UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE ESTÁNDARES EN MATERIA DE SEGURIDAD INFORMÁTICA

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniera en Computación

P R E S E N T A

Denise Betancourt Sandoval

ASESORA DE INFORME

M.I. Norma Elva Chávez Rodríguez

Ciudad Universitaria, Cd. Mx., 2017

Índice

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

Introducción

En los últimos años, las organizaciones han empleado Tecnologías de Información y Comunicación (TIC) para crear, procesar, almacenar y transferir información, permitiéndoles tomar decisiones vitales que influyen en el cumplimiento de su misión y objetivos.

En este sentido, la información se vuelve más importante, y al ser más versátil por encontrarse en diferentes formas (impresa, digital, o verbal) y en diversos estados (almacenamiento, procesamiento o transmisión), puede ser objeto de diversas amenazas como robo, sabotaje, divulgación, falsificación, entre otras. Por tal motivo, surge la necesidad de protegerla, implementando ambientes confiables adaptados a las nuevas tecnologías, soluciones técnicas, a un nuevo enfoque administrativo, tecnológico, cultural y legal, con el fin de garantizar que la información se mantenga disponible, íntegra y confiable.

Por consecuente, nos vemos inmersos en distintos ámbitos que permitan enfrentar los retos de la seguridad, creando estándares y buenas prácticas que incluyan controles de seguridad no sólo físicos y técnicos, sino también legales y administrativos.

El estándar ISO/IEC 27001:2013 es una referencia internacional utilizada para la selección de controles de seguridad de la información, así como para establecer, implementar, operar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

La Coordinación de Seguridad de la Información (CSI) /UNAM-CERT, siendo una organización que fomenta la cultura de seguridad de la información, tiene implementado y mantiene un Sistema de Gestión de Seguridad de la Información que cumple con los requisitos del estándar ISO/IEC 27001:2013.

Teniendo en cuenta lo anterior, en la redacción del siguiente informe de Trabajo Profesional describo las actividades profesionales que desarrollé para mantener y mejorar un SGSI, obteniendo la certificación del estándar ISO/IEC 27001 en su transición a la versión más reciente, cubriendo necesidades en materia de Seguridad de la Información de la Coordinación de Seguridad de la Información/UNAM-CERT.

CAPÍTULO 1

Descripción de la Coordinación de Seguridad de la Información/UNAM-CERT

CAPÍTULO 1 – Descripción de la Coordinación de Seguridad de la Información/UNAM-CERT

La Coordinación de Seguridad de la Información (CSI)/UNAM-CERT, como parte de la Dirección de Sistemas y Servicios Institucionales dentro de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM, es un punto de encuentro al cual puede acudir la comunidad de cómputo para obtener información, asesorías y servicios de seguridad; así como para intercambiar experiencias y puntos de vista a través de seminarios, pláticas, investigaciones, logrando con ello, establecer políticas de seguridad adecuadas, disminuir la cantidad y gravedad de los problemas de seguridad y difundir la cultura de la seguridad en cómputo.

En este sentido, la CSI es consciente de que la seguridad de los sistemas no está en las manos de unos cuantos, sino que depende de todos: usuarios, administradores y organizaciones que conforman la comunidad de cómputo.

A continuación, muestro un breve panorama de la CSI/UNAM-CERT, exponiendo su importancia no sólo a nivel universidad, sino también a nivel nacional.

1.1 Misión

Contribuir al desarrollo de la UNAM, a través de la prestación de servicios especializados, la formación de capital humano y el fomento de la cultura de seguridad de la información.

1.2 Visión

Consolidar a la UNAM como la entidad líder en materia de Seguridad de la Información en el país.

1.3 Objetivos

- Proporcionar servicios de seguridad de la información para la UNAM y otras organizaciones.
- Promover la cultura de seguridad de la información.
- Formar especialistas que desarrollen y apliquen estrategias de protección de la información.
- Difundir contenidos especializados en seguridad de la información.

- Colaborar con instituciones nacionales e internacionales en materia de detección y respuesta a incidentes.
- Elaborar políticas y lineamientos de seguridad de la información para las dependencias y entidades académicas universitarias.

1.4 Historia

Debido a la creciente evolución de los equipos de cómputo y a su incorporación en el desempeño de las actividades cotidianas, muchas organizaciones como industrias, gobiernos, corporativos e incluso universidades, han puesto total interés en establecer un área específica que se encargue de la Seguridad de la Información no sólo por su manejo en grandes volúmenes, sino también por las diversas formas y estados en las que ésta puede presentarse.

La Universidad Nacional Autónoma de México (UNAM), reconocida como una universidad de excelencia en el mundo académico, cuenta hoy con una red inalámbrica que posibilita la conexión en línea de todos sus usuarios desde cualquier punto de Ciudad Universitaria y las facultades de estudios superiores. Sin embargo, desde años anteriores se tuvo la necesidad de hacer algo al respecto sobre la seguridad de la información debido a la presencia de personas con capacidades e intereses de destruir los muros de seguridad impuestos por el sistema, además de que éstos se veían aún más debilitados por falta de una legislación referente al tema.

Para enfrentar la situación de aquel entonces en la UNAM, el ingeniero Diego Martín Zamboni creó el Área de Seguridad en Cómputo, la cual ha evolucionado con el paso de los años en paralelo con los avances tecnológicos y el surgimiento de nuevas amenazas dirigidas a los sistemas informáticos, hasta convertirse en la actual Coordinación de Seguridad de la Información. Examinaremos ahora algunos acontecimientos que considero más sobresalientes en la historia de la CSI/UNAM-CERT.

- Año 1993

La CSI/UNAM-CERT tuvo su primer contacto con el “Coordination Center” de Carnellie Mellon de Estados Unidos, o Computer Emergency Response Team (CERT/CC). El CERT/CC es el primer equipo de respuesta a incidentes de todo el mundo y ha hecho diversas contribuciones en el área de seguridad de la información.

Ese mismo año, el Ingeniero Diego Martín Zamboni creó el Equipo de Respuesta a Incidentes en Seguridad en Cómputo, perteneciente a la entonces Dirección General de Servicios de Cómputo Académico (DGSCA), hoy DGTIC.

- Año 1994

El Área de Seguridad en Cómputo organizó la primera edición del Día Internacional de la Seguridad en Cómputo en México (DISC), que en años posteriores se utilizó para ofrecer pláticas de concientización de seguridad.

- Año 1998

Las pláticas del DISC fueron ofrecidas por ponentes de organizaciones especializadas en seguridad, de México y del extranjero. Esta edición del DISC es considerada como la primera edición del Congreso de Seguridad en Cómputo de UNAM-CERT.

- Año 1999

El Lic. Juan Carlos Guel López toma la jefatura del Área de Seguridad en Cómputo y bajo su liderazgo se convierte en el Departamento de Seguridad en Cómputo (DSC), se aumentan los recursos asignados a la organización, tanto humanos como materiales, lo que permitió que se ampliara el ámbito de acción del DSC a otras dependencias de la UNAM.

- Año 1999 – 2001

En México no existía ningún equipo de respuesta a incidentes que fuera reconocido internacionalmente, por lo que se vio la necesidad de ubicarse como punto de contacto internacional para atender incidentes no sólo en RED-UNAM, sino en México, por esa razón se inició el trámite y se obtuvo la acreditación ante el Forum of Incident Response Security Teams (FIRST). Al mismo tiempo, la acreditación le permitió a UNAM-CERT obtener visibilidad internacional para lograr acuerdos con grupos nacionales e internacionales.

- Año 2003

Mediante la colaboración de la ANUIES (Asociación Nacional de Universidades e Instituciones de Educación Superior), se crea la Red Nacional de Seguridad en Cómputo (RENASEC), con el objetivo de albergar y compartir las iniciativas, acuerdos y noticias en materia de seguridad informática, a más de 145 Instituciones de Educación Superior del país.

- Año 2005

UNAM-CERT se une al Proyecto Honeynet mediante Honeynet UNAM-CHAPTER. La participación de UNAM-CERT en el Proyecto Honeynet le permitió establecer nuevos

vínculos con organizaciones internacionales y estar a la vanguardia de nuevas tecnologías de detección de intrusos, análisis de malware, respuesta a incidentes y cómputo forense.

- Año 2010

El Departamento de Seguridad en Cómputo se convierte en Subdirección de Seguridad de la Información. Se obtiene la certificación ISO 27001:2005 para el proceso de respuesta y atención a incidentes de seguridad.

- Año 2014

La Subdirección cambia su nombre a Coordinación de Seguridad de la Información (CSI), con lo que se actualiza el alcance y el ámbito de acción de la organización.

- Año 2015

Se realizó la transición del estándar ISO/IEC 27001:2005 a la versión actual ISO/IEC 27001:2013, con la que la CSI mantiene la certificación de esta norma.

1.5 Servicios

Una de las principales actividades de la CSI/UNAM-CERT es proporcionar servicios a la Universidad. Éstos ayudan a aumentar la seguridad de la infraestructura tecnológica, la cual es base indispensable de numerosos procesos que requieren una adecuada administración y protección ante diversas amenazas.

Los servicios que la CSI/UNAM-CERT ofrece a organizaciones internas y externas son:

- Implementación de un SGSI de acuerdo al estándar ISO/IEC 27001
- Auditoría informática
- Análisis forense
- Análisis de vulnerabilidades y pruebas de penetración
- Análisis de tráfico de red
- Análisis de riesgos
- Respuesta a incidentes de seguridad de la información
- Revisión de configuraciones
- Creación de políticas de seguridad de la información
- Revisiones de seguridad para aplicativos web

Asimismo, la CSI/UNAM-CERT también brinda capacitación y actualización constante para la comunidad universitaria, por lo que cuenta con un portafolio de cursos que proporciona a través del Congreso de Seguridad en Cómputo y un Plan de Becarios en Seguridad Informática.

1.5.1 Congreso de Seguridad en Cómputo

En el Congreso de Seguridad en Cómputo se ofrecen cursos y talleres especializados a nivel nacional en seguridad de la información, respondiendo a necesidades de la industria tecnológica en nuestro país.

Desde el año 1998 hasta la fecha, se han presentado quince Congresos de Seguridad en Cómputo, generalmente de manera anual y con una duración de ocho días. Cada uno de ellos presenta diversas líneas de especialización con sus respectivos cursos, como son:

Línea 1. Cómputo forense y legislación relacionada

- L1.a Legislación forense
- L1.b Introducción al análisis forense y sistemas de archivos
- L1.c Análisis forense en sistemas Linux
- L1.d Análisis forense en sistemas Windows
- L1.e Análisis forense de tráfico de red
- L1.f Análisis de memoria volátil
- L1.g Bases de análisis forense de dispositivos móviles

Línea 2. Análisis de vulnerabilidades, técnicas de intrusión y pentest

- L2.a Pruebas de penetración y hacking ético
- L2.b Técnicas y métodos de intrusión
- L2.c Análisis de vulnerabilidades
- L2.d Pruebas de penetración en aplicaciones web
- L2.e Pruebas de penetración en red

Línea 3. Detección de intrusos y tecnologías honeypot

L3.a Introducción a la detección de intrusos

L3.b Técnicas de análisis de tráfico de red

L3.c Herramientas para detección de tráfico sospechoso

L3.d Monitoreo de seguridad de red

L3.e Tecnologías honeypot

Asimismo, algunos de los talleres que se imparten son:

- Análisis de software malicioso
- Aspectos legales de la seguridad informática
- Desarrollo seguro de aplicaciones web
- Fundamentos sobre Sistema de Gestión de la Continuidad del Negocio (SGCN)
- Hardening en sistemas operativos Linux
- Implementación del SGSI (ISO/IEC-27001:2013)
- Seguridad en Apache HTTPD y manejadores de contenido
- Seguridad en servicios en redes Windows
- Seguridad Operativa
- Virtualización y hardening de servidores Windows

También, a través de conferencias, la CSI acerca a la comunidad con las opiniones e investigaciones de reconocidos expertos en seguridad informática a nivel nacional e internacional.

1.5.2 Plan de Becarios en Seguridad Informática

El Plan de becas ofrece capacitación especializada a estudiantes regulares de los últimos semestres de las carreras de informática, cómputo y afines, tanto para escuelas y facultades de la UNAM como de otras universidades.

En la actualidad, la duración de este plan de becas es de catorce a dieciocho meses, y han sido doce generaciones de alumnos quienes han recibido capacitación en materia de seguridad. Hoy en día, los cursos están agrupados en cinco módulos:

1. **Seguridad en redes y sistemas operativos**
    a. Introducción a la seguridad informática
    b. Introducción al sistema operativo Linux
    c. Utilerías y programación Shell
    d. Administración y seguridad en redes
    e. Administración y seguridad en Windows
    f. Administración y seguridad en Linux
    g. Scripts para administración en Windows
2. **Programación orientada a la seguridad**
    a. Programación con Phyton
    b. Seguridad en base de datos
    c. Lenguaje C y llamadas al sistema
    d. Programación con PERL
    e. Programación orientada a objetos (C#)
    f. Desarrollo seguro de aplicaciones móviles
    g. Seguridad en aplicaciones web
3. **Análisis de vulnerabilidades y hacking ético**
    a. Pruebas de penetración
    b. Análisis de vulnerabilidades
    c. Criptografía y sus aplicaciones
4. **Monitoreo de seguridad en redes y respuesta a incidentes**
    a. Análisis de software malicioso
    b. Detección de intrusos y tecnologías Honeypot
    c. Seguridad perimetral
    d. Respuesta a incidentes
    e. Análisis forense
    f. Legislación
5. **Gestión de la seguridad de información**
    a. ISO 27000 y auditorías
    b. Administración de proyectos

El objetivo de este plan es formar recursos humanos especializados en el campo de seguridad informática a través de capacitación en metodologías y técnicas para proteger la información y la infraestructura tecnológica de las organizaciones.

1.6 Estructura organizacional

La Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) contribuye al logro de los objetivos de la UNAM como punto de unión de la comunidad universitaria para aprovechar los beneficios que las tecnologías de la información y las comunicaciones puedan aportar a la docencia, la investigación, la difusión de la cultura y la administración universitaria.

La DGTIC está dividida en diez áreas, cuenta con dos Coordinaciones, cinco Direcciones, una Subdirección y una Unidad Administrativa, guiados bajo la Dirección General del Dr. Felipe Bracho Carpizo (véase Ilustración 1.1).

ILUSTRACIÓN 1.1, ORGANIGRAMA DGTIC

Como lo mencioné al inicio de este Capítulo 1, la Coordinación de Seguridad de la Información/UNAM-CERT es parte de la Dirección de Sistemas y Servicios Institucionales

(DSSI), la cual resalto en el organigrama mostrado, junto con otros departamentos y coordinaciones entre las que destacan:

- Coordinación de la Unidad de Voto Electrónico
- Coordinación de Súper cómputo
- Departamento de Visualización y Realidad Virtual
- Departamento de Firma Electrónica Avanzada
- Departamento de Administración de Servidores
- Servicios del Centro de Datos

La Coordinación de Seguridad de la Información apoya a la DSSI a cumplir con sus objetivos. Además de los servicios que ofrece, también organiza diversos eventos, imparte cursos, seminarios, pláticas, difunde información y realiza investigaciones con apoyo de su personal capacitado en diferentes áreas de seguridad de la información.

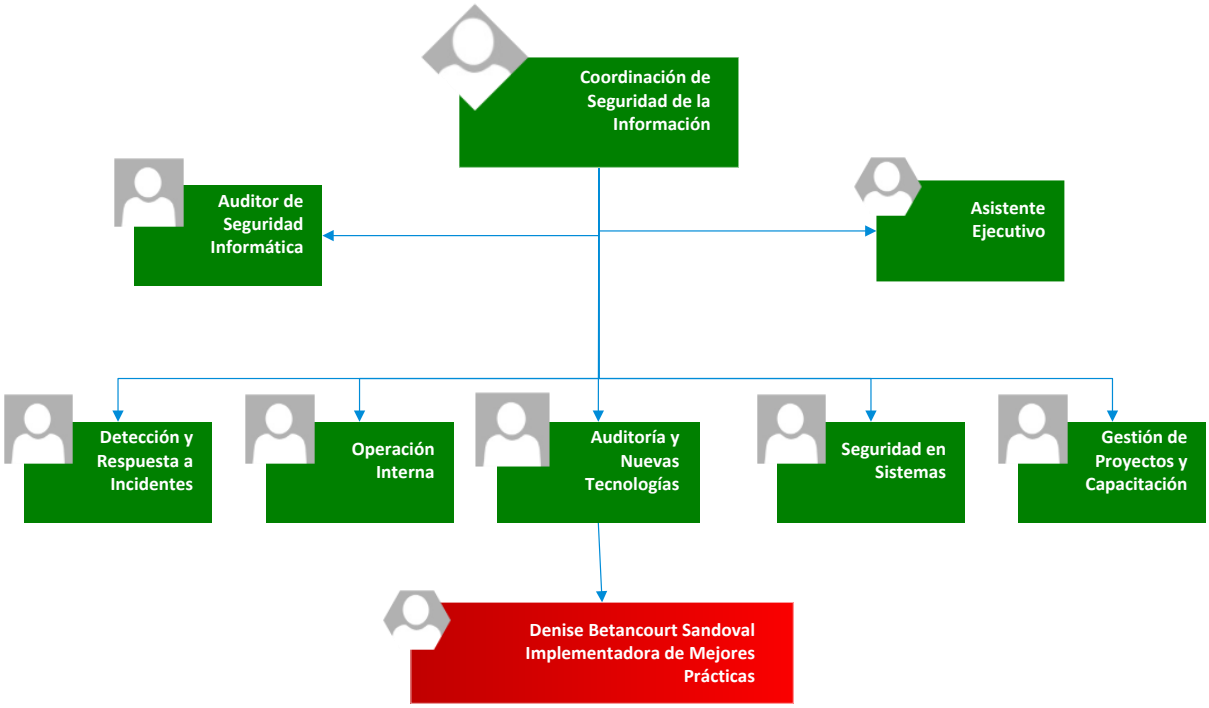

ILUSTRACIÓN 1.2, ORGANIGRAMA CSI/UNAM-CERT

Los cinco departamentos que conforman la Coordinación de Seguridad de la Información, como se muestra en la Ilustración 1.2, son los siguientes:

- Auditoría y Nuevas Tecnologías
- Detección y Respuesta a Incidentes
- Operación Interna
- Seguridad en Sistemas
- Gestión de Proyectos y Capacitación

En particular, el departamento de Auditoría y Nuevas Tecnologías cuenta con personal que desempeña actividades en los puestos de:

- Analista de Vulnerabilidades
- Especialista en Pentest
- Implementador de Mejores Prácticas

En lo que a mí respecta, me desempeñé en el puesto de "Implementador de Mejores Prácticas", mismo que describo más a detalle en el siguiente capítulo.

CAPÍTULO 2

Puesto de trabajo

CAPÍTULO 2 – Puesto de Trabajo

2.1 Ingreso al puesto de trabajo

Estando en mi último semestre de la carrera de Ingeniería en Computación (2014-1), en el módulo de redes y seguridad, decidí participar en la convocatoria para formar parte de la octava generación del Plan de Becarios en Seguridad Informática de la CSI/UNAM-CERT, la cual iniciaría en el mes de agosto de 2013.

El Plan de Becarios, del cual hablé en el Capítulo 1, maneja un proceso de selección que consiste en exámenes de conocimientos, pruebas psicométricas y entrevistas con miembros de la CSI/UNAM-CERT. El examen de conocimientos engloba diversos temas como sistemas operativos, redes, bases de datos, programación, matemáticas y lógica.

En este sentido, el haber adquirido conocimientos en la Facultad de Ingeniería, me dio la capacidad para afrontar las pruebas del proceso de selección, obteniendo un resultado aprobatorio para que yo pudiera ser parte de los treinta seleccionados que formaríamos la octava generación del Plan de Becarios en Seguridad Informática.

De ello se desprende parte de mi formación como ingeniera en computación, incorporando conocimientos que la Facultad me había otorgado y otros más específicos a través de capacitación en metodologías y técnicas para proteger la información y la infraestructura tecnológica de las organizaciones.

No obstante, a finales de octubre de 2014 se liberó una vacante para el puesto de Implementador de Mejores Prácticas, perteneciente al Departamento de Auditoría y Nuevas Tecnologías, por lo que poco antes de concluir con el Plan de becarios (febrero de 2015), evaluaron mis habilidades desarrolladas hasta ese momento junto con mis conocimientos adquiridos, y fui invitada a laborar en la CSI/UNAM-CERT en noviembre de 2014.

2.2 Descripción del puesto Implementador de Mejores Prácticas

En la Coordinación de Seguridad de la Información, cada uno de los puestos que la integran tienen como base una formación académica y habilidades deseables para el cumplimiento de las actividades desarrolladas en la organización.

El puesto de Implementador de Mejores Prácticas, perteneciente al departamento de Auditoría y Nuevas Tecnologías, requiere de personas que hayan estudiado una licenciatura o sean estudiantes de los últimos semestres en la carrera de ingeniería en computación, ingeniería en telecomunicaciones o carreras afines.

En ese sentido, mi función principal en la CSI fue:

> Dirigir y coordinar el proceso de implementación de un Sistema de Gestión de Seguridad de la Información de acuerdo al estándar ISO/IEC 27001, para mejorar la seguridad de la información a nivel organizacional.

Las habilidades que requería para el desempeño del puesto fueron:

- Evaluación y análisis de la información
- Generación de políticas
- Ejecución de auditorías
- Conocimientos de estándares y mejores prácticas de seguridad informática
- Conocimiento de los procedimientos en la metodología para los marcos de referencia y creación de informes

2.3 Actividades del puesto Implementador de Mejores Prácticas

Como lo mencioné anteriormente, uno de los servicios que brinda la CSI/UNAM-CERT es la Respuesta a Incidentes de seguridad de la información.

La información generada y manipulada dentro del proceso de Manejo de Incidentes debe ser segura, es decir, que se conduzca bajo características de confidencialidad, integridad y disponibilidad, y debe garantizar la continuidad en sus operaciones. Para ello se consideró la implementación, operación, revisión, mantenimiento y mejora de un SGSI, de ahí que mis actividades recurrentes en la CSI/UNAM-CERT como Implementadora de Mejores Prácticas fueron:

- Mantener y mejorar el Sistema de Gestión de Seguridad de la Información.
- Brindar asesorías a dependencias de la UNAM o externas
- Traducción y publicación de noticias de seguridad informática

2.3.1 Mantener y mejorar el Sistema de Gestión de Seguridad de la Información

Para un mejor entendimiento de esta actividad, la dividiré en tres actividades secundarias:

Actividad 1: *Publicar y comunicar las políticas y procedimientos de seguridad*

Objetivo: Mantener un nivel de conciencia elevado en cuanto a seguridad de la información, políticas y procedimientos internos para disminuir la probabilidad de ocurrencia de incidentes en la CSI/UNAM-CERT.

Periodicidad: Mensual. Realicé la actividad una vez cada mes, desde que ingresé hasta que finalicé mi estancia en la CSI/UNAM-CERT (noviembre 2014 a enero 2016).

Desarrollo: La manera más eficiente de publicar y comunicar los documentos importantes del SGSI al personal de la CSI/UNAM-CERT, fue a través de sesiones informativas con presentaciones y dinámicas recreativas, dando a conocer los aspectos más relevantes que permitían cumplir con la confidencialidad, integridad y disponibilidad de la información manejada en la Coordinación.

Resultados: El cumplimiento de las políticas y procedimientos internos es notable ya que el número de incidentes se ve reducido y el personal es más consciente de los temas relacionados con el Sistema de Gestión de Seguridad de la Información.

Actividad 2: *Coordinar y dirigir todo el marco de seguridad de la información*

Objetivo: Aplicar los estándares en materia de seguridad informática incluyendo sus controles de seguridad.

Periodicidad: Mensual o cada vez que haya un cambio significativo en la infraestructura de la CSI/ UNAM-CERT.

Desarrollo: El proceso de Manejo de Incidentes de la CSI/UNAM-CERT ha sido una de las actividades primordiales. Es por ello que se tiene implementado el SGSI basado en el estándar ISO/IEC 27001 para identificar riesgos de seguridad y seleccionar los controles adecuados para su gestión.

Sin embargo, el SGSI, al operar de manera cíclica, debe mejorarse continuamente. Por esta razón, se hacen revisiones considerando riesgos y controles que se tienen implementados o que necesitan implementarse para gestionar de manera adecuada dichos riesgos.

Cabe destacar que las actividades involucradas en el proceso de Manejo de Incidentes tienen relación con otras normas, como son:

- ISO 31000 para la gestión de riesgos

- ISO/IEC 27002 como guía de buenas prácticas para implementar controles

- ISO/IEC 27004 para métricas y medidas

- ISO/IEC 27005 gestión de riesgos de seguridad de la información, entre otros estándares.

Aunque estas normas listadas como ejemplo se toman como referencia para el SGSI, el estándar ante el cual la CSI/UNAM-CERT está certificada es el ISO/IEC 27001.

Resultados: Desde el año 2010 hasta la actualidad, la Coordinación de Seguridad de la Información mantiene certificado el proceso de Manejo de Incidentes en cumplimiento al

estándar ISO/IEC 27001. Y también, se posiciona como una de las entidades líderes en materia de Seguridad de la Información en el país.

Actividad 3: *Actualizar y controlar los documentos de seguridad que integran el SGSI*

Objetivo: Actualizar los documentos que forman parte del Sistema de Gestión de Seguridad de la Información cada ciclo, una vez que se haya llevado a cabo el análisis de riesgos o cuando haya un cambio significativo.

Periodicidad: Mensual o cada vez que haya un cambio significativo en la estructura de la CSI/ UNAM-CERT.

Desarrollo: Como parte de uno de los controles del estándar ISO/IEC 27001, en el documento *Declaración de Aplicabilidad (SoA)*, se especificó que los responsables de los controles son los responsables de mantener actualizados los documentos asociados a su control.

No obstante, existe un *proceso de Control de cambios* que permite gestionar los cambios realizados en infraestructura, aplicaciones, información y personal que pertenece a la CSI/UNAM-CERT. En éste se señala que cada vez que se requiera un cambio, el solicitante debe llenar el *Formato de Control de cambios* y especificar su prioridad. Posteriormente, me da aviso a mí como implementadora de mejores prácticas y me entrega el formato, y lo reviso para decidir si el cambio es factible; en caso de que sí lo sea, yo informo al responsable del recurso para que autorice y genere el cambio. Por último, registro la solicitud en la Lista maestra de documentos y doy seguimiento al estado del cambio.

Resultados: Cada ciclo se revisa el contenido, validez, estructura de los documentos que integran el Sistema de Gestión de Seguridad de la Información y se cuenta con un control de cambios que es monitoreado a través de la Lista maestra de documentos.

2.3.2 Brindar asesorías a dependencias de la UNAM o externas

La Coordinación de Seguridad de la Información/UNAM-CERT ha participado con Instituciones para fortalecer la calidad y seguridad de la información; en lo que a mí respecta, he apoyado en verificar infraestructura y, evaluar el cumplimiento de normas y seguridad de sus procesos.

También, a través del UNAM-CERT, participé como colaboradora en el Congreso Seguridad en Cómputo 2014, y como instructora en el Congreso Seguridad en Cómputo 2015, impartiendo los talleres: Implementación del SGSI (ISO/IEC 27001:2013) I e Implementación del SGSI (ISO/IEC 27001:2013) II. De modo similar, fui instructora de la

novena generación del Plan de Becarios en Seguridad Informática de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC).

2.3.3 Traducción y publicación de noticias de seguridad informática

Colaboré en la traducción del idioma inglés al español de noticias relevantes sobre Seguridad de la Información en el portal web de la Coordinación de Seguridad de la Información (https://www.seguridad.unam.mx/), verificando su contenido y redacción entendible para cualquier usuario común. Asimismo, contribuí en la traducción del boletín mensual **"OUCH! Asegurando tu red doméstica"**, y en la publicación de la edición 24 de la revista **".Seguridad de la detección al aprendizaje"**.

CAPÍTULO 3

Proyecto Transición del estándar ISO/IEC 27001 para el SGSI de la CSI/UNAM-CERT

Capítulo 3 – Proyecto Transición del estándar ISO/IEC 27001 para el SGSI de la CSI/UNAM-CERT

3.1 Antecedentes

Entendiendo que la visión de la CSI/UNAM-CERT es consolidar a la UNAM como la entidad líder en materia de Seguridad de la Información en el país, y que el proceso de Manejo de Incidentes es actividad fundamental para la CSI, existió la necesidad de adoptar el estándar ISO/IEC 27001, ampliando el panorama de contenido técnico-legal con base en lineamientos a seguir para cumplir con la seguridad de la información.

El estándar ISO/IEC 27001 es actualmente el marco internacional reconocido de las mejores prácticas para un SGSI, el cual ayuda a identificar riesgos de seguridad y seleccionar los controles adecuados para su gestión.

Como se mencionó anteriormente en el apartado de historia y en las actividades del puesto de Implementador de Mejores Prácticas, luego de que en el año 2010 la CSI/UNAM-CERT obtuviera la certificación ISO/IEC 27001:2005 para el proceso de Manejo de Incidentes, transcurrió tiempo en el que el SGSI iba siendo más estable, maduro y efectivo. Sin embargo, la Organización Internacional para la Estandarización (ISO), -derivado del prefijo griego “isos” que significa “igual”-, reorganizó publicaciones de algunas normas con una nueva estructura de Anexo SL y modificaciones en los contenidos, por lo que el estándar ISO/IEC 27001 cambió de la versión 2005 a su versión actual 2013.

3.2 Contexto de mi participación profesional

La CSI/UNAM-CERT, comprometida con la Seguridad de la Información, programó auditorías de seguimiento para los meses de febrero y agosto de 2015 con AENOR -entidad reconocida para desarrollar tareas de normalización y certificación- para mantener y mejorar el SGSI.

En los primeros meses de mi estancia como Implementadora de Mejores Prácticas, participé en la Auditoría de Seguimiento en febrero de 2015, y en ésta se presentaron observaciones a considerar para el SGSI, entre algunos aspectos fueron el Análisis de riesgos, el Comité de Seguridad, y el manejo de información documental. Así pues, los auditores me hicieron hincapié en atender dos puntos importantes como son la Revisión del SGSI por la Alta dirección y la Auditoría interna.

Lo anterior, me dio a la tarea de establecer un plan de acciones correctivas inmediatas para robustecer y mejorar el SGSI. Además, desarrollé un plan de transición ISO/IEC 27001:2005

– ISO/IEC 27001:2013 junto con mi compañero Diego Valverde Rodríguez, auditor interno de la CSI/UNAM-CERT, para posteriormente, implementar las actividades acordadas con la aprobación de los miembros del Comité de Seguridad y teniendo el apoyo de la Alta dirección.

3.3 Descripción del proyecto

Como lo mencioné en los antecedentes, el estándar ISO/IEC 27001:2005 cambió a su versión actual 2013. Esta transición implicaría nuevas tareas y cambios respecto a la mejora y mantenimiento del SGSI de la CSI/UNAM-CERT. Además, dicha transición tenía que realizarse antes del mes de agosto de 2015, ya que la Coordinación tenía actividades relacionadas con el Plan de Becarios, y la fecha de vencimiento para conservar el proceso de Manejo de Incidentes de la CSI certificado era el 1° de octubre de 2015, por lo que mis ocupaciones en el puesto de Implementador de Mejores Prácticas se enfocaron en este tema principalmente.

Así pues, el objetivo fue proporcionar a la CSI/UNAM-CERT las bases necesarias para la transición efectiva del estándar ISO/IEC 27001 en su versión más reciente, antes de la auditoría de revisión de esta adaptación (agosto de 2015).

3.4 Diseño

Para cumplir con el objetivo planteado, tuve que conocer y distinguir los cambios en los requerimientos del estándar. Entre los principales fueron:

0. **Prólogo normativo - Introducción**

La sección enfocada al modelo PDCA ha sido eliminada, lo que la reduce considerablemente. Ahora, las organizaciones son libres de utilizar algún otro enfoque para la mejora continua, por lo que PDCA es sólo una propuesta.

1. **Prólogo normativo – Alcance**

Antes, se tenía que justificar cualquier exclusión de los controles vista como necesaria para satisfacer el criterio de aceptación del riesgo, y proporcionar evidencia de que los riesgos asociados han sido aceptados por las personas responsables. La reciente versión, no incluye ninguna referencia para la exclusión de los controles en el Anexo A.

2. **Prólogo normativo – Referencias normativas**

En la versión anterior, se hace referencia al “ISO/IEC 27002:2005 Código de prácticas para la gestión de la seguridad de la información”. Sin embargo, ahora el estándar “ISO/IEC

27000 Información general y vocabulario" adquiere mayor relevancia ya que se convierte en la única referencia normativa.

3. Prólogo normativo – Términos y definiciones

Los términos y las definiciones son excluidos del estándar ISO/IEC 27001, y en su lugar se hace referencia al ISO/IEC 27000, sólo hay que asegurarse de emplear la versión actualizada para el correcto uso de los términos.

4. Contexto de la organización

Esta nueva cláusula establece el contexto para el SGSI. Considera factores internos y externos con los requisitos de las *partes interesadas* -término que reemplaza el de *stakeholders*- para determinar el alcance del SGSI.

5. Liderazgo

Se trata de una nueva cláusula que considera los requisitos específicos para que en la "alta dirección" se asignen responsabilidades y autoridades relevantes a la seguridad de la información.

Asimismo, en la versión 2005 se tenía como requisito el desarrollo de una política del SGSI, documento orientado al control del SGSI y enfocado en los administradores de alto nivel. Mientras que en la versión 2013 se tiene como requisito el desarrollo de la política de seguridad de la información, que describe cualquier lineamiento de seguridad.

6. Planeación

Se muestran los requisitos del estándar relacionados con la evaluación de riesgos de seguridad de la información, así como para el tratamiento aplicable en función de los criterios de aceptación de los mismos.

Algo muy importante es que esta cláusula quita la identificación de activos, amenazas y vulnerabilidades como pre-requisito de identificación de riesgos. Incluso, ya no se hace referencia a los *dueños de activos*; ahora se emplea el término *propietario o dueño del riesgo* como la persona o entidad con la responsabilidad y autoridad para gestionar el riesgo.

7. Soporte

Se considera que las organizaciones deben determinar y proveer los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el SGSI. Además, se tienen en cuenta requisitos para competencia, concientización, comunicación e información documentada. Éste último punto es un término nuevo que reemplaza las referencias en la versión del estándar anterior, de "documentos" y "registros".

8. Operación

La organización debe asegurar que los planes y procesos de las cláusulas anteriores, se determinen y controlen. También trata sobre el desempeño en la evaluación de riesgos y la implementación del plan de tratamiento de riesgos de seguridad de la información

9. Evaluación del desempeño

En esta cláusula se determina qué información necesita para evaluar el desempeño de seguridad de la información y la efectividad del SGSI, determinando qué medir y controlar, los métodos del cómo, a quién y cuándo.

Para el caso de la auditoría interna, se elimina el requerimiento de que los auditores no deben auditar su propio trabajo, y se cubre este punto con el requerimiento de asegurar la objetividad e imparcialidad.

Otro punto a resaltar es que se eliminó el requerimiento de mantener las revisiones de la gestión al menos una vez al año. Ahora sólo se establece que tendrán lugar a intervalos planeados.

10. Mejora

La mejora continua del SGSI ya no contempla las acciones preventivas en la reciente versión. Sin embargo, se crearon nuevos requerimientos para las acciones correctivas, reaccionando ante las no conformidades y trabajando con las consecuencias. Se asegura que las acciones correctivas son apropiadas a los efectos de las no conformidades encontradas.

Derivado de lo anterior, y revisando el estatus del SGSI de la CSI/UNAM-CERT, noté puntos específicos que nos hacía falta considerar para la mejora del SGSI, por lo que antes de cualquier cambio, sostuve una reunión con el Comité de Seguridad para darles a conocer los principales ajustes y modificaciones que había que realizar para iniciar con las actividades de transición del estándar ISO/IEC 27001. Para un mejor entendimiento, les hablaré del Comité de Seguridad en el siguiente punto.

3.4.1 Comité de Seguridad

Es un grupo integrado por la alta dirección y jefes de áreas funcionales de la CSI/UNAM-CERT. Tiene la responsabilidad de asegurar que los objetivos son identificados, se satisfacen los requisitos de la organización y se integran en procesos relevantes. También son los responsables de:

- Revisar, actualizar y aprobar la Política de Seguridad de la Información, así como otras políticas

- Revisar la efectividad de la implementación
- Asegurar la implementación coordinada de controles de seguridad de la información
- Proveer dirección y apoyo a las iniciativas de seguridad, así como los recursos necesarios
- Aprobar la asignación de roles y responsabilidades específicas para la seguridad de la información en la CSI
- Iniciar planes y programas para promover la concienciación y capacitación
- Definir criterios de aceptación de riesgos
- Autorizar auditorías internas y externas de seguridad

TABLA 3.1, COMITÉ DE SEGURIDAD UNAM-CERT.

Rol dentro del Comité de Seguridad	Puesto	Descripción
Presidente	Coordinador de Seguridad de la Información	Garantiza y aprueba los cambios en los procesos de operación que requieran de controles de seguridad que el Comité determine. Provee además el voto de calidad en el Comité de Seguridad.
Coordinador SGSI	Implementador de Mejores Prácticas	Tiene el conocimiento y habilidades necesarias para llevar a cabo las actividades propias del SGSI satisfactoriamente. Como Implementador de buenas prácticas debe contar con el don de mando y capacidad de análisis, además de conocer los procesos de operación de la CSI/UNAM-CERT. Elabora el plan del ciclo del SGSI y da seguimiento para su cumplimiento. Posee voto en las decisiones tomadas en el Comité de Seguridad.
Vocales técnicos	Jefe de departamento de Auditoría y Nuevas Tecnologías	Representan a cada departamento de la CSI/UNAM-CERT. Toman decisiones en el Comité de Seguridad según su área de operación. Brindan soluciones reales, viables y aplicables a situaciones que les atañen.
	Jefe de departamento	

	de Detección y Respuesta a Incidentes	
	Jefe de departamento de Operación Interna	
	Jefe de departamento de Seguridad en Sistemas	
	Jefe de departamento de Gestión de Proyectos y Capacitación	

3.5 Desarrollo

Con el fin de asegurar que se proporcionen con las bases necesarias para la transición efectiva del estándar, se establecieron las siguientes actividades, las cuales se desglosan más adelante para el proceso de transición:

a) Listar todas las partes interesadas
b) Definir interfaces en el Alcance del SGSI
c) Alinear los objetivos del SGSI con los de la Coordinación de Seguridad de la Información/UNAM-CERT
d) Hacer cambios en la Política de Seguridad (actualmente Política del SGSI)
e) Hacer cambios al proceso de evaluación de riesgos
f) Identificar el estatus de los controles en la declaración de aplicabilidad
g) Obtener aprobación de los dueños del riesgo
h) Decidir qué hacer con ciertos procedimientos de gestión
i) Escribir nuevas políticas y procedimientos
j) Reorganizar los controles
k) Medición y presentación de informes

a) Partes interesadas

Se llevó a cabo una junta con el Comité de Seguridad donde se establecieron todas las partes interesadas del SGSI de la CSI/UNAM-CERT, entendiendo como "partes interesadas" las personas u organizaciones que pueden influenciar la seguridad de la información de la CSI/UNAM-CERT o ser influenciadas por ella y sus requerimientos; personas que pueden ser afectadas por las actividades de continuidad de negocios.

Al término de la reunión, se identificaron como partes interesadas:

Clientes:

- Dependencias y Entidades Académicas de la UNAM
- Usuarios finales
- Equipos de Respuesta a Incidentes
- Áreas de DGTIC

Entidades de Colaboración:

- Honeynet Project
- Equipos de Respuestas a Incidentes
- ISP
- Shadowserver

Agencias gubernamentales:

- PGR
- SEGOB
- Policías Cibernéticas

Proveedores:

- Subdirección de Operación de la Red
- Proveedores internos
- Canales de distribución de equipo de cómputo y soporte técnico

Patrocinadores:

- DGTIC

Medios:

- Subdirección de Comunicación e Información

Del mismo modo, el Comité de Seguridad me apoyó a establecer los requerimientos de dichas partes interesadas para la seguridad de la información. Mencionaré como ejemplo sólo los requerimientos del patrocinador DGTIC, por fines de confidencialidad.

Requerimientos de seguridad (del Patrocinador para con la CSI/UNAM-CERT):

- Disponibilidad de infraestructura (conectividad a internet, conectividad a Red UNAM y energía eléctrica), acceso a instalaciones 24x7
- Disponibilidad de procesos administrativos en fechas y horarios laborales para la UNAM
- Confidencialidad de la información asociada a incidentes
- Integridad de la información asociada a incidentes

Requerimientos de seguridad (de la CSI/UNAM-CERT para con el Patrocinador):

- Disponibilidad de servicio de Detección y Respuesta a Incidentes 5x8
- Confidencialidad de la información asociada a incidentes
- Integridad de la información asociada al proceso y manejo de incidentes

b) Interfaces en el Alcance del SGSI

En este punto se verificó y modificó la definición del Alcance del SGSI de la CSI/UNAM-CERT, al identificar las actividades críticas del proceso de Manejo de Incidentes y los puntos por los cuales interactuaban entradas y salidas de dicho proceso –interfaces- con las partes interesadas.

Para definir las interfaces, se reconocieron los puntos finales que se encontraban bajo control con las partes interesadas: límites lógicos como la red local, o límites físicos como inmueble u oficinas.

Este fue el resultado para el caso de los Clientes:

- Dependencias y Entidades Académicas de la UNAM
    - Límite físico: Instalaciones Universitarias
    - Límite TI: Conexión a internet, Red UNAM y otras redes que se utilicen dentro de las entidades académicas y dependencias, equipos propiedad de la Universidad

- Usuarios finales
    - Límite físico: Instalaciones de la CSI (atención personal)
    - Límite TI: Dispositivos electrónicos involucrados en Incidentes detectados o reportados a UNAM-CERT

- Equipos de Respuesta a Incidentes
    - Límite físico: Instalaciones de la CSI
    - Límite TI: Dispositivos electrónicos involucrados en Incidentes detectados o reportados a UNAM-CERT

- Áreas de DGTIC
    - Límite Físico: Instalaciones de la CSI
    - TI: Dispositivos electrónicos involucrados en Incidentes detectados o reportados a UNAM-CERT

Como bien lo comenté al inicio de este punto, esta actividad del proceso de transición me ayudó a tener una mejor definición del Alcance del SGSI, modificándolo para incluir los límites de infraestructura, así como activos de información derivados de las actividades del proceso de Manejo de Incidentes.

c) Objetivos del SGSI con los de la Coordinación de Seguridad de la Información/UNAM-CERT

Se realizó una revisión de los objetivos específicos del SGSI considerando la misión, visión y objetivos de la Coordinación de Seguridad de la Información/UNAM-CERT dentro de la Política de Seguridad. En este caso, propuse guiarnos a través del establecimiento de objetivos SMART –metodología ideada por George T. Doran-, entendiendo por ese acrónimo lo siguiente:

TABLA 3.2, OBJETIVOS SMART.

S	Specific	Específico
M	Measurable	Medible
A	Attainable	Alcanzable
R	Relevant	Relevante o Realista
T	Time-related	Con un tiempo determinado

Teniendo en cuenta lo anterior, junto con el Comité de Seguridad se definieron objetivos del SGSI compatibles con la estrategia de la CSI, algunos de ellos son:

1. Aprender, difundir, mejorar y socializar las actividades de la Coordinación de Seguridad de la Información/UNAM-CERT revisando el contenido, validez, estructura de al menos 10% de la cantidad de documentos cada semestre y actualizando en caso de requerirlo.
2. Concientizar al personal de la Coordinación de Seguridad de la Información/UNAM-CERT en aspectos relacionados con el Sistema de Gestión de Seguridad de la Información, estableciendo dos sesiones informativas y un examen por trimestre en el que un mínimo de 70% del personal lo acredite.
3. Preservar la confidencialidad, integridad y disponibilidad de la información durante el Proceso de Manejo de Incidentes manteniendo como máximo un incidente al año derivado de acceso no autorizado.

Asimismo, se cambió el nombre al documento Política del SGSI por Política de Seguridad de la Información.

d) Política de Seguridad

Conforme a la nueva versión del estándar, inicialmente se consideró no incluir los requisitos de la metodología de análisis de riesgos ni el criterio de evaluación de riesgos, y manejarla como información documentada aparte. Sin embargo, preferimos sólo mantener la referencia a la metodología de análisis y evaluación de riesgos OCTAVE Allegro.

No obstante, sí fue necesario modificar la Política de Seguridad debido a que en ella también expusimos cómo medir la efectividad del SGSI, y a consecuencia de que en el punto anterior modificamos los objetivos del SGSI alineados a la metodología SMART, cambié métricas como las que se muestran en la siguiente Tabla 3.3:

TABLA 3.3, EFECTIVIDAD DEL SGSI.

Objetivo	Métrica	Fórmula	Ideal	Meta	Frecuencia	Responsable	Fuente de información
Aprender, difundir, mejorar y socializar las actividades de la Coordinación de Seguridad de la Información/UNAM-CERT revisando el	Total de documentos registrados en la lista maestra	$\frac{Número\ de\ documentos\ revisados}{Total\ de\ documentos} x100$	100%	≥10%	Semestre	- Coordinador de Seguridad de la Información - Jefes de departamento de la CSI/UNAM-CERT	Lista maestra

contenido, validez, estructura de al menos 10% de la cantidad de documentos cada semestre y actualizando en caso de requerirlo.							
Concientizar al personal de la Coordinación de Seguridad de la Información/UNAM-CERT en aspectos relacionados con el Sistema de Gestión de Seguridad de la Información, estableciendo dos sesiones informativas y un examen por trimestre en el que un mínimo de 70% del personal lo acredite.	Porcentaje de acreditación mínima de 70% en exámenes trimestrales sobre las sesiones informativas a los integrantes de la CSI/UNAM-CERT	Número de sesiones informativas del SGSI	4 sesiones	3 sesiones	Trimestre	Coordinador del SGSI – Implementador de mejores prácticas	- Listas de asistencia a las sesiones informativas del SGSI - Exámenes del SGSI presentados trimestralmente de la CSI/UNAM-CERT
		$\frac{Número\ de\ exámenes\ acreditados}{Total\ de\ exámenes\ presentados} x\ 100$ *Examen acreditado ≥ 7	100%	≥70	Trimestre		
Preservar la confidencialidad, integridad y disponibilidad de la información durante el Proceso de Manejo de Incidentes manteniendo como máximo un incidente al año derivado de acceso no autorizado.	Número de incidentes contra la confidencialidad, integridad y disponibilidad de la información en el proceso de manejo a incidentes.	Número de incidentes de Seguridad de la información de acceso no autorizado	0	1	Anual	Coordinador del SGSI – Implementador de mejores prácticas	Registro de incidentes

e) Evaluación de riesgos

Para el análisis y evaluación de riesgos de la Coordinación de Seguridad de la Información/UNAM-CERT, se trabajó con la metodología OCTAVE Allegro, y en ésta consideramos la identificación del dueño del riesgo. Por fines de confidencialidad, les mostraré sólo el formato que empleamos para identificación de activos críticos de información:

TABLA 3.4, HOJA DE TRABAJO ALLEGRO 8.

Hoja de Trabajo Allegro 8	**PERFIL DEL ACTIVO DE INFORMACIÓN CRÍTICO**	
(1) Activo Crítico *¿Cuál es el activo crítico de la información?*	**(2) Razón de selección** *¿Por qué es importante el activo de información para la organización?*	**(3) Descripción** *¿Cuál es la descripción consensada del activo de información?*
(4) Dueño(s) *¿A quién pertenece el activo de información?*		
Dueño:		
(5) Requisitos de seguridad *¿Cuáles son los requisitos de seguridad para el activo de información?*		
☐ **Confidencialidad**	Sólo personal autorizado puede acceder a este activo de información.	
☐ **Integridad**	Sólo personal autorizado puede modificar este activo de información.	
☐ **Disponibilidad**	Este activo debe estar disponible para que el personal realice sus labores.	
	Este activo debe estar disponible **24** horas, **7** días/semana, **52** semanas/año.	
☐ **Otro**		
(6) Requisito de seguridad más importante *¿Cuál es el requisito de seguridad más importante para este activo?*		
☐ **Confidencialidad**	☐ **Integridad**	☐ **Disponibilidad** ☐ **Otro**

De esta manera, cada riesgo identificado tiene un dueño, y este cambio se estableció también en el documento *Procedimiento de análisis y evaluación de riesgos*, definiendo como "Dueño de riesgo" al Jefe de departamento o Coordinador con la responsabilidad y autoridad para gestionar el riesgo. Asimismo, dentro de dicho procedimiento, tenemos identificadas áreas de preocupación y posibles escenarios de amenaza, lo cual nos ayuda a determinar el impacto que causarían éstos en caso de materializarse. Nuevamente, les muestro un ejemplo del formato de la metodología OCTAVE Allegro:

TABLA 3.5, HOJA DE TRABAJO ALLEGRO 10.

Hoja de Trabajo Allegro 10		**RIESGO DEL ACTIVO DE INFORMACIÓN**			
Riesgo del Activo de Información	**Amenaza**	**Activo de Información**			
		Área de Preocupación			
		(1) Actor *¿Quién podría explotar la debilidad?*			
		(2) Medios *¿Cómo lo lograría el actor? ¿Qué harían?*			
		(3) Motivo *¿Cuál es la razón del actor para hacerlo?*			
		(4) Salida *¿Cuál sería el efecto sobre el activo de información?*	☐ **Divulgación** ☐ **Destrucción** ☐ **Modificación** ☐ **Interrupción**		
		(5) Requisitos de seguridad *¿Cómo serían violados los requisitos de seguridad?*			
		(6) Probabilidad *¿Cuál es la probabilidad de que este escenario de amenaza pueda ocurrir?*	☐ **Alto**	☐ **Medio**	☐ **Bajo**
	(7) Consecuencias *¿Cuáles son las consecuencias para la organización o el dueño del activo de información, como resultado de la salida y violación de los requisitos de seguridad?*		**(8) Severidad** *¿Qué tan severas son las consecuencias para la organización o dueño del activo por área de impacto?*		
			Área de Impacto	**Valor**	**Puntuación**
			Reputación y Confianza del Cliente		
			Financiero		

		Productividad		
		Seguridad y Salud		
		Multas y Penas Legales		
			Puntuación del Riesgo Relativo	

(9) Mitigación del Riesgo *Basado en la puntuación total del riesgo, ¿Qué acción tomará?*			
☐ **Aceptar**	☐ **Postergar**	☐ **Mitigar**	☐ **Transferir**

Para los riesgos que se han decidido mitigar, realizar lo siguiente:	
¿En qué contenedor se aplicarían los controles?	*¿Qué controles administrativos, físicos y técnicos aplicarían a este contenedor? ¿Qué riesgo residual será aceptado por la organización?*

La información recabada se estableció en un matriz considerando los riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad de la información dentro del alcance del SGSI. Cabe mencionar que, para el análisis de riesgos, el plan de acciones preventivas derivado de las auditorías externas e internas, es contemplado como parte del análisis y evaluación de riesgos.

f) Declaración de Aplicabilidad (SoA)

La Declaración de Aplicabilidad tuvo pocos cambios respecto a la inclusión de controles nuevos y a la exclusión de algunos que se complementaron con otros ya existentes, señalados en la nueva versión del estándar ISO/IEC 27001:2013. Además, mantuvimos la justificación de su inclusión, así como la clasificación de estatus de control al marcar la opción de si el control está o no aplicado (CA), o si aún está pendiente de aplicarse (S/N).

La siguiente Ilustración 3.3 muestra una parte inicial del SoA de la CSI/UNAM-CERT.

Controles ISO 27001:2013			CA	Aplica (S/N)	Justificación	Razones para seleccionarlos				Responsable	Documento de referencia
						RL	OC	RN/MP	RER		
Cláusula	Sección	Objetivo de control/Control									
A.5 Políticas de seguridad de la información	5.1	Gestión de la dirección para la seguridad de la información									
	5.1.1	Políticas para la seguridad de la información	▪	S	La política expresa el compromiso de la dirección y establece el enfoque de la CSI/UNAM-CERT para la gestión de seguridad de la información. En esta política se describen los objetivos de seguridad que desean cumplirse y se enlistan las políticas que complementan a esta política rectora.			▪		Comité de seguridad	POL-CSI-001 Política de Seguridad de la Información
	5.1.2	Revisión de la política de seguridad de la información	▪	S	La política de seguridad debe ser revisada periódicamente para garantizar que sea adecuada y efectiva.			▪		Implementador de mejores prácticas	POL-CSI-001 Política de Seguridad de la Información
A.6 Organización de la seguridad de la información	6.1	Organización interna									
	6.1.1	Roles y responsabilidades de la seguridad de la información	▪	S	Todo el personal involucrado en el SGSI debe entender completamente sus roles y responsabilidades y debe tener claro los procedimientos y funciones, así como los alcances y límites relacionados con la seguridad de la información que apliquen a los activos a su cargo.		▪	▪		Comité de seguridad	ESP-CSI-035 Descripción de puestos de trabajo de la CSI UNAM CERT POL-CSI-009 Política de condiciones de empleo para integrantes de la CSI/UNAM-CERT
										Implementador de mejores prácticas	MAN-CSI-001 Roles y responsabilidades del equipo de trabajo del SGSI
	6.1.2	Segregación de funciones	▪	S	Los sistemas, servicios e infraestructura son importantes para la operación de la Coordinación, por lo que es un riesgo que una sola persona tenga control total sobre los mismos, es por eso que necesitan definirse roles y responsabilidades para que diferentes personas se hagan cargo de su administración.			▪		Jefe del departamento de Seguridad en Sistemas	MAN-CSI-020 Control de acceso a las herramientas de los sistemas web
										Jefe del departamento de Seguridad en Sistemas	LIS-CSI-012 Lista de tareas y responsabilidades en el sistema SAI
										Jefe del departamento de Operación Interna	PRO-CSI-081 Segregación de tareas y responsabilidades de Operación Interna
	6.1.3	Contacto con autoridades	▪	S	Mantener contacto con las autoridades como seguridad pública, procuraduría, protección civil, autoridades universitarias, es importante en casos de emergencia, contingencia. Además es necesario especificar quién y bajo cuáles circunstancias es necesario contactar a las autoridades.	▪		▪		Implementador de mejores prácticas	PLA-CSI-001 Plan de continuidad del negocio
										Implementador de mejores prácticas	PLA-CSI-002 Plan de recuperación de desastres
	6.1.4	Contacto con grupos de interés especial	▪	S	Mantener contacto con asociaciones y especialistas en seguridad de la información permite a la CSI/UNAM-CERT intercambiar información para mantenerse al día en el uso de tecnologías, metodologías o en la aparición de nuevas amenazas que puedan afectar las operaciones.		▪	▪		Coordinador de Seguridad de la Información. Jefe del departamento de Gestión de Proyectos y Capacitación Jefe del departamento de Detección y Respuesta a Incidentes.	Honeynet Project, FIRST, ANUIES, AMIPCI, Proyecto Amparo, APWG, RENASEC, Congreso de Seguridad en Cómputo
	6.1.5	Seguridad de la Información en la gestión de proyectos		N	En la Coordinación no se cuenta con proyectos que sean direccionados a seguridad de la información						NA

Ilustración 3.3, Parte SoA.

g) Dueños del riesgo

Después del análisis y evaluación de riesgos, actualizamos el documento *Plan de Tratamiento de Riesgos*, el cual contiene:

- Objetivo de control/Control
- Riesgo
- Puntuación (del riesgo, derivado del análisis y evaluación de riesgos)
- Activo de información
- Riesgo Residual
- Actividad para gestionar el riesgo
- Periodo de realización
- Fecha de inicio
- Prioridad
- Documento de referencia
- Dueño del riesgo

Dicho documento, de carácter confidencial, fue presentado al Comité de Seguridad y posteriormente fue aprobado por el mismo, y por los dueños de los riesgos.

h) Qué hacer con ciertos procedimientos de gestión

En esta sección propuse al Comité de Seguridad volver obsoletos, con autorización de los dueños, los siguientes documentos:

- FOR-CSI-017 Formato para acciones preventivas del SGSI
- PRO-CSI-076 Procedimiento para acciones preventivas del SGSI

Además, solicité apoyo para que los responsables especificaran, en el resumen de sus documentos a cargo, el carácter de No obligatorio como lo marca el estándar ISO/IEC 27001:2013. Los documentos partícipes fueron:

- FOR-CSI-018 Formato para reportar acciones correctivas del SGSI
- FOR-CSI-202 Informe de auditoría interna
- FOR-CSI-022 Plan de auditoría SGSI
- FOR-CSI-012 Programa de auditoría interna
- PRO-CSI-073 Procedimiento de auditoría interna

- PRO-CSI-075 Procedimiento para acciones correctivas del SGSI

Cabe recalcar que, a pesar de que los documentos anteriores no son obligatorios, se dio la instrucción de que los procedimientos que involucran a cada uno de ellos deben seguirse conservando con la diferencia de que se pueden optar por otros métodos o procedimientos según a las conveniencias del funcionamiento del Sistema de Gestión de Seguridad de la Información.

i) Políticas y procedimientos

Para dar cumplimiento con el estándar, se creó el documento *ESP-CSI-040_Principios de Ingeniería en Seguridad en Sistemas de la Información* y se actualizó la Política para proveedores.

Esto es una muestra de la parte inicial del documento *ESP-CSI-040*:

1. Resumen

Una línea base del enfoque general de seguridad de la información que siguen todos los sistemas de TI de la Coordinación de Seguridad de la Información/UNAM-CERT en aspectos técnicos, procedimientos y documentación relacionada.

El documento se asocia con el control A.14.2.5 Principios de Ingeniería en Seguridad en Sistemas de la Información del ISO/IEC 27001:2013.

2. Objetivo

Proporcionar las bases para la aplicación efectiva de seguridad de la información a sistemas de TI dentro de las áreas de competencia de la CSI/UNAM-CERT.

3. Alcance

Lineamientos que aplican a los sistemas de información implementados en la Coordinación de Seguridad de la Información/UNAM-CERT relacionados con el proceso de Respuesta a Incidentes.

4. Roles y Responsabilidades

Es responsabilidad del Coordinador del SGSI actualizar la información contenida en este documento.

El Coordinador de Seguridad de la Información y los miembros del Comité de Seguridad son responsables de aprobar el contenido del documento.

Todo el personal de la Coordinación de Seguridad de la Información/UNAM-CERT deberá seguir los lineamientos derivados de los controles referenciados en este documento.

5. Desarrollo

Los siguientes principios tienen el propósito de establecer lineamientos de seguridad de la información en todo tipo de sistemas de TI en el proceso de Respuesta a Incidentes.

El listado de principios se apega a las 5 fases del ciclo de vida de los sistemas de información:

- Inicio
- Desarrollo/Adquisición
- Implementación
- Operación/Mantenimiento
- Eliminación

Distribuido en seis categorías:

1. Fundamentos de la seguridad
2. Basados en riesgos
3. Facilidad de uso
4. Incrementar resiliencia
5. Reducir vulnerabilidades
6. Relevancia de las redes de datos en el diseño

5.1. Fundamentos de la seguridad

Principio	Descripción	Referencia
1. Establecer una adecuada política de seguridad como "fundamento" para el diseño.	Política de seguridad que refleje el compromiso general de la organización con respecto a la seguridad de la información.	POL-CSI-001 Política de Seguridad de la Información
2. Tratar la seguridad como parte integral del diseño general de los sistemas.	Implementar la seguridad de manera integral en cada fase del ciclo de vida de los sistemas de información y no como una implementación posterior.	Documentación de los ambientes de prueba, manual técnico del SAI, Solicitudes y aprobaciones de cambio a los sistemas. -- GUI_CSI_007 Guía para realizar pruebas de penetración. GUI_CSI_028 Pruebas y revisiones de aplicaciones críticas en sistemas operativos modificados GUI_CSI_030 Aprobación y realización de pruebas en Bases de Datos GUI_CSI_032 Separación de las actividades de desarrollo, prueba y operación de los sistemas MAN-CSI-014 Servidores de pruebas del área de Seguridad en Sistemas MAN-CSI-021 Pruebas de validación dentro de las aplicaciones web PRO-CSI-065 Procedimiento para pruebas de compatibilidad de software y hardware PRO-CSI-002 Proceso de control de cambios MAN-CSI-022 Especificación del sistema SAI

3. Delinear claramente los límites de la seguridad física y lógica gobernada por las políticas de seguridad asociadas.	Diferenciar las ubicaciones y los activos de seguridad físicamente y lógicamente para establecer políticas claras para cada tipo en específico.	POL-CSI-005 Política de clasificación, respaldo y borrado de información POL-CSI-010 Política de autenticación y control de acceso
4. Asegurar que los desarrolladores están entrenados en cómo desarrollar software seguro	Garantizar la competencia en materia de seguridad de la información de los desarrolladores de software.	ESP-CSI-035 Descripción de puestos de la CSI-UNAM-CERT ESP-CSI-038 Medidas de gestión de seguridad de la información (métricas de capacitación y entrenamiento) POL-CSI-009 Política de condiciones de empleo para los integrantes de la CSI-UNAM-CERT

j) Reorganización de controles

Realicé una evaluación de los nuevos controles de la sección *Anexo A del estándar ISO/IEC 27001:2013*, y establecimos acciones para implementarlos:

- A.6.1.5 - Seguridad de la Información en gestión de proyectos

Deberá implementarse seguridad de la información a gestión de proyectos, independientemente del tipo de proyecto.

- A.12.6.2 – Restricciones en instalación de software

Reglas que controlan la instalación de software por usuarios deben ser establecidas e implementadas.

- A.14.2.1 – Política de desarrollo seguro

Reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas dentro de la CSI/UNAM-CERT.

- A.14.2.5 – Principios de ingeniería en seguridad en sistemas

Principios de ingeniería en seguridad en sistemas deben ser establecidos, documentados, mantenidos y aplicados a cualquier implementación de un desarrollo sistema de información.

- A.14.2.6 – Ambientes de desarrollo seguros

La CSI/UNAM-CERT debe establecer y proteger apropiadamente sus ambientes de desarrollo seguro para implementaciones de desarrollo de sistemas e integración, que cubran todo su ciclo de vida.

- A.14.2.8 – Pruebas de seguridad en sistemas

Las pruebas de funcionalidad de seguridad en sistemas deben ser llevadas a cabo durante el desarrollo.

- A.15.1.1 – Política de Seguridad de la Información para relaciones con proveedores

Requerimientos de seguridad de la información para la mitigación de riesgos asociados con el acceso de los proveedores a los activos de la CSI/UNAM-CERT deben ser documentados.

- A.15.1.3 – Cadena de suministro de tecnologías de la información y comunicación. (Añadido a la política de proveedores)

Acuerdos con proveedores deben incluir requerimientos para atender los riesgos de seguridad de la información asociados a servicios de tecnologías de información y comunicación y a la cadena de suministros del producto.

- A.16.1.4 – Evaluación y decisión de eventos de seguridad de la información

Los eventos de seguridad de la información deben ser evaluados y deberá decidirse si serán clasificados como incidentes de seguridad de la información.

- A.16.1.5 – Respuesta a incidentes de seguridad de la información

Incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.

- A.17.2.1 – Disponibilidad de instalaciones (infraestructura) de procesamiento de información

  Las instalaciones de procesamiento de información deben ser implementadas con suficiente redundancia para cumplir con los requerimientos de disponibilidad.

Al cabo de la revisión de los nuevos controles, realicé una junta con el Comité de Seguridad para delegar responsabilidades al personal de la CSI/UNAM-CERT para apoyar en el mapeo de los controles ya establecidos de la versión 2005 con los de la versión 2013 del estándar ISO IEC 27001.

k) Medición e informes

En este punto, fue necesario revisar que se realizara lo siguiente:

- Los objetivos de seguridad en la *POL-CSI-001 Política de Seguridad* deben ser medibles.
- El Plan de Tratamiento de Riesgo debe mostrar información de cómo será evaluado el control.
- En el SoA se debe mostrar información sobre la medición de estatus del control (si se ha logrado cumplir el objetivo).
- Definir en las políticas y procedimientos del SGSI de la Coordinación de Seguridad de la Información/UNAM-CERT un apartado donde se especifique el criterio con el que el documento será evaluado.
- Modificar el apartado de Roles y Responsabilidades dentro de la *POL-CSI-001 Política de Seguridad* añadiendo deberes u obligaciones correspondientes a las actividades de medición del SGSI y presentación de informes. (Definir claramente quién y qué se va a medir e informar).
- Revisar y actualizar el *ESP-CSI-038 Medidas de gestión de la información.*

Las acciones de mantenimiento y mejora del SGSI para la transición del estándar ISO/IEC 27001 se llevaron a cabo de febrero a agosto de 2015.

RESULTADOS

3.6 Resultados

Al ejecutar las actividades para el proyecto de transición del estándar, y gracias al impulso que le dio el Comité de Seguridad para con el personal de la Coordinación de Seguridad de la Información, y su participación para la toma de decisiones, se establecieron las bases necesarias para el cumplimiento satisfactorio con la reciente versión del estándar.

La auditoría de transición se llevó a cabo el día 27 de agosto del 2015. Por fines de confidencialidad mostraré sólo partes del informe, como imágenes, entregado por parte de nuestra entidad certificadora donde se exponen los resultados de la auditoría.

AENOR Asociación Española de Normalización y Certificación

UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO

Dirección General de Cómputo y de Tecnologías de Información y Comunicación.
(Coordinación de Seguridad de la Información / UNAM-CERT)

Informe de Auditoría

Nº EXPEDIENTE: **2013/1074/SI/01**	Nº INFORME: **03** TIPO DE AUDITORÍA: **SEGUIMIENTO 2 + ADAPTACIÓN**
NORMA DE APLICACIÓN: **UNE-ISO/IEC 27001:2014**	Requiere envío de PAC a AENOR: SI ■ NO ☐

Fecha de realización de la Auditoría: **2015-08-27**

ILUSTRACIÓN 3.4, INFORME AUDITORÍA (1)

AENOR Asociación Española de Normalización y Certificación

2013/1074/SI/01 **Nº DE INFORME: 03**	__/__/__ **Nº DE INFORME:**	__/__/__ **Nº DE INFORME:**

1. DATOS GENERALES

A. DATOS DE LA ORGANIZACIÓN

Nombre de la Organización	**UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO** **Dirección General de Cómputo y de Tecnologías de Información y Comunicación, (Coordinación de Seguridad de la Información / UNAM-CERT)**
Dirección	Circuito Exterior S/N Ciudad Universitaria, Coyoacán, Distrito Federal, México C.P. 04510
Representante de la Organización *(nombre y cargo)*	D. Rubén AQUINO / Dña. Denise BETANCOURT SANDOVAL Coordinador de Seguridad de la Información UNAM-CERT / Representante SGSI

B. EQUIPO AUDITOR

Función	Nombre	Iniciales	Entidad
AUDITOR]EFE	D.]orge]air HERRERA FLORES	]HF	AENOR MEXICO

C. MODIFICACIONES SOBRE EL ALCANCE DE LA CERTIFICACIÓN, SI PROCEDE

PROPUESTO: N/A

D. OBJETIVOS DE LA AUDITORÍA

Los objetivos de la auditoría son: determinar la conformidad del sistema de gestión de la organización / empresa auditada con los criterios de auditoría, evaluar su capacidad para cumplir con los requisitos legales, reglamentarios y contractuales aplicables, así como evaluar su eficacia para cumplir los objetivos especificados y cuando corresponda, identificar posibles áreas de mejora.

(Si procede, añadir objetivos específicos de la presente auditoría)

Se Indicará en el resumen de auditoría si se ha producido cualquier situación durante la auditoría que haya afectado a la consecución de sus objetivos (imposibilidad de evaluar una actividad, centro, requisito..)

ILUSTRACIÓN 3.5, INFORME AUDITORÍA (2)

AENOR Asociación Española de Normalización y Certificación

2013/1074/SI/01 Nº DE INFORME: 03	___/___/__/__ Nº DE INFORME:	___/___/__/__ Nº DE INFORME:

2. RESUMEN EJECUTIVO DE AUDITORÍA

Se ha realizado la Auditoría de Renovación al Sistema de Gestión de Seguridad de Información (SGSI) de la **UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO Dirección General de Cómputo y de Tecnologías de Información y Comunicación, (Coordinación de Seguridad de la Información / UNAM-CERT)** donde se ha comprobado la implantación del Sistema respecto a los requisitos especificados en la norma de referencia UNE-ISO/IEC 27001:2014 *"Tecnología de la información - Técnicas de seguridad - Sistemas de Gestión de Seguridad de la Información (SGSI)- Requisitos"* salvo para lo reflejado como no conformidad en el presente informe [redacted]

El alcance del SGSI se ha definido: *"Los sistemas de información que soportan a los procesos de Detección, Gestión y Análisis relacionados con el servicio de Respuesta a Incidentes que ofrece la Coordinación de Seguridad de la información/UNAM-CERT a las entidades académicas y dependencias de la UNAM, organizaciones externas y público en general, de acuerdo al documento de aplicabilidad vigente."* detallado en el documento **Definición del Alcance del SGSI (ESP-CSI-008)** definiendo características de la actividad empresarial, de la organización, de su ubicación, activos y tecnología incluyendo justificación de exclusión al alcance.

Se informa que la presente auditoría se ha realizado de forma conjunta con la auditoría de Adaptación a la última versión vigente del estándar ISO/IEC 27001. La revisión se ha realizado a las áreas de **Coordinación de Seguridad de la información (UNAM-CERT)** identificadas en los emplazamientos identificados en el Anexo al presente informe.

Los documentos revisados se indican en anexo 1, adjunto al expediente.

La auditoría de Seguimiento 2 (AS2) + Adaptación ha tenido una duración de **1** jornada/hombre. La comprobación de la documentación del SGSI se ha realizado durante toda la auditoría de certificación. La revisión del Análisis de riesgos se realizó durante **1** hora.

Así mismo, se ha comprobado que el Análisis de Riesgos realizado con la metodología **OCTAVE Allegro**, y a pesar de que los resultados que ella arroja son considerados como adecuados, la inversión de tiempo y esfuerzo ha ocasionado el pensar en cambiar de metodología o realizar modificaciones en aras de obtener resultados de calidad igual o similar pero con una reducción significativa de tiempo y esfuerzo.

La selección de controles para realizar las pruebas de cumplimiento se ha realizado en base al Informe de Análisis de Riesgos ***(REG-CSI-810)*** y a la declaración de aplicabilidad ***Declaración de Aplicabilidad (SoA) -2015 (ESP-CSI-036)*** con fecha **5 de Agosto 2015**. Además se incorpora al expediente el registro de AENOR R-DTC-063 con las pruebas realizadas sobre los controles, así como una matriz en presente informe de los controles revisados en la auditoría. **Nota.** Debido al tiempo que tomó la revisión para verificar la implementación de las características propias de la adaptación a la nueva versión del estándar de referencia, en este ejercicio de auditoría no fueron revisados controles por lo que el registro antes mencionado no será entregado.

Cambios significativos del sistema con respecto a la anterior visita:

- La capacitación del auditor interno sobre el curso de Auditor Líder ISO/IEC 27001:2013 (Certificado en trámite).

Conclusiones sobre el cumplimiento de los objetivos de la auditoría y la eficacia del sistema de gestión.

Se ha comprobado la implantación del Sistema respecto a los requisitos especificados en la norma de referencia UNE-ISO/IEC 27001:2014 si bien se comprueba un grado de madurez **inicial**.

3 de 14 R-DTC-002.10

ILUSTRACIÓN 3.6, INFORME AUDITORÍA (3)

Adicionalmente, muestro una copia del certificado otorgado a la Coordinación de Seguridad de la Información/UNAM-CERT después de haber concluido con el envío de evidencia y acciones correctivas solicitadas por la entidad certificadora (ver Anexo 1).

CONCLUSIONES

3.7 Conclusiones

El Sistema de Gestión de Seguridad de la Información de la CSI/UNAM-CERT, está implantado con un grado de madurez inicial. A pesar de que en la versión reciente del estándar ISO/IEC 27001:2013 ya no es obligatorio emplear el ciclo de Deming, se decidió continuar con su uso ya que nos permitió seguir planeando, operando, monitoreando y mejorando el funcionamiento del SGSI para mantenerlo actualizado y consolidado continuamente.

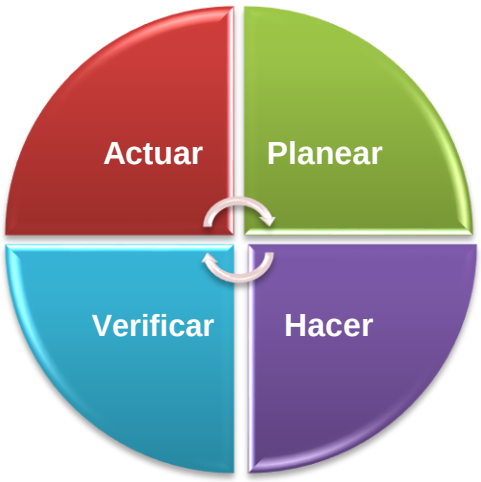

ILUSTRACIÓN 3.7, CICLO DEMING.

Tanto en la nueva versión del estándar como en la anterior, fue indispensable que el Implementador de Mejores Prácticas sostuviera contacto directo con la Alta Dirección para impulsar la efectividad del SGSI. Además, dicha implementación del SGSI ayuda a alcanzar la visión de la CSI/UNAM –CERT, que es consolidar a la UNAM como la entidad líder en materia de Seguridad de la Información en el país.

El uso de las Tecnologías de Información y Comunicación en constante crecimiento ha presionado a las organizaciones a utilizar estándares y buenas prácticas para enfrentar los retos de seguridad, ante eventualidades no deseadas. Sin embargo, no basta con tener conocimiento de que éstos existen, o de qué controles tiene, sino que también se requiere de la aplicación de conocimientos en el ámbito de la computación. Es en este punto donde comprendo que el haber sido alumna de la Facultad de Ingeniería, me ha permitido contar con la capacidad de analizar, planear, diseñar, organizar, producir, operar y dar soporte a problemas relacionados con seguridad de la información, redes, tecnologías de información, entre otras áreas.

En ese sentido, puedo demostrar que he adquirido experiencia profesional con base en conocimientos ingenieriles; pero también, al incorporarme al entorno laboral, me di cuenta de que mi perfil se complementa al trabajar con ética profesional, ser sociable con las personas de mi entorno, y estar abierta al aprendizaje continuo.

El proyecto que describí en este informe sobre la transición del estándar ISO/IEC 27001 para el SGSI, las múltiples actividades que realicé durante un año y dos meses que laboré como Implementadora de Mejores Prácticas en la Coordinación de Seguridad de la Información/UNAM-CERT, y la formación académica que recibí en la Facultad de Ingeniería, me dieron la posibilidad de emprender un nuevo reto en mi carrera profesional como Ingeniero Especialista en Seguridad Informática, en el Instituto Nacional Electoral.

Actualmente, estoy participando en dos proyectos relacionados entre sí, pero diferentes en cuanto a su gestión: Uno de ellos es la Implementación del SGSI, y el otro es el Plan de Recuperación en caso de Desastres. Ambos proyectos requieren conocimiento y experiencia para gestionar las estrategias de protección para los sistemas y servicios informáticos, mediante la implementación de mecanismos y estándares en materia de seguridad informática. Así pues, continúo aportando conocimiento eficiente que he adquirido durante mi trayectoria académica en la Facultad de Ingeniería, y con experiencia profesional en UNAM/CERT; cumpliendo con las expectativas que me pide el Instituto, y dando solución a las problemáticas que se presentan en el entorno de la Seguridad de la Información.

3.8 Referencias

BSI Standards Publication. *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.*

Coordinación de Seguridad de la Información. 2015. *Congreso Seguridad en Cómputo*. Recuperado el 19 de agosto de 2017, de https://www.seguridad.unam.mx/node/190

Martín Zamboni, *D. Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix.* Recuperado el 19 de agosto de 2017, de http://homes.cerias.purdue.edu/~zamboni/pubs/thesis-bs.pdf

Revista .Seguridad. 2017. Aproximación al Malware. Recuperado el 9 de septiembre de 2017, de https://revista.seguridad.unam.mx/numero-24/creditos

SANS Institute. 2016. OUCH! Febrero 2016. Recuperado el 9 de septiembre de 2017, de https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201602_sp.pdf

The British Standars Institution. 2017. Recuperado el 26 de agosto de 2017, de https://www.bsigroup.com/es-MX/seguridad-dela-informacion-ISOIEC-27001/

UNAM.2015. *DGTIC Organigrama*. Recuperado el 26 de agosto de 2017, de http://www.tic.unam.mx/organigrama.html

UNAM-CERT. 2017. *Acerca de la CSI*. Recuperado el 19 de agosto de 2017, de https://www.seguridad.unam.mx/content/acerca-de-la-csi

Certificado del Sistema de Gestión de Seguridad de la Información

AENOR
ER
Seguridad Información
UNE-ISO/IEC 27001

SI-0019/2014

AENOR, Asociación Española de Normalización y Certificación, certifica que la organización

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Dirección General de Cómputo y de Tecnologías de información y Comunicación, (Coordinación de Seguridad de la Información / UNAM-CERT)

dispone de un sistema de gestión de seguridad de la información conforme con la Norma UNE-ISO/IEC 27001:2014

para las actividades: Los sistemas de información que soportan a los procesos de Detección, Gestión y Análisis relacionados con el servicio de Respuesta a Incidentes que ofrece la Coordinación de Seguridad de la información/UNAM-CERT a las entidades académicas y dependencias de la UNAM, organizaciones externas y público en general, de acuerdo al documento de aplicabilidad vigente.

que se realizan en: Circuito Exterior S/N Ciudad Universitaria. 04510 - Coyoacán (DISTRITO FEDERAL - México)

Fecha de primera emisión: 2014-04-16
Fecha de última emisión: 2015-08-28
Fecha de expiración: 2017-04-16

AENOR Asociación Española de Normalización y Certificación

Avelino BRITO MARQUINA
Director General de AENOR

AENOR Asociación Española de Normalización y Certificación | Génova, 6. 28004 Madrid. España Tel. 902 102 201 – www.aenor.es

AENOR MÉXICO Av. Presidente Masaryk, 61 - Piso 14 Colonia Chapultepec Morales. CP 11570, Delegacion Manuel Hidalgo. México D.F. México - www.aenormexico.com

ENAC CERTIFICACIÓN Nº 01/C-SG028

IQNet

ILUSTRACIÓN 3.8, CERTIFICADO SGSI (1).

Information Security Management System Certificate

AENOR

ER

Seguridad Información

UNE-ISO/IEC 27001

SI-0019/2014

AENOR, Spanish Association for Standardization and Certification certifies that the organization

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Dirección General de Cómputo y de Tecnologías de información y Comunicación, (Coordinación de Seguridad de la Información / UNAM-CERT)

has an information security management system in accordance to the UNE-ISO/IEC 27001:2014 Standard

for the activities: Information systems that support Detection, Management and Analysis processes related to the Incident Response Service provided by UNAM/CERT Information Security Section to UNAM academic entities and dependences, third-party organizations and people at large, according to the current statement of applicability.

which is/are carried out in: Circuito Exterior S/N Ciudad Universitaria. 04510 - Coyoacán (DISTRITO FEDERAL - México)

First issued on: 2014-04-16
Last issued: 2015-08-28
Validity date: 2017-04-16

AENOR Asociación Española de Normalización y Certificación

Avelino BRITO
Chief Executive Officer

AENOR Asociación Española de Normalización y Certificación | Génova, 6. 28004 Madrid. España Tel. 902 102 201 – www.aenor.es

AENOR MÉXICO Av. Presidente Masaryk, 61 - Piso 14 Colonia Chapultepec Morales. CP 11570, Delegacion Manuel Hidalgo. México D.F. México - www.aenormexico.com

ENAC CERTIFICACIÓN Nº 01/C-SG028

IQNet

ILUSTRACIÓN 3.9, CERTIFICADO SGSI (2).

THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

IQNet and
AENOR
hereby certify that the organization

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO (Dirección General de Cómputo y de Tecnologías de información y Comunicación, (Coordinación de Seguridad de la Información / UNAM-CERT))

Circuito Exterior S/N Ciudad Universitaria.
04510 - COYOACÁN(DISTRITO FEDERAL)
México

for the following field of activities

Information systems that support Detection, Management and Analysis processes related to the Incident Response Service provided by UNAM/CERT Information Security Section to UNAM academic entities and dependences, third-party organizations and people at large, according to the current statement of applicability.

has implemented and maintains a

Information Security Management System

which fulfills the requirements of the following standard

ISO/IEC 27001:2013

First issued on: 2014-04-16 Last issued: 2015-08-28 Validity date: 2017-04-16

Registration Number: **ES-SI-0019/2014**

IQNet AENOR Asociación Española de Normalización y Certificación

Michael Drechsel
President of IQNet

Avelino BRITO
Chief Executive Officer

IQNet Partners*:
AENOR *Spain* AFNOR Certification *France* AIB-Vincotte International *Belgium* ANCE *Mexico* APCER *Portugal* CCC *Cyprus*
CISQ *Italy* CQC *China* CQM *China* CQS *Czech Republic* Cro Cert *Croatia* DQS Holding GmbH *Germany*
FCAV *Brazil* FONDONORMA *Venezuela* ICONTEC *Colombia* IMNC *Mexico* Inspecta Certification *Finland* IRAM *Argentina*
JQA *Japan* KFQ *Korea* MIRTEC *Greece* MSZT *Hungary* Nemko AS *Norway* NSAI *Ireland* PCBC *Poland*
Quality Austria *Austria* RR *Russia* SII *Israel* SIQ *Slovenia* SIRIM QAS International *Malaysia*
SQS *Switzerland* SRAC *Romania* TEST St Petersburg *Russia* TSE *Turkey* YUQS *Serbia*
IQNet is represented in the USA by: AFNOR Certification, CISQ, DQS Holding GmbH and NSAI Inc.
* The list of IQNet partners is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com

ILUSTRACIÓN 3.10, CERTIFICADO SGSI (3).