A continuación, se listan algunas de las actividades consideradas dentro de las funciones de la seguridad informática:

-Planear y establecer estrategias de seguridad informática de acuerdo a lineamientos principios y necesidades institucionales.

-Contar con un sistema de información estadístico para dar seguimiento a los proyectos y planes de acción con el fin de garantizar dentro de la institución su implantación control y seguimiento.

-Definir, elaborar, liberar, difundir y actualizar políticas y normas de seguridad informática que permitan a las áreas de la organización implantar y fortalecer mecanismos de protección de la información.

-Realizar campañas de capacitación, Difusión y concientización que eleven el nivel de recepción, entendimiento y conocimiento del personal en general sobre la materia.

-Realizar diagnósticos y evaluaciones de seguridad informática para identificar y minimizar los riesgos en los diferentes niveles funcionales, operativos y de sistema.

-Mantener la actualización sobre los avances tecnológicos en este campo, con el fin fortalecer esquemas de protección en la organización.

2.2 ¿Por qué se necesita la seguridad de la información?

La información y los procesos de apoyo, sistemas, y redes son uno de los recursos más importantes del negocio. Definir, lograr, mantener y mejorar la seguridad de la información es esencial para lograr el cumplimiento legal y sostenimiento de la imagen comercial. Las organizaciones y sus sistemas de información y redes enfrentan amenazas de seguridad de un amplio rango de fuentes, incluyendo fraude, espionaje, sabotaje y vandalismo.

Las causas de daño como el código malicioso, acceso no autorizado a la infraestructura o servidores y ataques de negación del servicio han llegado a ser más comunes, más ambiciosos y más sofisticados (ASS. Borguello Cristian Fabián, 2001).

La seguridad de la información y la infraestructura crítica del negocio es importante para ambos sectores público y de negocios del sector privado. En ambos sectores, la seguridad de la información funciona como un detonador para lograr el e-government o el e-business y evitar o reducir los riesgos pertinentes. La interconexión de las redes públicas y privadas y el compartir

recursos de información aumentan la dificultad de lograr el control de acceso. La tendencia a la informática distribuida también ha debilitado la efectividad del control central, especializado.

La seguridad que puede lograrse a través de los medios técnicos es limitada y debe apoyarse por una gestión apropiada y por los procedimientos. Identificando qué controles deben ser implementados, requiere planificación cuidadosa y atención al detalle. La gestión de la seguridad de la información requiere como mínimo la participación de todos los empleados de la organización, la participación de los accionistas, proveedores, clientes o terceras partes externas, la asesoría y consejo de especialistas en la materia también puede necesitarse.

2.3 ¿Cómo establecer los requerimientos de seguridad?

Es esencial que una organización identifique sus requerimientos de seguridad. Existen tres fuentes principales de los requerimientos de seguridad.

1. Evaluar los Riesgos de la Organización, mientras se tienen en cuenta la estrategia de negocio global de la organización y sus objetivos. A través de una valoración de riesgo, se identifican amenazas a los recursos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se estima el impacto potencial.

2. Requerimientos legales, estatutarios, reguladores y contractuales que la organización, sus socios comerciales, contratistas, y proveedores de servicios tienen que satisfacer y el ambiente socio-cultural.

3. Conjunto particular de principios, objetivos y requerimientos comerciales para la información que se procesa que una organización ha desarrollado para apoyar sus funcionamientos.

2.4 Evaluando los riesgos de seguridad Informática

Los requerimientos de seguridad son identificados mediante una valoración metódica de riesgos de seguridad, esta valoración sirve como ayuda para guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información. La valoración del riesgo debe repetirse periódicamente para estar atentos a cualquier cambio que pudiera influir en los resultados de la valoración. El gasto en los controles se necesita probablemente equilibrar contra el daño comercial que puedan ser resultado de las fallas de seguridad.

2.5 Punto de partida de seguridad de la información

Varios controles pueden ser considerados como un buen punto de partida para llevar a cabo la protección de la información. Los controles están basados en los requerimientos esenciales de tipo legislativo o se consideran ser una práctica común para la seguridad de la información (Jorge Mieres, 2009).

Los controles considerados esenciales a una organización desde un punto de vista legislativo incluyen, (dependiendo de la legislación aplicable):

a) Protección de los datos e información personal

b) Protección de archivos de la organización

c) Derechos de la propiedad intelectual

Controles considerados como práctica común para la seguridad de la información forman parte de los siguientes tópicos: Políticas de Seguridad y Organización, Seguridad de Personal, Seguridad Física, Seguridad de Medios de Comunicación y Eliminación de la Información, Administración del Sistema, Contingencia y Recuperación, Seguridad de Plataformas, Seguridad de Aplicaciones, Seguridad en la Red y Cumplimiento Legal y Regulatorio.

MARCO TEÓRICO METODOLÓGICO

3 Uso de Datos Personales

3.1 Antecedentes y Necesidades de Compartir información con Subcontratados.

Las empresas han evolucionado de la "autosuficiencia" a la "especialización" y, como consecuencia de ello, a la "subcontratación" por terceros de muchos de los productos, procesos o servicios que realizaban internamente (Nazario García Fernández, Alberto Gómez Gómez, Isabel Fernández Quesada, José Parreño Fernández, 2002).

La subcontratación se debe concebir como una responsabilidad compartida por el cliente y los proveedores de servicios. El esquema de subcontratación implica una relación a largo plazo entre cliente y proveedor: es un compromiso del cual surge una alianza estratégica en la que el cliente acepta el ofrecer al proveedor información clave y estratégica de su negocio para que el

proveedor pueda hacer su trabajo. A cambio el proveedor aportará recursos, tecnología, tiempo, personal y esfuerzo para integrarse de manera total al proceso de su cliente y para que, de esta manera puedan crecer juntos (Corporación Universitaria Remington, 2006).

Actualmente es muy común que se efectúen intercambios de información con proveedores de servicios que intervienen de manera diaria en la operación de las empresas, esto constituye un riesgo importante en la información, debido a que son muy pocas las empresas que aseguran que los subcontratados cuenten con los controles de seguridad adecuados y suficientes que garanticen la protección de la información de sus clientes, empleados o de la propia operación (procesos), a través, de revisiones de seguridad y auditorias, comúnmente las empresas que hacen uso de terceros solo se respaldan con un acuerdo de confidencialidad, sin tener certeza de que su información será utilizada de manera adecuada y para los fines convenidos dentro de los contratos de servicio.

3.2 Ley Federal de Protección de Datos Personales en Posesión de Particulares

En un mundo con gran despliegue tecnológico y donde la economía gira en torno a la información es de extrema importancia contar con una legislación que proteja los datos personales. En México es una necesidad clara y como prueba, desde 2001 se han presentado siete iniciativas que van desde las muy conservadoras hasta las muy liberales.

Las noticias recientes han presentado incidentes sobre el robo y tráfico de datos en México que demuestran las vulnerabilidades de los sistemas y el riesgo que representan para cualquier individuo u organización (Deloitte, 2011).

Los riesgos tecnológicos son un asunto de todos los días para los ejecutivos de las organizaciones. No es exagerado decir que las amenazas a la confidencialidad son un tema que cada día preocupa más, debido a que los riesgos se multiplican conforme avanza la tecnología.

Por esta razón, el 5 de julio de 2010 se publicó en el Diario Oficial de la Federación (DOF) la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDP), la cual tiene como objetivo proteger los datos personales en posesión de los particulares y regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de los individuos.

Bajo este contexto, la Ley mencionada anteriormente entró en vigor al día siguiente de su publicación en el DOF y las empresas cuentan con un plazo de 18 meses para implementar políticas y procedimientos, así como los mecanismos necesarios en recursos humanos, legal, tecnología, procesos e infraestructura para cumplir con dicha Ley. El Ejecutivo Federal expedirá el reglamento respectivo en el año siguiente a su entrada en vigor. En ese mismo periodo los responsables designarán a la persona o el departamento de datos personales a que se refiere el Artículo 30 de la Ley y expedirán sus avisos de privacidad a los titulares de esa información.

Las sanciones por faltas a la LFPDP van desde sanciones económicas (altas) hasta la privación de la libertad.

El Instituto Federal de Acceso a la Información y Protección de Datos Personales (IFAI PDP) es el encargado de promover y difundir el ejercicio del derecho a la información, resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de dependencias y entidades.

Lo anterior permite cuestionar: ¿qué capacidad tienen las compañías para hacerle frente a estos riesgos?, ¿existen controles robustos dentro de estas instituciones para la protección de datos en su confidencialidad, integridad y disponibilidad? Actualmente, ¿los procesos para el tratamiento de los datos de las empresas mexicanas cumplen con la LFPDP?

3.2.1 Objetivos y Alcances de la LFPDPPP.

-La finalidad de la LFPDPPP es proteger los datos personales en posesión de los particulares, al regular y controlar su tratamiento legítimo para garantizar la privacidad y el derecho a la autodeterminación informativa de las personas (Ernest & Young, 2011).

-A esta regulación están sujetos todos aquellos particulares –personas físicas o morales de carácter privado– que lleven a cabo la recolección y el tratamiento de datos personales.

-No están sujetos a esta ley las sociedades de información crediticia y personas que realicen recolección de datos personales para fines de uso personal y sin fines de divulgación o utilización comercial.

-La LFPDPPP se alinea a los compromisos internacionales adquiridos por México, así como a las directrices sobre la protección de la privacidad y flujo transfronterizo de datos de la Organización para la Cooperación y Desarrollo Económico (OCDE).

-Abarca las consideraciones de los Estándares Internacionales sobre Protección de Datos y Privacidad (Resolución de Madrid), al contemplar los principios rectores de la protección de

datos personales: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, mismos que deberán ser observados por los responsables del tratamiento de datos personales.

-Enfatiza el tema de los datos personales sensibles –aquellos que afecten a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste - al imponer reglas especiales para su tratamiento, así como sanciones más elevadas en caso de su incumplimiento o violación.

3.2.2 Obligaciones de los actores de la LFPDPPP.

-Toda información personal que se recabe estará sujeta al consentimiento de su titular, salvo ciertas excepciones, como los casos previstos por ley donde se tenga el propósito de cumplir obligaciones entre el titular y el responsable o en situaciones de emergencia, debiendo otorgarse el consentimiento en ciertos supuestos, de manera expresa e incluso por escrito en caso de datos sensibles, permitiéndose para ello el uso de los medios electrónicos, ópticos o de cualquier otra tecnología que permita su autenticación.

-Se introduce la obligación de informar y limitar el tratamiento de datos personales a las finalidades previstas en el aviso de privacidad que deberá darse a conocer por quien recabe la información.

-En el aviso de privacidad se deberán establecer los mecanismos y procedimientos para que el titular revoque su consentimiento y ejerza sus derechos en cualquier momento y de manera

gratuita para Acceder, Rectificar, Cancelar u Oponerse al uso de sus datos personales (estos derechos son conocidos por su acrónimo ARCO).

-Toda persona (salvo por las excepciones especificadas anteriormente) que efectúe el tratamiento de datos personales deberá adoptar medidas de carácter jurídico, operativo y tecnológico, ya que este ordenamiento dispone que los datos deberán mantenerse correctos y actualizados, cancelándose y eliminándose cuando hayan dejado de ser necesarios.

-A más tardar el 5 de julio de 2011, todos aquellos que recaben datos personales deben designar a una persona o departamento como responsable exclusivo del tratamiento de los mismos y de atender los requerimientos del titular en el ejercicio de sus derechos ARCO.

3.2.3 Derechos del titular

-Para fortalecer la protección de datos personales, la LFPDPPP prevé un procedimiento de protección de derechos ante el IFAI al que podrá recurrir el titular de los datos en los casos en que se vean vulnerados sus derechos.

-Los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa contra las resoluciones que dicte dicho Instituto.

3.2.4 Sanciones

-Otorga al IFAI la facultad de imponer sanciones a los particulares que van desde un apercibimiento hasta multas desde los 100 hasta 320,000 días de salario mínimo vigente en el Distrito Federal, con doble imposición para los casos de reincidencia, las cuales pudieran duplicarse en aquellos casos de infracciones relativas a datos personales sensibles.

-Introduce la tipificación de delitos en materia del tratamiento indebido de datos personales, con penas que podrán ser desde los tres meses hasta los cinco años de prisión.

4 Marco Normativo

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001- 27002 (ISO 27000, 2005).

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean

conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

En la siguiente figura (Figura 1.4.) se explica de manera grafica la Gestión de Riesgos que propone el SGSI sobre el que se construye ISO 27001- 27002, considerando las etapas de Planificación, Identificación y Análisis de Riesgos y Dirección y Control de los riesgos, en esta ultima etapa se considera la mitigación, transferencia y aceptación del riesgo.

Figura 1.4 Gestión de Riesgos

4.1 Serie ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. La seguridad puede ser vista como una medida de robustez de un sistema, respecto a una política de seguridad (Viega J., 2001).

4.2 Origen

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution), es responsable de la publicación de importantes normas como: 1979 Publicación BS 5750 - ahora ISO 9001, 1992 Publicación BS 7750 - ahora ISO 14001, 1996 Publicación BS 8800 - ahora OHSAS 18001 La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información. En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007 manteniendo el contenido, así como el año de publicación formal de la revisión.

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van desde 27000 a 27019 y de 27030, 27044, pasando por 27001, 27002, 27003, 27004, 27005, 27006, 27007, 27011, 27031, 27032, 27033, 27034 y 27799.

4.3 Directrices del Estándar ISO 27001-27002

ISO 27001 - 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la

información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2005 del estándar incluye las siguientes once secciones principales:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones, aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

4.4 Implementación

4.4.1 Desarrollo conceptual.

En función a lo estipulado en la LFPDPPP las empresas que recaben datos de personas físicas deberán considerar los siguientes lineamientos: establecer y mantener medidas seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra acceso o tratamiento no autorizado. Por esta razón las pequeñas y medianas empresas deben revisar y analizar el impacto de esta ley en sus procesos de negocio, identificando dónde se debe reforzar el nivel de seguridad de acceso a la información, además de revisar posibles modificaciones a los avisos de privacidad, ejercicio de derechos, contratos con terceros, y reforzar con sus las reglas que los impactan.

Adicionalmente todos los terceros con los que se comparten datos personales y personales sensibles de acuerdo a la LFPDPPP, están obligados al cumplimiento del punto de vista de un encargado (titular). Sin embargo, es muy importante, de acuerdo a lo establecido por la ley, es obligación del responsable establecer una cláusula de protección de los datos personales en el contrato con el encargado por lo que en estricto sentido con dicha cláusula las pequeñas y medianas empresas estarían protegidas en caso de que el encargado sufra una vulneración de seguridad.

4.4.2 Actividades de apoyo para la implementación de Auditoria basada en ISO 27001

A continuación, se propone un listado de once pasos que las PyMEs deberán seguir si desean implementar la Metodología de Evaluación de Seguridad Informática:

4.4.2.1 Obtener el apoyo de la dirección

Es indispensable que la dirección destine suficientes recursos humanos para que trabajen en la implementación y el suficiente dinero. Para esto se deberá convencer a los directores de las empresas de financiar la implementación de la Metodología, para esto se deberá hacer un trabajo previo presentando los beneficios, aunque los beneficios son muchos, mencionaré algunos de los más importantes:

-Cumplimiento. - es el que demuestra el "rendimiento de la inversión" más rápidamente. Si una organización debe cumplir con diversas normas sobre protección de datos, privacidad y control de TI (especialmente si se trata de una organización financiera, de salud o gubernamental), la Metodología propuesta puede permitir hacerlo de la manera más eficiente.

-Ventaja de comercialización. - en un mercado cada vez más competitivo, a veces es muy difícil encontrar algo que lo diferencie ante la percepción de sus clientes. La Metodología puede ser un verdadero punto a favor, especialmente si usted administra información sensible de sus clientes.

-Disminución de gastos. - existe una ganancia financiera si se disminuyen los gastos ocasionados por incidentes. Probablemente sí se produzcan en su empresa interrupciones de servicio o esporádicos filtrados de datos.

La verdad es que aún no existe una metodología ni tecnología que pueda calcular cuánto dinero se puede ahorrar si evita ese tipo de incidentes. Pero siempre es oportuno alertar a la dirección sobre estos casos.

4.4.2.2 Definir el alcance

El primer paso en la implementación de la Metodología es la definición del alcance. En ese contexto, el mundo exterior no son sólo los clientes, socios, proveedores, etc., sino también los departamentos de la organización que no están dentro del alcance definido.

4.4.2.3 Definir la metodología de Evaluación de riesgos

La evaluación de riesgos es la tarea más compleja del proyecto; su objetivo es definir las reglas para identificar los activos, las vulnerabilidades, las amenazas, las consecuencias y las probabilidades, como también definir el nivel aceptable de riesgo. Si esas reglas no están definidas claramente, las PyMEs podrían encontrarse en una situación en la que obtendría resultados inservibles. (Consejos sobre la evaluación de riesgos para empresas pequeñas)

La evaluación de riesgos es un proceso durante el cual una organización debe identificar los riesgos de seguridad de la información determinando su probabilidad e impacto. En otras

palabras, la organización debe reconocer todos los potenciales problemas con su información, cómo podrían suceder y qué consecuencias podrían tener. El objetivo de la evaluación de riesgos es encontrar qué controles se necesitan para disminuir el riesgo; la selección de controles se denomina proceso de tratamiento de riesgos y, en la ISO 27001, estos controles son tomados del Anexo A, donde se especifican 133 controles.

La evaluación de riesgos se realiza identificando y evaluando activos, vulnerabilidades y amenazas. Un activo es todo lo que tenga valor para la organización: hardware, software, personal, infraestructura, datos (en diversos formatos y medios), proveedores y socios, etc. Una vulnerabilidad es una debilidad en un activo, proceso, control, etc. que pueda ser explotado por una amenaza. Una amenaza es cualquier causa que pueda infligir daño a un sistema u organización. Un ejemplo de una vulnerabilidad es la falta de software antivirus; y una amenaza relacionada es el virus informático.

Teniendo todo esto en cuenta, si su organización es pequeña, usted realmente no necesita una herramienta sofisticada para realizar la evaluación de riesgos. Todo lo que necesita es una hoja de cálculo de Excel, buenos catálogos de vulnerabilidades y amenazas y una buena metodología de evaluación de riesgos. La tarea principal pasa realmente por evaluar la probabilidad y las consecuencias, y esto no es posible hacerlo con cualquier herramienta, es algo que los propietarios de sus activos, con el conocimiento que tienen sobre los mismos, tienen que evaluar.

Pasos básicos para la valuación y el tratamiento:

-Definir y documentar la metodología (incluyendo los catálogos) y distribuirlos a todos los propietarios de activos de la organización.

-Organizar entrevistas con todos los propietarios de activos para que ellos identifiquen sus activos y las vulnerabilidades y amenazas relacionadas. En el segundo paso solicitarles que evalúen la probabilidad e impacto si ocurriera un riesgo en particular.

-Consolidar los datos en una única hoja de cálculo, calcular los riesgos e indicar qué riesgos no son aceptables.

-Para cada riesgo que no sea aceptable, escoger uno o más controles de la ISO 27001 y calcular cuál sería el nuevo nivel de riesgo luego de la implementación de esos controles.

La evaluación y tratamiento de riesgos son los verdaderos pilares de la seguridad de la información y de la ISO 27001, pero esto no significa que tengan que ser complicados. Lo puede hacer de una manera sencilla, y su sentido común es lo que en realidad importa.

4.4.2.4 Realizar la evaluación y el tratamiento de riesgos

Implementar lo que se definió en el paso anterior. En organizaciones más grandes puede demandar varios meses, por lo tanto, debe coordinar esta tarea con mucho cuidado. Lo importante es obtener una visión integral de los peligros sobre la información de su organización.

El objetivo del proceso de tratamiento de riesgos es reducir los riesgos no aceptables, en este paso, se debe redactar un Informe sobre la evaluación de riesgos que documente todos los pasos tomados durante el proceso de evaluación y tratamiento de riesgos. También es necesario conseguir la aprobación de los riesgos residuales; ya sea en un documento separado o como parte de la Declaración de aplicabilidad.

4.4.2.5 Redactar la Declaración de aplicabilidad

Luego de finalizar su proceso de tratamiento de riesgos, sabrá exactamente qué controles del Anexo necesita (hay un total de 133 controles, pero, probablemente, no los necesite a todos). El objetivo de este documento (generalmente denominado DdA) es enumerar todos los controles, definir cuáles son aplicables y cuáles no.

4.4.2.6 Redactar el Plan de tratamiento del riesgo

El objetivo del Plan de tratamiento del riesgo es definir claramente cómo se implementarán los controles de la DdA, quién lo hará, cuándo, con qué presupuesto, etc. Este documento es, en realidad, un plan de implementación enfocado sobre los controles de sus terceros (proveedores); sin el cual, usted no podría coordinar los pasos siguientes del proyecto.

4.4.2.7 Determinar cómo medir la eficacia de los controles

En esta etapa se tendrá que determinar cómo medirá el logro de los objetivos establecidos tanto para cada control aplicable de la Declaración de aplicabilidad.

4.4.2.8 Implementar programas de capacitación y concienciación

Si quiere que sus empleados implementen todas las nuevas políticas y procedimientos, primero debe explicarles por qué son necesarios y debe capacitarlos para que puedan actuar

según lo esperado. La falta de estas actividades es el segundo motivo principal por el fracaso de implementación de la Metodología.

4.4.2.9 Hacer funcionar la Metodología de Evaluación de Seguridad

Esta es la parte en que la Metodología se transforma en una rutina diaria dentro de su organización. La palabra más importante aquí es: "registros". A los auditores les encantan los registros; sin registros le resultará muy difícil probar que una actividad se haya realizado realmente. Pero, ante todo, los registros deberían ayudarle. Con ellos, usted puede supervisar qué está sucediendo, sabrá realmente si sus empleados (y proveedores) están realizando sus tareas según lo requerido.

Aquí es donde se cruzan los objetivos de los controles con la metodología de medición; debe verificar si los resultados que obtiene cumplen con lo que se estableció en los objetivos. Si no se cumplen, es evidente que algo está mal y debe aplicar medidas correctivas y/o preventivas.

4.4.2.10 Revisión por parte de la dirección

La dirección no tiene que ejecutar la Metodología, pero sí debe saber qué está sucediendo; es decir, si todo el mundo ejecutó sus tareas, si se obtienen los resultados deseados, etc. En base a estos aspectos, la dirección debe tomar algunas decisiones importantes.

4.4.2.11 Medidas correctivas y preventivas

El objetivo de la Metodología de Evaluación de Seguridad a Informática es garantizar que todo lo que está mal (las denominadas “no conformidades”) sea corregido o, con algo de suerte, evitado. Por lo tanto, la Metodología requiere que las medidas correctivas y preventivas se apliquen sistemáticamente; es decir, que se identifique la raíz de una no conformidad, se solucione y se controle.

4.4.3 ¿Cómo realizar esta tarea en una PyME?

La Metodología de Evaluación de Seguridad propuesta requiere determinar a través de las leyes actuales Mexicanas que hacen referencia al uso de información de personas físicas, el impacto del servicio que se está subcontratando, es decir en base a las propiedades de la información (Confidencialidad, Integridad, Disponibilidad e Irrefutabilidad), el tamaño del impacto en caso de que la información sea interceptada por un tercero o accedida por un usuario no autorizado, modificada sin autorización, indisponibilidad del servicio y las repercusiones del uso inadecuado del logo o la marca de la empresa contratante.

Las pequeñas y medianas empresas deberán considerar que cualquier intercambio de información deberá ser sujeto a una Evaluación de Seguridad Informática, los proveedores deberán remediar cualquier desviación detectada durante la evaluación antes de la firma de un contrato de prestación de servicios de acuerdo a la Metodología propuesta.

Algunos de los servicios relevantes sujetos a revisión que podrían sr tercerizados son:

- Almacenamiento y digitalización de documentos.
- Impresión de cartas, publicidad o cualquiera que contenga información de clientes o empleados.
- Desarrollo de páginas web, hosteo de páginas web, encuestas online, etc.
- Call Center.
- Servicios de Recursos Humanos como reclutamiento, cálculo de nómina y aportaciones, administración de beneficios, etc.
- Iniciativas de Ventas y Mercadeo.
- Recuperación de cartera vencida.
- Servicios Legales.
- Servicios de Traducción.
- Avalúos.

Es importante entender que cualquier tipo de tercerización si bien puede generar ahorros para las pequeñas y medianas empresas, también trae consigo riesgos de seguridad, principalmente, por la confidencialidad, integridad y disponibilidad de la información que será accedida, almacenada y/o procesada por terceras partes, provocando daño reputacional, perdidas monetarias o de negocio, actividad criminal y problemas de tipo legal.

Para conocer los requerimientos legales y regulatorios, y tener la certeza de que los terceros cuentan con medidas de seguridad apropiadas para proteger la información que se les comparte se requiere ejecutar una Evaluación de Seguridad Informática a todos los proveedores que les aplique, el tiempo óptimo para ejecutar el proceso es antes de la implementación de los servicios, asegurando que cualquier desviación de seguridad sea mitigada antes de la puesta en producción.

Para que las pequeñas y medianas empresas puedan asegurar el cumplimiento con la LFPDPPP de los terceros que actúen como encargados del tratamiento de datos personales de clientes o empleados, se propone la revisión de controles a 3 niveles: Legales, Organizacionales y Técnicos.

Legales: Como parte del contrato las pequeñas y medianas empresas deberán agregar una cláusula de confidencialidad que soporte la corresponsabilidad en materia de datos personales; la cláusula deberá incluir por lo menos, tratar únicamente los datos personales conforme a las instrucciones del responsable, no tratar los datos personales para una finalidad distinta a la acordada en el contrato, implementar medidas de seguridad conforme a la ley, guardar confidencialidad respecto de los datos personales, suprimir los datos personales una vez cumplida la prestación contractual y no transferir datos personales a menos que el responsable así lo determine.

Organizacionales: Existen diferentes controles a nivel organizacional que la ley exige a los responsables de la protección de datos personales, por lo que los encargados deberán cumplir con dichos controles: contar con un aviso de privacidad (identidad y domicilio de quien los recaba, finalidad del tratamiento, limitantes con respecto al a divulgación de los datos, medios para ejercer derechos Acceso, Rectificación, Cancelación y Oposición); el encargado deberá designar a un responsable de la protección de los datos personales, deberá contar con una ventanilla de atención a los derechos ARCO y capacitar a las personas involucradas en el tratamiento de los datos personales para el cumplimiento con la ley.

Técnicos: Las pequeñas y medianas empresas deben identificar los tipos de datos personales que se trataran en su nombre, la sensibilidad de los mismos y el número de titulares para determinar el riesgo inherente de los datos.

El tratamiento de datos personales por terceros por necesidades de negocio u operación está consentido por la LFPDPPP; únicamente se debe asegurar la protección de los datos de acuerdo, entre otras cosas, a su riesgo inherente. Para el cálculo del riesgo inherente se consideran las siguientes categorías.

- Datos de Identificación.
- Datos de Tarjetas bancarias.
- Datos Jurídicos.
- Datos de Autenticación.
- Datos Patrimoniales.
- Datos de Ubicación.
- Datos de Salud.
- Origen, creencias e ideológicos.

Por definición en la ley, los datos personales se clasificación en 2 categorías DATOS PERSONALES y DATOS PERSONALES SENSIBLES, tomando en cuenta el riesgo inherente de los mismos. Con el objetivo de ejecutar una Evaluación de Seguridad Informática mas a detalle se recomienda clasificar los datos personales en 4 categorías (Bajo, Medio, Alto y Critico), siendo el criterio para determinar el riesgo inherente.

Riesgo inherente Bajo.

Datos de Identificación: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, correo electrónico, lugar y fecha de nacimiento, nacionalidad, información de familiares, puesto de trabajo, lugar de trabajo, lengua, escolaridad, referencias familiares y personales e información migratoria.

Riesgo inherente Medio.

Datos de tarjetas bancarias: Número de tarjeta, datos de banda magnética.

Datos Jurídicos: Expediente jurídico incluyendo, penales, amparos, demandas, contratos.

Datos de autenticación: usuarios y contraseñas, información biométrica, firma autógrafa y electrónica, fotografías, IFE y Pasaporte.

Datos Patrimoniales: saldos bancarios, estados de cuenta, número de cuenta, bienes inmuebles, información fiscal, historial crediticio, ingresos/egresos, buro de crédito, seguros, afores, sueldos y salarios y servicios contratados.

Datos de Ubicación: dirección física y ubicación del titular.

Riesgo inherente Alto.

Datos de Salud: información médica con el estado de salud física y mental, pasada, presente o futura.

Origen, creencias e ideológicos: origen racial o étnico, afiliación sindical, costumbres, opiniones políticas, preferencia sexual y hábitos sexuales.

Riesgo inherente Critico.

Datos de tarjetas bancarias: fecha de vencimiento, número de identificación personal PIN y códigos de seguridad (CVV, CVV2). (Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2014)

4.5 Beneficios

Entre los principales beneficios que proporcionará la implementación de la Metodología de Evaluación de Seguridad Informática mediante un proceso sistemático, documentado y conocido por toda la organización se encuentran:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los terceros / proveedores tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001…).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.

- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

CAPITULO II

OBJETO DE ESTUDIO

1 Descripción del Objeto de Estudio.

La Metodología de Evaluación de Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas (PyMe), pretende servir como apoyo a las empresas en el sector público y privado en el municipio de Toluca, Estado de México, que requieran subcontratar operaciones o procesos a través de outsourcing y que mediante esta estrategia proporcionen información de Personas Físicas a terceros.

Este trabajo se orienta básicamente a las empresas en el municipio de Toluca que operen con escalas bajas de producción, utilicen tecnologías adaptadas y sean de propiedad familiar o su financiamiento proceda de fuentes propias, dedicadas a la venta, administración y producción de bienes y servicios. La estructura de las empresas a las que pudiera aplicarse la Metodología propuesta dependerá en gran medida de su estructura organizacional que estará definida por:

-División del trabajo. Se trata de conocer las labores que son realizadas en el negocio, si son suficientes, si pueden ser realizadas en el tiempo que dura la jornada laboral, si están repartidas equitativamente.

-Procedimientos. La expresión de la forma en que se realizan las cosas. Esta expresión debemos compararla con la forma en la que "deberían" de realizarse. Existen niveles en los

procedimientos, que, de acuerdo a su extensión, agrupan a diferentes áreas administrativas y puestos de la empresa. Existen también métodos de control para los procedimientos, generalmente a través de los formatos o en las últimas décadas, los sistemas de información. Los procedimientos deben ser lo suficientemente detallados para poder conocer exactamente qué está pasando en cada punto del proceso, pero sin exagerar como para que se vuelvan imposibles de realizar, ni tan poco definidos que dejen lagunas de decisión.

-Puestos. Es el rol que cada persona realizara en la empresa. Aquí lo primero es saber cuál es la función del puesto, que hace, como contribuye a la consecución del objetivo de la empresa.

-Organigrama. Esta es la representación gráfica de la organización, y de cómo fluye la comunicación dentro de ella, y de las relaciones que existen entre las diversas áreas y puestos. Viendo el organigrama de una empresa se puede tener una idea certera de lo que está pasando en ella.

-Manuales Administrativos. Los manuales constituyen una de las herramientas con que cuentan las organizaciones para facilitar el desarrollo de sus funciones administrativas y operativas.

(Asociación de economía aplicada, C. Aybar Arias / A. Casino Martínez / J. López García, 2003).

2 Subcontratación.

La finalidad del outsourcing o subcontratación por parte del proveedor es facilitar el trabajo a la empresa (PyME) realizando unas tareas con un alto contenido de especialización. De esta forma la empresa cliente puede emplear todo su tiempo y esfuerzo a realizar su negocio principal y aquel que conoce y domina.

Las tareas que suelen externalizarse son las tareas muy técnicas y que se dejan en manos de expertos externos. Como pueden ser las tareas de fiscalidad compleja o la de los servicios informáticos o el outsourcing de las tecnologías de la información.

El outsourcing está en alza y ha sido y es la oportunidad de muchas pymes que han encontrado en el desarrollo de esta actividad, que les ceden las grandes compañías, una nueva fuente de ingresos.

Desde luego, las actividades que pasan a desarrollar empresas externas son aquellas que no son estratégicas para el negocio de las empresas cliente o para las que no se tiene especial capacidad en ellas.

Se denomina outsourcing a la estrategia mediante la cual una parte o el total de un proceso interno de un negocio o institución, contrata a un "tercero". Al evaluar los servicios proporcionados por un proveedor externo, las empresas o instituciones buscan obtener todos o alguno de los siguientes objetivos:

1. Optimizar sus costos operativos y/o administrativos.

2. Utilizar recursos especializados con los que no se cuentan internamente o no es conveniente contar con ellos.

3. Implementar mejores prácticas en procesos donde el "tercero" tiene experiencia por haberlas desarrollado en otras instituciones y/o negocios.

Sin embargo, la diferencia de expectativas puede originar problemas en la relación cliente/proveedor. (Política Digital, Innovación gubernamental NEXOS, 2007)

3 Tipo de Proveedores.

Como primer paso se deberá identificar a todos los proveedores que proporcionan un servicio a la empresa dentro de los que podemos identificar 3 tipos de acuerdo a la gestión de servicios propuesta en ITIL V3.

ITIL considera tres tipos diferentes de proveedores de servicios:

-Tipo I o proveedor de servicios interno

-Tipo II o unidad de servicios compartidos

-Tipo III o proveedores de servicio externos

Aunque los aspectos generales de la gestión del servicio son comunes a todos ellos existen obvias diferencias en los aspectos organizativos en cada caso.

Cada tipo de proveedor de servicios tiene sus ventajas e inconvenientes que pasamos a analizar.

3.1 Proveedores de Servicios Interno (TIPO I).

Esta opción sólo es recomendable cuando los servicios prestados forman parte esencial en el posicionamiento estratégico de la organización.

3.2 Unidades de Servicios Compartidos (TIPO II).

Este tipo de proveedor presta servicio a diferentes unidades de negocio que operan bajo un paraguas común.

3.3 Proveedores de Servicios Externos (TIPO III).

Estos proveedores ofrecen sus servicios en el mercado a diferentes clientes que frecuentemente serán competidores entre sí. Las ventajas de la contratación externa de los servicios son evidentes, siempre que estos no formen parte integrante del núcleo del negocio del cliente, se resumen en:

-Mayor flexibilidad y oferta.

-Se minimizan los riesgos pues estos son compartidos entre una amplia red de clientes.

-Procedimientos estandarizados. (ITIL V3 Gestión de Servicios, 2011)

4 Proceso.

De acuerdo a las funciones y servicios que proporcione un tercero las PyMEs deberán definir si en función de la Metodología propuesta, los proveedores son sujetos a una Evaluación de

Seguridad Informática, considerando que cualquier departamento o persona que pertenezca a la empresa podrá solicitar su ejecución.

4.1 Análisis de Impacto al Negocio y Alcance.

Una vez que se identifica que se requiere iniciar una Evaluación de Seguridad Informática el primer paso es definir el alcance de la evaluación y nivel de impacto al negocio.

Frente a posibles amenazas, interrupciones y errores humanos de la actividad de una organización, el análisis de impacto al negocio (AIN) permite determinar aspectos tales como:

-Interrupción máxima admisible.

-Límite máximo de pérdida o divulgación de datos admisible.

-Límite máximo de modificación de datos accidental o intencional admisible.

El análisis de impacto al negocio debe ser desarrollado mediante entrevistas con cada responsable de las principales actividades de riesgo en la empresa que determine hacer uso de la subcontratación o intercambiar datos con terceros, procurando mostrar de forma práctica como realizar el análisis de impacto.

El proceso de análisis de impacto considera la evaluación cuantitativa y cualitativa sobre la posibilidad de sufrir pérdidas o daños, para definir el nivel de impacto al negocio se deberán tomar en cuenta tres factores de riesgo:

-Tipo de datos de acuerdo al riesgo inherente que representen.

-Volumen.

-Medios de transmisión de la información.

-Confidencialidad.

-Integridad.

-Disponibilidad.

Al momento de realizar el análisis de impacto al negocio se deberán considerar los peores escenarios posibles que tengan en cuenta todos los procesos e infraestructura necesaria para el desarrollo de la actividad. (Innovación y Gestión de Recursos Técnicos, 2016)

La primera sección del documento AIN propuesto, será dedicada para el registro de información general básica que identifique al proveedor.

Datos Generales	
Nombre del tercero:	Razón Social
Representante:	Nombre del respresentante legal
Direcciòn:	Direcciòn de las instalaciones o centro de datos

Posteriormente se deberá registrar la unidad de negocio que pretende subcontratar operaciones, así como una detallada descripción del servicio sujeto a evaluación de seguridad informática.

Datos del Servicio	
Unidad de Negocio (solicitante)	Nombre del departamento o unidad de negocio que solicita
Descripciòn del Servicio:	Descripciòn detallada del servicio

Es indispensable que el área de negocio identifique el tipo de datos que serán compartidos con el proveedor que proporcionará el servicio de acuerdo a su riesgo inherente. Los valores obtenidos para esta sección serán de 2-RI BAJO, 3-RI MEDIO, 4-RI ALTO y 5-RI CRÍTICO.

Riesgo Inherente BAJO.

Datos de Identificación:	Nombre		Estado Civil		Puesto de trabajo		
	Teléfono		Correo Electrónico		Lugar de trabajo		
	Edad		Lugar de Nacimiento		Lengua		
	Sexo		Fecha de Nacimiento		Escolaridad		
	RFC		Nacionalidad		Referencias familiares y personales		
	CURP		Información de familiares		Información migratoria.		

Riesgo Inherente MEDIO.

Datos de tarjetas bancarias:	Número de tarjeta						
	Datos de banda magnética.						
Datos Jurídicos:	Expediente jurídico						
Datos de autenticación:	Usuarios		Información biométrica		Fotografías		
	Contraseñas,		Firma autógrafa y electrónica		IFE y/o Pasaporte.		
Datos Patrimoniales:	Saldos bancarios		Bienes inmuebles		Ingresos/Egresos		
	Estados de cuenta		Información fiscal		Seguros/Afores		
	Número de cuenta		Historial crediticio		Sueldos y salarios		
			Buro de crédito		Servicios contratados		
Datos de Ubicación:	Dirección física						
	Ubicación del titular.						

Riesgo Inherente ALTO.

Datos de Salud:	Información médica con el estado de salud física y mental, pasada, presente o futura.	

Origen, creencias e ideológicos:	Origen racial o étnico		Costumbres		Preferencia sexual		
	Afiliación sindical		Opiniones políticas		Hábitos sexuales		

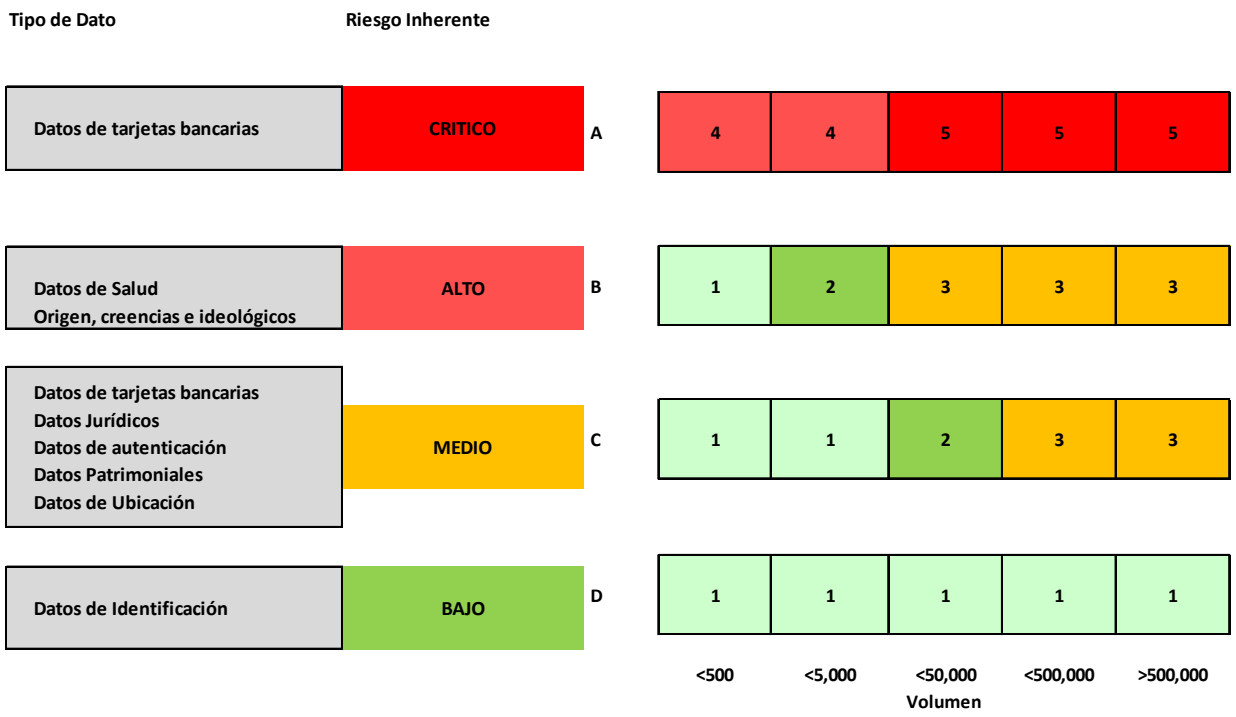
Riesgo Inherente CRÍTICO.

Datos de tarjetas bancarias:	Fecha de vencimiento	
	Número de identificación personal PIN	
	Códigos de seguridad CVV, CVV2	

Se deberá considerar el volumen de datos que la unidad de negocio compartirá con el proveedor, preferentemente se deberá cuantificar en base anual o durante el tiempo que se tendrá una relación contractual con el proveedor (menos de un año).

Datos de hasta 500 titulares	
Datos de entre 501 hasta 5,000 titulares	
Datos de entre 5,001 hasta 50,000 titulares	
Datos de entre 50,001 hasta 500,000 titulares	
Datos de más de 500,000 titulares	

En base al riesgo inherente por el tipo de dato y el volumen que serán compartidos podremos determinar el nivel de riesgo por tipo de dato como se muestra en la siguiente tabla:



Los valores obtenidos para esta sección serán de 1 a 5, a continuación, se detallan los niveles mencionados:

Riesgo de dato Nivel 1:

-El riesgo inherente de los datos es BAJO, sin importar el número de titulares.

-El nivel de riesgo inherente sea MEDIO y se comparta una base de hasta 5,000 titulares.

-El nivel de riesgo inherente sea ALTO y se comparta una base de hasta 500 titulares.

Riesgo de dato Nivel 2:

-El nivel de riesgo inherente de los datos sea MEDIO y se comparta una base de hasta 50,000 titulares.

-El nivel de riesgo inherente de los datos sea ALTO y se comparta una base de hasta 5,000 titulares.

Riesgo de dato Nivel 3:

-El nivel de riesgo inherente de los datos sea MEDIO y se comparta una base de más de 50,000 titulares.

-El nivel de riesgo inherente de los datos sea ALTO y se comparta una base de más de 5,000 titulares.

Riesgo de dato Nivel 4:

-El nivel de riesgo inherente de los datos sea CRÍTICO y se comparta una base de hasta 500 titulares.

-El nivel de riesgo inherente de los datos sea CRÍTICO y se comparta una base de más de 500 y hasta 5,000 titulares.

Riesgo de dato Nivel 5:

-El nivel de riesgo inherente de los datos sea CRÍTICO y se comparta una base de más de 5,000 titulares.

Una vez obtenido el nivel de riesgo por dato, se debe identificar el formato en el que se transmitirá la información, así como el medio de transmisión, los medios de transmisión se enlistan de acuerdo a la seguridad del medio, siendo el primero uno de los más inseguros y el último el más adecuado de acuerdo al formato de la información. Los valores obtenidos para esta sección serán de 1 a 5 dependiendo del nivel de seguridad del medio.

Formato	Informacón electrónica
	Información física

Fax	
Mensajería	
Teléfono	
Correo electrónico en claro	
Correo electrónico cifrado	
Correo electrónico en claro con adjunto cifrado	
Carga de archivo a Página web	
SFTP	
Web Services	
VPN	
Enlace dedicado	
OTRO	

Por último, para calcular de manera adecuada el Impacto al Negocio total, la unidad de negocio deberá considerar los impactos de que la información sea divulgada, modificada o que exista una interrupción del servicio por parte del proveedor, se diseñaron preguntas por sección como se muestra a continuación. Los valores obtenidos para esta sección serán de 1, 3 y 5 de acuerdo al impacto definido por la unidad de negocio.

Confidencialidad

En la siguiente escala, cual considera usted que sería el impacto si la información compartida con el tercero fuera revelada?

Bajo	
Medio	
Alto	

Elija el daño reputacional que podría provocarle la divulgación no autorizada de la información

Bajo	
Medio	
Alto	

Existe alguna sancion de carácter legal o regulatorio en caso de que la información fuera divulgada?

NO	
SI	

Integridad

Cuál sería el impacto si la información compartida con el tercero fuera modificada de manera no autorizada?

Bajo	
Medio	
Alto	

Elija el daño reputacional que podría provocarle la modificación no autorizada de información

Bajo	
Medio	
Alto	

Existe alguna sancion de carácter legal o regulatorio en caso de que la información fuera modificada sin autorización?

NO	
SI	

Disponibilidad

Si se presentara una interrupción del servicio por cuanto tiempo podría soportar la operación sin impactar a sus clientes?

12 horas	
3 días	
1 semana	

Cuando se encuentren contestadas las secciones descritas anteriormente en el AIN propuesto, podremos obtener un valor de 1 a 5 en cada sección, obteniendo el promedio de cada sección y aplicando un redondeo en caso de que el resultado obtenido sea con cifras decimales.

IMPACTO TOTAL POR SECCIÓN	
	Valor redondeado
Tipo de Datos	PromTD
Volumen de Datos	PromVD
Medio de Transmisión	PromMT
Confidencialidad	PromC
Integridad	PromI
Disponibilidad	PromD

Cuando se obtengan los valores por sección, se deberá aplicar la siguiente formula que nos permitirá determinar el Impacto al Negocio real de acuerdo a la siguiente escala:

PromTD+PromVD+PromMT+PromC+PromI+PromD / 6 (redondear)

MUY BAJO	1
BAJO	2
MEDIO	3
ALTO	4
MUY ALTO	5

El resultado del AIN definirá el nivel de seguridad requerido para el servicio que será proporcionado por los terceros o proveedores, el impacto MUY BAJO definirá un conjunto de controles básicos que mitiguen el riesgo de tercerizar las operaciones de una PyME, al contrario de un impacto MUY ALTO que requerirá la aplicación de controles más robustos. Siempre se deberá verificar que el resultado del AIN sea correcto y lo más preciso posible de acuerdo a la necesidades y requerimientos de las áreas de la empresa.

Para los Impactos Muy bajo (1) y Bajo (2) – Se deberán revisar controles básicos de seguridad, considerando que representa el menor impacto para las PyME.

Para un impacto Medio (3), Alto (4) y Muy Alto (5) – Se deberá solicitar el llenado del cuestionario de seguridad a los terceros y deberá ser regresado al solicitante para su análisis. Se recomienda analizar la posibilidad de llevar a cabo la revisión remota o en las instalaciones del tercero en cuestión.

De acurdo al nivel de impacto obtenido, los cuestionarios incluirán una serie de controles basados en la Norma ISO IEC 27002 que aseguren la protección de información de las personas físicas compartida. El auditor encargado de realizar las revisiones, no deberá asumir u omitir la revisión de todos los controles aplicables de acuerdo al alcance de la revisión.

4.1.1 Evaluaciones de Seguridad Remotas o en Sitio.

Generalmente la decisión de llevar a cabo la revisión remota o en sitio será determinada por el Nivel de impacto al negocio; sin embargo, existen factores a considerar como, la manera en que la información será accedida por el tercero, el tipo de datos, el volumen, etc.

Las revisiones remotas serán aceptadas cuando se obtiene un impacto 2 o superior, las revisiones remotas pueden ser ejecutadas por correo electrónico, teléfono y tecnologías de comunicación por video y voz.

Se recomienda para los impactos 4 y 5 ejecutar una revisión en sitio particularmente cuando los terceros, procesen o almacenen tipos de datos con riesgo inherente ALTO o CRÍTICO, utilicen tecnologías para transmitir externamente datos con riesgo inherente ALTO o CRÍTICO. Mientras sea posible las revisiones en sitio deberán ser ejecutadas en instalaciones del proveedor

en las que se almacenen o procesen los datos o en las que se ejecute la operación o servicio que proporcionen.

4.2 Preparación de Evaluaciones de Seguridad

El auditor deberá revisar las respuestas de cada control de seguridad aplicable dentro del cuestionario de seguridad con la intención de preparar una lista de controles basada en los dominios que detecte con más debilidades dentro del cuestionario. Es importante que antes de ejecutar cualquier tipo de evaluación, el auditor pueda tener visibilidad del alcance del servicio y la importancia de la información que se estará intercambiando con el tercero en cuestión, ya que de esta manera podrá identificar la eficacia de los controles de seguridad en materia informática que tienen implementados cliente y proveedor para el intercambio de información y específicamente el proveedor para el tratamiento (almacenamiento y procesamiento) adecuado de la información de clientes o empleados del contratante.

Si durante la preparación el auditor llegará a identificar controles no aceptables o deficientes, es responsabilidad del auditor reportarlo a las unidades de negocio.

4.3 Introducción a la Evaluación de Seguridad

Cuando se inicie una Evaluación de Seguridad Informática es recomendable agendar una conferencia telefónica entre el auditor y el proveedor en la que se explique el antecedente, alcance, objetivos y propósito de la evaluación.

4.4 Ejecución de la Evaluación de Seguridad

Los propósitos de la Evaluación de Seguridad Informática son:

-Explicar a los terceros los requerimientos de la empresa en materia de seguridad de la información.

-Establecer las expectativas de la empresa en función de la protección de su información.

-Validar y evaluar los controles aplicables de acuerdo a las respuestas de los proveedores en el cuestionario de seguridad.

-Dar seguimiento y probar la efectividad de los controles en los que se identifiquen huecos de seguridad o deficiencias.

-Solicitar y recolectar evidencias que soporten la implementación de los controles de seguridad aplicables.

-Ejecutar evaluaciones en sitio (instalaciones del proveedor), en caso de que se considere necesario.

Las Evaluaciones de Seguridad ayudarán a las empresas a obtener el detalle de los controles bajo los que se procesara o almacenara su información. Es aceptable que el auditor ejemplifique o proporcione una guía de los controles de seguridad implementados en la empresa sin revelar información privilegiada.

Durante la ejecución de la Evaluación de acuerdo a las respuestas de los terceros en el Cuestionario de Seguridad, el auditor podrá solicitar evidencia que le permita asegurarse de la implementación, implementación parcial y ausencia de los controles de seguridad, tanto de

manera remota como en sitio. Al término de la aplicación del cuestionario de seguridad, el auditor deberá proporcionar un listado de requerimientos para que el proveedor proporcione la información solicitada como sustento de lo comentado durante la evaluación.

4.5 Discusión de los Riesgos/Deficiencias Identificados

Al final de la revisión, el auditor deberá discutir los riesgos o deficiencias en los controles de seguridad identificadas que deberán ser atendidas por el tercero de acuerdo a las necesidades de la PyME.

4.6 Reporte de los Riesgos/Deficiencias Identificados

El auditor deberá preparar un Reporte de Seguridad, a través, del que se comunicarán los resultados a la unidad de negocio.

El reporte deberá describir claramente los riesgos o deficiencias identificados durante la evaluación de seguridad, el riesgo asociado, la clasificación del riesgo y las recomendaciones para su remediación.

El reporte de Seguridad deberá tener la siguiente estructura:

Datos Generales.

En esta sección se deberá poder identificar, el tipo de evaluación ejecutada, la fecha en que se ejecutó, nombre de la unidad de negocio solicitante, nombre del evaluador, nombre del proveedor, servicio, etc.

DATOS GENERALES

Tipo de Evaluación

Evaluación Remota: [ ] Evaluación en Sitio: [ ]

Fecha de ejecución:	dd/mm/aaaa
Fecha de generación de Reporte:	dd/mm/aaaa
Unidad de negocio:	
Nombre del Servicio:	
Nombre del Evaluador:	
Nombre del Proveedor:	
Dirección del Proveedor:	

Introducción.

Se deberá especificar el objetivo de la revisión, el servicio al que corresponde y el proveedor que será contratado para tercerizar la actividad.

INTRODUCCIÓN

El presente reporte pertenece a la Evaluación del servicio (Nombre del servicio) cualquier otra relación con el tercero requerira una evaluación adicional. El reporte de evaluación no implica la aprobación para ninguna relación actual o futura con (Nombre del proveedor).
El objetivo de la evaluación es confirmar que los controles de seguridad implementador por (Nombre del proveedor) son adecuados para proporcionar confidencialidad, privacidad e integridad de los datos.

Conclusiones.

Dentro de las conclusiones se incluirán las calificaciones obtenidas durante la revisión en base al Análisis de Impacto al Negocio, la Exposición y el Riesgo Total, como se explica a continuación.

AIN (Impacto)

Evaluación de Impacto

Basado en los resultados del AIN completado por el área solicitante del servicio y tomando en cuenta el riesgo asociado del servicio fue catalogado con un impacto (Nivel de Impacto al Negocio), sin tomar en cuenta los controlesde mitigación por parte del tercero.

Escala AIN

1-Muy Bajo	2-Bajo	3-Medio	4-Alto	5-Mu yAlto

Exposición

Evaluación de Exposición

La exposición al riesgo después de evaluar los controles de seguridad implementados por (Nombre del proveedor) fue catalogada como una exposición (Nivel de exposición)

Exposición

1-Insignificante	2-Aceptable	3-Tolerable	4-Preocupante	5-Mayor

Los criterios numéricos definidos para la variable Exposición se muestran en la tabla Nº 1 adjunta. El evaluador debe seleccionar y asignar el valor que, de acuerdo a su experiencia o juicio profesional, describa la posibilidad de que los controles no implementados generen un suceso o exposición.

Tabla Nº 1 Exposición

Valor	Descripción	Definición
1	Insignificante	La ausencia del control es insignificante para la organización. El control debe asegurarse mediante la existencia de procedimientos, políticas o estándares documentados y actualizados.
2	Aceptable	Es aceptable para la organización. Se requieren comprobaciones para asegurar que se mantiene la eficacia de las medidas de control.
3	Tolerable	Es tolerable para la organización. Se deben tomar medidas para reducir el riesgo, las medidas para reducir el riesgo deben implantarse en un periodo determinado.
4	Preocupante	Es preocupante para la organización. No debe comenzarse la relación contractual con el proveedor hasta que se hayan implementado controles que reduzcan el riesgo.
5	Mayor	No debe comenzar con la relación contractual, en caso de que se tenga una relación contractual existente se deberá suspender, hasta que el riesgo sea reducido a nivel aceptable. En caso de que no sea posible reducir el riesgo, deberá considerar no establecer una relación con este proveedor.

Riesgo Total

El riesgo total estará calculado por el cruce de los valores obtenidos en el Análisis de Impacto al Negocio (Columna AIN) y la exposición, obtenida de acuerdo a la implementación y cumplimiento con los controles de seguridad (Fila Exposición) en la intersección de estos valores se encontrará el riesgo total que representa el proveedor.

Riesgo Total

A - Crítico	B - Alto	C - Medio	D -Bajo

Evaluación de Riesgo Total

De acuerdo a la matriz de riesgos para la evaluación de seguridad informática, el riesgo TOTAL asociado con (Nombre del proveedor) ha sido determinado como (Riesgo Total) de acuerdo a la siguiente escala.

	Exposición				
AIN	**1**	**2**	**3**	**4**	**5**
1	D	D	C	C	C
2	D	C	C	B	B
3	C	C	B	B	A
4	C	B	B	A	A
5	C	B	A	A	A

Alcance.

Dentro de la sección de alcance se deberá hacer referencia a los dominios aplicables durante la Evaluación de Seguridad Informática llevada a cabo para el tercero en cuestión, considerando la versión de 2005 del estándar 27001:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.

6. Gestión de las Comunicaciones y Operaciones.

7. Control de Accesos.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

9. Gestión de Incidentes en la Seguridad de la Información.

10. Gestión de Continuidad del Negocio.

11. Cumplimiento.

Riesgos /Deficiencias.

Los riesgos/deficiencias identificados durante la evaluación se deberán presentarse a manera de resumen en una tabla en la que se indique la Categorización como se muestra en la siguiente imagen.

Tabla de Riesgos

Categoría	No. De Deficiencias identificadas
ALTO	
MEDIO	
BAJO	

Posteriormente se deberá proporcionar el detalle de cada riesgo/deficiencia identificado incluyendo un identificador numeral del riesgo, categoría, dominio ISO, antecedente, riesgo asociado y recomendación.

Riesgos/Deficiencias

Identificador	Categoría	Dominio	Antecedente	Riesgo Asociado	Recomendación
	ALTO				
	MEDIO				
	BAJO				

Definición de Términos

Si bien la clasificación de las deficiencias encontradas se define de acuerdo a la experiencia de evaluador, a continuación, se presenta una definición a alto nivel.

ALTO	Deficiencia considerable o combinación de fallas que podrían ocasionar un impacto considerable.
MEDIO	Deficiencia significativa o combinación de fallas que podrían ocasionar un impacto significante.
BAJO	Menores deficiencias en políticas o procedimientos que estén a cargo de la administración.

4.7 Seguimiento y Cierre de Riesgos/Deficiencias

Debido a que las relaciones con el tercero son del dominio de las Unidades de Negocio o departamento solicitantes de la empresa, es responsabilidad del encargado del departamento asegurar que los riesgos/deficiencias sean mitigadas de acuerdo a la recomendación del auditor, para esta etapa el área de negocio deberá compartir un extracto de las recomendaciones con los terceros. Se sugiere asegurar la remediación de los riesgos de alta prioridad antes de concluir la relación contractual entre la empresa y el tercero. La remediación deberá ser registrada dentro de un plan de trabajo proporcionado por el tercero al responsable de la unidad de negocio, las acciones para solventar los riesgos/deficiencias serán presentar evidencias de implementación o documentación que se apeguen a las recomendaciones, estas evidencias deberán ser evaluadas por el auditor para asegurar que se cumplió con la recomendación.

Los riesgos de prioridad media y baja si bien no se considera necesaria su remediación antes de concluir la relación contractual, deberán reflejar una escala de tiempo aceptable (hasta 90 días) para su remediación.

El plan de Trabajo deberá tener la siguiente estructura:

Datos Generales.

En esta sección se deberá poder identificar, el tipo de evaluación ejecutada, la fecha en que se ejecutó, nombre del evaluador, nombre del proveedor, etc.

DATOS GENERALES

Tipo de Evaluación

Evaluación Remota: [ ] Evaluación en Sitio: [ ]

Fecha de ejecución:	dd/mm/aaaa
Fecha de generación de Reporte:	dd/mm/aaaa
Unidad de negocio:	
Nombre del Evaluador:	
Nombre del Proveedor:	

Registro de Acciones y Evidencias

Para la administración de las deficiencias detectadas en el Plan de Trabajo, se deberá proporcionar el detalle de cada riesgo/deficiencia identificado incluyendo un identificador numeral del riesgo, categoría, dominio ISO, riesgo asociado, recomendación, fecha en la que se tiene planeada la implementación de controles que mitiguen el riesgo, acciones que tomará el proveedor para su mitigación, descripción de la evidencia presentada para cerrar la deficiencia y el status.

Identificador	Categoría	Dominio	Riesgo Asociado	Recomendación	Fecha de Cierre	Accioness	Evidencia de cierre	Status
	ALTO							
	MEDIO							
	BAJO							

4.8 Re-revisiones

Es indispensable mantener un seguimiento de los controles de seguridad implementados por los proveedores que proporcionen servicios a las PyMEs.

Para los impactos 1 a 4 la frecuencia de las revisiones de acuerdo al riesgo total obtenido se recomienda: A – 2 años, B – 3 años, C – 4 años y D – 7 años; para los impactos 5 se recomienda realizar la re-revisión por lo menos de manera anual.

CAPITULO III

DIAGNÓSTICO (Dominios)

Se realiza un diagnóstico de los dominios y controles de seguridad que deberán ser adoptados por los terceros de las Pequeñas y Medianas empresas que almacenen o procesen información de personas físicas. El objetivo principal es definir los controles de seguridad base con los que deberán cumplir los proveedores, de acuerdo al servicio que proporcionen, los terceros deberán apegarse a las recomendaciones para lograr un ambiente seguro, estos controles de seguridad deberán ser implementados por el (os) terceros considerando su naturaleza o giro, el tamaño de la infraestructura y el riesgo que represente para las PyMEs.

1 Política de Seguridad de la Información

Las políticas de Seguridad se basan en el contexto en el que opera una organización y suelen ser considerados en su redacción los fines y objetivos de la organización, las estrategias adoptadas para alcanzar sus objetivos, la estructura y los procesos adoptados por la organización, los objetivos generales y específicos relacionados con el tema de la política y requisitos de las políticas procedentes de niveles más superiores (legales de obligado cumplimiento, del sector al que pertenece la organización, de la propia organización de niveles superiores o más amplios, ...) relacionadas.

La gerencia debería establecer de forma clara las líneas de las políticas de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo

políticas de seguridad en toda la organización. Algunos de los controles que se deberán considerar al evaluar el este dominio se enlistan a continuación.

-Deberá existir una política de seguridad de la información documentada.

-Deberá haber un responsable de actualizar y mantener la política de seguridad.

-Deberá haber procedimientos y políticas documentados que aseguren que la política sea leída y entendida por el personal.

-El personal deberá recibir las políticas por lo menos cada dos meses.

-La política seguridad de la información deberá contener por lo menos:

- Clasificación de la información, manejo de la información según su clasificación y control de accesos considerando: sistemas de control de acceso físico, administración de accesos físicos, accesos para no empleados, seguridad de dispositivos de datos, seguridad de medios físicos, escritorios limpios y destrucción de medios físicos.
- Políticas de seguridad relacionados con los recursos humanos, incluyendo lo siguiente: terminación o cambio de rol de empleados, revisión de antecedentes, confidencialidad.
- Política de seguridad de sistemas y redes, que incluyen lo siguiente: control de accesos, configuraciones, detección prevención de intrusos, auténticas y monitoreo, pruebas de vulnerabilidad y probar su penetración.
- Requisitos de uso aceptable.
- Políticas de Cifrado de Información, en la que se incluya: cuando es requerido el cifrado, métodos y herramientas de cifrado permitidas.

-Las políticas de seguridad deberán ser formalmente revisadas y actualizadas por lo menos una vez por año.

-Las excepciones a las políticas de seguridad deberán ser soportadas por una evaluación y aceptación del riesgo por la Alta Dirección.

2 Organización de la Seguridad de la Información

El objetivo del presente dominio es establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la organización. Para ello se debería definir formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de las políticas de seguridad, la coordinación de la implementación de la seguridad y la asignación de funciones y responsabilidades. Algunos de los controles que se deberán considerar al evaluar el este dominio se enlistan a continuación.

-Debe haber un grupo o persona con la responsabilidad de Seguridad de la Información.

-Debe haber un grupo o persona responsable de vigilar el cumplimiento de las políticas de seguridad de la información.

3 Gestión de Activos de Información

El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos. Algunos de los controles que se deberán considerar al evaluar el este dominio se enlistan a continuación.

-Deberá haber una política documentada respecto a la administración de activos (servidores, equipos de cómputo, aplicaciones, dispositivos de red, etc.).

-Deberá haber un inventario de hardware y software en el que se identifiquen los activos en los que se almacene o procese información.

-Se deberá asignar formalmente a un dueño de los activos de información.

4 Seguridad de los Recursos Humanos

El objetivo del presente dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento. Algunos de los controles que se deberán considerar al evaluar el este dominio se enlistan a continuación.

-Los roles y responsabilidades del personal deberán estar formalmente documentados de acuerdo a la Política de Seguridad de la Información de la empresa.

-Las responsabilidades deberán estar definidas de manera que se permita la segregación de funciones, se deberá considerar que una función no deberá desempeñar dos o más tareas dentro del mismo proceso.

-Deberá existir una política o programa de contratación formalmente documentados.

-La revisión de antecedentes por lo menos deberá considerar: revisión de identidad del candidato, antecedentes escolares y personales y antecedentes criminales.

-Las nuevas contrataciones requieren por lo menos, firmar acuerdos de confidencialidad, uso aceptable y código de ética.

-Deberá haber un programa de concientización en temas de seguridad para todos los empleados, consultores y terceros que estén involucrados en el procesamiento de información.

-Deberá existir un proceso disciplinario documentado para el no cumplimento con políticas de seguridad de la información.

-Deberá existir un proceso formalmente documentado para los cambios de departamento y terminación laboral.

-Deberá existir un proceso documentado para asegurar la eliminación de accesos a la información y los sistemas, en caso de terminación laboral, que incluya: notificación, remoción de accesos y confirmación de la revocación de accesos.

-Debe haber un procedimiento documentado para asegurar la eliminación de accesos a la información y los sistemas, en caso de cambio de rol, que incluya: notificación, remoción de accesos y confirmación de la revocación de accesos.

5 Seguridad Física y Ambiental

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados. Algunos de los controles que se deberán considerar al evaluar el este dominio se enlistan a continuación.

-Todas las ventanas, techos, paredes y puntos de acceso en edificios que almacenen información deberán ser protegidos adecuadamente: no deberán existir ventanas externas, no deberá haber espacios entre el piso, las paredes y el techo, barreras y defensas.

-Deberá haber una política formalmente documentada que requiera que el equipo de TI como estaciones de trabajo y laptops, se bloqueen cuando no se están utilizando o estén sin supervisión.

-Los mecanismos de control de acceso por ejemplo tarjetas de proximidad y sistemas de control de acceso biométrico incluyendo la autorización y la revisión y revocación deberán estar incluidos en una política de seguridad documentada.

-Deberá existir un procedimiento documentad para controlar la perdida de credenciales y factores de autenticación para el control de acceso.

-Los controles de acceso a áreas seguras deberán ser revisados por lo menos cada 6 meses y revocados inmediatamente cuando el acceso no sea requerido.

-El acceso físico por personal externo a la empresa deberá ser restringido, supervisado y revocado inmediatamente cuando no sea requerido.

-Todos los puntos de entrada y salida de las áreas de TI deberán ser registrados y monitoreados.

-El circuito cerrado de televisión (CCTV) deberá ser instalado en áreas en las que se almacene, procese o trasporte información delicada.

-Los videos del CCTV deberán ser almacenados por lo menos durante 90 días.

-Los servidores que alojen información deberán residir en un centro de datos o cuarto de servidores cerrado y de acceso limitado.

-Los controles ambientales del cuarto de servidores o centro de datos deberán ser debidamente monitoreados: aire acondicionado, sistema de detección de incendios, sistema ininterrumpido de energía, extintores, etc.

-Deberán existir políticas de seguridad documentadas que prohíban fumar, beber y comer, dentro del centro de datos.

-SI e centro de datos o cuarto de servidores es compartido, los equipos en los que se aloje la información deberán residir en jaulas o gabinetes cerrados.

-Los medios de almacenamiento externo que contengan información deberán ser almacenados de forma segura y de acceso limitado solo a los que tengan necesidad de negocio.

-Los dispositivos que contengan información como PCs, Laptops o dispositivos de almacenamiento externa no deberán ser extraídos de las instalaciones sin una autorización y aprobación adecuada.

-La información recibida por correo postal o mensajería deberá ser almacenada en un ambiente seguro.

-La información no deberá ser intercambiada a través de Fax.

6 Gestión de las Comunicaciones y Operaciones

Asegurar la operación correcta y segura de los medios de procesamiento de la información mediante el desarrollo de los procedimientos de operación apropiados. Algunos de los controles que se deberán considerar al evaluar el este dominio se enlistan a continuación.

-Deberá tener una política de seguridad documentada que defina el uso y administración de medios de almacenamiento removible.

-Los puertos USB para la conexión de medios de almacenamiento deberán ser deshabilitados o forzados a su cifrado completo.

-La información deberá ser cifrada mientras se encuentre en reposo, sea transmitida o transportada, de acuerdo a los siguientes algoritmos de cifrado (AES, IDEA o Blowfish con una llave de por lo menos 256 bits y PGP con una llave de 2048).

-Deberá existir un procedimiento formalmente documentado respecto a la eliminación y destrucción segura de información, en papel, equipos de cómputo, servidores y en dispositivos de almacenamiento externo.

- Cuando la información cumpla su periodo de retención valido o no se requiera su uso dentro de la organización, deberá ser eliminada de manera segura.

-Debe haber una política formalmente documentada que requiera el respaldo de información.

-Los respaldos de información deberán almacenarse de manera cifrada.

-Todos los respaldos de información deberán almacenarse en una ubicación segura.

-Deberá existir un inventario de respaldos.

-Los respaldos de información deberán ser probados, para a segura la disponibilidad en el momento que se requiera.

-Deberán existir estándares de configuración de plataformas para equipos de cómputo o servidores formalmente documentados.

-Deberá existir un procedimiento para la identificación de nuevas vulnerabilidades o amenazas de seguridad.

-Los Antivirus deberán ser utilizados en estaciones de trabajo o portátiles, así como, en servidores que puedan ser afectados por malware o virus.

-Deberá contar con una política de seguridad documentada referente a software Antivirus.

-Ningún usuario deberá tener facilidades para deshabilitar el software antivirus a excepción de los usuarios con privilegios de administrador.

-El uso de herramientas administrativas deberá ser exclusivo de usuarios administradores.

-La información deberá ser transmitida de manera seguro haciendo uso de protocolos de red seguros (TLS, SSH, IPSec)

-Deberá existir un procedimiento documentado con respecto a pruebas de vulnerabilidad y penetración a la red.

-Se deberá ejecutar de manera anual pruebas de vulnerabilidad y penetración a la red.

-Los accesos a la red deberán ser limitados de acuerdo a las necesidades de negocio (evitar reglas Any to Any).

-Los dispositivos de red deberán ser configurados para denegar todos los accesos por default.

-Todos los accesos a la red deberán ser registrados.

-Deberá haber implementados dispositivos de red para la detección y prevención de intrusos.

-Los eventos de red deberán ser revisados periódicamente como parte de un procedimiento de seguridad.

-Todas las conexiones a la red externa deberán terminar en un Firewall.

-Los accesos web deberán ser administrados a través de una solución de filtrado (proxy).

-El correo electrónico de tipo web, deberá ser bloqueado.

-Los servidores y estaciones de trabajo que procesen o almacenen información no deberán conectarse a más de una red al mismo tiempo.

-Para acceder a un segmento de red se deberá autenticar a través de un modem.

-Debe haber una política de seguridad documentada para redes inalámbricas.

-Las conexiones inalámbricas deben ser autenticadas por protocolos seguros (WPA/WPA2).

-Los accesos a la red inalámbricas deberán ser autenticados por usuarios únicos.

-Todos los accesos a la red inalámbrica deberán ser registrados.

-Deberán ejecutarse escaneos periódicos para los puntos de acceso inalámbricos.

7 Control de Accesos

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento. Algunos de los controles que se deberán considerar al evaluar el este dominio se enlistan a continuación.

-Deberá existir una política documentada de control de accesos en la que se considere por lo menos, uso de cuenta, políticas de construcción de contraseñas, nivel de acceso apropiado de acuerdo a la necesidad de conocimiento, y registros y monitoreo de accesos.

-El control de acceso deberá estar implementado en aplicaciones, sistemas operativos, bases de datos y dispositivos de red, asegurando que los usuarios tengan los mínimos privilegios.

-Deberá haber un procedimiento continuo de revisión de privilegios para validar que todos los accesos son autorizados y cuentan con los privilegios adecuados de acuerdo a las necesidades negocio.

-Todas las cuentas deberán ser asignadas a solo un usuario.

-Los identificadores de usuario deberán ser creados de manera que no revelen el nivel de acceso.

-Las cuentas compartidas deberán estar formalmente documentadas y autorizadas por la alta dirección.

-Las contraseñas deberán apegarse a los siguientes criterios: mínimo 7 caracteres, mayúsculas, minúsculas, números y caracteres especiales.

-Las cuentas de usuario deberán ser bloqueados después de 5 intentos fallidos.

-Las cuentas de usuario deberán ser desactivadas después de 90 días de inactividad.

-Las contraseñas deberán expirar después de 90 días y se deberá requerir a los usuarios su cambio.

-Los sistemas deberán desplegar un aviso, antes de solicitar la autenticación en el que se advierta que los sistemas solo son accedidos por usuarios autorizados y un acceso no autorizado será considerado como un acto criminal.

-Los usuarios deberán ser forzados a cambiar la contraseña en el primer inicio de sesión.

-Debe haber una política que prohíba a los usuarios compartir sus contraseñas.

-Debe haber una política que prohíba a los usuarios almacenar de manera electrónica o en papel sus contraseñas.

-Debe haber una política que requiera que los usuarios y contraseñas por default deben ser cambiados antes de poner un sistema en producción.

-Debe haber un equipo o autoridad dedicados al reseteo de contraseñas.

-Las contraseñas deben ser almacenadas de manera cifrada para evita su divulgación.

-Las contraseñas deberán ser cifradas cuando sean transmitidas por la red.

-La autenticación exitosa o fallida debe ser registrada y revisada.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información. Algunos de los controles que se deberán considerar al evaluar el este dominio se enlistan a continuación.

-Deberá existir un procedimiento formal de administración de cambios, para los cambios en producción.

-Para la implementación de cambios se deberán obtener aprobaciones de múltiples niveles.

-Los cambios o instalación de parches deberán ser probados en un ambiente de pruebas.

-Se deberán ejecutar pruebas de vulnerabilidad por lo menos cada 3 meses para aplicaciones críticas.

-El uso del siguiente software deberá estar restringido: mensajería publica, software para compartir archivos P2P, juegos y software recreativo, cualquier software no autorizado, software recibido de cualquier fuente, software desarrollado por empleados y software distribuido en revistas.

-Deberá ejecutarse una evaluación de riesgos para las aplicaciones de terceros.

9 Gestión de Incidentes en la Seguridad de la Información

El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno. Algunos de los controles que se deberán considerar al evaluar el este dominio se enlistan a continuación.

-Debe haber un procedimiento o programa de administración de incidentes que considere por lo menos: detección del incidente, notificación del incidente, categorización, resolución, registro y reporteo.

-Debe haber un equipo de respuesta a incidentes o eventos de seguridad de la información.

-Se deben documentar los incidentes de seguridad generando una base de conocimientos.

10 Gestión de Continuidad del Negocio

El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad. Algunos de los controles que se deberán considerar al evaluar el este dominio se enlistan a continuación.

-Deberá existir un programa o política de Continuidad de Negocio formalmente documentada.

-Deberá haber un Plan de Contingencia documentado para cada instalación en la que se almacene o procese información.

-EL plan de continuidad deberá ser probado por lo menos 1 vez por año.

-EL sistema interrumpido de energía deberá ser utilizado para los sistemas críticos.

-Todas las instalaciones en las que se almacene información deberán contar con un respaldo de energía.

-Se deberá establecer un tiempo de recuperación objetivo (RTO).

-Se deberá establecer un punto de recuperación objetivo (RPO).

-Se deberá notificar a los clientes como parte del Plan de Continuidad o de Recuperación de Desastres.

-Se deberá definir un árbol de llamadas definido con cada uno de los clientes.

-El árbol de llamadas deberá ser probado por lo menos 1 vez por año.

11 Cumplimiento

El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos. Algunos de los controles que se deberán considerar al evaluar el este dominio se enlistan a continuación.

-Debe haber implementado un proceso para asegurar el cumplimiento con las legislaciones locales que impacten la relación con los terceros, sus clientes o empleados.

-Se deberán ejecutar auditorias periódicas para asegurar cualquier cumplimiento de carácter legal o regulatorio.

-Toda la información recolectada por el tercero, perteneciente a clientes o empleaos deberá tener una necesidad valida de negocio. (Portal ISO 27002, 2005)

CAPITULO IV

PROPUESTA DE CUESTIONARIO PARA LA EVALUACION DE SEGURIDAD INFORMÁTICA.

En la actualidad la información es considerada uno de los objetos de mayor valor para las empresas, no es exagerado decir que las amenazas a la confidencialidad son un tema que cada día preocupa más, debido a que los riesgos se multiplican conforme avanza la tecnología. Es por ello que las PyME tienen la necesidad de identificar sus requerimientos de seguridad, con el propósito de proteger la información registrada, independientemente del lugar en que se localice: impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que la conocen.

La evolución de las empresas y los negocios ha incrementado el uso de la subcontratación de servicios, esto se presenta principalmente cuando se ve reflejado en ahorro de costos y falta de personal especializado para ejecutar una actividad, la subcontratación se debe concebir como una responsabilidad compartida por el cliente y los proveedores de servicios. El esquema de subcontratación implica una relación a largo plazo entre cliente y proveedor: es un compromiso del cual surge una alianza estratégica en la que el cliente acepta el ofrecer al proveedor información clave y estratégica de su negocio para que el proveedor pueda hacer su trabajo. A cambio el proveedor aportará recursos, tecnología, tiempo, personal y esfuerzo para integrarse de manera total al proceso de su cliente (Corporación Universitaria Remington, 2006).

En cumplimiento con la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDP) publicada el 5 de julio de 2010 en el Diario Oficial de la Federación (DOF), la cual tiene como objetivo proteger los datos personales en posesión de los particulares y regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de los individuos.

Se propuso esta Metodología de Seguridad Informática que tiene como base el Análisis de Impacto al Negocio, la clasificación de Datos Personales y Datos Personales Sensibles, así como el cuestionario de seguridad, para fortalecer la protección de datos personales y evitar sanciones que van desde un apercibimiento hasta multas desde los 100 hasta 320,000 días de salario mínimo vigente en el Distrito Federal, por infracciones relativas a datos personales sensibles.

1 Finalidad del Cuestionario de Seguridad

El cuestionario de seguridad propuesto a continuación, se basa en la utilización recomendaciones de las mejores prácticas en la gestión de la seguridad de la información de ISO/IEC 27000 (27001-27002), que es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), estos controles proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Este cuestionario deberá ser compartido con los proveedores y completado por los mismos en un tiempo razonable, se divide en una serie de secciones independientes, en cada una de ellas se tratarán aspectos particulares de la seguridad de la información. La información proporcionada

por los proveedores en este cuestionario será utilizada por las PyMEs para evaluar los controles de seguridad durante la Evaluación de Seguridad Informática y se utilizarán como una declaración por parte del proveedor.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. El número total de controles suma 144 entre todas las secciones, aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

A continuación, se describe la aplicabilidad y controles de seguridad considerados para cada dominio:

1.1 Política de Seguridad de la Información (PSI).

Dentro del dominio PSI se consideraron 3 subdominios y 9 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los impactos 1 y 2 solo serán aplicados los controles PS-100, 101, 103 y 108.

1.1.1 Administración y Soporte para la Seguridad de la Información

PSI-100	D1.1	Administración y Soporte para la Seguridad de la Información	Existe una política de Seguridad Documentada?
PSI-101			Hay una persona que le de mantenimiento y revise la Politica de Seguridad?
PSI-102			Se realiza una revisión y aprobación formal por la gerencia de las Políticas de Seguridad por lo menos anualmente?
PSI-103			Tiene procedimientos que seguren que la Política es leida por todo su personal?
PSI-104			Se proporcionan las políticas al personas por lo menos cada 12 meses?

1.1.2 Clasificación de la Información

PSI-105	D1.2	Clasificación de la Información	Cuenta con una política de clasificación de la Informaión documentada?
PSI-106			Existen procedimientos que incluyan los métodos para el manejo de información de acuerdo a su clasificación?

1.1.3 Uso Aceptable y Excepciones

PSI-107	D1.3	Uso aceptable y Excepciones	Dentro de la política se cubren los requisitos de uso aceptable?
PSI-108			Para las excepciones a la polìtica se requiere hacer una evaluación formal de riesgo?

1.2 Organización de la Seguridad de la Información

Dentro del dominio OSI se consideraron 3 subdominios y 11 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los impactos 1 y 2 solo serán aplicados los controles OSI-103, 104, 106, 107 y 108.

1.2.1 Dirección de la administración y soporte para la Seguridad de la Información

OSI-100	D2.1	Dirección de la administración y soporte para la Seguridad de la Información	Existe una persona o equipo que tenga la responsabilidad directa de la Seguridad de la Información dentro de su organización?
OSI-101			Existe una persona o equipo responsable de asegurar el cumplimiento de las polìticas de seguridad (ej. Auditoria Interna)?
OSI-102			Realiza revisiones de seguridad de la información a su organización independientes del personal de TI?

1.2.2 Dispositivos Móviles

OSI-103	D2.2	Dispositivos Móviles	Existe una política relacionada a la regulación de dispositivos móviles proporcionados por la compañía o de propiedad del personal?
OSI-104			Los dispositivos se bloquean de manera automática después de un periodo de inactividad, requieriendo de una contraseña para su desbloqueo?
OSI-105			Los dispositivos móviles son administrados de manera centralizada con la finalidad de prevenir la escalación de privilgeios o la instalación de aplicaciones no autorizadas?
OSI-106			Los datos almacenados en dispositivos móviles se encuentran cifrados?
OSI-107			La actualización de los dispositivos, incluyendo parches de seguridad son requeridos?
OSI-108			Se requiere software anti-malware para dispositivos en riesgo de una infección?

1.2.3 Administración Remota

OSI-109	D2.3	Administración Remota	Se encuentra implementada la función de localización remota para los dispositivos de la compañía?
OSI-110			De manera remota, los dispositivos de la compañía pueden ser deshabilitados o la información que contienen puede ser borrada?

1.3 Gestión de Activos de Información.

Dentro del dominio GAI se consideraron 3 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los impactos 1 y 2 no es mandatorio aplicar este dominio.

GAI-100			Tiene una política o programa de gestión de activos de información implementado para inventariar servidores, aplicaciones, estaciones de trabajo, dispositivos de red, etc.?
GAI-101			Tiene un inventario actual documentado de activos hardaware y software para almacenar y/o procesar información de sus clientes?
GAI-102			Se asignan formalmente los dueños de los activos de información?

1.4 Seguridad de los Recursos Humanos.

Dentro del dominio SRH se consideraron 6 subdominios y 16 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los impactos 1 y 2 solo serán aplicados los controles SRH-103, 104, 107, 112, 113 y 115.

1.4.1 Roles y Responsabilidades

SRH-100	D4.1	Roles y Responsabilidades	Se definen y dcoumentan los roles y responsabilidades de seguridad de acuerdo con la política de seguridad de la información de la organización?
SRH-101			Se definen los roles y responsabilidades de seguridad de manera que haya una segregación de funciones apropiada?
SRH-102			Incluyen las descripciones de puestos una definición o especificación de sus responsabilidades relacionadas a la seguridad de la información?

1.4.2 Selección y Reclutamiento

SRH-103	D4.2	Seleeción y Reclutamiento	Se tiene una política o programa implementada de selección y recluetamiento de personal?
SRH-104			El programa de selección y reclutamiento considera por lo menos revisar: antigüedad en domicilio, verificación de empleo anterior, grado de estudios comprobados, referencias creditias, etc.
SRH-105			Se incluye una revisión de identidad dentro de la pre-selección de candidatos?
SRH-106			Se incluye una revisión de antecedentes penales dentro de la pre-selección de candidatos?

1.4.3 Acuerdos

SRH-107	D4.3	Acuerdos	Se requiere que el personal de nuevo ingreso firme un acuerdo de confidencialidad o no divulgación?
SRH-108			Se requiere que el personal de nuevo ingreso firme un acuerdo de uso aceptable?
SRH-109			Se requiere que el personal de nuevo ingreso firme un acuerdo de código de ética?

1.4.4 Capacitación

SRH-110	D4.4	Capacitación	Se tiene un programa de concientización y capacitación en seguridad de la información?
SRH-111			Se requiere que sus empleados participen en capacitaciones anuales de seguridad de la información?

1.4.5 Incumplimiento

SRH-112	D4.5	Incumplimiento	Se tiene documentado un proceso disciplinario por no cumplimiento con las política de seguridad de la información?

1.4.6 Terminación

SRH-113	D4.6	Terminación	Tiene una política o proceso documentado para las terminaciones de empleo, cambio de estátus, función o departamento?
SRH-114			Tiene un procedimiento implementado para asegurar la adecuada eliminación de los accesos a información de sus clientes ante una terminación o cambio de funciones? El proceso deberá incluir lo siguiente: Notificación, eliminación y confirmación de la revocación de acceso.
SRH-115			Se requiere que el personal regrese todos los actvos de TI en su posesión una vez que se presenta la terminación de empleo o cambio de área?

1.5 Seguridad Física y Ambiental.

Dentro del dominio SFA se consideraron 4 subdominios y 20 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los impactos 1 y 2 solo serán aplicados los controles SFA-100, 112, 113, 114, 116, y 117.

1.5.1 Controles de Seguridad Física

SFA-100	D5.1	Controles de Seguridad Física	Están potegidas las ventanas, techos, paredes y puntos de acceso alos edificos que almacenan información con medidas adecuadas?
SFA-101			Se revisa el acceso físico a las áreas seguras cuando menos cada 6 meses y se revoca inmediatamente cuando ya no es requerido?
SFA-102			Se restringe y supervisa el acceso fisico por personal externo ademas de revocarse cuando ya no es requerido?
SFA-103			Se registran y revisan los accesos en los puntos de entrada y salida de las áreas seguras de TI?
SFA-104			Se tiene instalado un circuito cerrado de televisión en áreas en que se almacene, procese o transporte información?
SFA-105			Se almacenan cuando menos 90 días las grabaciones del sistema CCTV?
SFA-106			Los servidores que contienen información residen en un centro de datos con acceso limitado?
SFA-107			Si el centro de datos es compartido con otros arrendatarios, los equipos que contienen información residen en un gabinete cerrado?

1.5.2 Controles Ambientales

SFA-108	D5.2	Controles Ambientales	Son monitoreados los controles ambientales dentro del centro de datos?
SFA-109			Tiene medidas de detección y supresión de fuego en el centro de datos?
SFA-110			Está prohibido fumar, comer e ingerir bebdas en el centro de datos?
SFA-111			Las áreas en las que se procesa información están protegidas contra amenazas de incendio, inundación, terremotos, explosiones, motines y otros desastres naturales o provocados por el hombre?

1.5.3 Medios de Almacenamiento externo

SFA-112	D5.3	Medios de Almacenamiento Externo	Los medios de almacenamiento que contienen información se mantienen en un ambiente seguro con acceso limitado?
SFA-113			Tiene restricciones para llevar dispositivos que contengan información fuera de sus intalaciones sin la autorización adecudad?
SFA-114			Tiene procedimientos para la eliminación y/o destrucción de medios físicos?
SFA-115			Cuando los dispositivos que almacenan información ya no son utilizados se dejan iegibles antes de sacarlos de las instalaciones?
SFA-116			Tiene una política implementada que requiera que el equipo de TI sea bloqueado asegurado cuando no esté bajo supervisión?

1.5.4 Información en Papel

SFA-117	D5.4	Información en Papel	Se procesa o almacena nformación recibida vía correo postal en un ambiente seguro?
SFA-118			Tiene controles implementados para prevenir que se intercambie información vía Fax?
SFA-119			La información impresa en papel es resguardada en un ambiente seguro?

1.6 Gestión de las Comunicaciones y Operaciones.

Dentro del dominio GCO se consideraron 6 subdominios y 43 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los impactos 1 y 2 solo serán aplicados los controles GCO-104, 106, 118, 121, 123, 124, 127, 128, 131, 132, 133, 135, 137, 140 y 141.

1.6.1 Escaneos de vulnerabilidades y Pruebas de penetración

GCO-100	D6.1	Escaneos de Vulnerabilidades y Pruebas de Penetración	Se tiene un proceso de Escaneo de Vulnerabilidades?
GCO-101			Se tiene un proceso para identificar nuevas amenazas y vulnerabilidades de seguridad?
GCO-102			Se lleva a cabo evaluaciones de vulnerabilidad o pruebas de penetración al ambiente de TI por lo menos 1 vez por año?
GCO-103			Se realizan pruebas al código, cambios, parches en plataformas de desarrollo o de control de calidad previo a su implementación?

1.6.2 Antivirus

GCO-104	D6.2	Antivirus	Se utilizan productos Antivirus en servidores y estaciones de trabajo?
GCO-105			Se tiene una política o proceso documentado de antivirus / antimalware?
GCO-106			Es posible para los usuarios inhabilitar el software antivirus?

1.6.3 Respaldos de Información

GCO-107	D6.3	Respaldos de Información	Se tiene una política o proceso documentado que requiera que la información sea respaldada?
GCO-108			Los medios de almacenamiento de respaldo son almacenados fuera de las instalaciones?
GCO-109			Los respaldos de información fuera de las instalaciones son almacenados en una ubicación segura?
GCO-110			Cuenta con un inventario actualizado de respaldos?
GCO-111			Se aplican pruebas a los respaldos para garantizar que se podrán recuperar cuando sea necesario?

1.6.4 Seguridad de la Red

GCO-112	D6.4	Seguridad de la Red	Se mantiene un registro de todos los acceos a la red?
GCO-113			Los eventos de la red son revisados?
GCO-114			Se registran los accesos a través de redes inalambricas?
GCO-115			Se cuenta con una solución de administración de eventos implementada?
GCO-116			Se cuenta con una política de acceso remoto?
GCO-117			El acceso a la red est limitado solo para puertos y protocolos requeridos?
GCO-118			Se tiene acceso a la información utilizando protocolos seguros (SFTP, TL, SSH, etc.)?
GCO-119			Los dispositivos de red se encuentran configurados para denegar los accesos por defecto?
GCO-120			Se cuenta con sistemas de detección y prevención de intrusos?
GCO-121			Todas las conexiones a la red externas se encuentran protegidas por un Firewall?
GCO-122			El acceso remoto requiere autenticación de doble factor?
GCO-123			La información es almacenada en todo momento en equipos de la empresa?
GCO-124			Se asegura que los equipos de cómputo no administrados por la compañía se conecten a la red interna?
GCO-125			Los cambios a sistemas operativos y aplicaciones son probados antes de ser puestos en producción?
GCO-126			Los requerimientos de seguridad son considerados para cualquier cambio en el hardware, software o ambiente de TI?
GCO-127			Se cuenta con políticas para el uso de redes inalámbricas?
GCO-128			Las conexiones inalámbricas son autenticadas utilizando WPA/WPA2?
GCO-129			Se utiliza una segmentación de la red mediante firewalls para restringir el tráfico?

1.6.5 Configuración de Equipos

GCO-130	D6.5	Configuración de Equipos	Se tiene un procedimiento para lograr la configuración segura de equipos de cómputo, laptops, servidores y dipositivos de red?
GCO-131			Se restringe el acceso a herramientas de administración a usuarios con privilegios estándar?
GCO-132			El acceso a internet es administrado por una solución de filtrado web?
GCO-133			Se bloquea el acceso a cuentas de correo de tipo web?
GCO-134			Los servidores o equipos de trabajo están configurados para prohibir que se conecten a mas de una red al mismo tiempo?
GCO-135			Los puertos USB están deshabilitados o son protegidos física y lógicamente contra acceso no autorizado?
GCO-136			Cuenta con herramientas de prevención de perdida de datos?
GCO-137			Se encuentra restringido el uso del siguiente software; mensajería instantanea, aplicaciones para compartir archivos P2P, juegos, etc.

1.6.6 Cifrado

GCO-138	D6.6	Cifrado	Cuenta con una política de Cifrado de información en la que se establezca, cuando es requerido el cifrado y los métodos o herramientas utilizados?
GCO-139			Los respaldos de información se encuentran cifrados?
GCO-140			La información está cifrada mientras se encuentra almacenada en servidores, estaciones de trabajo, laptops o medios de almacenamiento extraible?
GCO-141			La información está cifrada cuando es transmitida fuera de la red de la compañía?
GCO-142			La información está cifrada cuando es transportada fuera de las instalaciones de la compañía?

1.7 Control de Accesos.

Dentro del dominio CA se consideraron 4 subdominios y 24 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los

impactos 1 y 2 solo serán aplicados los controles CA-100, 101, 103, 104, 105, 110, 112, 113, 114, 115, 116, 117, 121 y 123.

1.7.1 Políticas de Control de Accesos

CA-100	D7.1	Políticas de Control de Accesos	Cuenta con una política de control de accesos en la que se considere por lo menos: uso de cuenta y contraseñas, acceso apropiado y registro de accesos?
CA-101			La política requerie que se tengan controles de acceso para aplicaciones, sistemas operativos, bases de datos y dispositivos de red con los menores privilegios requeridos?
CA-102			Existe un proceso para otorgar y aprobar todos los accesos a los sistemas que almacenen, procesen o transporten información?
CA-103			Existe una política que prohiba que los usuarios compartan sus contraseñas?
CA-104			Existe una política que prohiba que los usuarios escriban o mantengan en papel sus contraseñas?
CA-105			Existe una política o procedimiento que requiera que las contrseñas de fábrica sean removidas, deshabilitadas o cambiadas antes de que el dispositivo o sistema sea puesto en producción?
CA-106			Todas las peticiones para la creación, cambio y eliminación de privilegios son documentadas y se mantienen por un periodo mínimo de 6 meses?

1.7.2 Registro y Revisión de Accesos

CA-107	D7.2	Registro y revisión de accesos	Se registran y archivan todas las solicitudes aprobadas para otorgar accesos?
CA-108			Se tiene una revisión periódica para revalidar que todos los accesos están autorizados y tienen una justificación legitima de negocio?
CA-109			Las actividades del uso de cuentas adinistrativas en los sitemas son atribuibles a una sola persona?
CA-110			Se documenta y autorizaformalmente por la gerencia el uso de identificadores compartidos?
CA-111			Todos los accesos exitososo y fallidos se encuentran registrados y son revisados?
CA-112			Se prohibe a los usuarios finales tener privilegios de administrador en sus computadoras o laptops?

1.7.3 Identificadores de usuario y construcción de contraseñas

CA-113	D7.3	Identificadores de usuario y construccion de contraseñas	Los identificadores de usuarios son creados de manera que no revelen el nivel de aceso asignado?
CA-114			Los requerimientos de construcción de contraseñas seguras para los sistemas que almacenan, procesan o transportan información, cumplen con los siguientes puntos? Longitud (mínimo 7 caracteres), Complejidad (por lo menos 3 de los siguientes 4: mayúsuculas, minúsculas, números y caracteres especiales)
CA-115			Las cuentas de usuario son bloqueadas después de 5 intentos fallidos de acceso?
CA-116			Las cuentas de usuario son desactivadas tras 90 días de inactividad?
CA-117			Las contraseñas expiran a menos cada 90 días requiriendo al usuario el cambio de la misma?
CA-118			Los sitemas despliegan una advertencia al usuario antes de otorgar el acceso, indicando que los sistemas solo pueden ser accedidos por usuarios autorizados o que cualquier acceso no autorizado puede ser considerado un acto criminal en ciertas jurisdicciones?
CA-119			Las contraseñas se encuentran almacenadas de manera cifrada a modo de prevenir su fácil divulgación?
CA-120			Las contraseñas se encuentran cifradas cuando son transmitidas a través de la red?
CA-121			Se autentica el acceso directo a sistemas operativos?
CA-122			Las sesiones del sistema operativo se desconectan después de un determinado periodo de inactividad?

1.7.4 Reseteo de contraseñas

CA-123	D7.4	Reseteo de contraseñas	La autoridad o responsabilidad del reseteo de contraseñas se encuentra restringida a persona autorizadas o se realiza a través de una herramienta automatizada?

1.8 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

Dentro del dominio ADMSI se consideraron 8 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los impactos 1 y 2 no es mandatorio aplicar este dominio.

ADMSI-100			Existe una política referente al ciclo de vida de desarrollo de sistemas?
ADMSI-101			El acceso al código fuente e los programas se encuentra restringido solo a personal de desarrollo?
ADMSI-102			Se llevan a cabo pruebas de los controles de seguridad como parte de las pruebas de la aplicación?
ADMSI-103			Se llevan a cabo validaciones automáticas de datos para detectar valores fuera de rango, caracteres invalidos o datos incompletos?
ADMSI-104			Las aplicaciones mantienen pistas de auditoria de las actividades?
ADMSI-105			Las aplicaciones residen en servidores dedicados o sistemas que cumplan una función?
ADMSI-106			Se cuenta con una metodología y procedimientos documentados para el desarrollo de software?
ADMSI-107			Se mantiene un ambiente de desarrollo segregado?

1.9 Gestión de Incidentes en la Seguridad de la Información.

Dentro del dominio GIS se consideraron 5 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los impactos 1 y 2 solo serán aplicados los controles GIS-102.

GISI-100			Cuenta con una política o procedimiento de manejo de incidentes de seguridad, que considere su identificación, notificación, clasificación, resolución y reporte?
GISI-101			Existe un equipo de respuesta a incidentes de seguridad?
GISI-102			Cuenta con un procedimiento para notificar a sus clientes a cerca de cualquier incidente de seguridad que se presente en su compañía?
GISI-103			Se mantiene la documentación de los incidentes?
GISI-104			Existe un proceso para que la información obtenida durante los incidentes de seguridad sea utilizada para reducir la probabilidad de futuros incidentes?

1.10 Gestión de Continuidad del Negocio.

Dentro del dominio GCN se consideraron 5 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los impactos 1 y 2 solo serán aplicados los controles GCN-100.

GCN-100			Cuenta con un programa implementado de Continuidad del Negocio?
GCN-101			Cuenta con un programa de Contingencia y/o Recuperación de Desastres implementado?
GCN-102			Prueba de manera regular (por lo menos cada 12 meses) su Plan de Continuidad del Negocio?
GCN-103			Notifica a sus clientes como parte del programa de Recuperación de Desastres?
GCN-104			Cuenta con un arbol de llamadas definido para cada uno de sus clientes?

1.11 Cumplimiento.

Dentro del dominio C se consideraron 4 controles de seguridad, para los impactos 3, 4 y 5 se deberán aplicar todos los controles según se considere, mientras que para los impactos 1 y 2 solo serán aplicados los controles GCN-102 y 103.

C-100			Cuenta con un proceso implementado para asegurar el cumplimiento con requerimientos legislativos y regulatorio que impactan la relación con sus clientes?
C-101			Se realizan auditorias para asegurar el cumplimiento con cualquier requerimiento legal o regulatorio?
C-102			Toda la información que solicita a sus clientes tiene una necesidad legitima de negocio?
C-103			Se destruye o elimina información (en papel o en formato electrónico) obtenida de sus clientes al final de su periodo de renteción?

De acuerdo a los controles de seguridad propuestos por dominio y subdominio, para las evaluaciones de seguridad informática aplicadas a proveedores con impactos 3,4 y 5 se aplicará un total de 144 controles, mientras que para los proveedores con impacto 1 y 2 se aplicarán 52 controles de seguridad como se muestra en la siguiente tabla. (SeguInfo dominios 27001 y 27002, 2010)

Dominio	AIN 3-4-5	AIN 1-2
PSI	9	4
OSI	11	5
GAI	3	0
SRH	16	6
GCO	20	6
CA	43	15
ADMSI	24	14
GIS	8	0
GCN	5	1
CA	5	1
Total	**144**	**52**

2 Estructura del Cuestionario de Seguridad

El cuestionario de seguridad deberá tener una estructura clara, por lo que deberá contar con información que le permita completar el cuestionario de manera adecuada, en la primera sección se deberá poder identificar información con respecto a los controles requeridos y el dominio al que pertenecen.

ID	Sección	Dominio / Subdominio	Control

Es responsabilidad del proveedor responder al nivel de implementación de cada uno de los controles, así como la descripción detallada de las medidas que se consideran para cada uno de los controles de seguridad.

Implementaciòn			Descripciòn del control
SI	Parcial	NO	

De igual forma se deberá considerar una sección para que el evaluador pueda describir los controles revisados durante la Evaluación de Seguridad Informática, así como, las evidencias que sustenten la implementación de los controles.

Comentarios del Evaluador	Evidencias Presentadas

La información proporcionada en este cuestionario será utilizada por las PyMEs para evaluar los controles de seguridad implementados al momento de la evaluación y podrán ser consultados para cualquier trabajo que haya de realizarse.

Aportaciones

La propuesta de una Metodología de Evaluación de Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas (PyMEs), que accedan a información de Personas Físicas tiene como fin evaluar y mejorar la eficacia y eficiencia de una organización, los sistemas de TI deben estar sometidos a controles de calidad y auditoría informática debido a que las computadoras y los centros de procesamiento de datos son susceptibles a los delitos informáticos, la delincuencia y el terrorismo.

Sus beneficios son:

- Cuidado y mejora de la imagen pública.
- Generación de confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Genera un balance de los riesgos en TI.

Las fases que componen la metodología propuesta de auditoría informática son:

a) Planear, obtener y entender los procesos de negocio.
b) Analizar y evaluar los controles de seguridad implementados para determinar la probable efectividad y eficiencia de los mismos.
c) Aplicación de pruebas para verificar la efectividad de los procedimientos de control.

d) Informar los resultados de la auditoría, con el fin de reportar las sugerencias correspondientes a las oportunidades de mejora encontradas
e) Efectuar el seguimiento para evaluar el nivel del cumplimiento y el impacto de las recomendaciones realizadas.

El objetivo de llevar a cabo esta metodología es que las organizaciones aseguren que sus procesos de negocio y nuevos proyectos en conjunto con los constantes cambios de las tecnologías de información cubran las necesidades de sus clientes de manera eficiente y oportuna y al mismo tiempo ayude a cumplir con las disposiciones generales de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares certificando que los proveedores de las empresas aplicables proporcionen un tratamiento adecuado a la información que garantice su uso para los fines convenidos dentro del marco de un contrato.

Para alcanzar la Propuesta de la Metodología de Evaluación de Seguridad Informática, aplicada a Proveedores de Servicios de Pequeñas y Medianas Empresas (PyMEs), que accedan a información de Personas Físicas, es indispensable conocer la naturaleza de las organizaciones y hacer un análisis de riesgos y posibles amenazas sobre la información, identificando, analizando y diseñando controles de seguridad, ofreciendo a las empresas un estudio de su esquema de seguridad en relación a la norma ISO 27000.

TERMINOS Y DEFINICIONES

Para los propósitos de este documento se citan los siguientes términos y definiciones:

Activo cualquier elemento que tenga un valor para la organización [ISO/IEC 13335-1:2004]

Amenaza causa potencial de un incidente no deseado que puede producir daño a un sistema u organización [ISO/IEC 13335-1:2004]

Análisis de Riesgo uso sistemático de información para identificar las fuentes y estimar el riesgo [ISO/IEC Guide 73:2002]

Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema [http://es.scribd.com/bonyfer9306/d/6079889-Seguridad-Informatica]

Control significado de manejo del riesgo. Medios que auxilian a la administración de los riesgos, incluso las políticas, los procedimientos, las pautas, prácticas o estructuras organizacionales que pueden ser de tipo administrativo, técnico, de gestión, o de naturaleza legal. Nota *La palabra control se usa como un sinónimo para resguardo o contramedida*.

Evaluación del Riesgo el proceso de comparar el riesgo estimado contra el criterio de un riesgo dado determina la importancia del riesgo [ISO/IEC Guide 73:2002]

Evento de Seguridad de la Información es una ocurrencia identificada de un sistema, servicio o estado de la red indicando una posible brecha de la política de seguridad de información o fracaso de sus resguardos, o una situación previamente desconocida que puede ser pertinente a la seguridad. [ISO/IEC TR 18044:2004]

Facilidades de Procesamiento de Información cualquier sistema de procesamiento de información, servicio o infraestructura, o las localidades físicas que los alojan.

Gestión del Riesgo las actividades coordinadas para dirigir y controlar una organización con respecto al riesgo Nota *La gestión del Riesgo incluye típicamente valoración de riesgo, tratamiento de riesgo, aceptación de riesgo y comunicación del riesgo*. [ISO/IEC Guide 73:2002]

Impacto: medir la consecuencia al materializarse una amenaza. [http://es.scribd.com/bonyfer9306/d/6079889-Seguridad-Informatica]

Incidente de Seguridad de Información un incidente de seguridad de la información se indica por un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio mediante las amenazas a la seguridad de la información. [ISO/IEC TR 18044:2004]

Pauta una descripción que clarifica lo que debe hacerse y cómo, para el logro de los objetivos establecidos en las políticas [ISO/IEC 13335-1:2004]

Política intención y dirección global como formalmente fue expresada por la gerencia o administración.

Riesgo combinación de la probabilidad de un evento y su consecuencia [ISO/IEC Guide 73:2002]

Riesgo Residual riesgo remanente luego de una amenaza de seguridad [ISO/IEC Guide 73:2002]

Seguridad de Información, preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades, fuertemente relacionadas tales como la autenticidad, la responsabilidad, non-repudio, y fiabilidad también pueden ser involucradas.

Sistema Informático: Un sistema informático es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: hardware, software y las personas que lo usan. [http://www.alegsa.com.ar/Dic/sistema%20informatico.php]

Tercera Parte esa persona o institución que se reconocen como un ser independiente de las partes involucradas, con respecto a un problema, trabajo o labor en cuestión [ISO/IEC Guide 2:1996]

Tratamiento del Riesgo proceso de selección y aplicación de medidas para modificar el riesgo [ISO/IEC Guide 73:2002]

Valoración del Riesgo proceso global de análisis de riesgo y evaluación de riesgo [ISO/IEC Guide 73:2002]

Vulnerabilidad una debilidad de un recurso o grupo de recursos que pueden explotarse por uno o más amenazas [ISO/IEC 13335-1:2004]

Riesgo es la vulnerabilidad ante un potencial perjuicio o daño para las unidades, personas, organizaciones o entidades. [https://www.auditool.org]

Riesgo inherente, es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior. Este riesgo surge de la exposición que se tenga a la actividad en particular y de la probabilidad que un choque negativo afecte la rentabilidad y el capital de la compañía. El riesgo inherente es propio del trabajo o proceso, que no puede ser eliminado del sistema; es decir, en todo trabajo o proceso se encontrarán riesgos para las personas o para la ejecución de la actividad en sí misma. [https://www.auditool.org]

Riesgo residual, es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel de riesgo al que está sometido una compañía nunca puede erradicarse totalmente. Por ello, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar o mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable). El riesgo residual puede verse como aquello que separa a la compañía de la seguridad absoluta.

El riesgo residual es aquél que permanece después de que la dirección desarrolle sus respuestas a los riesgos. El riesgo residual refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la dirección para mitigar el riesgo inherente. [https://www.auditool.org]

REFERENCIAS.

-Academia Latinoamericana de Seguridad Informática (2009) – "Unidad 1 Introducción a la Seguridad Informática" - Modulo 1 (Consultado, agosto 2011) http://carolinacols.files.wordpress.com/2012/03/fundamentos-bc3a1sicos-de-seguridad-informc3a1tica.pdf

-Escuela Colombiana de Ingeniería Julio Garabito (2008) "Seguridad y Protección de la Información", Introducción a los Conceptos de Seguridad de la Información. Fascículo 2 https://docs.google.com/:profesores.is.escuelaing.edu.co (Consultado, agosto 2011)

-Universidad Nacional del Nordeste Argentina U.N.N.E (2001) "Seguridad de la Información" Seguridad de los Sistemas Operativos http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGUNIX012.htm (Consultado, septiembre 2011)

-Empresa Oficial de Servicios Públicos de Yumbo Colombia (2010) "Seguridad Informática" http://www.espyumbo.com/portalespy/index.php?option=com_content&view=article&id=78:seguridad-informatica&catid=41:notibanner (Consultado Agosto 2011)

-Poder Judicial Republica de Honduras (2003) "Infotecnología" www.poderjudicial.gob.hn/institucional/organizacion/dependencias/infotecnologia/documents (Consultado, abril 2011)

-Universidad de las Américas Puebla (2000) "Conceptos Básicos de Seguridad Informática"http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf (Consultado, septiembre 2011)

-Simson Garfinkel and Eugene H. Spafford (1996)" Practical Unix & Internet Security" http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node12.html (Consultado, septiembre 2011)

-Seguridad de la Información Segu-Info (2005) "Amenazas Lógicas – Tipos de Ataques" http://www.segu-info.com.ar/ataques/ataques.htm (Consultado, agosto 2011)

-HOWARD, John D. (1989-1995) "Thesis: An Analysis of security on the Internet. Carnegie Institute of Technology. Carnegie Mellon University. 1995. EE.UU. http://www.cert.org. Capítulo 12–Página 165

-David Luis de la Red Martínez (2001) "Seguridad de Sistemas" http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGUNIX012.htm (Consultado, septiembre 2011)

-Universidad de Cuautitlán Izcalli (2009) "Delitos Informáticos en México y el Mundo" http://www.delitosinformaticos.mx/blog/ (Consultado, septiembre 2011)

-Organización de los Estados Americanos (2001) "Manual de Delitos Informáticos"

http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf - Manual de Delitos Informáticos: Generalidades Dr. Santiago Acurio del Pino (Consultado, agosto 2011)

-Nazario García Fernández, Alberto Gómez Gómez, Isabel Fernández Quesada, José Parreño Fernández. (2002) "Aspectos Relevantes del proceso de Contratación de Servicios" http://www.adingor.es/Documentacion/CIO/cio2002/5%20Log%C3%ADstica/C067.pdf (Consultado, octubre 2011)

-Corporación Universitaria Remington (2006) "La Subcontratación como Herramienta para la Gestión" http://www.authorstream.com/Presentation/aSGuest16774-175602-subcontratacion-outsourcing-la-subcontrataci-como-herramienta-para-gesti-log-stica-entertainment-ppt-powerpoint/ (Consultado, octubre 2011)

-Deloitte (2011) "Ley Federal de Protección de Datos Personales en Posesión de Particulares" - pag.3 - www.deloitte.com (Consultado, septiembre 2011)

-Ernest & Young (2011) "Nueva legislación en materia de protección de datos personales" www.ey.com (Consultado, octubre 2011)

-ISO 27000 (2005) "Sistema de Gestión de la Seguridad de la Información" http://www.iso27000.es/sgsi.html (Consultado, septiembre 2011)

-Viega J., (2001), "Building Secure Software: How to avoid security problems the right way".

-Alejandro Corletti, Director de Seguridad Informática de NCS, (2008) http://www.laflecha.net/canales/seguridad/articulos/metodologia-de-implantacion-y certificacion-de-iso27001/ 20 Mar 2008 (Consultado, septiembre 2011)

-Dejan Kosutic (2010) "Lista de Apoyo para Implementación de ISO 27001" http://blog.iso27001standard.com/es/2010/09/28/lista-de-apoyo-para-implementacion-de-iso-27001/ (Consultado, septiembre 2011)

-Omar Alejandro Herrera Reyna (2007), "Comentarios, Experiencias y Tips sobre Seguridad de la Información", Candado digital, http://candadodigital.blogspot.mx/2007/10/la-funcin-de-seguridad-informtica-en-la.html#!/2007/10/la-funcin-de-seguridad-informtica-en-la.html (Consultado, septiembre 2011)

-ASS. Borghello, Cristian Fabian (2001) "Seguridad Informática sus Implicancias e Implementación" Universidad Tecnológica Nacional.

http://wwwisis.ufg.edu.sv/wwwisis/documentos/EB/005.8-B644s__Seguridad%20informatica.pdf (Consultado, agosto 2011)

-Jorge Mieres (2009), Evil Fingers "Ataques Informáticos, Debilidades de Seguridad comúnmente explotadas" https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf (Consultado, octubre 2011)

-Política Digital, Innovación gubernamental, Nesxos (2007), "Outsourcing, ¿Qué es?, ¿Para que sirve?, ¿Cómo se hace?" ISSN 1665-1669, No. 40 http://www.politicadigital.com.mx/pics/edito/multimedia/481/num_40_multimedia.pdf, (Consultado, septiembre 2015)

-Asociación de economía aplicada, C. Aybar Arias / A. Casino Martínez / J. López García (2003) "Estrategias de Estructura y Capital en la PYME: Una aproximación empírica", Estudios de Economía aplicada, abril, año/ vol 21 / numero 001 , Madrid España http://redalyc.uaemex.mx/ redalyc/pdf/301/30121108.pdf Consultado 15 09 2012

-ITIL V3 Gestión de Servicios (2011) http://itilv3.osiatis.es/estrategia_servicios_TI/introduccion_objetivos_proveedores_servicios.php (Consultado, septiembre 2015)

-Instituto Federal de Acceso a la información y Protección de Datos, Secretaria de Datos Personales, Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2014) http://inicio.ifai.org.mx/nuevo/Gu%C3%ADa%20obligaciones%20de%20la%20LFPDPPP.pdf (Consultado, febrero 2017)

-Portal de ISO 27002 http://www.iso27000.es/iso27002.html (Consultado, febrero 2017)

-Innovaciòn y Gestón de recursos Técnicos (2016) http://ingertec.com/isso-223301-consejos-para-la-realizacion-del-bia/ (Consultado, febrero 2017)

-SeguInfo dominios ISO 27001 y 27002 (2010) https://seguinfo.wordpress.com/2010/06/28/dominios-de-iso-27001-e-iso-27002/ (Consultado, febrero 2017)