Universidad de Sonora

Departamento de Ingeniería Industrial

Ingeniería en Sistemas de Información

Reporte de prácticas profesionales

Revisión y aplicación de Políticas de Seguridad de la Información NMX-I-27001/ISO/IEC 27001 en la Infraestructura que da soporte al proceso CFDI de Prodigia Procesos Digitales Administrativos SA de CV

Presenta: Jorge Eduardo Cruz León

Tutor: Dr. Raquel Torres Peralta

ÍNDICE

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

Como parte de los requisitos para acreditar la titulación como Ingeniero en Sistemas de Información en la Universidad de Sonora, es necesario llevar a cabo las Prácticas Profesionales, ya sea en empresas de orden gubernamental o del sector privado, en estas, el alumno aplica sus conocimientos y habilidades adquiridos durante su formación académica. Como requisito normativo, el alumno debe de cubrir un total de 340 horas como practicante, lo cual tiene un valor curricular de 20 créditos.

El proyecto fue realizado en Prodigia Procesos Digitales Administrativos SA de CV, empresa dedicada al desarrollo de software y negocios fiscales. El alcance de este proyecto es enfocado a uno de sus productos denominado “Pade”, el cual consiste en una plataforma enfocada a emitir timbrado fiscal y el proceso de CFDI(PAC), la cual cuenta con autorización por parte del Servicio de Administración Tributaria (SAT) para validar los CFDI generados por un contribuyente, para finalmente agregarle a las facturas el sello digital del SAT.

El proyecto se llevó a cabo en el departamento de Seguridad de la Información al cual pertenezco, donde se vigila y aplica el correcto cumplimiento con la normatividad vigente en base a la norma internacional ISO/IEC 27001.

El propósito principal del Sistema de Gestión de Seguridad de la información es cumplir con los objetivos establecidos los cuales están enfocados a proteger la información por medio de la implementación de planes de tratamiento, que consideran la implementación y mantenimiento de controles físicos, administrativos y técnicos de seguridad relacionados con las instalaciones, recursos humanos, sistemas o aplicaciones, equipo y medios móviles e infraestructura tecnológica.

El proyecto consta en enfocar esfuerzo por proteger los 3 pilares de la Seguridad de la Información, los cuales consisten en salvaguardar la Confidencialidad, Integridad y Disponibilidad de la información.

Entendemos el concepto de la Seguridad de la Información como la preservación de la Confidencialidad, Integridad y Disponibilidad de la Información:

- Confidencialidad. Propiedad de la información debe estar solamente accesible a personas, proceso y entes autorizados.
- Integridad: Propiedad de la información de no ser modificada de forma no autorizada y siempre bajo los criterios establecidos para su operación.
- Disponibilidad: Propiedad de la información de estar accesible en los momentos establecidos para su uso.

Para su consecución, es indispensable la interrelación en el mismo nivel entre los tres elementos fundamentales siguientes:

- Personas. Conocimiento adecuado de su responsabilidad en la Seguridad de la Información y el uso adecuado de los controles implementados.
- Procesos. Políticas y procedimientos adecuados a la estrategia de Seguridad de la Información Institucional.
- Tecnología. Implementación controles tecnológicos que faciliten el ejercicio de la Seguridad de la Información.

Prodigia establece la ejecución de auditorías de tal forma que la organización pueda cumplir en tiempo y forma con los requerimientos corporativos, además de actuar de manera proactiva en la detección y mitigación de posibles riesgos y/o vulnerabilidades.

2. DESCRIPCIÓN DE LA EMPRESA

La ubicación física de las instalaciones de Prodigia Proceso Administrativos S.A de C.V se encuentra en: Blvd. A. Quiroga 21. Col. Quinta Emilia, Torre N2, Primer Piso, Interior 3. (Figura 2.1).

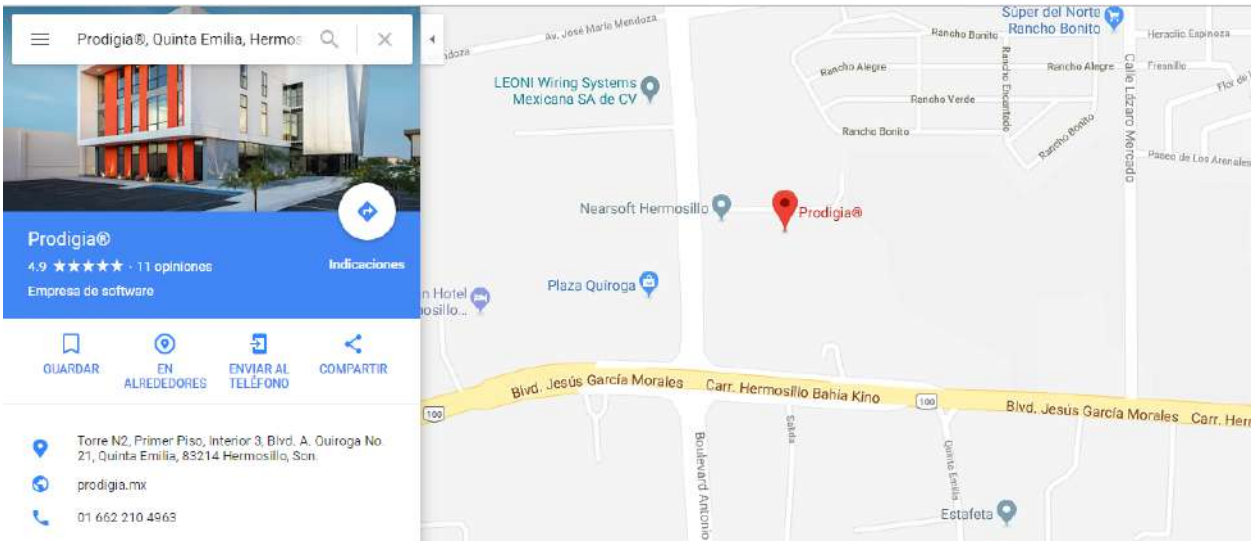


Figura 1 - 2.1Ubicación de Prodigia

La empresa se encuentra certificada como Proveedor Certificado de Comprobantes Fiscales Digitales por Internet (PCCFDI) por el SAT y por la norma internacional ISO/IEC 27001 Seguridad de la Información. Sus actividades principales son la emisión de facturas electrónicas y timbrado de las mismas, así como la producción de software tales como su plataforma digital PADE, Odoo (ERP), software de servicio (SaaS), etc.

Ubicada en el segundo piso de la torre N2 (Figura 2.2); La empresa cuentan con varios departamentos a cargo de la Dirección del Ing. Gustavo Aguilar A. (CEO), el departamento de Recursos Humanos y Administración a cargo de Susana González (CFO), el departamento de Desarrollo, el departamento de Comercialización, el

departamento de Soporte técnico y el departamento de Seguridad de la Información al cual está enfocado este documento.

Figura 2 - 2.2 Ubicación física de las oficinas de Prodigia

3. JUSTIFICACIÓN DEL PROYECTO REALIZADO

El practicante se encargará de la revisión y la correcta aplicación de las Políticas de Seguridad de la Información y procedimientos a la infraestructura tecnológica de la empresa que da soporte al servicio de CFDI para timbrado fiscal, mismo que debe de cumplir con los requisitos de la norma ISO/IEC 27001 y la matriz de controles PCCFDI emitida por el SAT.

La verificación se llevará a cabo mediante la revisión de las configuraciones en los servidores de la infraestructura de la empresa (IaaS), mismas que deben de cumplir con todas las políticas de seguridad que estén relacionadas con los procesos de facturación de Prodigia.

El practicante realizará una Auditoría en los procesos involucrados en las labores del departamento de seguridad de la información, mismas que como resultado arrojará si las políticas están correctamente implementadas en la infraestructura y las respectivas implementaciones de las mismas para estar alineados a la norma ISO/IEC 27001 y la autoridad SAT establecen.

El proceso de auditoría se compone de las siguientes fases:

- Análisis de controles
- Reporte de análisis
- Revisión de no cumplimiento de controles
- Remediación de los no cumplimientos

Durante la estancia profesional el practicante llevará a cabo las siguientes tareas y procesos:

- Documentar los procesos realizados en la infraestructura
- Implementar políticas de seguridad en infraestructura
- Realizar pruebas de seguridad, escaneo de vulnerabilidades y remediarlas
- Generar evidencias para auditorías internas y externas
- Mantener actualizada la documentación del SGSI correspondiente
- Realizar respaldo del gestor documental Alfresco

- Participar en reuniones de revisión de avances
- Participar en reuniones de planeación
- Evaluar que la capacidad técnica y operativa que necesita el departamento esté operando correctamente
- Elaborar documento de resultados del departamento para la reunión gerencial
- Levantar y dar seguimiento a tickets en el portal del centro de datos relacionados a la infraestructura
- Instalar y configurar alfresco
- Revisar y analizar logs para identificar problemáticas de servidores
- Realizar control de activos físicos de la empresa

La participación en estos procesos se da con el fin de mejorar la gestión e implementación de los controles en los activos que dan soporte al proceso de facturación y timbrado de CFDI, así como la adquisición de experiencia y desarrollo de aptitudes en el ámbito personal y profesional, tales como:

- Creatividad
- Trabajo sobre objetivos
- Trabajo en equipo
- Facilidad para la delegación de actividades
- Creación de ambientes favorables para la comunicación y expresión del equipo de trabajo
- Capacidad para toma de decisiones objetivas
- Capacidad para la fijación de metas y objetivos
- Capacidad de negociación
- Manejo y solución de Conflictos
- Liderazgo

4. OBJETIVOS DEL PROYECTO

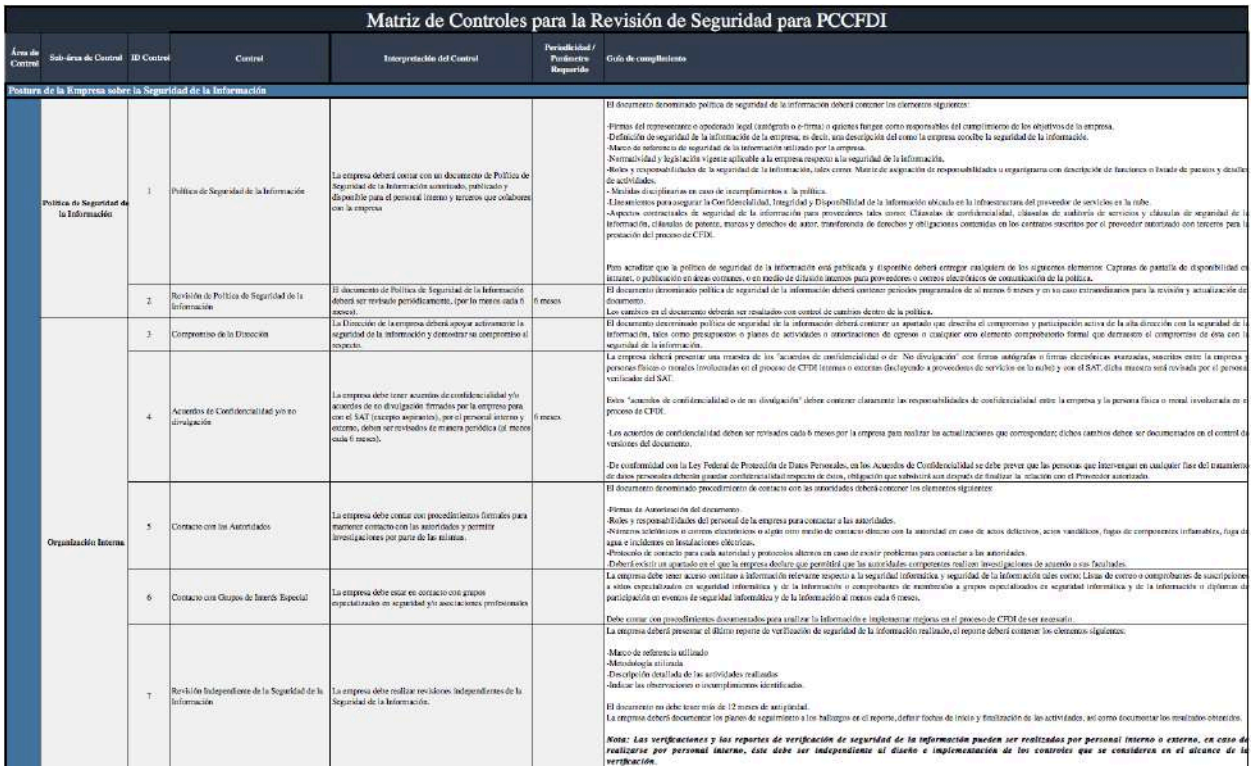
El objetivo inicial de todo proyecto de prácticas profesionales consiste en una mayor formación laboral y profesional del practicante para adecuarse mejor en el ámbito empresarial y sus respectivos procesos de cada ámbito profesional que en este caso aplican al área ingenieril con especialidad en sistemas de información.

Realizar una auditoría periódicamente a la infraestructura que da soporte al proceso de CFDI es de vital importancia debido a que se pueden identificar las vulnerabilidades, verificar su criticidad y proponer las medidas correctivas para corregirlas, con el fin de evitar accesos no autorizados o pérdida en la disponibilidad de los servicios críticos.

El practicante debe de cumplir con los siguientes requerimientos y actividades, las cuales son:

- Capacitarse en norma ISO/IEC 27001, ISO 22301, Matriz de controles para PCCFDI 2018
- Aplicar los conocimientos adquiridos en la formación académica y capacitación de estancia profesional a los requisitos en la empresa Prodigia Procesos Digitales Administrativos SA de CV.
- Colaborar con el departamento de desarrollo para alcanzar los resultados y obtener evidencia de los procesos para solventar no-cumplimientos de las auditorías.
- Generar y actualizar documentación relacionada con los controles a solventar de las auditorías, tales como Políticas y Procedimientos.
- Entregar resultados y evidencia de los controles solventados relacionados a las auditorías

De igual forma el objetivo simultáneo de este proyecto consiste en ayudar a la empresa a conservar su certificación como proveedor autorizado de certificación(PAC), debido a que por normatividad vigente la dependencia del SAT se permite realizar auditorías eventualmente, por lo que la documentación debe de estar actualizada y al corriente para evitar incidencias cada que se presente una auditoría oficial, por lo que, Prodigia realiza auditorías internas de manera semestral para en base a sus resultados remediár y estar alineados al cumplimiento de los requisitos del SAT.



Matriz de Controles para la Revisión de Seguridad para PCCFDI

Área de Control	Sub-área de Control	ID Control	Control	Interpretación del Control	Periodicidad / Periodicidad Requerido	Guía de cumplimiento
Postura de la Empresa sobre la Seguridad de la Información						
	Política de Seguridad de la Información	1	Política de Seguridad de la Información	La empresa deberá contar con un documento de Política de Seguridad de la Información autorizado, publicado y disponible para el personal interno y terceros que colaboren con la empresa		El documento denominado política de seguridad de la información deberá contener los elementos siguientes: -Firmas del representante o apoderado legal (autógrafa o e-firma) o quienes fungen como responsables del cumplimiento de los objetivos de la empresa. -Definición de seguridad de la información de la empresa, es decir, una descripción del como la empresa concibe la seguridad de la información. -Marco de referencia de seguridad de la información utilizado por la empresa. -Normatividad y legislación vigente aplicable a la empresa respecto a la seguridad de la información. -Roles y responsabilidades de la seguridad de la información, tales como: Matriz de asignación de responsabilidades o organigrama con descripción de funciones o fotode de puestos y detalle de actividades. - Medidas disciplinarias en caso de incumplimientos a la política. -Lineamientos para asegurar la Confidencialidad, Integridad y Disponibilidad de la información ubicada en la infraestructura del proveedor de servicios en la nube. -Aspectos contractuales de seguridad de la información para proveedores tales como: Cláusulas de confidencialidad, cláusulas de auditoría de servicios y cláusulas de seguridad de la información, cláusulas de patente, marcas y derechos de autor, transferencia de derechos y obligaciones contenidas en los contratos suscritos por el proveedor autorizado con terceros para la prestación del proceso de CFDI. Para acreditar que la política de seguridad de la información está publicada y disponible deberá entregar cualquiera de los siguientes elementos: Capturas de pantalla de disponibilidad en internet, o publicación en áreas comunes, o en medio de difusión internos para proveedores o correos electrónicos de comunicación de la política.
		2	Revisión de Política de Seguridad de la Información	El documento de Política de Seguridad de la Información deberá ser revisado periódicamente, (por lo menos cada 6 meses).	6 meses	El documento denominado política de seguridad de la información deberá contener periodos programados de al menos 6 meses y en su caso extraordinarios para la revisión y actualización de documento. Los cambios en el documento deberán ser resultados con control de cambios dentro de la política.
	Organización Interna	3	Compromiso de la Dirección	La Dirección de la empresa deberá apoyar activamente la seguridad de la información y demostrar su compromiso al respecto.		El documento denominado política de seguridad de la información deberá contener un apartado que describa el compromiso y participación activa de la alta dirección con la seguridad de la información, tales como presupuestos o planes de actividades o amonestaciones de egresos o cualquier otro elemento comprobatorio formal que demuestre el compromiso de ésta con la seguridad de la información.
		4	Acuerdos de Confidencialidad y/o no divulgación	La empresa debe tener acuerdos de confidencialidad y/o acuerdos de no divulgación firmados por la empresa para con el SAT (excepto aspirantes), por el personal interno y externo, deben ser revisados de manera periódica (al menos cada 6 meses).	6 meses.	La empresa deberá presentar una muestra de los "acuerdos de confidencialidad o de No divulgación" con firmas autógrafas o firmas electrónicas avanzadas, suscritos entre la empresa y personas físicas o morales involucradas en el proceso de CFDI (internas o externas (incluyendo a proveedores de servicios en la nube) y con el SAT; dicha muestra será revisada por el personal verificador del SAT. Estos "acuerdos de confidencialidad o de no divulgación" deben contener claramente las responsabilidades de confidencialidad entre la empresa y la persona física o moral involucrada en el proceso de CFDI. -Los acuerdos de confidencialidad deben ser revisados cada 6 meses por la empresa para realizar las actualizaciones que correspondan; dichos cambios deben ser documentados en el control de versiones del documento. -De conformidad con la Ley Federal de Protección de Datos Personales, en los Acuerdos de Confidencialidad se debe prever que las personas que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar la relación con el Proveedor autorizado.
		5	Contacto con las Autoridades	La empresa debe contar con procedimientos formales para mantener contacto con las autoridades y permitir investigaciones por parte de las mismas.		El documento denominado procedimiento de contacto con las autoridades deberá contener los elementos siguientes: -Firmas de Autorización del documento. -Roles y responsabilidades del personal de la empresa para contactar a las autoridades. -Números telefónicos o correos electrónicos o algún otro medio de contacto directo con la autoridad en caso de actos delictivos, actos vandálicos, fugas de combustibles inflamables, fuga de agua e incidentes en instalaciones eléctricas. -Protocolo de contacto para cada autoridad y protocolos alternos en caso de existir problemas para contactar a las autoridades. -Deberá incluir un apartado en el que la empresa declare que permitirá que las autoridades competentes realicen investigaciones de acuerdo a sus facultades.
		6	Contacto con Grupos de Interés Especial	La empresa debe estar en contacto con grupos especializados en seguridad y/o asociaciones profesionales		La empresa debe tener acceso continuo a información relevante respecto a la seguridad informática y seguridad de la información tales como: Listas de correo o comprobantes de suscripciones a sitios especializados en seguridad informática y de la información o comprobantes de membresías a grupos especializados en seguridad informática y de la información o diplomas de participación en eventos de seguridad informática y de la información al menos cada 6 meses. Debe contar con procedimientos documentados para analizar la información e implementar mejoras en el proceso de CFDI de ser necesario.
		7	Revisión Independiente de la Seguridad de la Información	La empresa debe realizar revisiones independientes de la Seguridad de la Información.		La empresa deberá presentar el último reporte de verificación de seguridad de la información realizado, el reporte deberá contener los elementos siguientes: -Marco de referencia utilizado -Metodología utilizada -Descripción detallada de las actividades realizadas -Indicar las observaciones o incumplimientos identificados. El documento no debe tener más de 12 meses de antigüedad. La empresa deberá documentar los planes de seguimiento a los hallazgos en el reporte, definir fechas de inicio y finalización de las actividades, así como documentar los resultados obtenidos. ***Nota: Las verificaciones y los reportes de verificación de seguridad de la información pueden ser realizados por personal interno o externo, en caso de realizarse por personal interno, este debe ser independiente al diseño e implementación de los controles que se consideren en el alcance de la verificación.***

Figura 3 - 4.1 Matriz de controles para la revisión de seguridad para PCCFDI

La Matriz de controles para la revisión de seguridad para PCCFDI (Figura 3) muestra un conjunto de controles que el aspirante a PAC debe de cumplir ya sea para conservar u obtener su certificación como PAC. La Matriz está compuesta por 86 controles que el aspirante debe de cumplir para poder obtener y conservar su certificación como PAC, estos están compuestos por diferentes áreas, sub áreas, el ID respectivo de cada control, el nombre del control, la interpretación del control, la periodicidad de revisión de cada control (en caso de que aplique) y la guía de cumplimiento, la cual, nos describe los requisitos que se deben de cumplir de cada control.

Una de las mayores consideraciones de este proyecto es que, para lograr llevar a cabo la auditoría de una forma exitosa y adecuada, se requiere capacitarse la norma ISO/IEC 27001 y en la Matriz de controles para la revisión de seguridad para PCCFDI, relacionados al departamento de Seguridad de la Información.

5. ALCANCES Y LIMITACIONES

Los alcances de este proyecto son múltiples, ya que con esta auditoría se pretende estar alineados a la normatividad y validaciones del SAT, lo cual desemboca en una mejor gestión a nivel empresarial de la documentación así como los procesos relacionados al servicio de facturación que la empresa provee como PAC, ya que los departamentos contarán con un mejor control de la documentación que puedan requerir o bien, una mejor calidad en las actividades realizadas por el personal.

Con esta auditoría se pretenden revisar varios controles que tienen posibilidad de mejora, pues al corregir los controles se espera reducir las observaciones recibidas por parte del SAT y así tener la documentación actualizada al día para que en futuras auditorías no tener reincidencias y observaciones en los controles y ser un PAC de primer nivel.

Otro apoyo fundamental es la comunicación con el con el equipo gerencial y el líder de proyectos, pues este mismo es el que provee las evidencias sobre la implementación de las políticas de seguridad de la información que da soporte al servicio de facturación CFDI 3.3 en la infraestructura del centro de datos.

La limitación más grande al momento de realizar el proyecto fue la confidencialidad y disponibilidad de la documentación yacente en los controles del SGSI de Prodigia Procesos Digitales Administrativos SA de CV, ya que por políticas de seguridad de la empresa no se puede divulgar información clasificada como reservada ya que existe un convenio de confidencialidad firmado con la empresa y podría ser acreedor a sanciones en caso de divulgar información de este carácter por contener información sensible de los clientes del servicio de timbrado y las bases de datos pertenecientes a la empresa.

Otra limitante que se presentó durante la auditoría es el factor tiempo, pues es una limitante de gran importancia ya que cada control u observación requiere distinto tiempo de solventación por lo que es difícil estimar la cantidad de tiempo que se va requerir para solventar y generar evidencias de los distintos controles u observaciones encontradas.

6. FUNDAMENTO TEÓRICO DE LAS HERRAMIENTAS Y CONOCIMIENTOS APLICADOS

a. Gestor documental Alfresco

Alfresco es una herramienta de control documental enfocada en la gestión de los documentos y sus versiones, es una plataforma abierta, moderna y segura que activa procesos y contenido de manera inteligente para acelerar el flujo del negocio. Ofrece el camino más rápido para que las personas interactúen con la información y para que las empresas respondan a las cambiantes necesidades empresariales.

Esta cuenta con distintos módulos que nos permiten compartir documentos, actualizarlos, iniciar flujos para su aprobación, subir diferentes versiones de los documentos y gestionar permisos a los diferentes niveles de usuarios.

Figura 4 - 6.1 Logo de Alfresco®

b. Portal de control de SoftLayer

SoftLayer es una empresa de IBM, dedicada a proveer servicios en la nube (IaaS) desde sus 24 centros de datos en Estados Unidos, Latino America, Asia, Australia y Europa. Softlayer Ofrece productos y servicios que incluyen servidores virtuales, redes, soluciones de big data, soluciones cloud computing privada entre otros servicios.

Una de las ventajas que Prodigia encuentra al ser cliente de Softlayer es su alta disponibilidad de servicio que ofrecen, ya que con esto cubrimos la parte de disponibilidad de servicio que por norma requerimos cumplir ante el sat (99.75% de disponibilidad al mes)

Figura 5 - 6.2 Logo de SoftLayer by IBM.

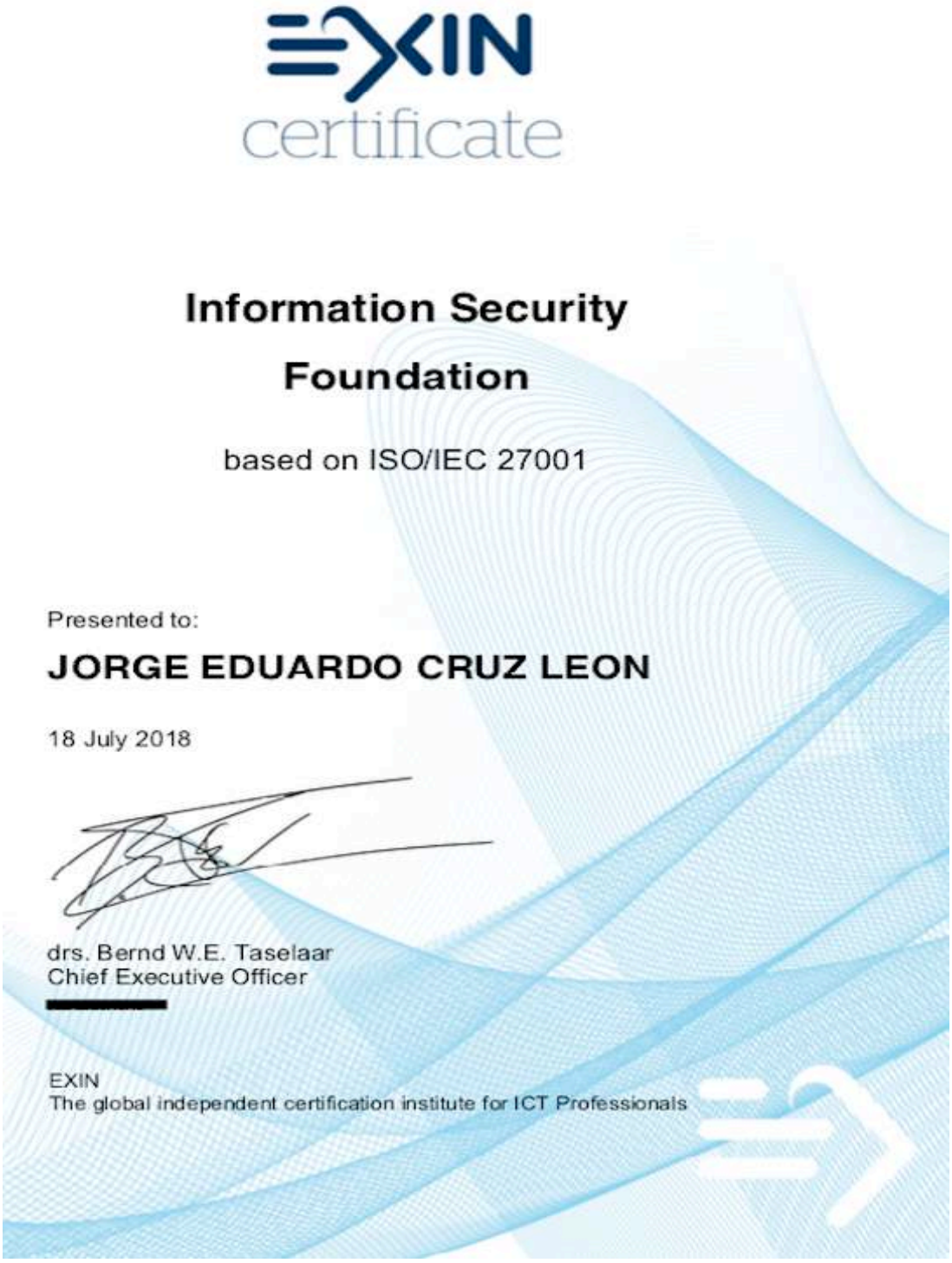
c. Fundamentos de Seguridad de la Información

ISO 27001 es una norma internacional que permite la disponibilidad, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

El propósito del Sistema de Gestión de Seguridad de la Información es cumplir con los objetivos establecidos los cuales están enfocados a proteger la información por medio de la implementación de planes de tratamiento, que consideran la implementación, operación y mantenimiento de controles físicos, administrativos y técnicos de seguridad relacionados con las instalaciones, recursos humanos, sistemas o aplicaciones, equipo y medios móviles e infraestructura tecnológica.

Figura 6 - 6.3 Logo de certificación ISO 27001



1Figura 6.4 Certificado en fundamentos en norma ISO 27001 Seguridad de la información

d. Fundamentos de CFDI SAT 3.3

En el ámbito laboral, la tecnología ha sido una piedra angular en el desarrollo de todos los niveles y áreas de negocio, pues con cada año el rubro empresarial se ha vuelto más dependiente de la tecnología, la facturación comenzó como una captura manual, la cual después pasó a ser por medio de mecanografía para hoy en día digitalizarse, para a partir de 2014 toda la facturación fiscal de cada empresa se realiza por vía electrónica; Las facturas electrónicas son archivos informáticos escritos en formato XML, para ser válidos estos deben ser timbrados a través de la aplicación del SAT o por un proveedor autorizado de certificación (PAC). Los PAC son empresas que cuentan con la autorización del SAT para la generación de facturas. De esta forma todo contribuyente físico o moral debe tener en consideración los documentos técnicos que especifican la estructura, forma y sintaxis que deben contener los CFDI que expidan los contribuyentes, lo cual permite que la información se integre de manera organizada en el comprobante, y harán referencia a la versión 3.3.

En este documento se describe cómo se debe realizar el llenado de los datos a registrar en el Comprobante Fiscal Digital por Internet. Como miembro activo del departamento de soporte el practicante deberá dominar los conocimientos generales de la documentación oficial del SAT, teniendo a su alcance la guía de llenado de CFDI 3.3 que es un documento cuyo objeto es explicar a los contribuyentes la forma correcta de llenar y expedir un CFDI, observando las definiciones del estándar tecnológico del Anexo 20 (Estipula las validaciones técnicas para los tipos de datos de cada atributo) y las disposiciones jurídicas vigentes aplicables, la matriz de errores (Catálogo de los mensajes posibles a recibir al momento de recibir un timbrado no exitoso) y los Catálogos de claves a utilizarse en los atributos requeridos.

7. ACTIVIDADES REALIZADAS Y DESARROLLO DE LA IMPLEMENTACIÓN.

Para poder conocer los fundamentos base en la norma ISO/IEC 27001 fue necesario tomar una capacitación en la Ciudad de México, misma al concluir con la capacitación se me certificó en los Fundamentos de Seguridad de la Información en la norma ISO/IEC 27001, al concluir con la certificación, se procedió a revisar los controles basados en la norma ISO 27001 de la empresa, por lo que fue necesario realizar una auditoría interna, la cual arrojó como resultado las observaciones de los controles en los cuales no cumplimos, y en base a ello se realizó un análisis de como se trabajaría para solventarlos las siguientes semanas.

De inicio se procedió a establecer los parámetros de búsqueda para los controles analizados, sobre los cuales se establecieron los niveles de severidad:

No cumple: Documentación de políticas y procedimientos o evidencias incompletas, o inexistentes.

Oportunidad de mejora: Mejora en documentación de políticas y procedimientos o evidencias.

Cumple: Documentación de políticas y procedimientos o evidencias completas, no requiere modificaciones.

Aunado a esto, se definen los criterios de auditoría que son las normas de referencia del sistema de gestión aplicable, documentos del sistema de gestión propios de la organización. Manuales o planes de sistema de gestión, procedimientos, instrucciones de trabajo, documentación general de la organización y marco legal y normativo aplicable.

Después de haber establecido los parámetros de hallazgos, se procedió a establecer las fases del proceso de la auditoría, los cuales consisten en:

Fase de reconocimiento: Su importancia radica en determinar el objetivo del análisis y se obtiene la mayor información sobre el mismo realizando una revisión detallada de los controles basándose en la norma.

Fase de Enumeración: El objetivo es obtener información relativa a los usuarios, equipos y servicios en la infraestructura generando conexiones activas con los sistemas y realizando consultas directas para obtener dicha información. Esta fase se realiza en las instalaciones de la organización.

Fase de Reporte: Se realiza un ejercicio de análisis de riesgo para determinar el impacto a la organización con respecto de las vulnerabilidades y amenazas encontradas, proponiendo soluciones para mitigar el riesgo encontrado a un nivel tolerable para la organización.

Remediación de Controles: Después de obtener los resultados de la auditoría, se presentó el plan para llevar a cabo la remediación de los controles que no cumplen con los requisitos de la norma establecida, siempre y cuando dando prioridad a los hallazgos que mayor atención requieran según la criticidad en el servicio. Para estas remediaciones se estableció:

1. Proceder con los planes de remediación de los hallazgos con riesgo Alto y concluirlos en un plazo no mayor a 2 meses.
2. Proceder con los planes de remediación de los hallazgos con riesgo Medio y concluirlo en un plazo no mayor a 6 meses.
3. Por último, se puede evaluar el costo-beneficio de atender las vulnerabilidades de riesgo bajo y en caso de que se decida remediarlas, proceder con los planes de remediación de los hallazgos procurando que se atiendan dentro de un plazo de 12 meses

Toda evidencia y modificaciones realizadas son subidas a la herramienta de gestión documental Alfresco, para llevar un control de las correcciones y versionamientos de las mismas (ver Figura 7), cada control con no conformidad fue revisado minuciosamente para al momento de recabar evidencia y realizar modificaciones en documentos se pudiera solventar conforme a los requerimientos de la matriz del SAT.

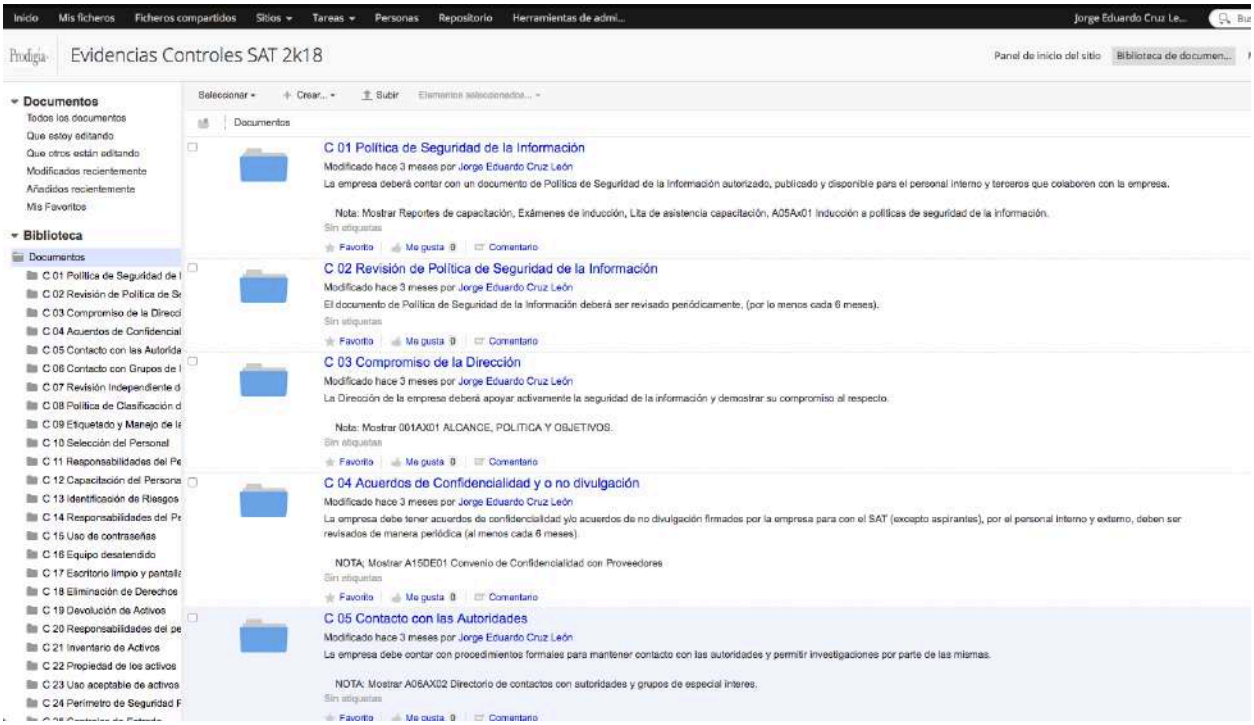


Figura 7 - 7.1 Evidencia en Gestor Documental Alfresco

Después de recabar evidencia y realizar las modificaciones necesarias a los documentos, se procedió a revisar los resultados obtenidos, con lo que se concluye que fueron solventados los hallazgos de la auditoría.

Durante el proceso de recaudación de evidencia, se realizaron modificaciones en la infraestructura de CFDI para cumplir con los requerimientos del SAT, estos consistieron en:

- Se realizaron cambios en los permisos de usuarios y de root sobre su forma de inicio de sesión
- Se modificó el tiempo de inactividad de sesión permitido para que el sistema desconecte a los usuarios que sobrepasan 12 minutos de inactividad en el servicio de timbrado
- Se modificó el puerto por defecto para conectarse por medio de SSH
- Se modificó los requerimientos de los usos de contraseñas, tales como longitud mínima y máxima, número mínimo y máximo de mayúsculas y minúsculas, número mínimo de dígitos requeridos para la contraseña, número mínimo de

caracteres especiales y el número de caracteres que deben de ser diferentes con respecto a la contraseña anterior

- Se crearon triggers de audición para revisar los logs de S.O. en el cual se muestra el historial de comandos ejecutados por usuarios
- Se realizó configuración de firewalls, agregando y modificando reglas de bloqueo existentes, tales como denegar, rechazar o filtrar conexiones
- Se modificaron las reglas de los iptables de los firewalls
- Se realizó respaldo de Alfresco y modificaciones en las configuraciones de sus usuarios
- Se cambiaron permisos de usuarios en los servidores

Se modificaron las siguientes políticas para cumplir con los requisitos establecidos ante el SAT:

- 001AX01 Alcance, Política y Objetivos del SGSI.
- A06PO01 Política de dispositivo móvil – Uso aceptable de activos.
- A06PO02 Política de teletrabajo.
- A06PO03 Política de seguridad para todos los proyectos de la organización.
- A08PO01 Política de Clasificación de la Información.
- A09PO01 Política de control de acceso.
- A10PO01 Política sobre el uso de controles criptográficos.
- A11PO01 Política de pantalla y escritorio limpio – Equipo desatendido.
- A11PO02 Política de cableado eléctrico y telecomunicaciones
- A12PO01 Política de respaldos.
- A13PO01 Política de transferencia de información.
- A14PO01 Política de desarrollo seguro.
- A15PO01 Política de seguridad para personal visitante o externo.

Observaciones: la mayoría de las configuraciones realizadas son de orden técnico, ya que la documentación general si cumplia con la normatividad y requerimientos del SAT.

8. CONCLUSIONES Y RECOMENDACIONES

Durante mi estancia en Prodigia Procesos Digitales Administrativos SA de CV me dí cuenta que es una empresa altamente comprometida con la Seguridad de la Información de sus clientes, ya que se ha encargado de implementar un Sistema de Gestión de Seguridad de la Información basado en la norma internacional ISO/IEC 27001, lo cual demuestra la importancia que se le da al comprometerse a revisar y mejorar los controles y procesos del Sistema de Gestión Seguridad de la Información en una periodicidad de seis meses mediante la actualización de la valoración de riesgos y de los planes de tratamiento de riesgos, el establecimiento de políticas para la mejora continua, la realización de auditorías internas, revisiones por la dirección, capacitaciones continuas en temas de seguridad de la información y la implementación de acciones de mejora. Así mismo, como parte del compromiso y participación activa de la dirección de Prodigia Procesos Digitales Administrativos SA de CV con la seguridad de la información, se generan presupuestos para temas relacionados, los cuales pueden incluir: capacitaciones, certificaciones, simposios de seguridad de la información, actualizaciones en temas relacionados a la seguridad de la información, adquisición de licencias de software que ayude a mitigar riesgos en seguridad de la información, adquisición de infraestructura tales como firewall o hardware que ayude a proteger los activos que intervienen en el proceso de CFDI.

Como recomendación, es necesario no dejar caer el SGSI por darle importancia a otras actividades del día a día, ya que si no se encuentra en constante mejora y actualización, este caería en desuso lo cual al momento de presentarse alguna auditoría podría provocar múltiples hallazgos y observaciones negativas con lo cual estaría en riesgo de perderse alguna de las certificaciones como proveedor autorizado de certificación (PAC)

9.BIBLIOGRAFÍA

Prodigia Procesos Digitales y Administrativos SA de CV. (2017, 10 de Abril). Documentación e Información relacionada a la Certificación de norma ISO/IEC 27001, Disponible en: http://prodigia.mx/empresa/seguridad-de-la-informacion/ [Recuperado 04 de Octubre, 2018]

Plataforma Pade.
Servicios y descripción del producto PADE, Disponible en : http://pade.mx/ [Consultado el 04 de Octubre, 2018]

SoftLayer by IBM
Infraestructura informática en la Nube (IaaS) : https://www.ibm.com/cloud-computing/bluemix/es/cloud-servers [Consultado el 04 de Octubre, 2018]

Matriz de Controles para la revisión de Seguridad para PCCFDI: omawww.sat.gob.mx/informacion_fiscal/factura.../cfdi/MatrizControlesPCCFDI.xls [Consultado el 04 de Octubre, 2018]

UNIVERSIDAD DE SONORA

COORDINACIÓN DIVISIONAL DE: _____

PRÁCTICAS PROFESIONALES

FPP-4

DEPARTAMENTO: _____

UNIDAD REGIONAL: _____ CAMPUS: _____

REPORTE FINAL DE ACTIVIDADES

Periodo: Del 30 / Abril / 2018 al 30 / Agosto / 2018

Cantidad de 340 Horas de un total de 340 Avance: 100 %

Nombre del practicante: Cruz León Jorge Eduardo

Expediente: 21 2201501 **Programa Educativo (Licenciatura):** _____

Nombre del Programa/Proyecto: Revisión y Aplicación de políticas de seguridad de la información NMX-I-27001/ISO/IEC 27001 en infraestructura que da soporte al proceso CFDI

Datos de la Unidad Receptora (Razón Social): Prodigia Procesos Digitales Administrativos SA. de C.V.

Responsable de la Unidad Receptora (Nombre/Puesto): Luis Arturo Rodríguez Lares

Contacto: Teléfono/UR: 210 4963 Ext. _____ Celular: _____

DESCRIPCIÓN GENERAL DE ACTIVIDADES
El practicante se capacitará en la norma internacional ISO/IEC 27001 para adquirir y aplicar los conocimientos adquiridos en el Sistema de Gestión de Seguridad de la Información en la infraestructura que da soporte al proceso de CFDI de Prodigia.

RETROALIMENTACIÓN

En caso de requerirse, anexar reportes, formatos, diagramas que apoyen las actividades realizadas.

Observaciones Generales:

Jorge Eduardo Cruz León Nombre y firma del alumno	Nombre y firma del tutor de prácticas profesionales Unison.	Luis Arturo Rodríguez Lares Nombre y firma del responsable de la unidad receptora Sello de la UR

Prodigia
PRODIGIA PROCESOS DIGITALES ADMINISTRATIVOS SA DE CV
PPD/101129 EA3

Original entregar en físico a Tutor de Prácticas Profesionales y **Copia** *alumno.*
***Enviar en PDF al** Coordinador o Responsable de Prácticas Profesionales de la carrera.*

(25/04/2018)

Prodigia®

Prodigia Procesos Digitales Administrativos S.A. de C.V.

Hermosillo, Sonora a 08 de Octubre de 2018

A QUIEN CORRESPONDA:

Por medio de la presente hago de su constar que **Jorge Eduardo Cruz León** número de expediente **212201501** de la carrera de Ing. Sistemas De la Información en la Universidad de Sonora llevo a cabo sus prácticas profesionales en nuestra empresa **Prodigia Procesos Digitales Administrativos SA de CV** ubicada en Antonio Quiroga 21 int 3 Col. Quinta Emilia, Hermosillo, Sonora México, C.P. 83214 en el periodo de *30 de Abril al 30 de Agosto* del presente año, el área de desarrollo, en el proyecto "Revisión y aplicación de Políticas de Seguridad de la Información NMX-I-27001/ISO/IEC 27001 en la Infraestructura que da soporte al proceso CFDI de Prodigia Procesos Digitales Administrativos SA de CV" el cual consto de una duración de ***340 horas***.

Sin más por el momento quedo a sus órdenes.

Atentamente.

Prodigia
PRODIGIA PROCESOS DIGITALES ADMINISTRATIVOS
SA DE CV

Ing. Luis Arturo Rodriguez Lares
Responsable Prodigia Procesos Digitales Administrativos SA de CV

Torre N2, Blvd. Antonio Quiroga No. 21 Interior 3 Primer Piso, Colonia Quinta Emilia CP. 83214
Tel.- (662) 210 49 63 Hermosillo, Sonora, México