Biblioteca INFOTEC

Ciudad de México, a 17 de febrero de 2025

VISTO BUENO DE TRABAJO TERMINAL

Maestría en Gestión de Innovación de las Tecnologías de Información y Comunicación (MGITIC)

UNIDAD DE POSGRADOS
PRESENTE

Por medio de la presente se hace constar que el trabajo de titulación:

"Gobierno de Seguridad Informática a través de la implementación de un framework"

Desarrollado por la alumna: **Claudia Rodríguez Sosa**, bajo la asesoría de la **Dra. Juana Hernández Chavarría**, cumple con el formato de Biblioteca, así mismo, se ha verificado la correcta citación para la prevención del plagio; por lo cual, se expide la presente autorización para entrega en digital del proyecto terminal al que se ha hecho mención. Se hace constar que la alumna no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión digital del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Dr. Juan Antonio Vega Garfias
Subgerente de Innovación Gubernamental

JAVG/jah

C.c.p. Mtra. Analy Mendoza Rosales. – Encargada de la Gerencia de Capital Humano. - Para su conocimiento.
Claudia Rodríguez Sosa. – Alumna de la Maestría en Gestión de Innovación de las Tecnologías de Información y Comunicación. – Para su conocimiento.

MGITIC

MAESTRÍA EN GESTÍON DE INNOVACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"GOBIERNO DE SEGURIDAD INFORMÁTICA A TRAVÉS DE LA IMPLEMENTACIÓN DE UN FRAMEWORK"

SOLUCIÓN ESTRATÉGICA EMPRESARIAL
Que para obtener el grado de MAESTRA EN GESTIÓN DE INNOVACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Claudia Rodríguez Sosa

Asesora:

Dra. Juana Hernández Chavarría

Ciudad de México, junio, 2020.

CONACYT

INFOTEC POSGRADOS

Agradecimientos

A Dios, por permitirme tener esta vida maravillosa, por la familia que me prestó pero sobre todo gracias por darme una hermosa hija, cuya presencia iluminó mi vida desde el momento de su llegada. Fernanda, eres y serás siempre mi motor, mi motivación y mi amor más sublime.

Gracias a mi esposo Carlos, cuyo apoyo incondicional y amor me permitieron concluir mi maestría. Te dedico todos mis esfuerzos y mis logros.

A mis maravillosos padres, su ejemplo me acompaña en todo momento y por el cual mantengo disciplina y constancia. La vida entera me será insuficiente para agradecerles.

Un especial agradecimiento para la Dra. Juana Hernández, su disposición, apoyo, y guía permitió la conclusión éste trabajo. Aprecio enormemente haberme acompañado en este proceso.

Tabla de contenido

Índice de figuras

Índice de cuadros

Siglas y abreviaturas

IMSS	Instituto Mexicano del Seguro Social
DIDT	Dirección de Innovación y Desarrollo Tecnológico
TIC	Tecnologías de Información y Comunicaciones
MAAGTICSI	Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información
ASI	Administración de la Seguridad de la Información
OPEC	Operación de los Controles de Seguridad de la Información y del ERISC
ERISC	Equipo de Respuesta a Incidentes de Tecnologías de la Comunicación
DOF	Diario Oficial de la Federación
ISO	International Organization for Standarization – Organización Internacional de Estandarización
IEC	International Electrotechnical Commission – Comisión Electrotécnica Internacional
STPS	Secretaría del Trabajo y Previsión Social
SGSI	Sistema de Gestión de Seguridad de la Información
SFP	Secretaría de la Función Pública
ADS	Administración de Servicios
SNTSS	Sindicato Nacional de Trabajadores del Seguro Social
CCT	Contrato Colectivo de Trabajo
CNCyC	Centro Nacional de Capacitación y Calidad
IUA	Inventario Único de Aplicaciones
CVOED	Centro Virtual de Operación en Escenarios de Desastre

Glosario

“A”

Acceso: Tipo específico de interacción entre un sujeto y un objeto que resulta en el flujo de información de uno a otro. Es el privilegio de un sujeto para utilizar un objeto.

Acceso Remoto: Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación ya sean telefónicas o por medio de redes de área amplia que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autentificación.

Access Control List (ACL): Lista secuencial de condiciones de permiso y negación que definen las conexiones a las que se les permitirá el paso a través de dispositivos, normalmente routers. Lista de los sujetos que pueden tener accesos a diferentes objetos, mostrando cuáles son los privilegios con los que cuenta cada uno de ellos.

Activos Críticos de información: Aquellos recursos en términos de información que en su ausencia podrían menoscabar la operación del Instituto.

Activo de información: Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.

Activo de información clave: El activo de información que resulta esencial o estratégico para la operación y/o el control de una infraestructura crítica, o incluso de una que no tenga este carácter, pero cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura o en los servicios que soporta.

Activo primario: El activo de información asociado a las funciones sustantivas de una Institución.

Activo de soporte: El que apoya o complementa a un activo primario en su función.

Administrador: Persona de confianza y con los conocimientos suficientes para ser responsable de un grupo de servidores, usuarios y otros dispositivos de interconexión. El administrador normalmente no es la persona adecuada para las operaciones relacionadas con la seguridad.

Amenaza: A cualquier posible acto que pueda causar algún tipo de daño a los activos de información de la Institución.

Análisis de riesgos: El uso sistemático de la información para identificar las fuentes de vulnerabilidades y amenazas a los activos de TIC, a la infraestructura crítica o a los activos de información, así como efectuar la evaluación de su magnitud o impacto y estimar los recursos necesarios para eliminarlas o mitigarlas.

Anónimo: Con respecto a los datos, es la condición de no ser capaz de identificar o asociar datos o información con un individuo en particular.

Auditoria: Examinación independiente del producto de un trabajo o conjunto de productos resultado de uno o más trabajos para validar su compatibilidad con estándares, normas, especificaciones, arreglos contractuales o cualquier otro tipo de criterio.

Autenticación o autentificación: Proceso que permite validar la identidad de un usuario o un dispositivo como: servidores, switches, routers, firewalls, entre otros. Establece la identidad del emisor y del receptor de la información, permitiendo la comprobación de que “alguien” es quien dice ser.

Autoridad Certificadora (CA): Tercera persona confiable que autoriza la validez de un certificado, es responsabilidad de la autoridad certificadora el registro, distribución y revocación de los certificados cuando la información contenida en ellos se vuelve inválida.

Autorización: Proceso que brinda derechos de acceso a usuarios, grupo de usuarios o sistemas específicos.

“B”

Bases de datos: Sistemas que cuentan con un conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente para su uso posterior.

Bitácoras o Logs: Registro de mensajes arrojados por los sistemas de información, los cuales permiten contar con información de los mismos**.**

“C”

Caballo de Troya: Programa de computadora con una aparente o real funcionalidad que contiene funciones escondidas que pueden explotar clandestinamente autorizaciones legitimas de algún proceso en perjuicio de la seguridad.

Clave Privada: Los datos que el firmante genera de manera secreta y utiliza para crear su firma electrónica avanzada, a fin de lograr el vínculo entre dicha firma electrónica avanzada y el firmante. (Congreso General de los Estados Unidos Mexicanos, 2012)

Clave Pública: Los datos contenidos en un certificado digital que permiten la verificación de la autenticidad de la firma electrónica avanzada del firmante. (Congreso General de los Estados Unidos Mexicanos, 2012)

Certificado Digital: El mensaje de datos o registro que confirme el vínculo entre un firmante y la clave privada. (Congreso General de los Estados Unidos Mexicanos, 2012)

Certificado digital: Un certificado es una identidad electrónica única y segura que debe ser compatible con un estándar. Los certificados contienen típicamente el nombre del usuario y su llave pública.

Código malicioso: Código que es intencionalmente incluido en un sistema para propósitos no autorizados.

Confidencialidad: La característica o propiedad por la cual la información sólo es revelada a individuos o procesos autorizados.

Control de accesos: Proceso que permite limitar el flujo de información de los recursos del sistema a personas o sistemas autorizados en la red.

Contraseña: Secuencia de caracteres requerida para acceder un sistema de cómputo.

Controles o Salvaguarda: Consiste en la definición y desarrollo de procedimientos para minimizar el grado de riesgo producto de las vulnerabilidades existentes en las instituciones.

Código de conducta: Conjunto de reglas generales relativas al comportamiento del personal dentro de una Institución.

"D"

Detección de intrusos: Detección de intentos de acceso interno o externo por medio de sistemas de software experto que operan con las bitácoras de los sistemas o con la información disponible en la red.

Disponibilidad: La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

Dominio Tecnológico: Las agrupaciones lógicas de TIC denominadas dominios, que conforman la arquitectura tecnológica de la Institución, los cuales podrán ser, entre otros, los grupos de seguridad, cómputo central y distribuido, cómputo de usuario final, telecomunicaciones, colaboración y correo electrónico, internet, intranet y aplicativos de cómputo.

"E"

Encriptación o cifrado: Proceso matemático donde los datos de un mensaje, por seguridad, son codificados para protegerlos de accesos no deseados.

Estándar: Fundamentos definidos para determinar calidad y aceptación.

Escaneo: Conjunto de pruebas con herramientas especializadas a la infraestructura tecnológica que permite conocer las vulnerabilidades del mismo.

“F”

Falso positivo: Alarmas provocadas por sistemas de detección de intrusos, las cuales no son siempre un ataque, sino actividad normal de la operación de la Institución. Los falsos positivos se tienen que analizar para verificar la veracidad de estas alarmas.

Firewall: Combinación de recursos de hardware y software posicionados entre una red local o segura y una red externa o insegura, normalmente Internet. El firewall asegura que las comunicaciones realizadas entre la red de una Institución y la red insegura estén de acuerdo a los controles de seguridad de la Institución. Un firewall registra y controla las comunicaciones, decidiendo que información debe pasar, rechazar, encriptar y registrar.

Firma Electrónica Avanzada: El conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa. (Congreso General de los Estados Unidos Mexicanos, 2012)

“G”

Gusano: Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevos sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.

“H”

Hack: Cualquier programa en el cual una parte significativa del código fue originalmente otro programa.

Hacker: Persona con amplios conocimientos tecnológicos que intenta tener acceso no autorizado a un ambiente de cómputo en el cual dicha persona no tiene ningún privilegio o permiso. El propósito de un hacker puede ser entretenimiento, beneficios personales o económicos, robo, entre otros.

Hardware: Se denomina hardware o soporte físico al conjunto de elementos materiales que componen una computadora. En dicho conjunto se incluyen los dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, armarios o cajas, periféricos de todo tipo y otros elementos físicos.

"I"

Impacto: Al grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.

Integridad: La acción de mantener la exactitud y corrección de la información y sus métodos de proceso.

Incidente: A la afectación o interrupción a los activos de TIC, a las infraestructuras críticas, así como a los activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.

"L"

Laptop: Equipos de cómputo portátiles.

"M"

Marco Normativo: Conjunto de leyes, normas, decretos, reglamentos, y demás disposiciones, de carácter obligatorio aplicables al Instituto.

Medios magnéticos: Son aquellos dispositivos físicos que permiten el transporte de información de un equipo a otro.

Módem: Dispositivo periférico de los equipos de cómputo que permite la conexión con redes externas o Internet.

“O”

Outsourcing: Término del idioma inglés con el que se define la modalidad de contratación por medio de la cual una Institución obtiene de un tercero la ejecución de determinadas actividades de su operación.

“P”

Programa de contingencia: El documento de planeación en el que se plantea la estrategia, el recurso humano en la UTIC, los activos y las actividades requeridas, para recuperar por completo o parcialmente un servicio o proceso crítico, en caso de presentarse un desastre o la materialización de un riesgo.

Privilegio: Derecho de un usuario para llevar a cabo diversas actividades u operaciones relacionadas con el sistema, como por ejemplo, apagar el sistema, cargar controladores de dispositivos.

Puerta Trasera: Punto de entrada a un programa o sistema que se encuentra escondido o disfrazado, y representa una potencial vulnerabilidad, normalmente son creados para la administración y mantenimiento. Una secuencia de caracteres de control permite el acceso a la cuenta de administrador del sistema. Si la puerta trasera se llega a conocer, usuarios no autorizados o código malicioso podrán tener acceso y causar daños.

“R”

Recursos de procesamiento de información: Es toda aquella infraestructura tecnológica que se encarga de llevar a cabo procesos con la información del Instituto.

Redes Virtuales (VPN): Red con segmentos públicos en los cuales la información que pasa a través de ellos es cifrada para asegurar las comunicaciones seguras.

Riesgo: La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información del Instituto.

“S”

Segregación de funciones: Principio de diseño que separa las tareas operativas y administrativas que pueden implicar un conflicto de control en sus requerimientos. Estos requerimientos deben separarse en dominios distintos. El objetivo de la Segregación de funciones es asegurarse que ningún individuo por si solo pueda comprometer la seguridad, características y funciones de un sistema.

Seguridad de la información: la capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.

Sesión: Intercambio de mensajes, este intercambio puede llevarse a cabo con o sin la protección de un mecanismo de llaves.

Sistema de Detección de intrusos (IDS): Conjunto de procesos, gente e infraestructura que permiten identificar y responder a actividades maliciosas que tienen como objetivo dañar recursos de cómputo y de red.

Software: Se refiere a todas las aplicaciones o programas que se encuentran funcionando en cualquier equipo computacional o de comunicación.

“T”

Token: En términos de seguridad es una contraseña que puede ser utilizada una sola vez, comúnmente generada al momento en que se necesita por un dispositivo de hardware.

“U”

User-ID: Identificador único de usuario.

“V”

Virus: Programa que se replica a el mismo en sistemas de cómputo incorporándose en otros programas que son compartidos con otros sistemas de computadoras; una vez que se encuentra en un nuevo sistema, el virus puede causar daños al sistema que está afectado, estos daños van desde la pérdida de información y daños a la memoria hasta daños que impidan la utilización de la computadora sin antes haberle reinstalado el sistema operativo.

Vulnerabilidades: Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a la infraestructura crítica, así como a los activos de información.

“W”

Wireless: Referido a comunicaciones inalámbricas, en las que no se utiliza un medio de propagación físico, de ondas electromagnéticas, radiaciones o medios ópticos. Estás se propagan por el espacio vacío sin medio físico que comunique cada uno de los extremos de la transmisión.

“Z”

Zona Desmilitarizada (DMZ): Zona en donde se ubica una computadora o red fuera de una red confiable o segura, pero también protegida de la red insegura, normalmente Internet.

Introducción

El Instituto Mexicano del Seguro Social (IMSS), es la institución de salud más grande de Latinoamérica, con más de la mitad de la población mexicana afiliada. A septiembre de 2017, contaba con un total de 55’419,246 derechohabientes adscritos (Instituto Mexicano del Seguro Social, 2017). Tiene como función obligatoria, el cumplimiento al Artículo 123: “Toda persona tiene derecho al trabajo digno y socialmente útil; al efecto, se promoverán la creación de empleos y la organización social de trabajo, conforme a la ley” (Consejo de la Judicatura Federal, 2019) de la Constitución Política de los Estados Unidos Mexicanos y su cobertura se persigue como un mandato constitucional. Adicionalmente, la Ley del Seguro Social establece que la seguridad social tiene como finalidad garantizar el derecho a la salud, la asistencia médica, la protección de medios de subsistencia y los servicios sociales, así como el otorgamiento de una pensión según aplique el cumplimiento de los requerimientos legales que pueda darle soporte médico y económico (Instituto Mexicano del Seguro Social, 2014).

La Dirección de Innovación y Desarrollo Tecnológico (DIDT), es una dirección de soporte a los procesos sustantivos del Instituto, que busca la modernización tecnológica del IMSS a través de diversos servicios de Tecnologías de la Información y Comunicaciones (TIC). Como parte sustantiva de éste cumplimiento, la Secretaría de la Función Pública emite Manuales Administrativos de Aplicación General, y en particular para tecnologías de la Información el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicaciones (MAAGTICSI). Dicho Manual, dedica al tema de Seguridad de la Información dos procesos: ASI – Administración de la Seguridad de la Información (II. Organización) y OPEC – Operación de los Controles de Seguridad de la Información y del ERISC (III. Entrega) (Secretaría de Gobernación, 2011).

El IMSS, en cumplimiento a estos lineamientos, ha llevado a cabo las implementaciones correspondientes a dichos procesos. Los hallazgos derivados

de estas implementaciones, da como resultado la necesidad de reforzar al interior de la Institución, el tema de seguridad de la información y evidencia las consecuencias de un mal manejo de la misma.

Es precisamente en el último punto, donde se requiere incrementar el acatamiento de los aspectos legales relacionados con el cumplimiento de la legislación vigente en materia de protección de datos personales:

- ✓ Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Cámara de Diputados del H. Congreso de la Unión, 2017).

Esta Ley ordena al Estado Mexicano a garantizar la privacidad de los ciudadanos y cuidar que gobiernos, empresas, instituciones bancarias, personas e incluso sitios de Internet no incurran en un manejo irresponsable de los datos personales.

Adicionalmente al cumplimiento legal y normativo por parte del Instituto, el presente trabajo de tesis tiene como objetivo implementar un *framework* (marco de referencia) en materia de seguridad de la información, para reforzar la gobernabilidad y la protección al interior y exterior del IMSS; así como de los posibles cambios legales a futuro, basándose en mejores prácticas aprobadas a nivel internacional.

El trabajo es pertinente ya que aunque el IMSS no está considerado como una entidad de seguridad nacional, debido la cantidad de derechohabientes y a la información que procesa es necesario seguir todos los elementos de protección, conforme a la normatividad aplicable a las Secretarías de Estado tales como la Secretaría de Gobernación, la Secretaría de Marina o de la Defensa Nacional. Sin embargo, la dimensión y dispersión del IMSS hace muy complicado el seguimiento y protección de sus datos e información.

Estos retos se pretenden minimizar de manera eficiente a través de la implementación del *framework* planteado, sin contravenir las disposiciones normativas vigentes, de la mano con la Norma ISO/IEC 27000:2013. (Standard) El desarrollo del mismo se refleja en los tres capítulos del presente trabajo, desde el

momento en que se plantea el cumplimiento normativo, hasta el proceso de mejora contínua con la implantación de controles de seguridad nunca antes ejecutados.

Para ello, este trabajo de tesis plantea tres capítulos dedicados al *framework* de seguridad para el IMSS, considerando desde el cumplimiento esencial normativo aplicable, hasta la mejora contínua del Sistema de Gestión de Seguridad de la Información en el Instituto. A detalle:

Capítulo 1: En éste capítulo se aborda el enfoque básico de la seguridad de la información, bajo el contexto nacional así como la obligación normativa vigente al momento de realizar el trabajo de tesis. Asimismo, el desarrollo de la mejora del proceso de seguridad, de la mano de la implementación del marco de referencia propuesto.

Capítulo 2: Sin duda, uno de los principales retos a vencer en el proyecto planteado, es la gestión del cambio organizacional, no sólo por la cantidad de personal a la que se tiene que notificar del *framework* a implementarse, sino también por las nuevas políticas de seguridad que afectarán la forma en que se había estado trabajando en el IMSS con sus activos de información. El trabajo de tesis contempló un curso presencial, para posteriormente implementarlo en línea a fin de tener el mayor alcance posible.

Capítulo 3: En el último capítulo de este proyecto, se integró la evidencia de mejora al proceso de análisis de riesgos del IMSS, en donde se implementaron controles de seguridad realmente efectivos para la protección de las infraestructuras críticas del Instituto. Se muestra un ejemplo que permitió validar la efectividad el marco de referencia.

Finalmente, cerramos las conclusiones con una revisión de los resultados principales de los tres capítulos que buscaron cubrir una adecuada gestión en materia de seguridad de la información, al establecer herramientas, mecanismos y estándares comunes para lograr el gobierno de la seguridad de la información en el Instituto Mexicano del Seguro Social, sobre tres vertientes principales:

1. Establecimiento de políticas y lineamientos de seguridad específicos para la protección de la información institucional.
2. Generación de capacitación inédita en materia de seguridad de la información, tanto presencial como en línea.
3. Implementación de controles enfocados a la protección de ciberseguridad en el Instituto, cuya efectividad reforzó el análisis de riesgos al clasificar adecuadamente cada componente en posible riesgo.

Capítulo 1
La seguridad de la información

Capítulo 1. La seguridad de la información

Seguridad informática vs. Seguridad de la información

La seguridad de la información se refiere más a la protección de los datos, registros, bitácoras, etc. y tienen un enfoque más estratégico hacia las organizaciones, administración y toma de decisiones. Se debe proteger por temas de privacidad, legales y de propiedad.

La seguridad informática está más enfocada a la protección de los datos como tal, a través de herramientas, mejores prácticas, continuidad del negocio a través de las tecnologías de la información y protección interna y/o externa de la información. Algunos elementos que la caracterizan es el antivirus, *antimalware*[1], *firewalls*[2], análisis de vulnerabilidades, entre otros.

1.1 Aspectos fundamentales de la Seguridad Informática

El CID de la información, llamada también la "Tríada de la información", se refiere a la protección de las siguientes características:

Confidencialidad: Se refiere a garantizar que la información no será distribuida o difundida sin los permisos pertinentes.

Integridad: Es la característica de mantener íntegra la información, es decir con completitud en todos sus elementos, tal como se envía, sea recibida.

Disponibilidad: En todo momento que sea requerida, sea posible consultarla.

Otros elementos básicos de la seguridad de la información son los siguientes:

Activo de información: Es algo a lo que una organización directamente le asigna un valor y por lo tanto la organización debe proteger.

[1] El antimalware tiene un espectro de protección mayor al antivirus, ya que contempla la protección y prevención de ataques de otro tipo de software malicioso, incluyendo los virus informáticos.
[2] Los firewalls son dispositivos que filtran el tránsito de información evitando accesos no autorizados.

Autenticidad: Es el aseguramiento de la identidad respecto al origen cierto de los datos o información, el objetivo que se pretende es la comprobación de que dichos datos o información provienen realmente de la fuente que dice ser.

No repudio: Es un flujo de mensajes en el que se intercambian evidencias digitales de sus correspondientes envíos. Existen dos posibles maneras de registrar dicha evidencia así como la responsabilidad inherente de transacciones electrónicas:

- **No repudio en origen**: Busca proteger al emisor de no haber enviado el mensaje, ya que la evidencia de origen es generada por el creador y la prueba del envío la recibe (o retiene) el destinatario.
- **No repudio en destino**: El receptor no puede negar que recibió el mensaje, ya que la evidencia de recepción es generada por el destinatario, y será retenida por el emisor.

Estos servicios de no repudio se requieren para establecer la responsabilidad tanto de emisor como de destinatario en el envío de la información. (Onieva, López, & Zhou, 2009)

Gráficamente, los elementos que busca proteger son los siguientes:

Figura 1 *Pilares de la seguridad de la información.*

Fuente: *(OSIC - Observatorio Ciberseguridad, 2018)*

Los usuarios deben estar conscientes de la importancia de la información que procesan, del cumplimiento de políticas de seguridad establecidas, así como el cumplimiento de estos requerimientos para evitar riesgos (Martins, 2015).

Adicional a lo anterior, existen influencias internas y externas que pueden modificar los atributos de la información. Estos atributos pueden modificar la clasificación inicial de la información (pública o privada), el formato (escrito o digital) así como su ciclo de vida, dependiendo de las modificaciones que existan alrededor de las políticas y/o procedimientos legales que le dieron origen.

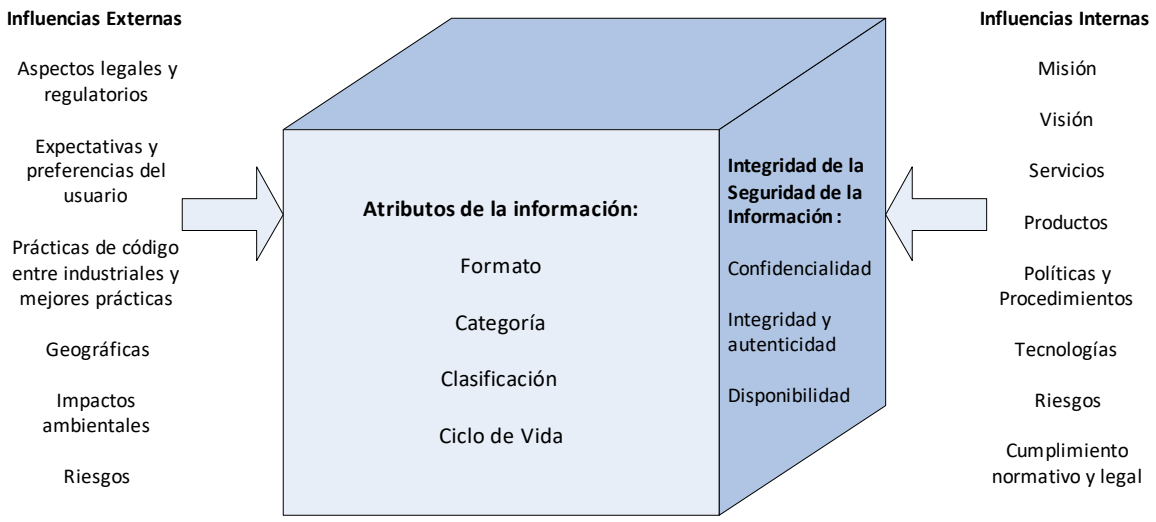


Figura 2 *Atributos de la información y las influencias con la seguridad de la información.*

Fuente: *(Martins, 2015)*.

Control de acceso

A continuación, se presentan algunos elementos o fases en los que se proporciona el control de acceso a servicios de TIC, haciendo énfasis en que no existen controles de seguridad infalibles, al tomar en cuenta que el comportamiento humano siempre resulta el más difícil de controlar.

- Etapas del control de acceso. La primera etapa, la de ***identificación***, la persona presenta sus credenciales de identificación, con ciertos permisos de acceso asociados. Para validar que efectivamente se trata quien dice ser, posteriormente viene la etapa de ***autenticación***, cuya asignación de permisos le son asociados bajo su responsabilidad. Una vez superadas las dos etapas anteriores, se obtiene acceso a los recursos solicitados mediante la etapa de ***autorización***. Finalmente, toda la actividad de este usuario debe ser registrada, a fin de tener trazabilidad de las acciones que realiza a través de la etapa de ***auditoría***.
- Mecanismos de autenticación. Existen tres tipos básicos de autenticación, aunque podemos encontrar otros aún más complejos o sofisticados:
  1. Por lo que uno sabe (contraseña)

2. Por lo que uno tiene (una llave criptográfica)[3]
3. Por lo que uno es (identificación biométrica)[4]

- Tipos de control de acceso. Existen diversos tipos de control de acceso. En este apartado, se mencionan controles de acceso lógico.
  i. Control de acceso discrecional (*Discretionary Access Control*-DAC, por sus siglas en inglés). Como su nombre lo dice, el acceso se da confiando en la discreción del usuario que ingresa. Como ejemplo, la mayoría de los sistemas operativos como Windows y algunas versiones de Unix utilizan este modelo.
  ii. Control de acceso mandatorio (*Mandatory Access Control*-MAC, por sus siglas en inglés). En este modelo cada sujeto (usuario) y objeto (recursos) están clasificados y asignados con etiquetas de seguridad. Las reglas de acceso, son definidas por el responsable de seguridad, configurado por el administrador, reforzado por el sistema operativo y soportado por aplicativos de seguridad. Debido a su alto nivel de confianza, este modelo es el más usado por el ejército.
  iii. Control de acceso basado en roles *(Role Based Access Control*-RBAC, por sus siglas en inglés). Este modelo es también llamado control de acceso no-discrecional, ya que hereda los privilegios conforme le corresponda a su rol. El usuario no tiene control sobre el perfil que le ha sido asignado. En el caso de implementación de RBAC, se requieren al menos dos elementos: El principio de mínimos elementos para el desempeño de sus actividades, y segregación de tareas, que se refiere a tener más de un usuario realizando tareas críticas a fin de reducir riesgos de fraude y otros similares.

[3] Las llaves criptográficas permiten codificar y decodificar mensajes, y son básicamente de dos tipos: simétricas y asimétricas. En ambos casos, refuerzan la confidencialidad de la información.
[4] La identificación biométrica permite, por medio de las características físicas de las persona, registrar su identidad. Existen varios elementos que pueden ser utilizados, tales como son huellas dactilares, red vascular, lectura del iris entre otros.

iv. Control de acceso a través de listas (*Access Control Lists*-ACL, por sus siglas en inglés). Se establecen listas de acceso con base a permisos de lectura, escritura o bien, de ejecución (*rwx – read, write, execution*).

1.2 Proceso de Seguridad de la Información en el IMSS

Para comprender el contexto del IMSS y el impacto que provocó la implantación del MAAGTICSI, es importante conocer las funciones, métodos y procedimientos para los esquemas de seguridad. El "Proceso Administración de la Seguridad de la Información - ASI", ejecuta las siguientes actividades:

1. Integrar el modelo de gobierno de seguridad de la información. En esta primera actividad se debe realizar la designación del Responsable de Seguridad de la Información en la Institución, así como la definición del Grupo Estratégico de Seguridad de la Información.
2. Operar y mantener el modelo de seguridad de la información. La segunda actividad de éste proceso, permitirá la integración del modelo de seguridad de la información en la institución.
3. Diseñar la estrategia para establecer el Sistema de Gestión de Seguridad de la Información (SGSI). El establecimiento del SGSI a través de objetivos y estrategias bien definidas acorde al alcance de la entidad.
4. Actualizar el catálogo de infraestructura esencial y activos clave. El catálogo de infraestructura esencial concentra las aplicaciones más importantes para la operación del Instituto así como los activos de tecnologias de la información clave que los sostienen Deben definirse los activos clave que conforman las infraestructuras críticas de la institución, considerando su operación crítica o fundamental.
5. Analizar el riesgo e impacto sobre procesos y servicios. Sobre matrices de riesgos tecnológicos, deben determinarse los escenarios más sensibles de las infraestructuras críticas, a fin de minimizar dicho impacto.
6. Definir los controles de seguridad de salvaguarda de las TIC. Sobre los escenarios de riesgo previamente detectados, deben definirse e

implementar controles de seguridad específicos para eficientar la operación de las tecnologías de la información y comunicaciones.

7. Mejorar el sistema de gestión de seguridad de la información. Con base a las revisiones periódicas de los elementos de seguridad que contemplan el SGSI, debe realizarse un proceso de mejora cuando alguno de sus elementos haya sido modificado (Secretaría de Gobernación, 2016).

La página de México Digital, diseñó una infografía del proceso de administración de la seguridad de la información, extracto cuyo fundamento se encuentra en el MAAGTICSI vigente (Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, 2016).

Este modelo se encuentra basado en el ciclo de *Deming* (*Plan – Do- Check – Act*):

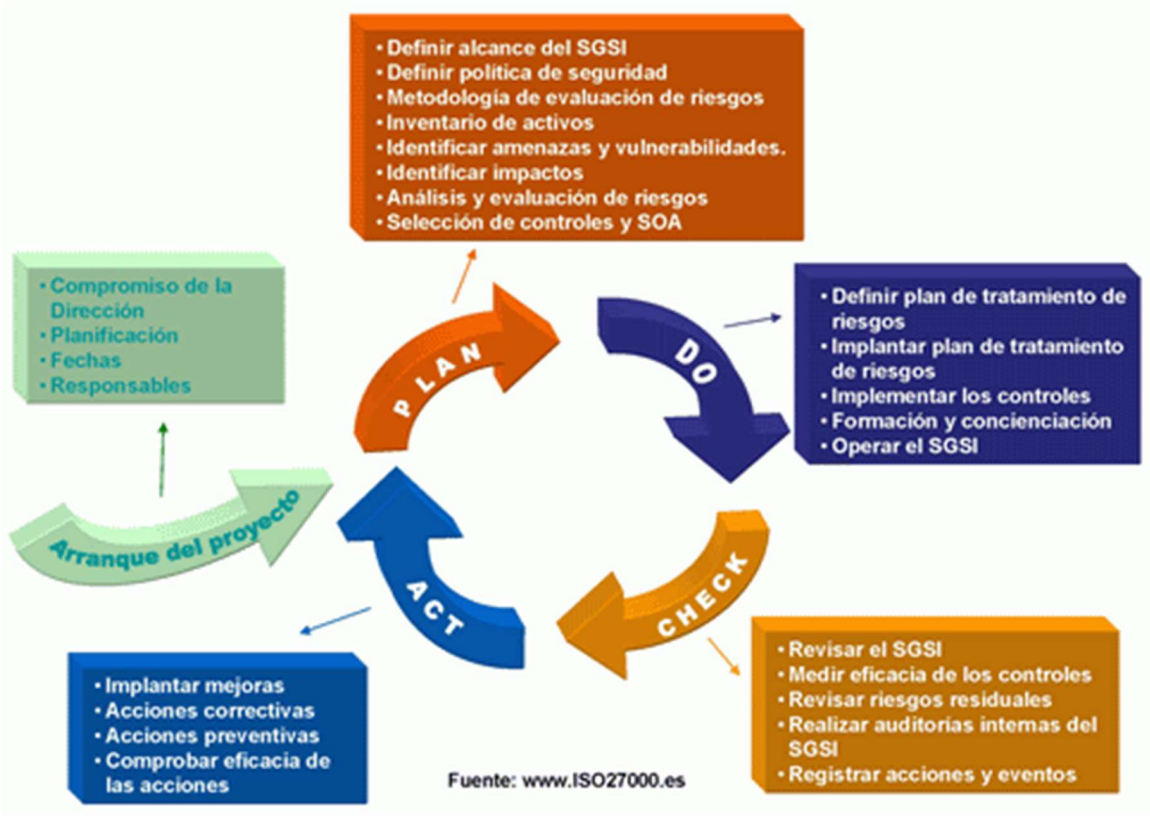


Figura 3 *Ciclo de Deming para el SGSI (Sistema de Gestión de Seguridad de la Información).*

Fuente: (ISO 27001 en Español, 2015).

1.3 Acotando el cumplimiento

Adicional a lo definido por la Secretaría de la Función Pública (SFP), el IMSS requería enmarcar el cumplimiento a través de lineamientos y políticas de seguridad de la información que sólo pueden ser aplicadas en su entorno. Se realizó un análisis de las necesidades de protección por dominio tecnológico, a fin de diseñar, elaborar e implementar diversas políticas de seguridad, a través de diversos documentos de control.

Se desarrollaron 15 políticas de seguridad apropiadas para el IMSS de manera conjunta con los responsables de los dominios de control en cuestión, a fin de delimitar los alcances de cumplimiento del propio Instituto. Bajo éste análisis, se compararon los elementos de cumplimiento del proceso de Administración de la Seguridad de la Información y sus reglas de la mano con la norma ISO/IEC 27001:2013 a fin de no omitir ningún elemento normativo para el IMSS. A partir de éste análisis se generaron éstos documentos de control con elementos comunes que facilitarían las futuras auditorías al marco de referencia; de tal manera, cada documento cuenta con el siguiente formato o plantilla:

1. Nomenclatura: Cada documento se desprende del proceso de seguridad como un "Activo".[5] Para llevar un adecuado control documental, se agrega un número consecutivo. De éste modo, tenemos la siguiente nomenclatura: ASI-ACT-##.
2. Objetivo del documento: Principal finalidad que persigue la política de seguridad planteada.
3. Alcance: Define la aplicabilidad de la política de seguridad, en el interior del IMSS.
4. Justificación: Los efectos legales y administrativos para los cuales fue creada la política en cuestión. Para el presente trabajo la justificación de todos los documentos de trabajo inmersos en el *framework* están

[5] Para efectos del presente trabajo, activo se refiere a la política de seguridad de la información interna aplicable para el IMSS.

avalados por el MAAGTICSI, el Manual de Organización de la DIDT y los dominios de la norma ISO/IEC 27001:2013.

5. Criterios aplicables: Dependiendo del dominio de seguridad, aspectos de control que deberán ser vigilados y atendidos en la política. En cada uno de éstos documentos de control, serán lo que le da sentido y propósito a cada política.
6. Controles asociados: A fin de poder generar indicadores de cumplimiento, a cada política se le desarrolló un control de seguridad como mínimo. Estos documentos también obedecen a la misma nomenclatura, como un anexo que se desprende de la política para su correcta identificación. De tal manera que cada control de seguridad sigue la siguiente nomenclatura: ASI-ACT##-AN##.
7. Control de versiones del documento: A fin de validar las actualizaciones de cada política y evitar obsolescencia, cada documento de control debe tener lo siguiente:
    - Versión. Que indique de manera ordenada, el proceso de avance o modificaciones que el documento de control vaya sufriendo.
    - Fecha. Momento en el que se realiza el cambio correspondiente.
    - Descripción del cambio. Breve reseña de la modificación realizada.
    - Responsable. Nombre y cargo del funcionario que haya realizado el cambio registrado.
8. Sección de firmas. Todo documento emitido como normativa a nivel nacional en el IMSS en materia de seguridad de la información, debe contener las firmas de elaboración, revisión y aprobación del mismo. Para el presente trabajo de tesis, todos los documentos elaborados para el *framework* de seguridad propuesto, fueron a cargo de la

investigadora con el apoyo conjunto de los responsables de los dominios tecnológicos[6] del Instituto.

1.3.1 Políticas de seguridad de la información

A continuación, se realiza un resumen de la normatividad interna emitida para estos efectos, como parte del esfuerzo de la solución estratégica planteada.

ASI-ACT-05 Criterios y controles aplicables a la seguridad física y en el personal. Establece los requerimientos de seguridad de la información que debe cumplir el personal del IMSS para proteger la operación de los bienes informáticos institucionales y prevenir accesos físicos no autorizados, pérdidas de información, robos o mal uso de los recursos. A éste documento de control, se generaron procedimientos y controles de seguridad con el apoyo del dominio A.11 Seguridad física y ambiental. (Standard)

ASI-ACT-06 Criterios y controles aplicables a la seguridad para terceros. Define los requerimientos de seguridad de la información solicitados por el IMSS que deberán cumplir terceros al acceder a instalaciones, infraestructura o sistemas de información para salvaguardarlos y hacer un uso apropiado de ellos. Para la generación de este activo se desarrollaron procedimientos y controles de seguridad basados en los dominios A.9 Control de accesos, A.11 Seguridad física y ambiental así como A.15 Relaciones con proveedores.

ASI-ACT-07 Criterios y controles aplicables al control de acceso. Busca promover el uso de métodos robustos de autenticación y control de acceso a sistemas de información, servicios o redes del IMSS con el fin de asegurar que los usuarios internos, externos o terceros con acceso a los servicios de información no comprometan la seguridad de los mismos. Los controles de seguridad generados para el cumplimiento de la politica, así

[6] Para MAAGTICSI, son agrupaciones lógicas de tecnologías de la información que conforman la arquitectura tecnológica de cada entidad o institución. Ejemplo: Telecomunicaciones.

como procedimientos y hojas de registro del mismo, estuvieron apoyados en la actividad 6 “Definición de controles mínimos de seguridad” (Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, 2016) así como el dominio A.9 Control de accesos.

ASI-ACT-08 Criterios aplicables a la protección de redes. Busca definir las premisas para la protección de las redes internas, así como la conectividad con redes externas involucradas, con el fin de garantizar su confidencialidad, integridad y disponibilidad. En la búsqueda de la protección de redes institucionales, se integraron controles del dominio A.9 Control de acceso, particularmente el control 9.1.2 Acceso a redes y a los servicios de red, del dominio A.13 Seguridad en las comunicaciones, control 13.1.1 controles de red así como del dominio A.6 Organización dela seguridad de la información el control 6.2.2 El teletrabajo. Del mismo modo, se buscó el cumplimiento en el MAAGTICSI Art. 11, fracción I que a la letra menciona “Establecer un dominio o segmento virtual en el uso compartido de redes de telecomunicaciones, lo cual se podrá realizar de manera individual o conjunta;” (Secretaría de Gobernación, 08).

ASI-ACT-09 Criterios aplicables a la mensajería instantánea y correo electrónico. Estos lineamientos establecen los criterios necesarios que regulen los servicios de mensajería instantánea y correo electrónico en el IMSS, para asegurar el uso racional, confiable y productivo de estas tecnologías en las actividades institucionales. Para la aplicación del marco de referencia propuesto, se tomaron como base los controles de acceso del documento ASI-ACT-07 Criterios aplicables al control de acceso, debido a que el Directorio Activo[7] institucional, es el proveedor de identidades en el IMSS, adicionándole controles asociados al dominio A.13 Seguridad en las comunicaciones, particularmente el control 13.2.3

[7] Servicio de directorio de red de la empresa Microsoft, utilizado en el IMSS para la gestión de identidades y registro de equipos y usuarios asociados a éstos.

Mensajería electrónica; a través de procedimientos y cartas responsivas para los usuarios.

ASI-ACT-10 Criterios aplicables al servicio institucional de Internet. Se definen los criterios necesarios que regulen el servicio de la internet para favorecer el uso seguro, racional y productivo de esta tecnología, así como para hacer uso eficiente de los recursos de red disponibles, contribuyendo así al cumplimiento de las actividades institucionales. Si bien el IMSS ya contaba con elementos de filtrado de contenido, la implementación del *framework* propuesto, permitió formalizar el cumplimiento de la navegación de Internet en el instituto a nivel nacional con los perfiles de acceso definidos en la política y los procedimientos que se diseñaron para éste efecto.

ASI-ACT-11 Criterios aplicables a la administración de bitácoras. Estos criterios establecen los lineamientos de almacenamiento y explotación de bitácoras de seguridad que permitan detectar, diagnosticar, auditar y analizar eventos anormales para mitigar riesgos de pérdida o alteración de información sensible. El IMSS maneja una cantidad considerable de información, cuyo almacenamiento total resulta imposible de manejar. Por lo anterior, el *framework* recopila las bitácoras de seguridad de las aplicaciones consideradas críticas o sensibles, con el apoyo de lo establecido en el dominio A.12 Seguridad de las operaciones, en específico el control 12.4.3 Registros del administrador y del operador.

ASI-ACT-12 Criterios aplicables a la protección de equipos de cómputo pertenecientes al Instituto. En este apartado se definen los lineamientos de seguridad aplicables a los equipos de cómputo que procesan, transmiten o almacenan información para asegurar el equipo de cómputo. El IMSS, es una de las instituciones con mayor número de equipo de cómputo en el Gobierno Federal, por lo que éste marco de referencia buscó privilegiar la protección de equipo de cómputo personal bajo su resguardo (incluyendo lap-tops, tabletas y móviles). Ésta política se

relaciona con otros activos tales como el ASI-ACT-10 Criterios aplicables al servicio institucional de Internet, además de los siguientes controles de la norma ISO 27002:

- 11.2.4 Mantenimiento de equipo.
- 11.2.5 Remoción de activos.
- 11.2.7 Reutilización o retirada segura de equipos.
- 11.2.8 Equipo de usuario desatendido.

ASI-ACT-13 Criterios aplicables a la protección contra virus y código malicioso. Se establecen los lineamientos para la administración de mecanismos de protección contra códigos maliciosos (virus, gusanos y caballos de Troya, etc.), para disminuir la posibilidad de ataques a equipos de cómputo, un intercambio seguro y confiable de información y con esto contribuir a los objetivos del Instituto. Para lograr la mayor cobertura de protección de los equipos de cómputo institucionales, se relacionó con otras políticas de seguridad, tales como:

- ASI-ACT-09 Criterios aplicables a la mensajería electrónica y correo electrónico.
- ASI-ASCT-14 Criterios aplicables a las actualizaciones de seguridad.

Del mismo modo, estos lineamientos se relacionan con el dominio A.16 Gestión de incidentes de la seguridad de la información.

ASI-ACT-14 Criterios aplicables a la administración de actualizaciones de seguridad en equipos de cómputo (servidores o computadoras personales dentro del Instituto). Estos lineamientos buscan asegurar que los sistemas del IMSS sean actualizados de forma oportuna y con base en un procedimiento que permita mantener el control de los cambios relacionados, para contribuir en la mitigación de riesgos y con esto disminuir los posibles impactos por vulnerabilidades asociados a los equipos de cómputo. El instituto consideró importante la creación de esta política debido a la falta de seguimiento por parte de las áreas usuarias

sobre la actualización de software, el cual tenía un gran impacto en la protección de la información institucional. Se relaciona con el documento ASI-ACT-16 Criterios aplicables al licenciamiento de software, así como los controles del dominio A.12 Seguridad en las operaciones: 12.5.1 Instalación de software en sistemas de producción y 12.6.1 Restricciones a la instalación de software.

ASI-ACT-15 Criterios aplicables al desarrollo y mantenimiento de software. Define los controles del proceso de desarrollo y mantenimiento de los sistemas de información automatizados, para evitar pérdidas, modificaciones y mal uso de los datos utilizados y generados por los sistemas desarrollados por el IMSS y con esto contribuir al logro de sus objetivos. El marco de referencia, para cubrir el ordenamiento de la normatividad determinada en el MAAGTICSI, desarrolló estos criterios para las fases de análisis, diseño, construcción (desarrollo), pruebas y despliegue (liberación) de los sistemas del instituto. Para lo anterior, se mencionan los aspectos más importantes para el ciclo de vida de desarrollo de aplicaciones. Dicho ciclo debe incluir elementos de control que minimicen huecos de seguridad en los sistemas que se desarrollan, en sus diferentes fases. A continuación, se muestra un diagrama con algunos de los elementos de seguridad que integró el *framework* propuesto:

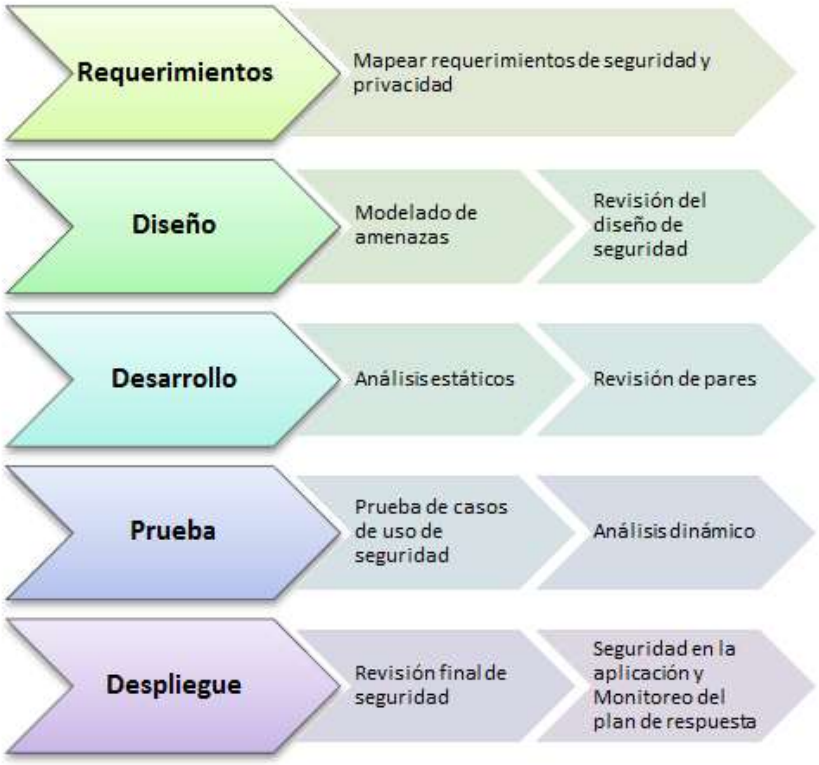


Figura 4 *Seguridad en el Ciclo de vida de desarrollo de software.*

Fuente: Elaboración propia, basado en el modelo de SDLC de Microsoft *(Microsoft)*.

Adicionalmente, en el marco del proceso ADS – administración de servicios, se ha generado una guía operativa de arquitectura. Dicha guía, busca definir las actividades, responsables, insumos y salidas para diseñar las arquitecturas de los proyectos nuevos o mantenimientos mayores realizados por el IMSS.

ASI-ACT-16 Criterios aplicables al licenciamiento de software. En estas políticas se establecen los lineamientos para la adquisición y uso de software autorizado, para evitar Incidentes de seguridad que comprometan la disponibilidad de la información derivado del uso de software sin licencia. Estos lineamientos tienen mucha relación con el documento ASI-ACT-15 Criterios aplicables al desarrollo y mantenimiento de sistemas, debido a que deben cumplirse los compromisos de licencias, arrendamientos de software y otros con proveedores en el instituto y se integra en el cuerpo

del documento. Con la finalidad de reducir la brecha de apego a la ISO/IEC 27002:2013; también se crearon controles basados en el dominio A. 14 Adquisición, desarrollo y mantenimiento de sistemas.

ASI-ACT-17 Criterios aplicables al cifrado de datos. El IMSS busca asegurar el tratamiento de la información clasificada como sensible, confidencial o reservada, durante su procesamiento, transportación y almacenamiento con base en mecanismos de cifrado, para disminuir el riesgo de robo o pérdida de información utilizada en los procesos institucionales. Particularmente, el instituto generó esta política con la finalidad de cumplir con la Ley de Firma Electrónica Avanzada (Cámara de Diputados del H. Congreso de la Unión, 2012) y administrar adecuadamente los certificados de seguridad bajo la normatividad emitida.

ASI ACT-18 Criterios aplicables a las bases de datos. Estos lineamientos establecen los controles de seguridad adecuados para respaldar y proteger las bases de datos utilizadas por el IMSS, con el fin de blindar la información sensible y elevar los niveles de seguridad en las transacciones operacionales. El caso particular de estos lineamientos, obedecieron al ámbito institucional, de tal forma que no hay controles asociados a otros estándares. Sin embargo, se generaron procedimientos y controles apegados a la operación de seguridad de la información, integrándose adecuadamente al *framework* propuesto.

ASI-ACT-19 Criterios aplicables al respaldo y borrado de información. Establecen los lineamientos de respaldo, recuperación y borrado de información sensible y clasificada como confidencial o reservada para mitigar riesgos de pérdida o alteración de ésta, con el fin de mantener la operación en forma segura y con ello contribuir al logro de sus objetivos. Estos lineamientos fueron elaborados con el apoyo del dominio A.12 Seguridad en las operaciones, control 12.3 Respaldos. Para cubrir el requerimiento de borrado seguro, se contrataron licencias con un

proveedor especializado en el tema, apegados a los procedimientos institucionales.

Toda esta documentación, son los lineamientos de seguridad que sirven como base para establecer el marco de operación en materia de seguridad de la información para el Instituto Mexicano del Seguro Social.

Capítulo 2

La cultura de la seguridad de la información

Capítulo 2. La cultura de la seguridad de la información.

Sin duda alguna la cultura de la seguridad tiene un impacto potencial en la seguridad de la información, es decir, entre más informado esté el personal responsable del manejo de la misma sobre su impacto en caso de daño o pérdida, más fácil será la administración de la seguridad de la información, en todos sus niveles y capas. En este trabajo de investigación se hará especial énfasis en el cambio organizacional y cultural enfocado a la seguridad de la información. Adicionalmente, el IMSS sigue siendo una entidad de cumplimiento del MAAGTICSI por lo que se pretende cumplir con el artículo 25 del Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de Tecnologías de la Información que a la letra menciona:

…" Artículo 25.- Las Instituciones instrumentarán un proceso de fortalecimiento de la cultura de la seguridad de la información, así como de mejora continua sobre los controles de seguridad de la información y del sistema de gestión de seguridad de la información, con base en lo señalado en el MAAGTICSI…"

2.1 Gestión del cambio cultural.

El marco de referencia (*framework*) que se propone, está enfocado en la planeación, seguimiento, monitoreo y resultados de su implementación mediante la medición de diversas variantes y objetos de resultado. Está basado en las siguientes dimensiones:

Estrategia. Se refiere a la aplicación adecuada de las diferentes estrategias de seguridad de la información, tales como planes de acción, políticas, objetivos, mejores prácticas, normas, lineamientos y prioridades que están diseñados para guiar a los miembros de la organización para alcanzar el objetivo de proteger los activos de información. El establecimiento de políticas formales, las mejores prácticas, directrices y controles ayudan a los empleados a que reciban un mensaje consistente y claro acerca de lo que está prohibido y las consecuencias

de violación. En el caso del IMSS, estas políticas y lineamientos se establecieron en la directriz rectora de seguridad de la información[8], posteriormente denominado "ASI ACT 00 Criterios y Controles de Seguridad de la Información" para finalmente conformar un total de 15 políticas de seguridad donde se definen los criterios a través de los cuales el IMSS determina la seguridad de la información para los activos de TIC a fin de minimizar el impacto de incidentes a través de controles de seguridad, establecidos en dicho documento. El detalle de cada una de estas políticas se mencionan en el primer capítulo del presente trabajo.

Tecnología. La dimensión de la tecnología en este contexto tiene que ver con las tecnologías de seguridad tales como *hardware, software*, servicios[9], *appliances*[10], y aplicaciones que se utilizan dentro de la organización para proteger los activos de información. De acuerdo con el marco, las medidas tecnológicas utilizadas por el IMSS, juegan un papel muy importante en el tema de seguridad de la información y su efectividad apoyará las medidas consideradas como parte del marco de referencia.

Organización. La estructura de la organización juega un papel muy importante en la cultura de seguridad de la información. En este contexto, la dimensión relacionada con la organización tiene que ver con la recopilación de la información sobre las creencias, símbolos, normas y conocimiento único y representativo de la organización. Una campaña publicitaria para reforzar el tema de seguridad de la información, es un buen ejemplo de esta dimensión. El conocimiento y sensibilidad que se tiene al tema de seguridad de la información en el IMSS es muy importante.

Contexto. Sin duda alguna una de las dimensiones que tenemos que incluir es el contexto en el que se desenvuelve el IMSS, y el impacto que tiene al interior de cualquier organización. En este caso el contexto proviene de lo que dicte el

[8] Primer documento donde se establecen lineamientos de seguridad en el Instituto, previo a la implementación del *framework* propuesto.
[9] Servicios de tecnologías de la información, tales como correo electrónico, impresión en red, etcétera.
[10] Aparatos o controles que combinan el uso de software y hardware para un propósito específico y sólo funcionan de manera unificada. Ejemplo: Software y Hardware Criptográfico.

Gobierno Federal, la administración de la función pública como tal. Lo anterior, por tratarse de una entidad sujeta a la normatividad que el Ejecutivo Federal determine. Adicional a esto, el contexto nacional, la conducta ética de los trabajadores y otros factores culturales determinan en gran medida la forma de administrar la seguridad de la información.

Gente. Es la clave de éxito para la cultura de la seguridad de la información, ya que en éste se centra la ejecución del proyecto. La dimensión de gente está relacionada con el comportamiento de cualquier persona dentro del IMSS que tenga relación directa con activos de información. La cultura de la seguridad de la información asegura que cada uno de los involucrados esté consciente de su responsabilidad.

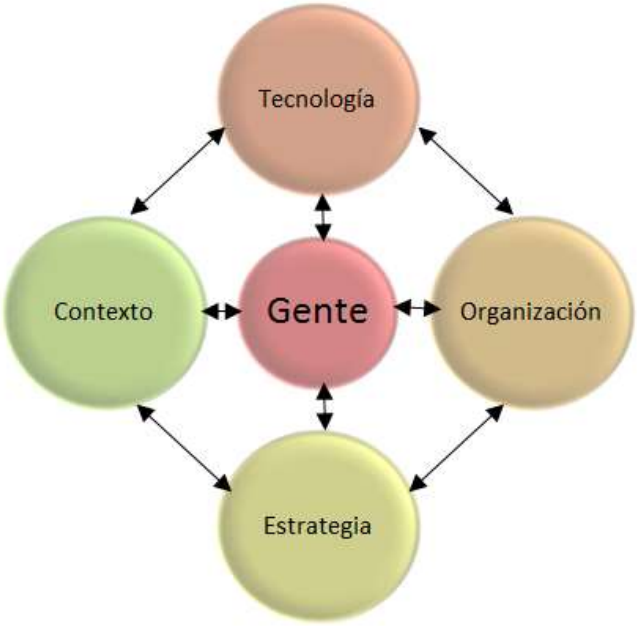


Figura 5 *Dimensiones en la gestión de la seguridad de la información.*

Fuente: Elaboración propia.

Será entonces, el factor humano la pieza clave de la gestión del cambio, considerando una investigación previa a su implementación y obtención de métricas y resultados al final del proceso.

Enfocándonos en la gestión del cambio, los dominios de apoyo para su implementación serán:

1. Dominio de conocimiento. Contempla la capacitación, el conocimiento en el tema o la experiencia del mismo, la aceptación de nuevos esquemas de seguridad y su adaptación.
2. Dominio de responsabilidad. Que el usuario esté consciente de la responsabilidad de la información que administra, sus insumos y resultados, así como el cumplimiento de controles y las consecuencias de omitirlos para su correspondiente aceptación de responsabilidad.
3. Dominio de administración. Está relacionado con las políticas de seguridad, práctica, dirección e interacciones entre otros procesos o áreas de negocio involucradas.
4. Dominio de sociedad y marco regulatorio. Este dominio está directamente relacionado con aspectos sociales y culturales, así como temas regulatorios o fiscalizadores de cumplimiento en materia de seguridad de la información (AlHogail, 2015).

Figura 6 *Herramientas para la administración del cambio.*

Fuente: *(AlHogail, 2015).*

Poniendo en orden estas herramientas para lograr una efectiva administración de cambio organizacional enfocado a la seguridad de la información, a continuación, se muestra una lista de lo que contempla cada una:

1. *Capacitación:* Para asegurar una capacitación efectiva, a los empleados involucrados se les debe indicar qué hacer, cuándo hacerlo y porqué debe ser realizado. La capacitación debe permitir el desarrollo de las habilidades del personal involucrado, así como incrementar la sensibilización de la importancia de la seguridad de la información, a fin de disminuir amenazas accidentales o maliciosas hacia los activos de información. Este proceso debe ser llevado a cabo en una mejora continua y de manera incremental para los empleados, ya que no todos tienen el mismo contexto en materia de seguridad informática y se debe dar seguimiento puntual. Además, es recomendable que un curso o taller de seguridad de la información, así como el contexto y el manejo de su información debe ser entregado a cada nuevo empleado del IMSS. A pesar de que a cada momento los riesgos de seguridad de la información aparecen continuamente, el esfuerzo para reforzar la seguridad debe ser de manera permanente, a fin de evitar estos nuevos riesgos. La interacción con los sistemas de información debe ser lo más segura posible, para proteger los activos de información y si no se tiene este sentido de alerta se pueden causar más riesgos al interactuar con la información.

   Un aspecto importante que debemos considerar dentro del IMSS, es que la mayor parte de los trabajadores son afiliados al Sindicato Nacional de Trabajadores del Seguro Social (SNTSS) y una minoría es personal de confianza. Debido a esto, es el Sindicato a través del Contrato Colectivo del Trabajo (CCT) que establece y determina los mecanismos mediante los cuales el trabajador de base recibe la capacitación de sus

agremiados. Para ello, el sindicato cuenta con una red de centros de capacitación cuya distribución obedece al menos a un centro por Estado de la República, donde imparten capacitación de todo tipo, siendo en su mayoría aquélla que obedece al cumplimiento del CCT, con base a la categoría (tipo de empleo) que el trabajador tiene. En la página del sistema de centros de capacitación y calidad, se encuentra la definición y propósito de cada Centro Nacional de Capacitación y Calidad (CNCyC); el cual se centra en el modelo educativo para los trabajadores del IMSS (Sindicato Nacional de Trabajadores del Seguro Social).

Debido a que el alcance es a nivel nacional, estos centros serán los principales facilitadores del despliegue de la estrategia de sensibilización a todos los trabajadores del IMSS.

2. *Establecer grupos de enfoque y talleres:* Como se mencionó anteriormente, la realización de talleres relacionados con la seguridad de la información tendrá un gran impacto en el acercamiento de los usuarios involucrados en el proyecto, incluso para mejorarlo durante el proceso. Particularmente para estos usuarios los talleres agregarán mucho más valor que a los usuarios normales debido al contenido de los mismos, ya que serán talleres con un propósito definido: apoyar a los grupos de enfoque que irán permeando a lo largo de la implementación, el esquema de seguridad de la información en todas las capas de información que anteriormente se habían mencionado.
3. *Seleccionar el equipo de los agentes de cambio y empoderarlos como equipo de trabajo en un esquema colaborativo*: Los agentes de cambio o líderes de cambio serán nuestros facilitadores para materializar el cambio al interior del Instituto. Estos perfiles deben ser cuidadosamente seleccionados, ya que para el logro de objetivos deben estar comprometidos y capacitados, convencidos de los beneficios de la implementación del proyecto. Son a estos perfiles con quien se debe tener mayor comunicación y retroalimentación. Ellos serán quienes

minimicen la confusión que pudiera haber entre los usuarios para evitar la resistencia.

4. *Motivar y capacitar a los empleados a fin de controlar el nivel de motivación entre ellos:* La motivación entre los empleados juegan un rol crítico para este proyecto, ya que, sin la motivación adecuada, los empleados sólo buscarán cumplir con los lineamientos normativos, pero no ser agentes de cambio. Es por ello que resulta importante ayudarlos a aceptar el cambio con la menor resistencia posible, esto permitirá que los empleados vean que es más fácil cumplir con los requerimientos de seguridad, que omitirlos causando daños irreparables.
5. *Identificar logros en el corto plazo, medidas e hitos a fin de mostrar beneficios que den continuidad de éxito al proyecto.* Es esencial la identificación de logros al corto plazo (*quick-wins*) de la implementación del proyecto, a fin de reforzar la confianza en el mismo y dar vista de sus beneficios. Estos logros a corto plazo, permiten no sólo mantener la certeza en la implementación, sino que ayuda a mantener motivados a todos los involucrados. Un buen ejemplo de esto, puede ser el cumplimiento por parte de los usuarios en la nomenclatura de contraseñas, reforzando a nivel equipo de cómputo, el acceso lógico seguro, etcétera.
6. *Involucrar a los empleados en la toma de decisiones hacia la implementación:* Las contribuciones de los empleados a través de su participación son importantes, ya que incrementa su sentido de pertenencia al ser conscientes de la responsabilidad que conlleva el cumplimiento de la seguridad informática que se relacione con el activo de información que administre. Los empleados del IMSS deben concientizarse sobre las posibles consecuencias o delitos resultantes de estas omisiones en caso de incurrir en ellas. En una primera fase, serán registradas evaluaciones y encuestas relacionadas con el proyecto a los usuarios involucrados, a fin de identificar posibles áreas de oportunidad en un despliegue de mayor alcance.

7. *Soporte de la administración*: Se debe establecer el compromiso desde el más alto nivel gerencial, a fin de tener el soporte necesario para la ejecución de todas las tareas. En este caso en particular, si existe la participación de proveedores para la realización de estas tareas, será necesario un seguimiento estrecho de cumplimiento por parte del líder de proyecto, a fin de que se obtengan los resultados esperados.
8. *Asegurar que se tienen los recursos suficientes, tanto de tiempo como de dinero*: Antes de proceder a ejecutar el programa para la gestión del cambio en el IMSS, se debe considerar que se tengan los recursos suficientes para no detener la implementación. Debe haber soporte por parte de la alta dirección, ya que, a diferencia de otros proyectos, el detener este proyecto implica un mayor impacto en la confianza de los usuarios. Adicionalmente, los tiempos que se le dedique a la capacitación de los usuarios debe ser respetado, así como todos los requerimientos deben estar plenamente identificados para emitir un alcance asequible.
9. *Comunicación*: La comunicación es un tema esencial para lograr una adecuada gestión del cambio y una buena implementación de la estrategia. La comunicación es la mejor forma de hacer tangibles los objetivos y logros de la implementación del proyecto, ya que al "vender" el proyecto con oportunidad comunicando a través de los diversos canales establecidos, el avance del cumplimiento de la implementación será tangible para todos los niveles involucrados. El comunicar adecuadamente el avance del proyecto puede ayudar a disminuir el estrés que pudiera llegar a causar entre los usuarios debido a que se aclaran todas las dudas y suposiciones que llegaran a tener. Existen diversos métodos de comunicación que pueden ser utilizados para lograr enviar el mensaje de manera contundente. Como ejemplo, diversos *posters* con estadísticas, gráficos y avances en la implementación del proyecto; correos electrónicos para los usuarios

motivando a seguir con el cumplimiento de la seguridad informática en su área de su competencia, talleres informativos, etc.

10. *Abrir diversos canales de comunicación para facilitar la retroalimentación y revisiones.* La retroalimentación continua es sumamente importante para proveer el soporte, evitar la confusión e incrementar el compromiso y sentido de pertenencia al proyecto dentro del IMSS. El compartir con los usuarios la experiencia de la implementación y cómo cada usuario lo vive en su perspectiva, ayuda a la implementación del tema de seguridad de la información e incluso descubrir otro tipo de requerimientos. El compromiso de devolver a los usuarios que se comunican adecuadamente con los responsables del proyecto es de vital importancia, debido a que, si no se les reitera la comunicación, difícilmente volverían a participar, haciendo más lento el proceso. En cambio, si se les reconoce su participación, estarán más motivados para continuar colaborando.

2.1.1 Segmentación de usuarios

La seguridad de la información es un tema del que muy pocas personas se encuentran conscientes, y es algo que involucra tanto la tecnología como a las personas. Por lo anterior, es necesario analizar si los usuarios tienen algún conocimiento sobre los posibles impactos que pudieran existir derivados de la falta de controles de seguridad y las amenazas a las que se encuentran expuestos (*hackers*, virus, *spam*[11] y programas maliciosos en general), adicional a otros mecanismos que los atacantes utilizan para obtener beneficios (*phishing*[12], ingeniería social[13], etc.) (DIng-Long Huang, 2010).

Una manera de identificar los tipos de usuario y su grado de conciencia en relación al tema de seguridad de la información, fue la integración de cuatro

[11] Correo electrónico no solicitado, considerado como “basura” que pudiera contener malware inserto.
[12] Es un conjunto de técnicas que son utilizadas para conformar un fraude informático, buscando información personal y bancaria de los usuarios.
[13] La ingeniería social utiliza las vulnerabilidades de los usuarios, engañándolos para obtener información valiosa para que los atacantes la usen en su beneficio. Este tipo de ataques va más enfocado al comportamiento o reacción humana.

grupos a partir de una breve encuesta que determinó dónde se encuentra en general la Institución según Shienger & Teufel (2003):

> Tipo 1 “Me siento tranquilo”: son aquéllos usuarios que se encuentran complacientes con las políticas de seguridad y las siguen sin resistencia.
>
> Tipo 2 “El riesgo está fuera”: son aquellos usuarios que consideran que los riesgos se encuentran fuera del IMSS y no les interesa mucho lo que ocurra dentro. La responsabilidad de la seguridad de la información está en manos del personal de tecnologías de la información quienes procuran que se filtren los riesgos informáticos.
>
> Tipo 3 “No me interesa”: son aquellos usuarios que no perciben ningún problema de seguridad de la información y, por consiguiente, la necesidad de cumplir con políticas de seguridad.
>
> Tipo 4 “Me siento intranquilo”: son usuarios que se encuentran intranquilos o inconformes con las actuales regulaciones o políticas de seguridad y consideran debe incrementarse.

El realizar esta categorización entre los usuarios ayudará a identiticar la mejor forma de implementar las estrategias de capacitación. Adicionalmente, es información base para comparar al final del proyecto los resultados obtenidos de la capacitación.

Para efectos de comportamiento en el uso de tecnologías de la información, así como la percepción que se tiene sobre la seguridad de la información, los usuarios más riesgosos son aquéllos que entran en la categoría tipo 2 y tipo 3. El tipo 2 se confía en que dentro del Instituto se encuentran todos los elementos de control por lo que no hace ninguna acción preventiva., traslada el riesgo de sus acciones a los responsables de la seguridad de la información institucional. El tipo 3, ni siquiera percibe que sus acciones pueden tener repercusiones a nivel laboral o personal, no le interesa en lo más mínimo y tampoco se involucra.

En cambio, los usuarios tipo 1 son el escenario ideal de cumplimiento, ya que es consiente del trabajo que realiza, pero sobre todo, en su comportamiento

hacia información que no le pertenece. El usuario tipo 4 es el más consciente y busca incluso mejoras en las regulaciones de seguridad implementadas. Es el usuario al que se le puede sacar mayor provecho hacia la mejora y reforzamiento en la seguridad de la información.

2.2 Un antes y un después.

El análisis de la segmentación de usuarios previamente definida, permitirá visualizar un avance en los conceptos, elementos y mecanismos de seguridad implementados a favor del IMSS. Lo cual, será evaluado posterior a la implementación del *framework* propuesto en el presente trabajo de investigación.

La mejor manera de integrar datos estadísticos para esta segmentación, fue la de integrar un reactivo en el cuestionario inicial en el curso presencial de seguridad de la información. Este cuestionario inicial fue formulado como parte del curso de seguridad de la información que se diseñó para el presente proyecto (Anexo 1).

La propuesta inicial de capacitación para el personal institucional, se visualizó para el personal de soporte técnico en las delegaciones, con la finalidad de que una vez que estén capacitados, repliquen el mismo curso y contenido en cada una de sus áreas de responsabilidad bajo un modelo de "*train the trainers*"[14]. Al ser personal que tiene el primer contacto con el usuario, será más fácil la entrega del curso elaborado.

Para lo anterior, se elaboró el siguiente mapa mental para plasmar los principales elementos del programa de capacitación en materia de seguridad de la información:

[14] Modelo bajo el cual se le otorgan las capacidades suficientes a los capacitadores para diseñar, planificar y entregar capacitación al interior de una empresa o institución.

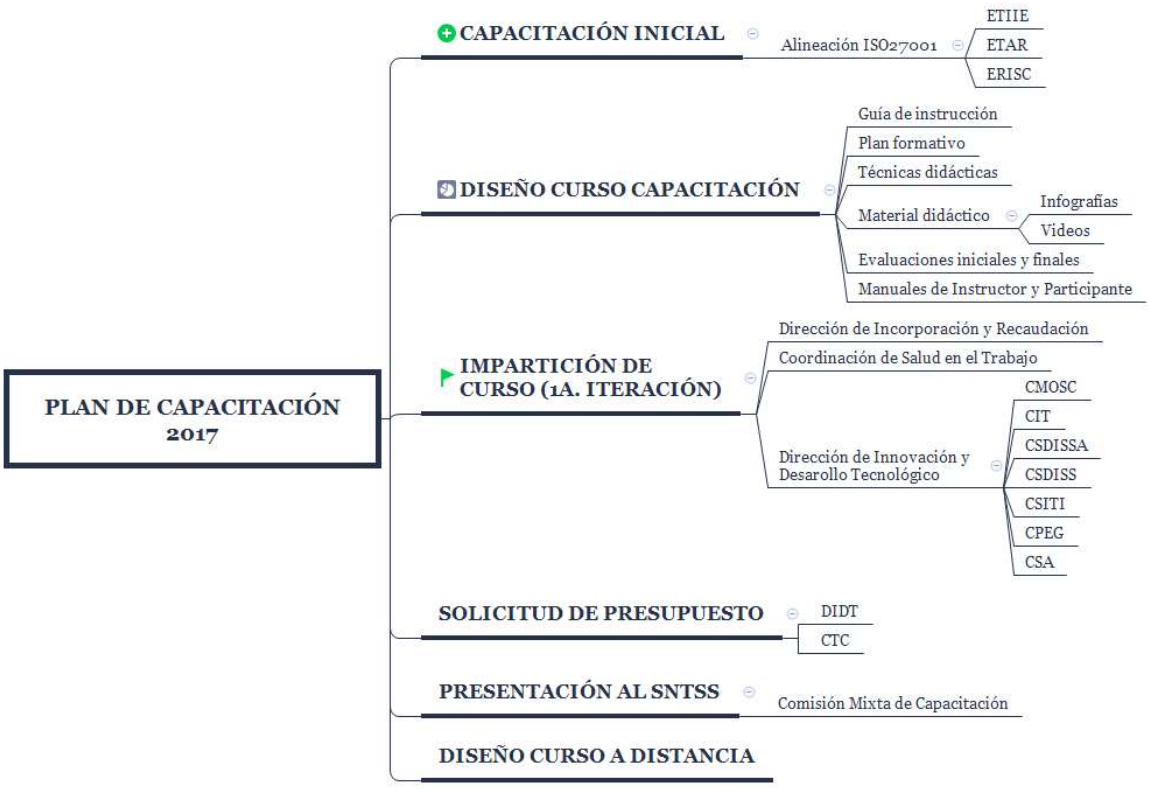


Figura 7 *Propuesta inicial para programa de capacitación.*

Fuente: Elaboración propia.

Como se muestra en el diagrama, se consideró que los primeros que deberían recibir la capacitación serían los integrantes de los diversos equipos de seguridad que se desprenden del cumplimiento normativo. La elaboración del curso y todo su contenido, se realizó bajo los requerimientos que el IMSS solicita a través de la Coordinación de Capacitación. Éste diseño, permitió que el registro de éste programa tuviera el aval de la Secretaría de Trabajo y Previsión Social bajo la nomenclatura PFV/09/012, para tener la garantía de valor curricular por competencias laborales. Un ejemplo de éstos, se anexa al presente trabajo (Anexo 2).

Al inicio de la entrega de ésta capacitación, no se realizaron gastos de viáticos o comisiones de traslado para los participantes, y los primeros resultados fueron muy favorables. Los primeros resultados de la segmentación de usuarios mencionada anteriormente, se muestran a continuación:

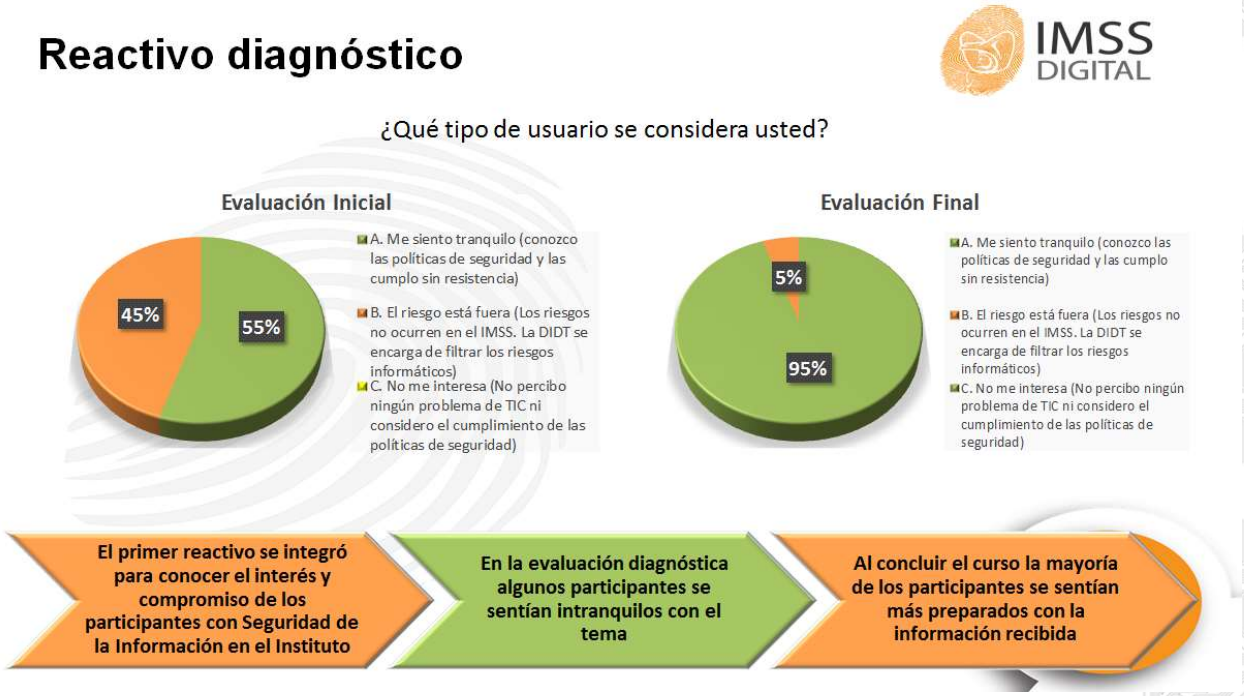


Figura 8 *Resultados de las encuestas de salida – curso de seguridad de la información.*
Fuente: Elaboración propia.

Como se puede observar, la evaluación inicial mostró 55% de satisfacción sobre las políticas de seguridad implementadas, pero el resultado final muestra un 95% de satisfacción, ya que posterior a la capacitación recibida, el personal se encuentra mucho más consiente de los esfuerzos realizados en materia de seguridad de la información.

Una vez que se demostró la importancia del curso en materia de seguridad de la información y el interés general de los usuarios institucionales, se pudo realizar la capacitación con presupuesto aprobado por la Dirección de Innovación y Desarrollo Tecnológico, para los usuarios en las Delegaciones del IMSS. En la siguiente figura se reliza una comparativa de resultados con éstos usuarios:

Figura 9 *Comparativa de capacitación entre usuarios en Nivel Central vs. Delegaciones (CDI's).*

Fuente: Elaboración propia.

Otro elemento importante de difusión interna, fueron los correos electrónicos con boletines de seguridad, los cuales promovían el cumplimiento de los nuevos lineamientos en materia de seguridad de la información. Un ejemplo de éstos (Anexo 3) contiene lineamientos del ASI-ACT-10 Criterios aplicables a la protección de equipo de cómputo perteneciente al Instituto.

Debido a que el Instituto tiene más de cuatrocientos mil empleados, el alcance para este curso de manera presencial es demasiado ambicioso. Por lo que se procedió a diseñar el modelo de curso en línea, cubriendo el mismo temario, con una duración de una semana. Al momento del cierre del presente trabajo de investigación, el IMSS tenía este proyecto en espera, ya que no se contaba con la infraestructura suficiente para su despliegue. Sin embargo, todo el material quedó diseñado y elaborado.

Capítulo 3
Taxonomía del riesgo

Capítulo 3. Taxonomía del riesgo

Para poder realizar una adecuada taxonomía o clasificación del riesgo en el IMSS, es necesario conocer y dominar el contexto bajo el cual opera y lo que es realmente importante para asignar los recursos adecuados en materia de TIC. La motivación de este análisis, proviene de la identificación de los activos del IMSS y a los cuales se requiere poner mayor énfasis y atención. Esto permitirá una administración de recursos mucho más adecuada a sus necesidades, pero sobre todo, a una gestión del riesgo más eficiente y eficaz.

3.1 Identificación de los activos clave de la entidad

La identificación de activos clave en el IMSS se realzó con base a su misión, establecida como sigue:

> ..." La misión del IMSS es ser el instrumento básico de la seguridad social, establecido como un servicio público de carácter nacional, para todos los trabajadores y sus familias" (Instituto Mexicano del Seguro Social, 2014).

El IMSS tiene dos vertientes funcionales que le dan sentido a su creación y operación, las cuales se muestran a continuación:

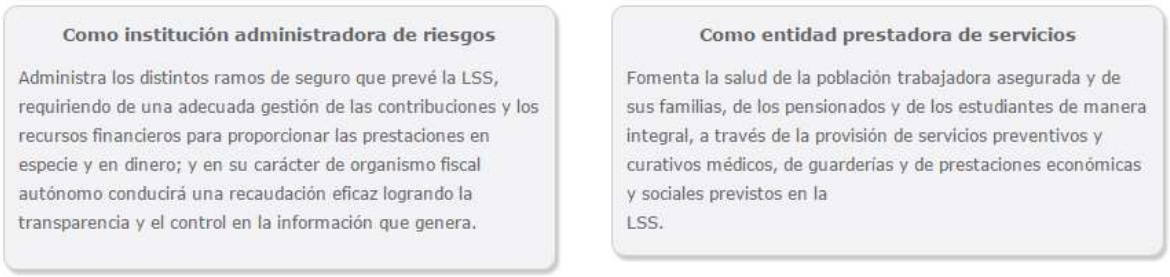


Figura 10 *Vertientes funcionales del Instituto Mexicano del Seguro Social.*

Fuente: *(Instituto Mexicano del Seguro Social, 2014)*

Bajo estas dos vertientes, se realizó la identificación de procesos de negocio críticos para su operación, a través de los cuales se obtuvo un levantamiento de activos de tecnologías de la información. Algunos de sus elementos fueron:

Identificación del activo. Que el activo esté soportando un proceso de negocio crítico para la institución.

Tipo de activo. Qué tipo de activo es, de información o de tecnologías de la información.

Dueño del activo. Se registró el dueño de la información, así como el dueño de la infraestructura tecnológica que la soporta y opera.

Clasificación. Se generó una matriz con diversas ponderaciones, permitiendo identificar aquéllas infraestructuras que tienen mayor impacto económico, social o de imagen, en caso de pérdida o caída del sistema.

Análisis de riesgos. Una vez que se obtuvo la matriz de infraestructura considerada como crítica, el IMSS procedió a realizar el reconocimiento de riesgo para cada aplicativo que formaba parte de éste catálogo de infraestructuras críticas.

Amenazas y agentes de amenaza. Esta lista se creó con base en los posibles agentes de amenaza y amenazas que pudieran materializar un riesgo. Este listado aplica para todas las entidades de la Función Pública, dado el escenario del IMSS se redujeron a las que podrían afectar su operación.

Vulnerabilidades. A partir del momento en que existe interés por obtener beneficios de la información con la que cuenta la institución, existe la posibilidad de buscar vulnerabilidades o puntos débiles en su protección para aprovecharla y materializar el riesgo. Existen diversos tipos de vulnerabilidades, las cuales pueden ser ambientales (desastres naturales, ubicación física, capacidad técnica, etc.), económicas (falta de recursos, escasez, etc.), normativas (falta de definición de procedimientos y/o políticas), sociales/culturales (comportamientos, conductas, relaciones, etc.), y/o técnicas (fallas en el sistema, puertos abiertos, malas configuraciones, etc.).

Escenarios de riesgo y Declaraciones de aplicabilidad

El reconocimiento del riesgo nos permite realizar actividades preventivas, reactivas y de remediación. Es precisamente el tratamiento a los riesgos lo que nos ayuda a minimizar el impacto del daño a la información considerada como sensible. Está comprobado que los costos por pérdida de información anual suelen ser incuantificable en muchos de los casos, por este motivo resulta de vital importancia tener dos programas en relación a los escenarios de riesgos identificados:

- Programa de mitigación de riesgos.
- Programa de contingencia a los riesgos.

Una vez que se obtienen los escenarios de riesgo recurrentes, es decir, basado en el factor de exposición y la posibilidad de repetición de la incidencia, se pueden generar declaraciones de aplicabilidad, que son “fichas ejecutivas” de reacción en caso de materializarse un escenario de riesgo dado. Estas declaraciones de aplicabilidad son una lista de actividades a realizar, de manera muy ejecutiva la descripción del escenario de riesgo, su ponderación, el responsable de la ejecución, así como el control de seguridad que permitirá disminuir o controlar el riesgo, protegiendo así la información o activo expuesto.

Posterior a la obtención de los resultados del análisis de riesgos, se integran los controles derivados de éste ejercicio, así como los controles mínimos de seguridad. Con la suma de ambos controles, se procede a la implementación del sistema de gestión de seguridad de la información SGSI en el IMSS. El programa de implementación del SGSI contempla también otros elementos que se basan en la ISO 27001:2013, a fin de obtener sus artefactos operacionales. Dichos elementos, serán evaluados y manejados en un proceso de mejora continua. Todos estos elementos son integrados en el repositorio del SGSI y se preservan para el siguiente ciclo y así continuar el cumplimiento del Ciclo de Deming, mencionado en el capítulo 1 del presente trabajo.

3.2 Un Sistema de Gestión de Seguridad de la Información (SGSI) implementado.

En el Instituto Mexicano del Seguro Social, durante el año de 2017 se realizó la primera implementación del sistema de gestión de seguridad de la información de manera

integral, es decir, con todas las fases que el ciclo de Deming determina y se detalla en el punto 1.2 del presente documento. A fin de obtener de manera gráfica las actividades, productos, activos y demás artefactos derivados de la ejecución del SGSI, se diseñó el siguiente gráfico (figura 11) en el cual es importante destacar lo siguiente:

Fase PLAN: En color verde, son actividades enfocadas a integrar el modelo de gobierno del SGSI, sus roles y responsabilidades. Del mismo modo, determina la criticidad de los activos de tecnologías de la información claves del IMSS que garanticen su operación, a fin de integrar un catálogo que es entregado al equipo que realiza un análisis de riesgos enfocado únicamente a dichos activos clave, para integrar controles de seguridad de la información.

Fase DO: En color amarillo, son aquéllas actividades que determinan la implementación del SGSI, con la implementación de los controles determinados en la fase previa, así como el registro de incidentes de seguridad ya catalogados como tal.

Fase CHECK: Actividades marcadas en azul, son aquéllas mediante las cuales se realiza una evaluación al SGSI misma que puede contemplar los productos elaborados, los controles implementados así como su eficiencia de operación. Se genera un informe que se entrega a la cuarta y última fase del ciclo.

Fase ACT: En color rojo, son actividades destinadas a llevar a cabo la mejora del SGSI, posterior a la validación de su desempeño. En caso de aplicar, se realizan actividades correctivas y preventivas que permiten el cierre del ciclo para proceder en una mejora continua del mismo.

El valor agregado del presente trabajo de tesis para este capítulo, son los artefactos operacionales del SGSI, a través de los lineamientos generados conjuntamente con las áreas de tecnologías de la información del IMSS, detallados previamente en el punto 1.3.

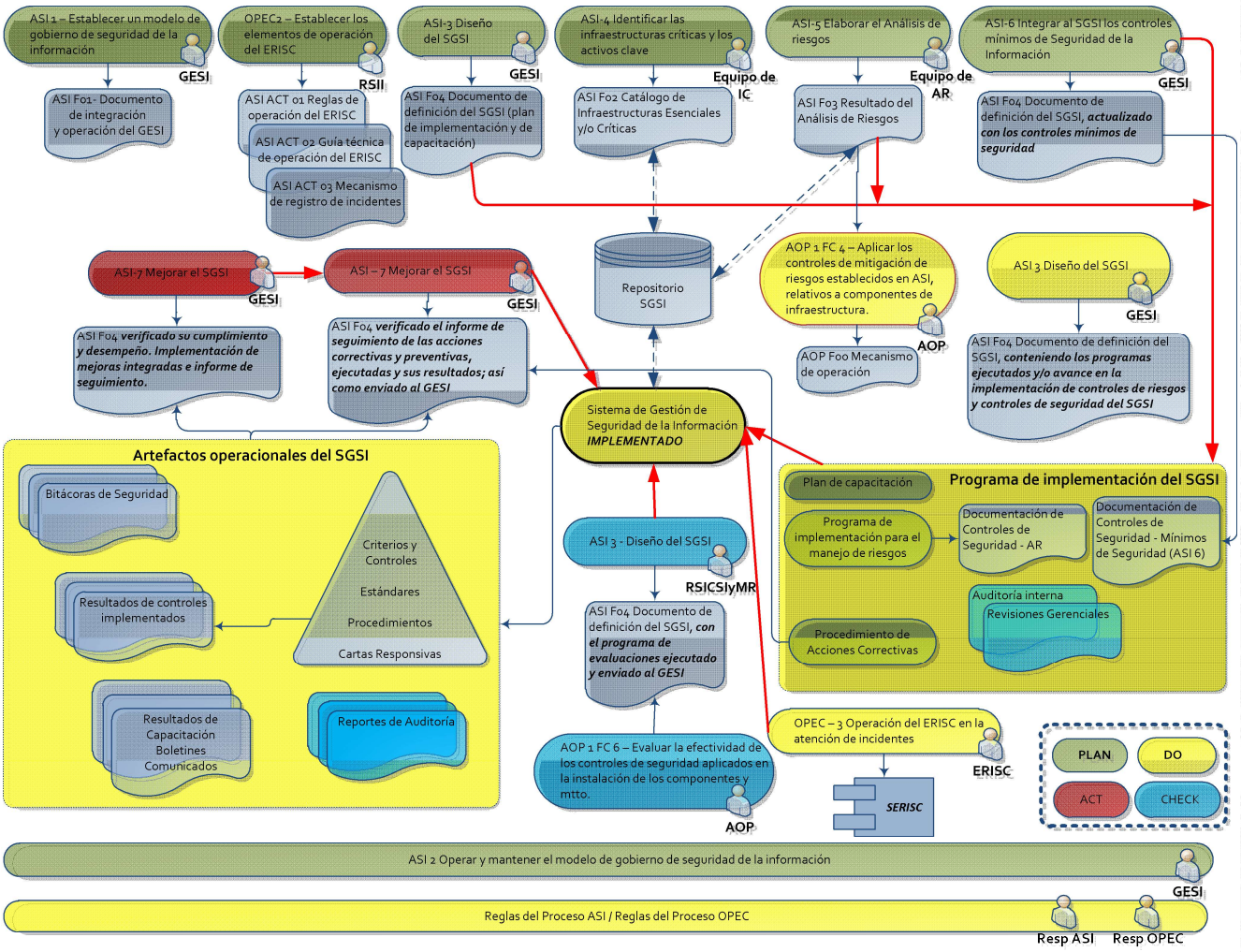


Figura 11 *Propuesta metodológica, framework de seguridad implementado en el IMSS.*

Fuente: Elaboración propia.

3.3 Taxonomía, clases, subclases y elementos.

Como ya se ha identificado, en el IMSS existen y operan diversos activos de información que permiten la entrega de los servicios que ofrece a la población derechohabiente. Estos, se encuentran registrados en un Inventario Único de Aplicaciones-IUA (Anexo 4) el cual contempla diversos servicios de TIC, que han sido clasificados como se muestra a continuación:

Figura 12 *Inventario Único de Aplicaciones correspondientes al registro del Q1 de 2018.*

Fuente: *(Instituto Mexicano del Seguro Social, 2018).*

El universo de aplicaciones registradas, apoyan la entrega de servicios de cara al derechohabiente y existen diversas relaciones entre ellas. Estas relaciones, permiten que los procesos de negocio institucionales operen de manera segura. Al estar expuestas a diversos riesgos, se plantea la taxonomía de riesgos que identifica y organiza estos riesgos en cuatro clases principales:

I. Acciones de la gente;
II. Fallas en los sistemas e infraestructura;

III. Fallas en procesos internos; y
IV. Eventos externos.

Cada clase, es dividida en subclases, los cuales a su vez se describen en elementos. Una vez que tengamos el nivel más atómico en su descripción, estaremos en posibilidades de describir sus atributos. La intención de esta taxonomía, es poder clasificar con un enfoque coherente y medible, los riesgos asociados que puedan afectar la operación de los servicios de TIC, y esto a su vez, provocar daño en la entrega de los servicios institucionales.

Los atributos de cada uno de los elementos, permitirá llegar a un análisis de vulnerabilidades comunes, que afecta o pueda afectar los activos de información identificados, ante la posibilidad de la materialización de un riesgo asociado. El encontrar factores comunes de riesgo a través de estos análisis de vulnerabilidades, permitirán un tratamiento de riesgos adecuados, a través de las siguientes estrategias:

- *Aceptar*. Una vez calculado el impacto del riesgo, se determina que puede ser aceptado.
- *Disminuir*. Se pueden fortalecer los controles existentes o implantar nuevos.
- *Transferir*. Mediante contratos o acuerdos compartidos, el riesgo puede ser traspasado a un tercero.
- *Evitar*. Puede llegarse el caso de eliminar el activo de información que genera el riesgo, evitando así mayores daños.

La siguiente taxonomía se encuentra basada en “Una Taxonomía de Riesgos Operacionales de Ciberseguridad” propuesta por James J. Cebula (2010), la cual está enfocada en riesgos operacionales en materia de tecnologías de la información.

Una forma de ver más claramente la estrategia planteada, se muestra el siguiente gráfico:

Figura 13 *Estrategia global para la taxonomía de riesgos en el IMSS.*

Fuente: Elaboración propia.

Se toman las 217 aplicaciones registradas en la Dirección de Innovación y Desarrollo Tecnológico, a través del Inventario Único de Aplicaciones, lo anterior con la finalidad de filtrar aquéllas que se consideren esenciales y/o críticas, para llegar a un total de 31 activos que pueden llegar a afectar la operación institucional en caso de fallar o degradar su desempeño. Finalmente, procedemos a ejecutar el proceso de análisis de riesgo para determinar los controles que serán implementados.

3.4 Análisis de vulnerabilidades.

El análisis de vulnerabilidades es una evaluación de las posibles debilidades que puedan presentar los activos de información, cuyas características son susceptibles de un daño dirigido. Por lo anterior, es el ejercicio que determina los escenarios de riesgo reales en la base tecnológica del IMSS. Este análisis de vulnerabilidades, comienza con una detección de amenazas[15] y agentes de amenaza[16] que, de manera conjunta pueden explotar una vulnerabilidad latente en la infraestructura institucional. Catalogaremos una lista común de amenazas con sus respectivos agentes de amenaza

[15] Una amenaza es un peligro latente que tiene cierta posibilidad de que ocurra podría afectar personas, circunstancias o en este caso, información.

[16] Un agente de amenaza es el medio por el cual la amenaza se concreta, muchas veces por intervención humana.

en un listado de vulnerabilidades comunes al interior. A dicho listado, se le agrega un número de referencia que permite una sola identificación a la combinación de ambos elementos:

No.	Amenaza	Agentes de Amenaza
1357	Deficiencia en el desarrollo	Personal interno inexperto (no intencional)
1358		Proveedor/Contratista
1354	Acceso no autorizado	Newbie
1101		Script Kiddies
1090		Hacker
1100		Ex-empleado
1355		Cracker
1359	Deficiencia en la configuración	Personal interno inexperto (no intencional)
1360		Proveedor/Contratista
1361	Intercepción de información	Hacker
1362		Newbie
1363	Denegación de Servicio	Hacker
1364		Script Kiddies
1365	Divulgación de información	Hacker
1366		Newbie
1367	Ejecución de comandos	Hacker
1368		Newbie
1369		Script Kiddies
1370	Afectación a la confidencialidad de la información	Hacker
1371		Newbie
1372		Script Kiddies
1373		Ex-empleado
1374	Inyección de código	Hacker
1375		Newbie
1376		Script Kiddies
1125	Suplantación de Identidad	Hacker
1356		Newbie
1135		Ex-empleado

1113	Código malicioso	Hacker

Cuadro 1 *Lista de Amenazas y Agentes de Amenaza en el Análisis de Riesgos Institucional.*

Fuente: *(Instituto Mexicano del Seguro Social, 2018)*.

A continuación, se listan estas vulnerabilidades, en muchos casos con infraestructuras críticas compartidas:

No.	Vulnerabilidades detectadas
1	Paginas por defecto
2	Sesión nula habilitada
3	Usuario anonymous habilitado
4	Ausencia de HSTS en el aplicativo
5	Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure
6	Enumeración de usuarios por SMTP
7	Open Relay
8	Cookie no marcados como HttpOnly
9	Método OPTIONS habilitado
10	Divulgación de información (Direcciones IP internas)
11	Usuario anonymous en FTP
12	Conexión a Escritorio Remoto
13	Inyección de código en WebLogic
14	Comunidad de SNMP pública
15	Inyección de SQL
16	Cross-Site Scripting
17	Credenciales Comunes
18	Servicio SSH Vulnerable a Ataques de Diccionario
19	Configuración por defecto

No.	Vulnerabilidades detectadas
20	Credenciales de usuario son enviadas en texto claro
21	Apache 2.x versión más antigua que 2.2.9
22	Servicio Telnet
23	Parámetro __VIEWSTATE descifrado
24	Revelación de información
25	Autocomplete habilitado
26	ClickJacking X-frame-options header missing
27	Listado de directorios
28	Servicio Vulnerable a Ataques Diccionario
29	Envenenamiento de TNS
30	Información sensible expuesta

Cuadro 2 *Lista de vulnerabilidades detectadas en las infraestructuras críticas del IMSS.* Fuente: *(Instituto Mexicano del Seguro Social, 2018)*.

A éste análisis de amenazas, se deben determinar los siguientes elementos:

Probabilidad de la existencia del agente de amenaza, que materialice el riesgo. La categorización y los valores correspondientes, se mencionan en la siguiente tabla:

Valor	Probabilidad de existencia del agente amenaza
0.9	Es casi seguro que existe
0.7	Es muy posible que exista
0.5	Es probable que exista
0.3	Es poco probable que exista
0.1	Es casi imposible que exista

Cuadro 3 *Existencia del "agente de amenaza" para el cálculo de P.* Fuente: *(Secretaría de la Función Pública, 2014)*.

Del mismo modo se procede a determinar el posible interés que genere provocar dicha afectación. La tabla siguiente determina los valores correspondientes:

Valor	Nivel de interés del agente amenaza
0.9	El interés es incontrolable
0.7	Se genera mucho interés
0.5	Se genera regular interés
0.3	Se genera poco interés
0.1	Casi no se genera interés

Cuadro 4 *Niveles de interés del agente de amenaza para el cálculo de P.*

Fuente: *(Secretaría de la Función Pública, 2014)*.

La capacidad del agente de amenaza, es un elemento importante a considerar. La siguiente tabla enuncia dichos valores:

Valor	Nivel de capacidad del agente amenaza
0.9	Los recursos son superiores
0.7	Cuenta con muchos recursos
0.5	Los recursos son regulares
0.3	Cuenta con muy pocos recursos
0.1	Los recursos son casi nulos

Cuadro 5 *Capacidad del agente de amenaza para el cálculo de P.*

Fuente: *(Secretaría de la Función Pública, 2014)*.

El último elemento para poder calcular la probabilidad de materialización del riesgo es el tipo de protección con el que cuenta, considerando su nivel de vulnerabilidad:

Valor	Vulnerabilidad del activo de información
0.9	Sin ningún tipo de protección

0.7	Muy poca protección
0.5	Medianamente protegido
0.3	Protección normal
0.1	Protección reforzada

Cuadro 6 *Vulnerabilidad del activo de información para el cálculo de P*.

Fuente: *(Secretaría de la Función Pública, 2014)*.

Para el cálculo de probabilidad, se toman los datos de los cuatro elementos, y finalmente promediarlos en un valor único de P.

Como ejemplo, en la siguiente tabla se muestra una vulnerabilidad detectada en un aplicativo denominado CVOED - Centro Virtual de Operación en Escenarios de Desastre (Gobierno de México - IMSS, 2018) con la aplicación de valores para cada parámetro, obteniendo lo siguiente:

Vulnerabilidad	Código	Amenaza	Agente Amenaza	Activo	Probabilidad de Existencia	E	Interés del agente de amenaza	valor	Capacidad del agente de amenaza	valor	Vulnerabilidades del activo	valor	P
Cross-Site Scripting	1357	Deficiencia en el desarrollo	Personal interno inexperto (no intencional)	CVOED	Es probable que exista	0.5	Casi no se genera interés	0.1	Los recursos son regulares	0.5	Sin ningún tipo de protección	0.9	0.50
	1358		Proveedor/ Contratista	CVOED	Es casi seguro que existe	0.9	Casi no se genera interés	0.1	Los recursos son regulares	0.5	Medianamente protegido	0.5	0.50
	1374	Inyección de código	Hacker	CVOED	Es probable que exista	0.5	Se genera mucho interés	0.7	Cuenta con muchos recursos	0.7	Sin ningún tipo de protección	0.9	0.70
	1375		Newbie	CVOED	Es poco probable que exista	0.3	Se genera mucho interés	0.7	Cuenta con muy pocos recursos	0.3	Sin ningún tipo de protección	0.9	0.55
	1376		Script Kiddies	CVOED	Es poco probable que exista	0.3	Se genera mucho interés	0.7	Cuenta con muchos recursos	0.7	Sin ningún tipo de protección	0.9	0.65

Cuadro *7* *Ejemplo aplicado en el activo CVOED para el cálculo de P*.

Fuente: (Instituto Mexicano del Seguro Social, 2018).

En el presente ejemplo, para el activo o sistema de información CVOED, la vulnerabilidad de "*Cross-Site Scripting*[17]", puede ser provocada por la amenaza derivada de una deficiencia en el desarrollo y/o inyección de código. Dicha vulnerabilidad puede ser materializada por diversos agentes de amenaza, que pueden resultar en personal interno inexperto, proveedor/contratista, *hacker*, *newbie*[18] o bien un *script kiddie*[19]. Si además se analiza la probabilidad más alta de que la vulnerabilidad sea materializada a través del riesgo como tal, es la existencia de un *hacker* que aproveche la deficiencia del desarrollador, para inyectar código y comprometer la integridad de la información.

El siguiente paso es la determinación de impactos para la valorización del riesgo. Los datos se muestran en la siguiente tabla:

	Impacto	**Humano (ih)**	**Material (im)**	**Financiero (if)**	**Operativo (io)**	**Imagen (ii)**
10	Desastroso	Muertes	Pérdidas graves no recuperables	Más de $1,000,000.00	Afectación de procesos críticos que no pueden restablecerse en menos de dos días	Difusión a nivel internacional
8	Gran impacto	Heridos	Pérdidas graves recuperables a largo plazo	Entre $100,000.00 y $1,000,000.00	Afectación de procesos críticos, que pueden restablecerse en menos de dos días	Difusión a nivel nacional
6	Regular impacto	Lesiones que producen una incapacidad	Pérdidas leves no recuperables	Entre $50,000.00 y $100,000.00	Afectación de varios procesos no críticos	Difusión a nivel local
4	Mínimo impacto	Lesiones leves	Pérdidas leves recuperables	Entre $10,000.00 y $50,000.00	Afectación de un proceso no crítico	Difusión dentro de la dependencia o entidad
2	Insignificante	Sin lesiones	Sin pérdidas materiales	Menor de $10,000.00	Sin afectación de procesos	Difusión dentro de la unidad

Cuadro 8 *Nivel de impacto para el cálculo de R.*

Fuente: *(Secretaría de la Función Pública, 2014).*

[17] Es una vulnerabilidad muy común en sitios web que permite la ejecución de código remoto por un atacante.
[18] Regularmente se trata de personas que aspiran a ser hackers buscando información disponible en la Internet.
[19] Estos personajes buscan información y utilizan software libre para hackear pero generalmente no cuentan con las habilidades técnicas suficientes para lograr un ataque efectivo.

A diferencia del cálculo de P, una vez evaluado cada uno de los cincos tipos de impacto, únicamente se utilizará el valor más alto que se haya obtenido, a fin de sustituirlo en la fórmula principal R= PI.

Finalmente, para la evaluación de los riesgos, se toma el valor obtenido para R, donde se aplicará la implementación de un control, sobre aquéllos que tengan valor mayor a 1.8. Para efectos del IMSS, el valor más alto obtenido en el cálculo del riesgo fue de 7.0, considerado muy alto dado los escenarios institucionales.

A raíz de los escenarios de riesgo encontrados, se elabora una lista de controles recomendados a implementar, donde el criterio de implementación será la mitigación/reducción del riesgo aplicable a infraestructura crítica institucional, cuyo enfoque de análisis es la seguridad de la información.

Para darle continuidad a los ejemplos presentados, a continuación, se muestra la tabla para la determinación de impactos de la anterior infraestructura crítica:

Vulnerabilidad	Código	Amenaza	Agente Amenaza	Activo	Impacto Humano	Nivel	Impacto Material	valor	Impacto Financiero	valor	Impacto Operativo	valor	Impacto de Imagen	valor	I	R
Cross-Site Scripting	1357	Deficiencia en el desarrollo	Personal interno inexperto (no intencional)	CVOED	Sin lesiones	2	Sin pérdidas materiales	2	Menor de $10,000.00	2	Sin afectación de procesos	2	Difusión dentro de la unidad	2	2	1
	1358		Proveedor/ Contratista	CVOED	Sin lesiones	2	Sin pérdidas materiales	2	Menor de $10,000.00	2	Sin afectación de procesos	2	Difusión dentro de la unidad	2	2	1
	1374	Inyección de código	Hacker	CVOED	Sin lesiones	2	Sin pérdidas materiales	2	Menor de $10,000.00	2	Afectación de procesos críticos, que pueden restablecerse en menos de dos días	8	Difusión a nivel nacional	8	8	5.6
	1375		Newbie	CVOED	Sin lesiones	2	Sin pérdidas materiales	2	Menor de $10,000.00	2	Afectación de varios procesos no críticos	6	Difusión a nivel nacional	8	8	4.4
	1376		Script Kiddies	CVOED	Sin lesiones	2	Sin pérdidas materiales	2	Menor de $10,000.00	2	Afectación de procesos críticos, que pueden restablecerse en menos de dos días	8	Difusión a nivel nacional	8	8	5.2

Cuadro 9 *Determinación de impactos en infraestructuras críticas del IMSS*.

Fuente: *(Instituto Mexicano del Seguro Social, 2018)*.

A continuación, se muestran los niveles de criticidad asociados a los escenarios de riesgo conducentes:

Niveles de Riesgo	
Crítico	
Alto	
Medio	
Bajo	
Nulo	

Cuadro 10 *Nivel de riesgo para los escenarios en el IMSS*.

Fuente: *(Instituto Mexicano del Seguro Social, 2018)*.

Número de riesgo	Riesgo	Aplicación	¿El servicio se encuentra expuesto a internet?	Causas (Agentes)	Nivel de Riesgo	Control Sugerido
1	Aplicación vulnerable a inyección de código SQL que permitiría acceso no autorizado a bases de datos que afecten la confidencialidad, integridad y disponibilidad de la información.	CVOED	Si	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker, Newbie, Script Kiddies		CTROL-AR-2018-01
2	Aplicación vulnerable a inyección de código SQL que permitiría acceso no autorizado a bases de datos que afecten la confidencialidad, integridad y disponibilidad de la información.	DAPSUA, SIAP	No	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-01
3	Aplicación vulnerable a ejecución de código JavaScript que permitiría desplegar ventanas o mensajes emergentes afectando la disponibilidad de la información.	CVOED, IDSE	Si	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker, Newbie, Script Kiddies		CTROL-AR-2018-01

Número de riesgo	Riesgo	Aplicación	¿El servicio se encuentra expuesto a internet?	Causas (Agentes)	Nivel de Riesgo	Control Sugerido
4	Aplicación vulnerable a ejecución de código JavaScript que permitiría desplegar ventanas o mensajes emergentes afectando la disponibilidad de la información.	SIMF	No	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-01
5	Aplicación que utiliza credenciales comunes o débiles permitiría el acceso no autorizado y la suplantación de identidad afectando la confidencialidad, integridad y disponibilidad de la información.	CVOED	Si	Hacker, Newbie, Ex-empleado		CTROL-AR-2018-02
6	Aplicación que utiliza credenciales comunes o débiles permitiría el acceso no autorizado y la suplantación de identidad afectando la confidencialidad, integridad y disponibilidad de la información.	NSSA, AUTOPAC	No	Hacker, Ex-empleado		CTROL-AR-2018-02
7	Aplicación vulnerable a ataque de diccionario o de fuerza bruta permitiría obtener las credenciales de acceso al servicio SSH afectando la confidencialidad, integridad y disponibilidad de la información.	CVOED, Sitio Web Institucional, AsigNSS, PREI, SIAP, SINOLAVE, SISTRAP, NSSA, CSI, IMSS Digital - Zona Aplicativa Patronal, IVRO, CVRO y SSF, DM. SICADIT, AUTOPAC	No	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-03
8	Aplicación que permite el envío de información en texto claro, la cual podría ser interceptada afectando la confidencialidad de la misma.	SIPARE, SAI, SAIF, Sitio Web Institucional, IDSE	Si	Hacker, Newbie		CTROL-AR-2018-04
9	Aplicación que permite el envío de información en texto claro, la cual podría ser interceptada afectando la confidencialidad de la misma.	SIMF, SINOLAVE, SICEH	No	Hacker		CTROL-AR-2018-04

Número de riesgo	Riesgo	Aplicación	¿El servicio se encuentra expuesto a internet?	Causas (Agentes)	Nivel de Riesgo	Control Sugerido
10	Aplicación que utiliza el servicio Telnet que permite el envío de información en texto claro, la cual podría ser interceptada afectando la confidencialidad de la misma.	CANASE, SIMF, SINDO, EBA y EMA, Certificación, SISCOB	No	Hacker		CTROL-AR-2018-06
11	Aplicación vulnerable a ataque de diccionario o de fuerza bruta permitiría obtener las credenciales de acceso al servicio web afectando la confidencialidad, integridad y disponibilidad de la información.	IDSE	Si	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker, Newbie, Cracker		CTROL-AR-2018-03
12	Aplicación vulnerable a ataque de diccionario o de fuerza bruta permitiría obtener las credenciales de acceso al servicio web afectando la confidencialidad, integridad y disponibilidad de la información.	SIMF	No	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-03
13	Aplicación vulnerable a ataque de diccionario o de fuerza bruta permitiría obtener las credenciales de acceso al FTP o a la base de datos DB2 afectando la confidencialidad, integridad y disponibilidad de la información.	SPES	No	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-03
14	Aplicación que cuenta con una versión vulnerable de Apache que permitiría realizar un ataque de denegación de servicio afectando la disponibilidad de la información.	SIPARE, Correo Electrónico	Si	Hacker, Script Kiddies		CTROL-AR-2018-05
15	Aplicación que muestre los usuarios utilizados en el formulario web para acceder en la aplicación permitiría realizar una lista de usuarios para intentar encontrar otros nombres de usuario y sus posibles contraseñas.	SAI, SAIF, Sitio Web Institucional	Si	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-07
16	Aplicación que muestre los usuarios utilizados en el formulario web para acceder en la aplicación permitiría realizar	SIMF	No	Personal interno inexperto (no intencional), Proveedor/Contratista,		CTROL-AR-2018-07

Número de riesgo	Riesgo	Aplicación	¿El servicio se encuentra expuesto a internet?	Causas (Agentes)	Nivel de Riesgo	Control Sugerido
	una lista de usuarios para intentar encontrar otros nombres de usuario y sus posibles contraseñas.			Hacker		
17	Aplicación que cuente con el usuario Anonymous habilitado en el FTP permitiría tener accesos no autorizados sin necesidad de una contraseña o con contraseñas conocidas para dicho usuario afectando la confidencialidad, integridad y disponibilidad de la información.	SIMF, SICEH	No	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-08
18	Servidor de aplicaciones Oracle WebLogic que no cuente con los parches de seguridad necesarios permitiría, mediante el uso de un script, la ejecución de comandos que afectarían la confidencialidad, la integridad y la disponibilidad de la información.	DAPSUA, AsigNSS, MAC, IVRO, CVRO y SSF, IMSS Digital - Zona Aplicativa Patronal, CSI, AUTOPAC	No	Hacker		CTROL-AR-2018-09
19	El Listener de Oracle permitiría que el tráfico que viaja en un canal de comunicación sea controlado y se afecte la confidencialidad y la integridad de la información.	PREI, DM, SICADIT, CSI, AUTOPAC	No	Hacker		CTROL-AR-2018-10
20	Aplicación que no cuente con la configuración adecuada de las cabeceras X-Frame Options permitiría redireccionamientos a sitios web o descargas de programas potencialmente maliciosos.	SAI, SAIF	Si	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-11
21	Servidor que tenga habilitada la sesión nula permitiría obtener información sobre el equipo.	SIMF	No	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-12

Número de riesgo	Riesgo	Aplicación	¿El servicio se encuentra expuesto a internet?	Causas (Agentes)	Nivel de Riesgo	Control Sugerido
22	Aplicación que no cuente con la configuración adecuada de las cookies permitiría obtener información del servidor, así como, la ejecución de código para el despliegue de ventanas o mensajes emergentes afectando la confidencialidad y la disponibilidad de la información.	ECE	No	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-13
23	Aplicación que mantenga configuraciones o instalaciones por defecto permitiría la divulgación de información de los servicios que son utilizados para el funcionamiento (páginas por defecto de Apache, ISS, WebLogic, PHP, etc.) y para la administración (Escritorio Remoto Disponible), del direccionamiento interno y la información de los proveedores del Instituto.	CVOED, SAI, SAIF, Sitio Web Institucional, IDSE	Si	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-14
24	Aplicación que mantenga configuraciones o instalaciones por defecto permitiría la divulgación de información de los servicios que son utilizados para el funcionamiento (páginas por defecto de Apache, ISS, WebLogic, PHP, etc.) y para la administración (Escritorio Remoto Disponible), del direccionamiento interno y la información de los proveedores del Instituto.	SIMF, Acceder Unificado, DAPSUA, AsigNSS, BDTU, SIAP, SINOLAVE, SICEH, ECE, IVRO, CVRO y SSF, IMSS Digital - Zona Aplicativa Patronal, CSI, AUTOPAC	No	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-14
25	Aplicación vulnerable a ataque POODLE permitiría el descifrado de la información que viaja a través de un canal que utiliza el protocolo SSLv3.	IMSS Digital-Zona Aplicativa Patronal	No	Hacker, Script Kiddies		CTROL-AR-2018-15
26	La ejecución de servidores falsos de red, que se encuentran a la escucha de consultas específicas de NBT-NS, LLMNR, mDNS, e intenta envenenar al emisor, permitiría obtener la información que se trata de transmitir.	Directorio Activo	No	Hacker		CTROL-AR-2018-16

Número de riesgo	Riesgo	Aplicación	¿El servicio se encuentra expuesto a internet?	Causas (Agentes)	Nivel de Riesgo	Control Sugerido
27	Servidor DNS que responda a petición de terceros sin tener el bit de recursión habilitado permitiría conocer los dominios que han sido resueltos y obtener información de los equipos que han sido visitados.	Directorio Activo	No	Hacker		CTROL-AR-2018-17
28	Aplicación que mediante NFS permita la lectura y escritura, en una carpeta compartida, a cualquier usuario, permitiría la modificación de la información no autorizada afectando la confidencialidad, integridad y disponibilidad de la misma.	AUTOPAC	No	Personal interno inexperto (no intencional), Proveedor/Contratista, Hacker		CTROL-AR-2018-18
29	Servidor Microsoft Exchange que no cuente con la configuración adecuada del parámetro "realm" permitiría conocer el direccionamiento interno	Correo Electrónico	Si	Hacker		CTROL-AR-2018-19

Cuadro 11 *Escenarios de riesgo enfocados a ciberseguridad en el IMSS.*

Fuente: *(Instituto Mexicano del Seguro Social, 2018)*.

La complejidad de los escenarios de riesgo encontrados como parte del análisis de riesgos a las infraestructuras críticas y/o esenciales del IMSS, permite identificar que existen una gran variedad de combinaciones en la construcción de aplicaciones. Lo anterior, puede evitarse intervenciones tempranas por parte de seguridad informática así como la homologación de criterios para el desarrollo de código seguro.

La última parte del análisis de riesgos consiste en el acompañamiento con cada líder de aplicativo que presenta vulnerabilidades, con la implementación del control de seguridad propuesto como parte de la estrategia de seguridad de la información.

Este acompañamiento, contempla la ejecución de actividades diversas, como puede ser la modificación de parámetros en las configuraciones por defecto

en las aplicaciones, o bien, evitar las contraseñas comunes. Algunos ejemplos se enlistan a continuación:

1. *Validación del número de intentos de inicio de sesión a los servicios y aplicaciones (5 intentos como máx.)*. Esta actividad implica cambios en el código de las aplicaciones a fin de limitar el número de intentos de acceso.
2. *Validación del uso de HTTPS[20] en las aplicaciones web de las infraestructuras esenciales y/o críticas*. Para subsanar esta vulnerabilidad, es necesario la implementación de un certificado de seguridad, el cual agregará una capa de seguridad a la navegación de la aplicación en Internet.
3. *Validación de la entrada y salida de datos de las peticiones realizadas en la aplicación web (caracteres no permitidos en formularios web y campos de URL[21]).* En la búsqueda de subsanar esta vulnerabilidad, lo que tendría que realizar el equipo de desarrollo, es la modificación en los campos de los formularios, a fin de cerrar el tipo de dato solicitado.

Para facilitar su interpretación, se muestra una lista de controles[22] a implementar, con base a su propósito:

Grupo de Riesgos	Control	Descripción del Control
Controles para mitigación de riesgos en aplicaciones web	CTROL-AR-2018-01	Validación de la entrada y salida de datos de las peticiones realizadas en la aplicación web (Caracteres no permitidos en formularios web y campos de URL)
	CTROL-AR-2018-03	Validación del número de intentos de inicio de sesión a los servicios y aplicaciones (5 intentos como máx.).
	CTROL-AR-2018-04	Validación del uso de HTTPS en las aplicaciones.
	CTROL-AR-2018-05	Validación del uso de versiones de Apache sin vulnerabilidades u obsoleto.
	CTROL-AR-2018-07	Validación de que el formulario web no muestra los nombres de usuario logueados en la aplicación.

[20] HTTPS: *Hypertext Transfer Protocol Secure* por sus siglas en inglés, es un mecanismo que incrementa la seguridad de comunicación entre el navegador y el servidor web donde se encuentra la información.
[21] URL: Uniform Resource Locator, es una secuencia de caracteres para poder localizar contenido en Internet.
[22] Controles de seguridad viables a implementar en el Instituto como parte del framework de seguridad.

Grupo de Riesgos	Control	Descripción del Control
	CTROL-AR-2018-11	Validación de la configuración adecuada de las cabeceras X-Frame Options en el servidor.
	CTROL-AR-2018-13	Validación de que las cookies de la aplicación web sean marcadas como HTTPOnly.
	CTROL-AR-2018-14	Validación de que las instalaciones no mantengan configuraciones por defecto o que permitan divulgación de información innecesaria.
	CTROL-AR-2018-15	Validación del uso del protocolo TLS 1.2 y no del protocolo SSLv3
Controles para mitigación de riesgos en servicios de Sistema Operativo	CTROL-AR-2018-03	Validación del número de intentos de inicio de sesión a los servicios y aplicaciones (5 intentos como máx.).
	CTROL-AR-2018-06	Validación del no uso del servicio Telnet en el servidor.
	CTROL-AR-2018-12	Validación de que la sesión nula en el servidor Windows se encuentre deshabilitada.
	CTROL-AR-2018-18	Validar el correcto control de acceso sobre los recursos compartidos del servidor.
Controles para mitigación de riesgos en Oracle WebLogic	CTROL-AR-2018-09	Validación de la instalación de los parches de seguridad necesarios en el servidor de aplicaciones WebLogic.
Controles para mitigación de riesgos en Oracle Listener	CTROL-AR-2018-10	Validación de la configuración adecuada en el Listener de Oracle.
Controles para mitigación de riesgos sobre control de acceso	CTROL-AR-2018-02	Validación de los usuarios y contraseñas para acceder a los servicios y aplicaciones.
	CTROL-AR-2018-16	Verificación de cuentas de usuario con permisos limitados.
	CTROL-AR-2018-18	Validar el correcto control de acceso sobre los recursos compartidos del servidor.
Controles para mitigación de riesgos en servidores	CTROL-AR-2018-08	Validación de que el usuario Anonymous no se encuentra habilitado en el servidor FTP.
	CTROL-AR-2018-17	Validar que la recursión se encuentre deshabilitada en el servidor DNS.

Cuadro 12 *Controles de seguridad propuestos para implementar.*

Fuente: *(Instituto Mexicano del Seguro Social, 2018)*.

La implementación de controles de seguridad cumple con el objetivo de minimizar los escenarios de riesgo detectados, que permitan un manejo aceptable

del riesgo. Algunos de estos controles implementados, no generaron costos para el Instituto, otros requirieron un esfuerzo adicional por parte de los áreas técnicas con afectaciones mínimas a la operación y muy pocos no fue factible su aplicación. En estos últimos casos se protocolizaron cartas de aceptación de riesgos[23] y formaron parte del programa de contingencia de riesgos, en los casos en que llegue a materializarse el escenario de riesgo, todos los involucrados actuarán conforme la gravedad que se presente. Las áreas de negocio al interior del IMSS como pueden ser la Dirección de Prestaciones Médicas, la de Finanzas, la de Prestaciones Económicas y Sociales, así como la Dirección Administrativa y las áreas técnicas como son la Dirección de Innovación y Desarrollo, se encuentran en un nivel de tranquilidad mayor, en relación al inicio del ejercicio de determinación de análisis de riesgos tecnológicos, gracias a las acciones realizadas. Además de todo lo anterior, permitió que el Instituto cumpliera con todas las disposiciones del MAAGTICSI vigente en su momento.

[23] En el tratamiento de riesgos, la última opción es aceptarlos. Se generan contratos formales mediante los cuales todas las áreas involucradas deben firmar de consentimiento y actuar mediante lo determinado en las cartas de aceptación de riesgos.

Conclusiones

Conclusiones

Al realizar el presente trabajo de investigación, se encontraron los siguientes retos:

1. Resistencia al cambio.
2. Entendimiento de la estrategia.
3. Factibilidades de cambio – económica, capacitación, técnica-
4. Seguimiento y auditorías de cumplimiento.

A fin de contrarrestar estos retos, existen diversos factores clave que ayudaron a minimizar la resistencia al proyecto:

Influencia en el cambio: Reconocer la necesidad y ventajas que implica la implementación de este *framework* para reforzar la seguridad de la información del IMSS, combinada con el compromiso de la alta dirección, resultaron ser aspectos fundamentales para lograr el cambio organizacional.

Una clara visión compartida: Los beneficios de la implementación de este proyecto no obedecerán a un grupo específico, sino a todo el IMSS si cada uno de los involucrados es consciente de la importancia de cumplir con la parte de la cual es responsable. Al hacer conciencia en cada trabajador institucional sobre la importancia de proteger archivos, identidades, diagnósticos, así como otra información sensible, se hizo mucho más fácil la implementación del marco de referencia propuesto.

Capacidad de cambio: Para lograr esto, se tuvieron que disponer de todos los recursos necesarios, incluyendo tiempo y recursos financieros para llevar a cabo la capacitación y soporte durante su implementación e iteraciones de mejora. Durante las semanas de capacitación presencial, resultó de mucha ayuda que las unidades donde se realizó se contó con la presencia de los participantes en tiempo y forma.

Acción: Durante la implementación del *framework*, fue muy importante el acompañamiento de cambio con todos los involucrados, manteniendo abiertos todos los canales de comunicación. La presencia de nuestros compañeros de

soporte técnico en las diferentes unidades donde se realizó la capacitación fue de vital importancia, así como los responsables de las infraestructuras críticas que formaron parte del análisis de riesgos desarrollado.

Posterior a la implementación de un marco de referencia de seguridad de la información, que ha contemplado las dimensiones más importantes para la protección de los activos de información considerados como críticos o esenciales, podemos encontrar que se ha logrado a los objetivos iniciales del presente trabajo de tesis.

Las políticas de seguridad, al ser publicadas en la intranet del IMSS y estar a la disposición de cualquier funcionario público, trabajador y proveedor que utiliza la infraestructura tecnológica del Instituto permitió el incremento en los esquemas de protección a la confidencialidad, integridad y disponibilidad de la información.

Los mecanismos y herramientas planteados para el logro del fortalecimiento de la cultura de la seguridad de la información tuvieron un impacto positivo en todos los niveles de administración institucional, gracias a los esquemas de capacitación que se replicaron mediante el programa de capacitación avalado por la Secretaría del Trabajo y Previsión Social.

Adicionalmente, el enfoque de ciberseguridad en el análisis de riesgos, permitió que el análisis de riesgos visualizara posibles esquemas de ataque externos a la institución, cuya implementación de controles específicos para las infraestructuras críticas del IMSS mitigaran los escenarios de riesgo a los que se encontraban expuestas, situación inédita en el ejercicio de seguridad informática institucional.

En general, los resultados fueron favorecedores, una vez ejecutada la implementación del *framework* de seguridad propuesto, a pesar de la resistencia al cambio que éste modelo representaba para los trabajadores del IMSS.

Bibliografía

AlHogail, A. (2015). Design and validation of information security culture framework. En A. AlHogail, *Computers in Human Behavior* (pág. 569). Saudi Arabia: Elsevier Science.

Alhogail, A., & Abdulrahman, M. (2014). A Framework of Information Security Culture Change. *Journal of Theoretical and Applied Information Technology*, 543.

Cámara de Diputados del H. Congreso de la Unión. (11 de 01 de 2012). *Ley de Firma Electrónica Avanzada.* Recuperado el 08 de Diciembre de 2018, de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf

Cámara de Diputados del H. Congreso de la Unión. (26 de 01 de 2017). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. Recuperado el 20 de 10 de 2017, de https://www.colmex.mx/assets/pdfs/10-LGPDPPSO_57.pdf?1493134086

Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico. (24 de Febrero de 2016). *ASI Proceso Administación de la seguridad de la información.* Recuperado el 21 de Noviembre de 2017, de https://www.gob.mx/cms/uploads/attachment/file/58680/ASI_Proceso_Administraci_n_de_la_Seguridad_de_la_Informaci_n.pdf

Congreso General de los Estados Unidos Mexicanos. (2012). *Ley de Firma Electrónica Avanzada.* Ciudad de México.

Consejo de la Judicatura Federal. (2019). *Constitución Política de los Estados Unidos Mexicanos.* Ciudad de México: Gobierno de México.

DIng-Long Huang, P.-L. P. (2010). Perception of information security. *Behaviour and Information Technology, 29*(3), 221-232.

Gobierno de México - IMSS. (2018). *Centro Virtual de Operaciones en Emergencias y Desastres*. Recuperado el 10 de abril de 2018, de http://cvoed.imss.gob.mx/

Instituto Mexicano del Seguro Social. (27 de 11 de 2014). *Conoce al IMSS*. Recuperado el 18 de 02 de 2015, de http://www.imss.gob.mx/conoce-al-imss

Instituto Mexicano del Seguro Social. (27 de 11 de 2014). *Conoce al IMSS*. Recuperado el 18 de 02 de 2016, de http://www.imss.gob.mx/conoce-al-imss

Instituto Mexicano del Seguro Social. (30 de Septiembre de 2017). *Población derechohabiente adscrita a Unidad de Medicina Familiar*. Recuperado el 19 de Octubre de 2017, de https://public.tableau.com/profile/imss.cpe#!/vizhome/PDA/DSH_PDA?publish=yes

Instituto Mexicano del Seguro Social. (2018). *Controles recomendados para AR.* Ciudad de México: Instituto Mexicano del Seguro Social.

Instituto Mexicano del Seguro Social. (2018). *Escenarios de Riesgo.* Instituto Mexicano del Seguro Social. Ciudad de México: IMSS.

Instituto Mexicano del Seguro Social. (2018). *Formato ASI F03 Documento de resultados del análisis de riesgos.* Ciudad de México: IMSS.

Instituto Mexicano del Seguro Social. (31 de marzo de 2018). *Inventario Único de Aplicaciones.* Recuperado el 13 de junio de 2018, de http://cid.imss.gob.mx/web/guest/inventariounicoaplicaciones

Instituto Mexicano del Seguro Social. (2018). *Matriz de análisis de riesgos.* Hoja de cálculo, IMSS, Ciudad de México.

ISO 27001 en Español. (2015). *Ciclo de Deming - Mejora continua*. Recuperado el 20 de 02 de 2016, de http://www.iso27000.es/sgsi_implantar.html#home

James J. Cebula, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks.* Software Engineering Institute of Carnegie Mellon.

Martins, A. D. (2015). *Information security culture and information protection culture: A validated assessment instrument.* South Africa: Elsevier Science at Science Direct.

Microsoft. (s.f.). *Microsoft Security Developement Lifecycle Resources .* Recuperado el 8 de Diciembre de 2018, de https://www.microsoft.com/en-us/securityengineering/sdl/

Onieva, J. A., López, J., & Zhou, J. (2009). Fundamentals of Non-repudiation. En J. A. Onieva, J. López, & J. Zhou, *Secure Multi-Party Non-Repudiation Protocols and Applications* (Vol. 43, págs. 17-18). Boston, MA: Springer.

OSIC - Observatorio Ciberseguridad. (2018). *Triada CIA*. Recuperado el 12 de Noviembre de 2019, de https://observatoriociber.org/triada-cia/

Schienger, T., & Teufel, S. (2003). *Information Security Culture, from Analysis to Change.* University of Fribourg: International Institute of Management in Telecommunications.

Secretaría de Gobernación. (2014 de mayo de 08). *Diario Oficial de la Federación.* Recuperado el 18 de noviembre de 2018, de http://www.dof.gob.mx/nota_detalle.php?codigo=5343881&fecha=08/05/2014

Secretaría de Gobernación. (29 de Noviembre de 2011). *Diario Oficial de la Federación.* Recuperado el 2017, de http://dof.gob.mx/nota_detalle.php?codigo=5221649&fecha=29/11/2011

Secretaría de Gobernación. (04 de febrero de 2016). *Diario Oficial de la Federación.* Recuperado el 21 de Noviembre de 2017, de http://dof.gob.mx/nota_detalle.php?codigo=5424367&fecha=04/02/2016

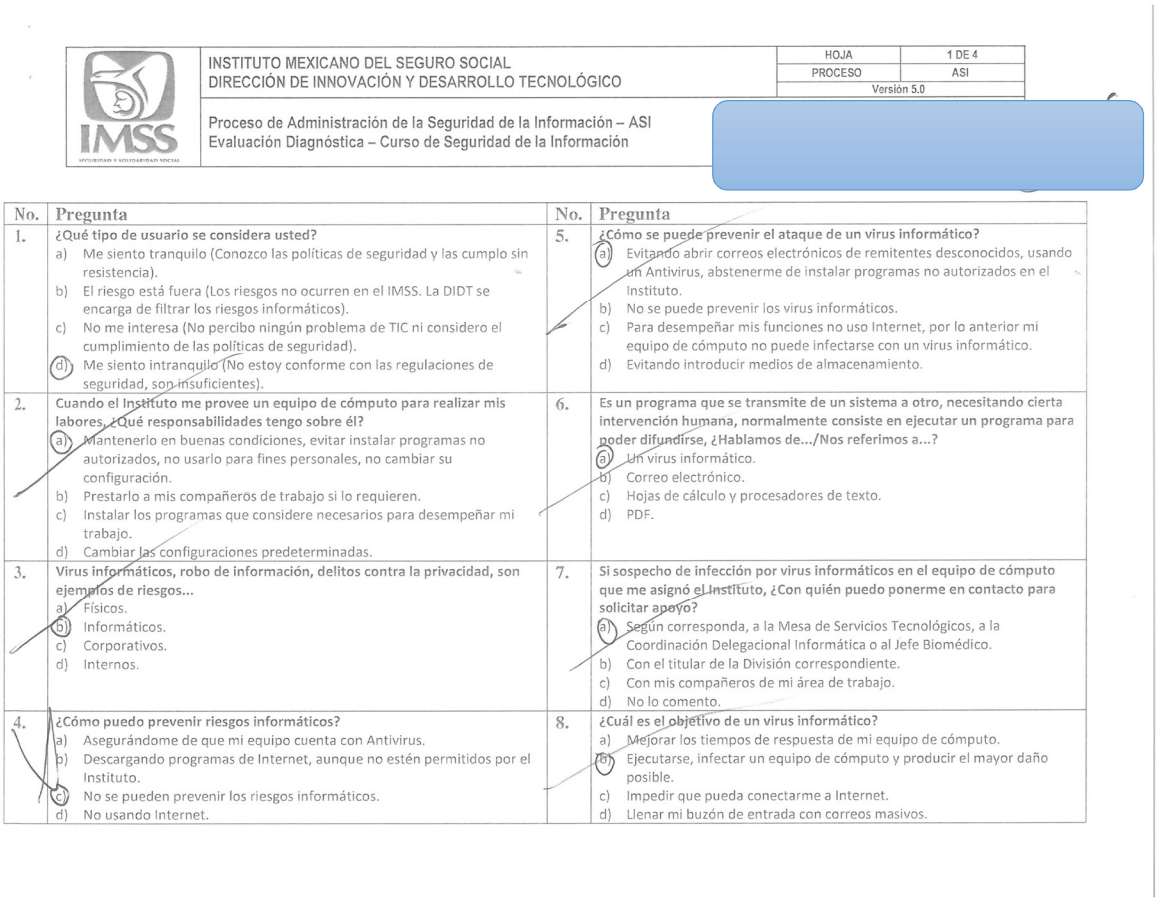
Secretaría de la Función Pública. (2014). *Formato ASI F3 Documento de resultados de análisis de riesgos.* Ciudad de México: Secretaría de la Función Pública.

Sindicato Nacional de Trabajadores del Seguro Social. (s.f.). *Sistema Centros de Capacitación y Calidad.* Recuperado el junio de 2017, de https://sicapacitacion.com/sistema-centros/

Standard, I. 2. (s.f.). *ISO - International Organization of Standarization.* Recuperado el 12 de Noviembre de 2018, de ISO/IEC 27001:2013Information technology — Security techniques — Information security management systems — Requirements: https://www.iso.org/standard/54534.html

ANEXOS

ANEXO 1



IMSS	INSTITUTO MEXICANO DEL SEGURO SOCIAL DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TECNOLÓGICO	HOJA	1 DE 4
		PROCESO	ASI
		Versión 5.0	
	Proceso de Administración de la Seguridad de la Información – ASI Evaluación Diagnóstica – Curso de Seguridad de la Información		

No.	Pregunta	No.	Pregunta
1.	**¿Qué tipo de usuario se considera usted?** a) Me siento tranquilo (Conozco las políticas de seguridad y las cumplo sin resistencia). b) El riesgo está fuera (Los riesgos no ocurren en el IMSS. La DIDT se encarga de filtrar los riesgos informáticos). c) No me interesa (No percibo ningún problema de TIC ni considero el cumplimiento de las políticas de seguridad). d) Me siento intranquilo (No estoy conforme con las regulaciones de seguridad, son insuficientes).	5.	**¿Cómo se puede prevenir el ataque de un virus informático?** a) Evitando abrir correos electrónicos de remitentes desconocidos, usando un Antivirus, abstenerme de instalar programas no autorizados en el Instituto. b) No se puede prevenir los virus informáticos. c) Para desempeñar mis funciones no uso Internet, por lo anterior mi equipo de cómputo no puede infectarse con un virus informático. d) Evitando introducir medios de almacenamiento.
2.	**Cuando el Instituto me provee un equipo de cómputo para realizar mis labores, ¿Qué responsabilidades tengo sobre él?** a) Mantenerlo en buenas condiciones, evitar instalar programas no autorizados, no usarlo para fines personales, no cambiar su configuración. b) Prestarlo a mis compañeros de trabajo si lo requieren. c) Instalar los programas que considere necesarios para desempeñar mi trabajo. d) Cambiar las configuraciones predeterminadas.	6.	**Es un programa que se transmite de un sistema a otro, necesitando cierta intervención humana, normalmente consiste en ejecutar un programa para poder difundirse, ¿Hablamos de.../Nos referimos a...?** a) Un virus informático. b) Correo electrónico. c) Hojas de cálculo y procesadores de texto. d) PDF.
3.	**Virus informáticos, robo de información, delitos contra la privacidad, son ejemplos de riesgos...** a) Físicos. b) Informáticos. c) Corporativos. d) Internos.	7.	**Si sospecho de infección por virus informáticos en el equipo de cómputo que me asignó el Instituto, ¿Con quién puedo ponerme en contacto para solicitar apoyo?** a) Según corresponda, a la Mesa de Servicios Tecnológicos, a la Coordinación Delegacional Informática o al Jefe Biomédico. b) Con el titular de la División correspondiente. c) Con mis compañeros de mi área de trabajo. d) No lo comento.
4.	**¿Cómo puedo prevenir riesgos informáticos?** a) Asegurándome de que mi equipo cuenta con Antivirus. b) Descargando programas de Internet, aunque no estén permitidos por el Instituto. c) No se pueden prevenir los riesgos informáticos. d) No usando Internet.	8.	**¿Cuál es el objetivo de un virus informático?** a) Mejorar los tiempos de respuesta de mi equipo de cómputo. b) Ejecutarse, infectar un equipo de cómputo y producir el mayor daño posible. c) Impedir que pueda conectarme a Internet. d) Llenar mi buzón de entrada con correos masivos.

1. Evaluación inicial a los participantes de la capacitación en seguridad de la información en el IMSS.

ANEXO 2

INSTITUTO MEXICANO DEL SEGURO SOCIAL

CONSTANCIA DE COMPETENCIAS O DE HABILIDADES LABORALES

DATOS DEL TRABAJADOR	
Nombre (Anotar apellido paterno, apellido materno y nombres (s))	URIBE MACEDO FRANCISCO
Clave Única de Registro de Población: UIMF860727HMCRCR05	Ocupación especifica (Catalogo Nacional de Ocupaciones) 1/: SALUD Y PROTECCIÓN SOCIAL
Categoría o Puesto: SOPORTE TEC ESPECIALIZADO E4	Matricula: 311380064

DATOS DE LA EMPRESA	
Nombre o razón social (En caso de persona física, anotar apellido paterno, apellido materno y nombre(s))	INSTITUTO MEXICANO DEL SEGURO SOCIAL
Registro Federal de Contribuyentes con homoclave (SHCP)	IMS-421231-I45

DATOS DEL PROGRAMA DE CAPACITACIÓN ADIESTRAMIENTO Y PRODUCTIVIDAD				
Nombre del curso	CURSO EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN			
Duración en horas: 8	Periodo de ejecución: De	Año Mes Día: 2018|05|07	a	Año Mes Día: 2018|05|08
Área temática del curso 2/	DESARROLLO PERSONAL Y FAMILIAR			
Agente capacitador (Externo o interno, según corresponda)	INSTITUTO MEXICANO DEL SEGURO SOCIAL			

Los datos se asientan en esta constancia bajo protesta de decir verdad, apercibidos de la responsabilidad en que incurre todo aquel que no se conduce con verdad.

Instructor/a o Tutor/a

CLAUDIA RODRÍGUEZ SOSA

Representantes de la Comisión Nacional Mixta de Capacitación y Adiestramiento

Por el Instituto

C.P. LUCIO CORTÉS SUAZO

Por las/los trabajadores

C. MÓNICA GARCÍA HERNÁNDEZ

DC-3

2. Constancia por competencias laborales avalada por la Secretaría de Trabajo y Previsión Social (STyPS).

ANEXO 3

3. Ejemplo de boletines electrónicos enviados al personal institucional como parte del reforzamiento de la cultiura de la seguridad de la información.

ANEXO 4

Inventario de Aplicaciones del Instituto Mexicano del Seguro Social

		SFP								
ID Inventario	ID	Publicado Herramienta SFP	Coordinación Responsable del Sistema o Servicio y con el área	Acrónimo / SIGLAS del Sistema o Servicio:	Nombre del Sistema o Servicio: (Indicar el Nombre del Nuevo Sistema o Servicio	Descripción Breve del Sistema o Servicio	Módulos del Sistema o Servicio	Tipo de Prioridad (Primaria o Secundaria)	Criticidad Operativa	El servicio es prestado por un Proveedor (SI/NO)
IMSS_APP_2	2	Si	CSDISS	ACCEDER UNIFICADO	Acceder Unificado	de los beneficiarios y de los asegurados o pensionados de forma presencial y no presencial. Permite consultar de forma presencial	derechohabientes Correccion de datos Cambio de clinica Prorrogas	Primaria	Alta	SI
IMSS_APP_3	3	NO	CSDISS	Actualización Dato CURP	Actualización Dato CURP	El sistema actualiza la CURP de un Ciudadano que accede al Portal Ciudadano, se realiza de forma NO	Actualización Dato CURP	Primaria	Media	NO
IMSS_APP_4	4	Si	CSDISS	ADMIN	Administración de Usuarios (ADMIN)	usuarios, permite llevar el registro de los usuarios de Subdelegaciones del Instituto que tienen acceso a los	N/A	Secundaria	Media	SI
IMSS_APP_5	5	Si	CSDISS	ADMPOS	Administración Puntos de Venta (ADMPOS)	Administración de Puntos de Venta para Tiendas IMSS.	Ventas y reportes de las ventas por dia en las tiendas del IMSS	Secundaria	Baja	SI
IMSS_APP_6	6	SI	CSDISS	ADO IMSS Digital	Almacenes de datos de operación	operación que conforman el Modelo de Gobierno de Datos IMSS Digital de fuentes de Información de los	N/A	Secundaria	Media	NO
IMSS_APP_7	7	Si	CSDISS	AltaPatronal	Alta Patronal (ALTAPATRONAL)	Soportar el proceso de asignación de número de registro patronal NRP del trámite de Alta patronal, registro	Módulo de Alta patronal, Módulo de Asignación de Registro	Primaria	Alta	NO
IMSS_APP_8	8	Si	CSDISS	ALTAPM IMSS Digital	Alta patronal persona moral no presencial (AltaPM)	Soportar el proceso de asignación de número de registro patronal NRP, Prestadoras de Servicios y su Inscripción en el Seguro de Riesgos de Trabajo ante el Instituto. Facilitar el registro al sector	Módulo de Registro de solicitudes de registro patronal a través del Portal Institucional. Módulo de Consulta solicitudes.	Primaria	Alta	NO
-	-	-	-	-	-	-	-	-	-	-

(Fragmento – Inventario Único de Aplicaciones)

4. Publicación interna del registro de aplicaciones validadas en el IMSS, para la construcción del catálogo de infrastructuras críticas.

Índice de términos