ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS
PROMOCIÓN I

TESIS DE GRADO MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TEMA: Desarrollo de una Guía para la implantación del Modelo de Gestión de la Seguridad de la Información en el Instituto Geográfico Militar

AUTOR: Ing. María Lorena Guevara Díaz

DIRECTOR: Ing. Vicente Merchán MSc.

SANGOLQUI, AGOSTO DEL 2014

CERTIFICACIÓN DEL DIRECTOR

Certifico que el presente trabajo fue realizado en su totalidad por la señora ingeniera MARÍA LORENA GUEVARA DÍAZ, como requerimiento a la obtención del título de MAGISTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS.

Quito, 22 de marzo del 2014

ING. VICENTE MERCHÁN, MSc.

PROFESOR DIRECTOR

DECLARACIÓN DE RESPONSABILIDAD

La presente tesis está fundamentada bajo la investigación bibliográfica respetando los derechos de autor, los conceptos desarrollados, análisis realizados y las conclusiones del presente trabajo; por lo tanto, son de exclusiva responsabilidad del autor.

María Lorena Guevara Díaz

AUTORIZACIÓN

La suscrita María Lorena Guevara Díaz, con cédula 1712250503, autoría del trabajo de tesis titulado: *Guía para la implantación del Modelo de Gestión de la Seguridad de la Información en el Instituto Geográfico Militar*, como requisito para optar por el título de Magister en Auditoría y Evaluación de Sistemas Tecnológicos; autorizo a la Biblioteca de la Universidad de las Fuerzas Armadas ESPE para que se publique con fines académicos y se visibilice su contenido respetando los derechos de autor.

María Lorena Guevara Díaz

AGRADECIMIENTO

Primero debo agradecer a Dios, que me ha proporcionado salud e inteligencia para superar cualquier obstáculo en la vida y alcanzar mis metas propuestas.

Al Instituto Geográfico Militar, mi segundo hogar, institución en la que laboro, por permitir realizarme como profesional y por hacer posible que incrementara mis conocimientos, apoyándome y brindándome la oportunidad de acceder a estudios de cuarto nivel.

A la Universidad de las Fuerzas Armadas "ESPE", alma máter, que me acogió en su seno y permitió adquirir nuevos conocimientos y experiencias profesionales.

A mi tutor, Ing. Vicente Merchán y oponente, Ing. Pedro Rivadeneira, quienes con su profesionalismo, experiencia y paciencia hicieron posible la elaboración del presente trabajo.

A mis maestros y compañeros de carrera, que directa o indirectamente, compartieron y transmitieron sus conocimientos, aportando positivamente en mi formación intelectual.

DEDICATORIA

A mis padres, ya que sin su ejemplo de vida y esfuerzo diario en inculcarnos a mí y a mis hermanas el trabajo duro y el sacrificio por lograr un sueño, este trabajo no hubiera sido posible.

A mi familia, porque su apoyo y consejo me permitió poner hasta mi último esfuerzo en culminar mi carrera.

A mis hijos, para que sea ejemplo de esfuerzo y constancia para lograr un sueño, para que nunca dejen de luchar, no importa la edad que tengan.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

El principal objetivo del presente tema de tesis es crear una Guía para la implantación de un Modelo de Gestión para la Seguridad de la Información para el Instituto Geográfico Militar, un marco de referencia a través del cual se podría crear la estructura orgánica y funcional dentro del Instituto para la Gestión de la Seguridad de la Información, para todas las áreas. Las normativas internacionales ISO/IEC 27001 (Requisitos para la Seguridad de la Información), 27002 (Código de Práctica para la Seguridad de la Información) y 27005 (Gestión de riesgos para la Seguridad de la Información) fueron tomadas como base para realizar el análisis y diagnóstico de la situación inicial de la institución, así como para emitir las conclusiones y recomendaciones. Los requisitos descritos en la ISO/IEC 27001, permitió establecer el grado de madurez de la institución frente a los requerimientos básicos que describe la norma, con el análisis de la ISO/IEC 27002 se logró aterrizar los requerimientos para la redacción y difusión de las políticas para la Seguridad de la Información, elaboradas por la Gestión de Tecnología y difundidas a través de la Dirección, y a través de la ISO/IEC 27005, se definió el alcance necesario para la Gestión de Riesgos, comenzando con una definición de los activos de información, sin la cual no sería posible analizar los riesgos inherentes sobre los activos sensibles de la institución, una vez establecidos los riesgos se deberían crear los controles necesarios para minimizar la probabilidad y el impacto, o aceptar los riesgos de ser el caso. Como conclusión de este análisis se determinó que en el IGM es necesario comenzar con la aplicación de buenas prácticas de Seguridad de la Información iniciando con el nombramiento del Oficial de Seguridad que lidere y encamine el proceso de implantación de la Seguridad de la Información, siempre respaldado del Comité de Seguridad.

PALABRAS CLAVES

IOS (ISO): International Organization for Standardization

SGSI: Sistema de Gestión de Seguridad de la Información

MAGERIT: Método de análisis de Gestión de Riesgos para IT.

IGM: Instituto Geográfico Militar

PHVA: Planificar - Hacer-Verificar-Actuar.

ABSTRACT

The main objective of this thesis topic is to create a guide for the implementation of a Management Model for Information Security for Instituto Geográfico Militar, a framework through which we could create the organizational and functional structure within the Institute for the Management of Information Security, for all areas. International standards ISO / IEC 27001 (Requirements for Information Security), 27002 (Code of Practice for Information Security) and 27005 (Risk Management for Information Security) were used as a basis for analysis and diagnosis of the initial situation of the institution, and to make findings and recommendations. The requirements described in ISO / IEC 27001, possible to establish the degree of maturity of the institution meet the basic requirements which describes the standard, with the analysis of the ISO / IEC 27002 will be managed to land requirements for the preparation and dissemination of policies for Information Security, developed by the Technology Management and disseminated through the steering, and through the ISO / IEC 27005, the need for risk management scope is defined, starting with a definition of assets information, without which it would not be possible to analyze the inherent risks on the sensitive assets of the institution, once established risks should create the necessary controls to minimize the likelihood and impact, or accept the risk if any. As a conclusion of this analysis it was determined that the IGM is necessary to start with the implementation of good practices Information Security starting with the appointment of Safety Officer to lead and routed the process of implementation of Information Security, always backed Safety Committee.

KEY WORDS

IOS (ISO): International Organization for Standardization
ISMS (SGSI): Information Security Management System
MAGERIT: Analysis Method Risk Management for IT.
IGM: Instituto Geográfico Militar
PDCA (PHVA): Plan - Do - Check - Act.

GENERALIDADES

INTRODUCCIÓN

En la actualidad las empresas en general, sean públicas o privadas, enfrentan varios riesgos inherentes de interconexión a la red de Internet; conectividad que es necesaria para no aislarse del mundo globalizado. Dichos riesgos tienen que ver con salvaguardar la información almacenada en medios físicos o la que viaja a través de la red; así como la protección de los accesos a los recursos que ofrecen los servicios del sistema.

A medida que ha ido evolucionando la tecnología se abren cada vez más puntos vulnerables que deben ser controlados y monitoreados para evitar fugas o posibles fraudes fruto del robo o intercepción de información vital. Creando la necesidad para que las empresas inviertan en recursos que apoyen el control de la seguridad de la información. Muchas empresas no valoran la información, dejando en estos casos de ser confidencial, permitiendo que muchas personas sin autorización tengan acceso a ella. La ingeniería social es uno de los grandes males que se encuentra al interior de las organizaciones, y no tiene fronteras para obtener la información necesaria.

El problema de seguridad de información en el mundo y principalmente en el Ecuador, es serio. En la actualidad contar con normas que regularicen el uso y acceso a la información, debería ser una política para poder minimizar el riesgo de que la información se fugue, se altere o lo que es peor que no esté disponible cuando se la requiera.

Pero, ¿qué hacer al interior de las empresas para proteger la información?, es la gran pregunta que se hacen muchas persona y organizaciones. Para esto, las empresas deberían identificar sus activos de información, principalmente aquellos que tienen nivel crítico en la empresa. Hacer una evaluación de riesgos y decidir cuáles son las opciones de tratamiento de cada uno de ellos para minimizar las posibilidades de que las amenazas puedan causar un daño sin proporciones por culpa de una vulnerabilidad "descuidada".

El estado ecuatoriano a través del Acuerdo No. 039-CG-2009 de la Contraloría General del Estado en el numeral 100-01 de Control Interno señala:

"*El control interno será responsabilidad de cada institución del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos y tendrán como finalidad crear las condiciones para el ejercicio del control.*

El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos. Constituyen componente del control interno el ambiente de control la evaluación de riesgos, las actividades de control, los sistemas de información y comunicación y el seguimiento"

Con esta base legal se da inicio a una nueva era en la Seguridad de la Información en el Ecuador. No es la excepción de su aplicación el caso del Instituto Geográfico Militar – IGM, como una entidad adscrita al Ministerio de Defensa Nacional. Donde es necesaria la elaboración de una Guía que instaure un Sistema de Gestión de Seguridad de la Información – SGSI que guíe los pasos hacia la implantación del Sistema de Gestión de Seguridad de Información.

PROBLEMA FUNDAMENTAL

El IGM es una institución estatal adscrita al Ministerio de Defensa, que genera información importante, la misa que no se encuentra dentro de un marco sistemático de gestión de Seguridad de la Información. Esta debilidad se traduce en los siguientes inconvenientes:

- No existe un gobierno que gestione la seguridad en los diversos ámbitos de la organización.
- No está formalizado el rol y la responsabilidad que deben tener los diferentes actores sobre los activos de información.
- Insuficientes herramientas de seguridad informática que ayuden a controlar los objetivos de la Seguridad de la Información.

Por lo tanto, debido a la gran cantidad de información crítica que maneja el IGM es necesario establecer políticas, normas y procedimientos puntuales para la manipulación, procesamiento y análisis de dichos datos. Por lo tanto, si se establece una Guía para la Implantación de un Modelo de Gestión de Seguridad de la Información en el IGM como primer paso hacia la implantación, se minimizarían los riesgos inherentes y de control a los que está expuesta la información: y se estarían maximizando los principios elementales de disponibilidad, integridad y confidencialidad para su confiabilidad al interior y exterior de la institución.

FORMULACIÓN DEL PROBLEMA

La falta de una Guía para la implantación del Modelo de Gestión de la Seguridad de la Información en el Instituto Geográfico Militar, influye en la decisión de autoridades y funcionarios de asumir una cultura de seguridad y protección de la información en la institución.

JUSTIFICACIÓN E IMPORTANCIA

- Acuerdo No. 039-CG-2009 de la Contraloría General del Estado, numeral 100 **Normas Generales,** numeral 100-01 **Control Interno** y numeral 410-10 **Seguridad de Tecnología de Información**.
- Plan Estratégico 2007-2010 del IGM, en el cual señala el objetivo estratégico No. 14 que dice: "Implementar Sistemas de Seguridad Integral".
- Cumplimiento de la Resolución No. 2012-08-IGM-e emitida por el Tcrn. de CSM Ing. Milton Chamorro, Director del IGM (E).

OBJETO DE INVESTIGACIÓN

El proceso de manejo y aseguramiento de la información en el Instituto Geográfico Militar, entidad adscrita al Ministerio de Defensa Nacional.

OBJETIVO GENERAL

El objetivo general de este trabajo es:

Desarrollar una Guía para la Implantación del Modelo de Gestión de la Seguridad de la Información en el Instituto Geográfico Militar tomando como base la recomendaciones de la norma ISO/IEC 27000, con el fin de salvaguardar la información crítica de la Institución y garantizar los principios elementales de integridad, confidencialidad y disponibilidad.

OBJETIVOS ESPECÍFICOS

En base al objetivo general, se establecen los siguientes objetivos específicos:

- Analizar y definir el alcance de la norma aplicable a la Institución.
- Analizar y determinar la situación actual del manejo de la información en la Institución.
- Diseñar el Modelo de Gestión propuesto de la Seguridad de la Información.

METODOLOGÍA DE LA INVESTIGACIÓN

Se realizará la búsqueda de información relevante con definiciones y experiencias en el contexto de la Seguridad de la Información, que aporten valor y significado de tesis.

Se analizará la norma ISO 27000 en todos sus aspectos para poder encontrar la mejor ruta para proponer su implantación dentro de la institución, se analizará la brecha de implementación de la situación actual del instituto frente a lo que queremos llegar tomando en cuenta el grado de madurez de la institución frente a la Seguridad de la Información, se relevará todas las normativas y procedimientos de Seguridad de la Información con las que actualmente se maneja el instituto y se las analizará para su posterior alineamiento a la norma ISO antes mencionada.

Del análisis se planteará una serie de pasos a seguir para iniciar con la guía propuesta de Gestión de la Seguridad de la Información dentro de la institución.

CAPÍTULO I

MARCO TEÓRICO Y METODOLÓGICO

1.1MARCO TEÓRICO

Un Sistema de Gestión de Seguridad de la Información según Alberts Dorofree (2003), puede definirse como aquel sistema que determine qué requiere ser protegido, por qué, de qué debe ser protegido y cómo.

En la versión 2005 de la ISO 27000 se define a un SGSI como la preservación de la confidencialidad, integridad, no repudio y confiabilidad".

En la versión 2008, la ISO 27001 define la importancia de la información como un activo de la empresa, dicha información puede estar impresa, digital y ser trasmitida por correo, por la red, en forma física y todas estas situaciones la expone a un sinnúmero de amenazas y vulnerabilidades que deben ser conocidas y controladas.

A continuación se resumen los fundamentos teóricos que se han estudiado para su uso y aplicación dentro de este tema de tesis:

1.1.1 NORMA ISO/IEC 27001:2005: TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) - REQUISITOS

Esta norma proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información, cuyos requerimientos sean fruto de una decisión estratégica tomando en cuenta las necesidades y objetivos de la organización así como los requisitos de seguridad, procesos, tamaño y estructura. El enfoque que realiza esta norma es **por proceso** lo que permite comprender los requisitos y la necesidad de establecer políticas y objetivos de Seguridad de la Información, administrar los riesgos de seguridad, supervisar y revisar el rendimiento y eficacia del SGSI, y asegurar la mejora continua con mediciones objetivas.

Esta norma se basa en el modelo "Planificar-hacer-verificar-actuar" para estructurar los procesos del SGSI. El SGSI debe estar diseñado a fin de asegurar la selección de los

controles más adecuados que protejan los activos de información y proporcionen las suficientes garantías a las personas interesadas.

El análisis del estándar inicia en el punto 4 ya que los numerales del 1 al 3 solamente especifican términos generales sobre la estructura de la norma y consideraciones generales para su lectura y aplicación.

4. Sistema de gestión de la seguridad de la información

4.1 Requisitos generales

Se debe crear, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI dentro del contexto de las actividades empresariales generales de la organización y de los riesgos.

4.2 Creación y gestión del SGSI

4.2.1 Creación del SGSI

Para iniciar el proceso se debe definir el alcance y los límites del SGSI, las políticas acorde a las características de la actividad, su ubicación, sus activos y tecnología, se deben establecer criterios de estimación de riesgos y todo con la aprobación de la Dirección. El enfoque de evaluación de riesgos debe contener los requisitos legales y reglamentarios, criterios de aceptación de riesgo y fijar los niveles de riegos aceptables. Para identificar los riesgos se deben identificar los activos y sus propietarios, identificar las amenazas, los impactos sobre la confidencialidad, integridad y disponibilidad. Para evaluar los riesgos se deben identificar fallos de seguridad, la probabilidad de ser afectados por fallos y la identificación y evaluación de las opciones para el tratamiento de riesgos. La selección de los controles para el tratamiento de riesgos debe responder directamente a la identificación y evaluación de riesgos. Todo esto con la aprobación de la Dirección y la aceptación razonable de los riesgos residuales. Cualquier exclusión de objetivos de control o riesgos inherentes debe poseer una documentación con la justificación de dicha omisión.

4.2.2 Implementación y operación del SGSI

El plan de tratamiento de riesgos debe contener las acciones de la Dirección, los recursos, las responsabilidades y las prioridades para dicho tratamiento, así como los controles seleccionados y el modo de medir la eficiencia de los controles, implementar programas de formación y de concienciación, gestionar la operación y recursos del SGSI, implementar procedimientos y otros controles para la detección temprana de eventos de seguridad y una respuesta ante cualquier incidente de seguridad.

4.2.3 Supervisión y revisión del SGSI

Se deben crear procedimientos de supervisión y revisión para detectar lo antes posibles las debilidades del SGSI, determinar las actividades delegadas, prevenir incidentes de seguridad y determinar si las acciones tomadas fueron eficaces para evitar la violación de la seguridad. Las revisiones deben ser periódicas para verificar el cumplimiento de la política y los objetivos del SGSI y de la eficacia de los controles para reducir los riesgos residuales. Como parte de la supervisión se deben planificar auditorías internas del SGSI por parte de la Dirección que ayuden a la actualización de los planes de seguridad y al registro de acciones e incidentes.

4.2.4 Mantenimiento y mejora del SGSI

Es necesario analizar e implementar las mejoras correctivas y preventivas en base a la experiencia de la propia institución o de otras instituciones similares, comunicar acciones y mejoras a todas las personas interesadas y asegurar que las mejoras alcancen los objetivos previstos.

4.3 Requisitos de la documentación

4.3.1 Generalidades

Debe ser una decisión directiva que toda la documentación en la que consten todas las acciones y políticas adoptadas estén registradas y disponibles para quien lo necesite, así como todos los procedimientos para una correcta planificación, operación y control de los procesos de seguridad y la eficacia de los controles.

4.3.2 Control de documentos

Toda la documentación debe ser legible y fácilmente identificable, la documentación obsoleta si es necesaria guardarla debe estar etiquetada.

4.3.3 Control de registros

El SGSI debe tener en cuenta cualquier requisito legal o regulatorio aplicable para la identificación, almacenamiento, protección, recuperación, retención y disposición de los registros.

5. Responsabilidades de la Dirección

5.1 Compromiso de la Dirección

La Dirección debe suministrar evidencias de su compromiso para crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI estableciendo roles y responsabilidades a los involucrados, comunicando a la organización la importancia de cumplir objetivos y políticas de seguridad, proporcionando recursos suficientes y emitir criterios de aceptación y niveles aceptables de riesgos.

5.2 Gestión de recursos

5.2.1 Provisión de los recursos

Es necesario determinar y proporcionar los recursos necesarios para establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI, para asegurar que los procedimientos de seguridad, para identificar y cumplir con los requisitos legales y reglamentarios, para la aplicación correcta de todos los controles implantados, para llevar a cabo revisiones periódicas que mejoren la eficiencia del SGSI.

5.2.2 Concientización, formación y capacitación

Todo el personal al que se hayan asignado responsabilidades definidas en el SGSI debe poseer las competencias necesarias para llevar a cabo las tareas asignadas y se debe mantener un registro de la educación, formación, aptitudes, experiencia y cualificaciones, se deben asegurar que todo el personal afectado sea consciente de la trascendencia y la importancia de las actividades de seguridad.

6 Auditorías internas del SGSI

Las auditorías internas del SGSI debe ser a intervalos planificados para poder verificar que se cumplen los requisitos de la norma en cuanto a seguridad de la información, que los controles sean implantados y se mantengan en forma efectiva y que den los resultados esperados, dichas auditorías deben ser objetivas e imparciales, los responsables del área auditada deben velar porque se realicen las acciones para eliminar disconformidades encontradas y sus causas.

7 Revisión del SGSI por la Dirección

7.1 Generalidades

La Dirección debe revisar el SGSI a intervalos planificados en cuanto a su convivencia, adecuación y eficacia. Los resultados de las revisiones deben estar claramente documentados y sus registros deben ser guardados.

7.2 Datos iniciales de la revisión

Los datos de las técnicas, productos o procedimientos que podrían utilizarse dentro de la organización pueden facilitar la revisión periódica, así como el estado de las acciones preventivas o correctivas y las vulnerabilidades o amenazas que fueron minimizadas, mediciones de eficacia y cualquier cambio que pudiera afectar el SGSI.

7.3 Resultados de la revisión

Los resultados de la revisión serán utilizados para mejorar la eficacia del SGSI, actualización de riesgos y el plan de tratamiento de riesgos, modificación de procedimientos y controles que afecten la seguridad de la información (requisitos, procesos del negocio, requisitos legales o reglamentarios, obligaciones contractuales, niveles y/o criterios de aceptación de los riesgos, recursos y eficacia de controles.

8 Mejora del SGSI

8.1 Mejora continua

Mediante el uso de la política y de los objetivos de la información de seguridad de la información, así como acciones preventivas y correctivas y de las revisiones tanto de Auditoría como de la Dirección.

8.2 Acción correctiva

Con el fin de eliminar las causas de las no conformidades, evaluar la necesidad de adoptar acciones para evitar las no conformidades, determinar e implantar las acciones correctivas necesarias y revisar las acciones correctivas realizadas.

8.3 Acción preventiva

Con el fin de eliminar las causas de las posibles no conformidades y poder elegir las acciones más apropiadas para minimizar los problemas potenciales, evaluar la necesidad de adoptar acciones para prevenir la ocurrencia de las no conformidades. La organización debe identificar los cambios en los riesgos, los requisitos de las acciones preventivas centrando la atención en los riesgos que hayan sufrido cambios significativos. La prioridad de las acciones preventivas debe determinarse basándose en los resultados de la evaluación de riesgos.

1.1.2 NORMA ISO/IEC 27002:2005: TÉCNICAS DE LA SEGURIDAD – CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La información es un activo vital para las empresas y por lo cual debe ser salvaguardada cualquiera que fuere su medio de uso (digital, impreso), los controles que se apliquen para su protección deben considerar los principales riesgos que corre dentro de la empresa y fuera de ella en el caso de fuga, peor aún cuando la empresa ha incursionado con transacciones móviles o en la nube.

Para la aplicación de controles se debe tomar en cuenta la legislación vigente en el país que se genera la transacción, la recurrencia de incidentes de seguridad en la empresa que hayan afectado la integridad y privacidad de los datos sensibles dentro de la empresa, el impacto y probabilidad de los riesgos gestionados.

El análisis del estándar inicia en el punto 4 ya que los numerales del 1 al 3 solamente especifican términos generales sobre la estructura de la norma y consideraciones generales para su lectura y aplicación.

4. Evaluación y tratamiento de riesgos

4.1 Evaluación de los riesgos de la seguridad

La evaluación de riesgos y selección de controles es una actividad que debe realizarse varias veces para cubrir las diferentes partes de la organización o sistemas individuales de información.

La evaluación de los riesgos debe tener un alcance definido para que sea eficaz y debe interlazarse con las evaluaciones de otras áreas.

4.2 Tratamiento de los riesgos de la seguridad

Antes de poder gestionar los riesgos, es necesario determinar qué riesgos la institución puede aceptar o no, qué controles pueden reducir los riesgos, qué riesgos pueden ser transferidos, qué acciones pueden prevenir los riesgos, qué legislación y regulaciones estatales se deben cumplir y qué costo de inversión van a tener todos los controles que se han planificado implementar.

Cualquier conjunto de controles elegidos deben ser monitoreados, valorados y mejorados en su eficiencia y eficacia.

5. Política de la seguridad

5.1 Política de la seguridad de la información

5.1.1 Documento de la política de la seguridad de la información

Es responsabilidad de la Dirección la emisión y aprobación de documentos de políticas de seguridad de la información, así como publicar y comunicarlas en forma adecuada y global. Dicha documentación debe establecer claramente la definición, metas y principios, controles y objetivos de control, responsabilidades generales y específicas de la seguridad de la información.

5.1.2 Revisión de la política de la seguridad de la información

La revisión de las políticas debe ser a intervalos planificados o cuando se produzcan cambios significativos y para dichas revisiones deben existir procedimientos establecidos y formalizados. Este proceso de revisión permite la retroalimentación, definir acciones preventivas y correctivas, identificación de amenazas, vulnerabilidades e incidentes. El resultado de estas revisiones debe finalizar en mejoras en los controles para la seguridad de la información.

6. Organización de la Seguridad de la información

6.1 Organización interna

Cuando hablamos de la organización interna estamos hablando de un marco referencial.

6.1.1 Compromiso de la dirección con la seguridad de la información

La dirección debería apoyar activamente delegando responsabilidades para la seguridad de la información. Es la dirección quien debería definir las metas, formular, revisar y aprobar políticas de la seguridad de la información, revisar la eficacia de la implementación en forma periódica para definir el rumbo y proporcionar los recursos necesarios, las funciones y responsabilidades, crear planes y programas para la concientización para todo el personal de la institución.

6.1.2 Coordinación de la seguridad de la información

La coordinación entre todo el personal líder de cada área es una actividad importante, ya que así, el personal se siente tomado en cuenta y podrá dar sus opiniones abiertamente sin pensar que es una obligación, sino más bien que son parte de los cambios. Esta comunicación involucra la cooperación y colaboración de todo el personal involucrado.

Toda esta comunicación permitirá identificar los no cumplimientos y sus razones, los cambios significativos de las amenazas, coordinar la implementación de controles, promover la educación, formación y concientización del personal, y recomendar las acciones apropiadas dependiendo de cada área.

6.1.3 Asignación de responsabilidades para la seguridad de la información

La definición de las responsabilidades es fundamental, definir al responsable de la protección de los activos individuales y para la ejecución de los procesos específicos de la seguridad, dicha definición debe estar documentada en forma detallada.

6.1.4 Proceso de autorización para los servicios de procesamiento de la información

Es la dirección la que autoriza los nuevos servicios de procesamiento de información, con todo lo necesario, sea hardware y software compatibles, ya que cualquier nuevo servicio puede introducir nuevas vulnerabilidades o se deberían colocar nuevos controles necesarios de acuerdo a los requerimientos de los nuevos servicios implantados.

6.1.5 Acuerdos sobre confidencialidad

Para poder implementar acuerdos de confidencialidad es necesario definir qué información debe ser protegida, la duración de los acuerdos de confidencialidad, las responsabilidades y las acciones a tomar cuando se incumplan, las acciones cuando se termine el acuerdo, derechos de auditar y monitorear ciertas actividades y la devolución o destrucción de información entregada.

6.1.6 Contacto con las autoridades

El contacto con las autoridades siempre debe ser en forma pertinente, porque una mala comunicación puede causar obstrucción antes que apoyo por parte de la dirección. La comunicación debe ser oportuna para informar sobre posibles incidentes identificados que pongan en peligro a la seguridad de la información.

6.1.7 Contactos con grupos de interés especiales

Puede ser con foros o asociaciones de profesionales sobre el tema necesario, lo que nos puede dar mejores prácticas y estar actualizados en temas de interés, se pueden recibir advertencias sobre incidentes externos o ataques y vulnerabilidades.

6.1.8 Revisión independiente de la seguridad de la información

Se recomienda realizar revisiones periódicas a intervalos planificados o cuando ocurran cambios significativos en la implementación de la seguridad de la información. Estas revisiones asegurarán la eficacia, idoneidad y propiedad de los controles y deberían ser realizadas por personas que tengan la experiencia y las habilidades adecuadas.

6.2 Partes externas

Se debe controlar el acceso a los servicios de procesamiento de información.

6.2.1 Identificación de los riesgos relacionados con las partes externas

Debe definirse el tipo de acceso que van a necesitar (físico, lógico, a través de la red, dentro de las instalaciones o fuera de ellas), el grado de sensibilidad de la información, los controles necesarios para su acceso, que personas van a accesar a

dichas información, el impacto de denegar el acceso, los incidentes históricos por accesos parecidos y las reglamentaciones legales que regirán estos accesos.

Las partes externas deben saber exactamente qué es lo que necesitan y sus obligaciones, responsabilidades y deberes que acarrea dichos accesos.

Todo el personal que no trabaje directamente como dueños de la información solicitada son considerados terceros.

6.2.2 Consideraciones de la seguridad cuando se trata con los clientes

Antes de dar los accesos correspondientes es necesario tomar en cuenta: los procedimientos para proteger los activos, la integridad de los datos, métodos de acceso permitido, los privilegios, los procesos para revocar los derechos de acceso o interrumpir la conexión entre los sistemas, los niveles de servicio y todo lo referente a asuntos legales.

6.2.3 Consideraciones de la seguridad en los acuerdos con terceras partes

Se deben considerar temas como acceso, procesamiento, comunicación o gestión de la información, sus controles asociados, y la confidencialidad, integridad y disponibilidad de la información sensible, que necesita la tercera parte. Al final del proceso tercerizado de debe garantizar la transferencia al personal interno para que las nuevas estructuras estén claras y los formatos sean los acordados, la descripción del servicio o del producto debe ser claro así como las responsabilidades civiles y los acuerdos sobre la propiedad intelectual.

7. Gestión de activos

7.1 Responsabilidad por los activos

Se deben identificar los responsables para todos los activos de información identificados y asignar la responsabilidad.

7.1.1 Inventario de activos

Todos los activos deben estar claramente identificados y debiéndose elaborar y mantener un inventario de todos los activos importantes, en dicha documentación debe especificarse el tipo de activo (información, activo de software, activo físico, servicio, personas, intangibles), el formato, la ubicación, la información de soporte, la información sobre licencias y el valor para el negocio.

7.1.2 Responsable de los activos

Cada uno de los responsables asignados debe garantizar que la información y los activos estén clasificados adecuadamente, revisar y definir periódicamente las restricciones y clasificaciones del acceso. La asignación puede ser hacia varios activos que actúan juntos para suministrar un servicio.

7.1.3 Uso aceptable de activos

Es necesario identificar, documentar e implementar las reglas sobre el uso aceptable de la información como correo electrónico y de Internet así como a través de dispositivos móviles, para que quede claro los límites que existen para el uso de la información y de los activos de la institución.

7.2 Clasificación de la información

La información tiene diferentes grados de sensibilidad e importancia.

7.2.1 Directrices de clasificación

La información se puede clasificar en términos de su valor, requisitos legales, sensibilidad e importancia para la institución.

Debería ser el responsable del activo el cual identifique su valoración, revisarlo periódicamente y asegurarse de que se mantenga actualizado y en el nivel adecuado. Con frecuencia la información cambia su valor después de un tiempo dado. La valoración que se da a la información es una manera corta de determinar la forma en que se debe manejar y proteger esta información.

7.2.2 Etiquetado y manejo de la información

La información que debe ser etiquetada comprende todos los activos de información en formatos físicos y electrónicos.

Deben definirse procedimientos para la cadena de custodia y el registro de cualquier evento importante de la seguridad.

Debe considerarse etiquetas electrónicas de ser necesario.

8. Seguridad de los recursos humanos

8.1 Previo a la contratación laboral

Las responsabilidades de la seguridad de la información se deben definir antes de la contratación laboral, donde se debe describir adecuadamente las actividades y los términos y condiciones del trabajo.

8.1.1 Funciones y responsabilidades

Se deben detallar en las funciones y responsabilidades, la implementación y el modo de actuar de acuerdo a las políticas de seguridad de la institución, los pasos que se deben seguir para proteger los activos de información contra accesos, divulgación, modificación, destrucción o interferencia no autorizada e informar sobre eventos de seguridad. Dichas funciones y responsabilidades deben ser claramente comunicadas al inicio de la actividad laboral.

8.1.2 Selección

Previo al proceso de selección se deben verificar los antecedentes de los candidatos en trabajos anteriores, y una vez realizada la selección se debe clasificar la información a la cual va a tener acceso y los riesgos asociados.

Es muy importante confirmar comportamiento anterior y las calificaciones profesionales y académicas, y si es posible incluso antecedentes crediticios y hasta criminales.

Para la selección del personal idóneo, se deben considerar la legislación vigente.

8.1.3 Términos y condiciones laborales

Como parte del proceso de contratación se debería formalizar un acuerdo de confidencialidad donde consten las responsabilidades del personal tanto dentro de las instalaciones como fuera de ellas. De igual forma deben estar correctamente redactadas las sanciones en el caso de incumplir lo acordado. Incluso debe definirse, si es necesario, responsabilidades incluso después de terminado el contrato laboral.

8.2 Durante la vigencia del contrato laboral

Se debería brindar un nivel adecuado de concientización, educación y formación en los procedimientos de la seguridad y el uso correcto de los servicios de procesamiento, así como inducción sobre procesos disciplinarios en el caso de violaciones de seguridad.

8.2.1 Responsabilidad de la dirección

Es necesario que la dirección provea un cierto grado de concientización sobre la seguridad ya que es mucho más probable que el personal motivado cause menos incidentes y sea más confiable.

8.2.2 Educación, formación y concientización sobre la seguridad de la información

La concientización en el personal de la institución debe ser adecuada, formal y debe actualizarse en forma regular sobre los requisitos, políticas y procedimientos de la institución.

Debe ponerse énfasis en las responsabilidades, funciones y habilidades e incluso a quien contactar para asesoría adicional.

8.2.3 Proceso disciplinario

Antes de aplicar un proceso disciplinario este debe ser verificado y se debe garantizar un tratamiento imparcial. En los casos grave de mala conducta el proceso debería permitir el retiro instantáneo de las funciones, los derechos de acceso y los privilegios y el acompañamiento inmediato fuera de las instalaciones, de ser necesario.

8.3 Terminación o cambio de la contratación laboral

Se deberían establecer responsabilidades para asegurar la gestión de la salida de empleados, contratistas o usuarios de terceras partes de la institución.

8.3.1 Responsabilidad en la terminación del contrato

Los contratos deberían incluir las responsabilidades y deberes válidos después de la terminación del contrato laboral.

8.3.2 Devolución de activos

En el proceso de terminación del contrato se debe incluir procesos de devolución del software previamente publicado, los documentos corporativos y de los equipos; es decir, de todos los activos de la organización que le fueron entregados. De igual forma, se debe garantizar que toda la información pertinente sea transferida a la organización y se elimine con seguridad del equipo.

8.3.3 Retiro de los derechos de acceso

Después de la terminación, se deberían reconsiderar los derechos de acceso de la persona, los cambios en un cargo se deberían reflejar en el retiro de todos los derechos de acceso. Los derechos de acceso a los activos de información y a los servicios de procesamiento de información se deberían reducir antes de la finalización o cambio del contrato laboral, dependiendo de una evaluación de factores de riesgos.

9. Seguridad física y del entorno

9.1 Áreas seguras

Los servicios de procesamiento deben estar ubicados en lugares físicos seguros con todas las protecciones físicas que amerite la información custodiada.

9.1.1 Perímetro de la seguridad física

Se debe utilizar perímetros de seguridad en áreas que contienen información y servicios de procesamiento de información. Dependiendo del tipo de información que se resguarde se deben colocar perímetros robustos físicamente con restricción de accesos a personal no autorizado, deberían colocarse sistemas anti-incendio con alarmas, monitoreo y deben realizarse pruebas periódicas según las normas regionales, nacionales e internaciones. Es recomendable colocar sistemas adecuados de detección de intrusos especialmente en las áreas desocupadas.

9.1.2 Controles de Acceso físico

Se deben llevar registros con fecha y hora de entrada y salida de visitantes y todos los visitantes deberían estar supervisados, las áreas donde se procesan o almacena información sensible deben tener acceso únicamente personal autorizado. Se recomienda usar identificaciones visibles y se debe notificar en forma inmediata la falta o mal uso de las identificaciones. De igual forma, los derechos de acceso a las áreas seguras se deberían revisar y actualizar con regularidad y revocadas cuando sea necesario.

9.1.3 Seguridad de oficinas, recintos e instalaciones

Se deben tener presentes los reglamentos y las normas pertinentes a la seguridad y la salud, las instalaciones claves no deben tener acceso directo al público.

9.1.4 Protección contra amenazas externas y ambientales

Los materiales combustibles o peligrosos se deberían almacenar a una distancia prudente de área de seguridad y se deberían proporcionar equipo apropiado contra incendios y ubicarlos adecuadamente.

9.1.5 Trabajo en áreas seguras

El personal solo debería conocer la existencia de un área segura o las actividades de ella en función de la necesidad, las áreas seguras vacías deberían tener bloqueo físico y se debería revisar periódicamente, no se debería permitir dispositivos de grabación fotográfica, de video, de audio, ni otro dispositivo de grabación como cámaras de seguridad en equipos móviles a menos que sean autorizados.

9.1.6 Áreas de carga, despacho y acceso público

El acceso al área de despacho y carga desde el exterior de la edificación debe estar restringido solo para personal autorizado e identificado, las puertas externas del área de despacho y entrega deberían estar aseguradas mientras las puertas internas estén

abiertas, el material que llega se debe inspeccionar para determinar posibles amenazas, los envíos entrantes y salientes se deberían separar físicamente cuando sea posible.

9.2 Seguridad de los equipos

Los equipos deben estar protegidos contra amenazas físicas y ambientales, se debe procurar reducir el riesgo de acceso no autorizado a la información y para protegerla contra pérdida o daño, se deben colocar controles especiales para la protección contra amenazas físicas y para salvaguardar los servicios de soporte.

9.2.1 Ubicación y protección de los equipos

La ubicación de equipos debe ser de tal modo que minimice el acceso innecesario a las áreas de trabajo, que se minimice el riesgo de visualización de la información por personas no autorizadas, se recomienda adoptar controles para minimizar el riesgo de amenazas físicas potenciales, se deben crear directrices para evitar comer, beber y fumar en las cercanías de los servicios de las áreas de procesamiento de datos, es necesario monitorear temperatura y humedad, aplicar protección contra rayos y adaptar filtros protectores a las fuentes de energía entrantes y a las líneas de comunicación, utilizar métodos especiales de protección para equipos ambientales industriales, los equipos de procesamiento de información deberían estar protegidos para minimizar el riesgo de fuga de información debido a filtración.

9.2.2 Servicio de suministro

Los servicios de suministro se deben inspeccionar regularmente y someter a las pruebas apropiadas para garantizar su funcionamiento adecuado y reducir cualquier riesgo debido a su mal funcionamiento o falla, se recomienda el uso de UPS (suministro de energía ininterrumpida) como contingencia en el caso de fallo de energía, también se recomienda el uso de iluminación de emergencia en el caso de fallo del suministro principal, el suministro de agua también debe ser estable y adecuado para alimentar el aire acondicionado, el equipo de humificación y los sistemas de extinción de incendios.

9.2.3 Seguridad del cableado

Las líneas de energía y de telecomunicaciones deben ser subterráneas en cuanto sea posible o tener protección alterna, los cables de energía deberían estar separados de los cables de comunicación para evitar interferencia, debe existir un plano del cableado para reducir posibles errores, se recomienda el uso de cableado de fibra óptica, conductos blindados electromagnéticos, acceso controlado a las áreas y módulos de cableado y a cuartos de cableado.

9.2.4 Mantenimiento de los equipos

Los mantenimientos deben ser acorde a las especificaciones e intervalos de servicio recomendado, solo el personal de mantenimiento autorizado debe realizar las reparaciones y el servicio de los equipos, deben generarse registro de todas las fallas reales o sospechadas y de todo el mantenimiento preventivo y correctivo, los controles deben ser apropiados al programa de mantenimiento para los equipos.

9.2.5 Seguridad de los equipos fuera de las instalaciones

Se debería observar en todo momento las instrucciones del fabricante para la protección del equipo, se deberían establecer coberturas adecuadas del seguro, para proteger el equipo fuera de las instalaciones.

9.2.6 Seguridad de la reutilización o eliminación de equipos

Se debe eliminar cualquier software licenciado y datos sensibles o asegurar que se haya sobrescrito de forma segura antes de la eliminación; los dispositivos que contienen información sensible se deben destruir físicamente o su información se debería destruir, borrar o sobrescribir usando técnicas que permitan que la información original no se pueda recuperar.

9.2.7 Retiro de activos de la propiedad

Para el retiro de los activos debe existir la autorización previa del personal que tenga la autoridad para dicho proceso, debe determinar un límite de tiempo y se debe registrar el equipo que ha sido retirado y se debe registrar cuando fue devuelto.

10. Gestión de comunicaciones y operaciones

10.1 Procedimientos operacionales y responsabilidades

Las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información deben estar formalmente establecidos.

10.1.1 Documentación de los procedimientos de operación

Se debe documentar y mantener a disposición los servicios de comunicación, incluyendo las interrelaciones con otros sistemas, el manejo de errores y otras condiciones excepcionales, contactos de soporte en caso de dificultades técnicas u operativas inesperadas, manejo de los medios e informes especiales, eliminación segura de los informes de tareas fallidas, procedimientos para el reinicio y la recuperación del sistema, gestión de los registros de auditoría y de la información del registro del sistema; los documentos formales y sus cambios deberían ser autorizados por la dirección.

10.1.2 Gestión del cambio

Debe existir un control estricto de la gestión del cambio, que registre e identifique los cambios significativos, la planificación y pruebas de cambios, evaluación de

impactos potenciales, procedimientos de aprobación formal, comunicación de los detalles del cambio, procedimientos de emergencia. Cuando se realicen los cambios es conveniente llevar un registro de auditoría que contenga detalles de dichos cambios, los cambios en el entorno operativo pueden tener impacto en la confiabilidad de las aplicaciones.

10.1.3 Distribución de funciones

Se debe tener mucho cuidado que ninguna persona puede tener acceso a modificar o utilizar los activos sin autorización o sin ser detectado.

Cuando haya dificultad para la distribución se deberían considerar otros controles como monitoreo de actividades, registros de auditoría y supervisión por la dirección.

10.1.4 Separación de las instalaciones de desarrollo, ensayo y operación

Se debe identificar el grado de separación entre los ambientes operativo, de prueba, de prueba y de desarrollo; definir y documentar las reglas para la transferencia de software; el software de desarrollo y operativo deben estar en diferentes dominios o directorios, los datos sensibles no se deberían copiar en el entorno del sistema de prueba, verificar que el personal de desarrollo y de pruebas no tengan acceso al sistema operativo y de información para poder introducir códigos no utilizados y sin probar o alterar los datos operativos, quienes desarrollan y realizan las pruebas imponen una amenaza a la confidencialidad de la información operativa.

10.2 Gestión de la prestación del servicio por terceras partes

La implementación de acuerdos, el monitoreo de su cumplimiento y la gestión de cambios asegura que los servicios que se prestan, cumplen los requisitos acordados con los terceros.

10.2.1 Prestación del servicio

La tercera parte debe mantener una capacidad de servicio suficiente y planes diseñados para garantizar la conservación de los niveles de continuidad del servicio acordado después de desastres o fallas significativas en el servicio.

10.2.2 Monitoreo y revisión de los servicios de terceros

Todos los servicios de terceros deben ser monitoreados en sus niveles de desempeño, los terceros deben suministrar información sobre los incidentes de la seguridad de la información y revisión de dicha información por parte de la organización.

10.2.3 Gestión de los cambios en los servicios por terceras partes

Los cambios en la prestación de los servicios deben ser gestionados teniendo en cuenta la importancia de los sistemas y procesos del negocio.

Las mejoras, el desarrollo de todos los sistemas o aplicaciones nuevas y los controles nuevos deben formar parte de la gestión de los cambios.

10.3 Planificación y aceptación del sistema

Es necesario hacer proyecciones de la capacidad futura para reducir el riesgo de sobrecarga del sistema.

10.3.1 Gestión de la capacidad

Es necesario tener un seguimiento y adaptación del uso de los recursos, y cuando sea necesario mejorar la capacidad y la eficacia de los sistemas, hay que poner atención a los recursos cuya adquisición toma mucho tiempo o requiere costos elevados para evitar cuellos de botella.

10.3.2 Aceptación del sistema

Deben definirse criterios de aceptación para los sistemas nuevos, actualizaciones y nuevas versiones tanto durante el desarrollo como antes de su implantación, y dichos criterios deben ser definidos, acordados, documentados para emitir una aceptación formal. Es conveniente llevar a cabo pruebas adecuadas para confirmar el cumplimiento pleno de todos los criterios de aceptación.

10.4 Protección contra códigos maliciosos y móviles

Para evitar, detectar y retirar los códigos maliciosos y controlar los códigos móviles.

10.4.1 Controles contra códigos maliciosos

Es necesario iniciar con la concienciación de los usuarios. Se debe manejar software de detección y reparación de códigos maliciosos, el acceso apropiado al sistema y controles en la gestión de cambios. Es vital que se prohíba el uso de software no autorizado.

Una vez establecidas los procedimientos adecuados es necesario realizar revisiones regulares del software y del contenido de datos de los sistemas, la instalación y actualización regular del software de detención y reparación de códigos maliciosos incluyendo archivos en medios ópticos, los adjuntos y las descargas del correo.

Es vital definir responsabilidades y procedimientos de gestión para tratar la protección de códigos maliciosos en los sistemas, planes adecuados para la continuidad del negocio, recolectar y verificar la información sensible con regularidad para evitar la inserción de código malicioso.

10.4.2 Controles contra códigos móviles

En el caso de código móvil, estos deben operar de acuerdo con la política de la seguridad claramente definida. Se debe considerar los bloqueos de cualquier uso de

códigos móviles, la recepción de código móvil, la activación de medidas técnicas, el control de recursos y controles criptográficos.

10.5 Respaldo

El objetivo de los respaldos es mantener la integridad y disponibilidad de la información, deben crearse procedimientos que hacer copias de la seguridad de los datos y probar sus tiempos de restauración.

10.5.1 Respaldo de la información

Los respaldos deben ser adecuados para garantizar que la información y el software esencial ser recuperen después de un desastre o una falla de los medios.

En un respaldo los registros deben ser exactos y completos; y, la extensión y la frecuencia de los respaldos de la información deben responder directamente a la continuidad de la operación de la organización.

Se recomienda que los respaldos sean ubicados en ubicaciones físicas lejanas con una apropiada protección física y ambiental. Los respaldos deben ser probados con regularidad y deberían ser encriptados para salvaguardar su integridad.

10.6 Gestión de la seguridad de las redes

Se debe tener una consideración cuidadosa del flujo de datos, las implicaciones legales, el monitoreo y la protección en la redes. Deben existir controles adicionales para proteger la información sensible que atraviesan las redes públicas.

10.6.1 Controles de las redes

Se deberían implementar controles de protección de los servicios conectados contra el acceso no autorizado, las responsabilidades y los procedimientos para la gestión de equipos remotos, proteger los sistemas y las aplicaciones conectadas para mantener la disponibilidad de los servicios de la red y los computadores conectados. Los controles se aplican consistentemente en toda la infraestructura del procesamiento de información.

10.6.2 Seguridad de los servicios de la red

Las características de la seguridad deberían ser identificadas en los niveles de servicio y los requisitos de gestión de los servicios particulares, los proveedores de servicios de red implementan estas medidas.

Las características de los servicios de red deberían tomar en cuenta la tecnología aplicada para la seguridad de los servicios de red, los parámetros técnicos requeridos para la conexión segura, los procedimientos para la utilización de los servicios de red para restringir el acceso a dichos servicios.

10.7 Manejo de los medios

Es necesario controlar y proteger de forma física la divulgación, modificación, retiro o destrucción de activos sin autorización y evitar la interrupción de las actividades del negocio.

10.7.1 Gestión de los medios removibles

El contenido de los medios removibles que ya no son necesarios debe hacérselos irrecuperables y se debería exigir una autorización para poder manipular dichos medios.

Las unidades de medios removibles sólo se deberían habilitar si existen razones del negocio que lo justifiquen, todos los medios se deberían almacenar en un ambiente seguro y vigilado y la información almacenada en los medios debería también estar almacenada en otro lugar seguro para evitar pérdidas de información.

10.7.2 Eliminación de los medios

La eliminación del contenido de los medios debería ser en forma segura y sin riesgo, con procedimientos acordes con la sensibilidad de la información contenida, los medios que contienen información sensible se deberían almacenar y eliminar de forma segura y dicha eliminación debería quedar registrado con el objeto de mantener pruebas de auditoría.

10.7.3 Procesamientos para el manejo de la información

Los procedimientos deben definirse para etiquetar, manejar, procesar, almacenar y comunicar la información, proporcionar restricción de acceso, protección y garantizar que los datos de entrada estén completos de acuerdo a su nivel de sensibilidad.

10.7.4 Seguridad de la documentación del sistema

El almacenamiento de la documentación debería ser seguro con la protección adecuada.

10.8 Intercambio de la información

Debería existir una política formal de intercambio que cumpla la legislación correspondiente.

10.8.1 Políticas y procedimientos para el intercambio de información

Deberían definirse procedimientos contra interceptación, copiado, modificación, enrutamiento inadecuado y destrucción de información sensible tanto en comunicación alámbrica como inalámbrica, utilizando técnicas criptográficas.

Debería haber procedimientos definidos para la retención y eliminación para toda la correspondencia, para no dejar información sensible o crítica en dispositivos de impresión, siempre recordando al personal en tomar las precauciones adecuadas.

Hay que evitar intercepciones telefónicas u otras formas no autorizadas, es necesario no intercambiar información sensible a través de medios no seguros y evitar recordar al personal no registrar datos demográficos.

La información podría verse amenazada debido a la falla de conciencia, de políticas o procedimientos sobre el uso de los servicios de intercambio de información.

10.8.2 Acuerdos para el intercambio

La dirección debería ser el responsable por controlar y notificar la transmisión, el despacho y recepción y garantizar la trazabilidad y el no repudio, así como la definición de normas para identificar los servicios de mensajería. Toda la información sensible y crítica debe ser correctamente etiquetada y deberían existir normas técnicas para registrar y leer la información y el software. Los acuerdos pueden ser electrónicos o manuales, de acuerdo a la necesidad.

10.8.3 Medios físicos para el tráfico

Contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización, para ello el transporte debe ser confiable y debería contar con procedimientos para la verificación de los servicios de mensajería.

Los controles deberían velar por la información sensible especialmente.

10.8.4 Mensajería electrónica

Debería definirse una protección adecuada al acceso no autorizado, modificación o negación de servicios, con niveles más sólidos de autenticación, se debe recordar que la mensajería electrónica tiene riesgos diferentes a los de la comunicación en papel.

10.8.5 Sistemas de información del negocio

Se deberían tener muy en cuenta las vulnerabilidades del sistema administrativo y contable y los sistemas de comunicación, se deberían crear políticas y controles para gestionar la forma en que comparten la información, así como las restricciones de servicios para usuarios específicos.

10.9 Servicio de comercio electrónico

Es necesario tomar en cuenta las implicaciones de la seguridad asociadas al uso de servicios de comercio electrónico.

10.9.1 Comercio electrónico

La información involucrada en el comercio electrónico debería ser protegida en contra de actividades fraudulentas, disputas por contrato y divulgación o modificación no autorizada, velando por la confidencialidad de datos o información sensible, escogiendo la selección del mejor convenio de forma de pago para evitar fraudes, evitando pérdidas o duplicación de la información sobre transacciones y la responsabilidad asociada con transacciones fraudulentas.

Se debería aplicar controles criptográficos para evitar una variedad de amenazas en la red.

10.9.2 Transacciones en línea

En necesario evitar transmisiones incompletas, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje enviado.

Se debe usar firmas electrónicas que validen y verifiquen la autenticidad de las transacciones y mantengan su confidencialidad, los protocolos de comunicación a utilizar deben ser seguros y cualquier almacenamiento de los detalles de la transacción debe estar en contornos privados.

Las transacciones en línea deben cumplir las leyes, reglas y reglamentos jurídicos del lugar donde se generen, procesen, terminen y/o almacenen las transacciones.

10.9.3 Información disponible al público

El sistema de acceso público debe estar protegido para evitar modificaciones no autorizadas y deberían ser probados frente a debilidades y fallas antes de ponerlo a disposición del público. Las entradas suministradas desde el exterior del sistema deberían ser verificadas y aprobadas.

Toda la información que se manipule dentro de esos sistemas debe estar protegida conforme a la legislación sobre protección de datos y se debería garantizar su procesamiento completo y exacto en forma oportuna, toda la información sensible debe estar protegida durante la recolección, procesamiento y almacenamiento.

10.10 Monitoreo

Se debería monitorear todos los sistemas y todos los eventos deben ser registrados con el fin de verificar los controles adoptados y revisar su cumplimiento.

10.10.1 Registro de auditorías

Todas las actividades de los usuarios especialmente los accesos deberían ser registrados para futuras investigaciones o auditorías. Dichos registros deben contar con información básica como fecha, hora, detalle de eventos, identidad o terminal, intentos aceptados y rechazados, cambios de configuración, uso de privilegios, uso de utilidades y aplicaciones, alarmas del control de acceso, activación y desactivación de los sistemas de protección.

Los registros para auditoria pueden contener datos personales confidenciales e indiscretos de ser necesario, pero dichos datos deben ser protegidos a accesos no autorizados.

10.10.2 Monitoreo del uso del sistema

Los registros del monitoreo deben ser revisados en forma regular y debe responder a una evaluación de riesgos sobre accesos autorizados, operaciones privilegiadas, intentos de acceso no autorizados, alertas o fallas del sistema, cambios o intentos de cambio de configuración y los controles de la seguridad del sistema.

Es vital tomar en cuenta que los factores de riesgos que deberían ser considerados son: valor, sensibilidad e importancia de la información implicada yel aprovechamiento de vulnerabilidades.

La función básica del monitoreo debería ser garantizar que los usuarios únicamente ejecuten actividades autorizadas explícitamente.

10.10.3 Protección del registro de la información

Se debería proteger la información contra el acceso o manipulación no autorizada, alteraciones en los tipos de mensajes que se registran, archivos de registro que se editen o eliminen y sobre la capacidad de almacenamiento en los archivos de registro.

Para facilitar la identificación de los eventos se aconseja el uso de utilidades del sistema o herramientas de auditoría.

10.10.4 Registros del administrador y del operador

Se debería registrar las actividades tanto del operador como del administrador del sistema, la hora en la que ocurrió el evento, información sobre el evento, que cuentas y procesos estuvieron involucrados.

Se puede emplear un sistema de detección de intrusos que esté fuera del control del sistema.

10.10.5 Registro de fallas

Las fallas se deberían registrar y analizar, tras lo cual deberían tomarse las acciones adecuadas, los problemas de procesamiento de la información o con los sistemas de comunicación deben mantener una revisión y registro de fallas para garantizar que éstas se resuelvan satisfactoriamente. El registro de errores y de fallas debería ser habilitado por el personal competente.

10.10.6 Sincronización de relojes

Los relojes de todos los sistemas deberían estar sincronizados y debería definirse un procedimiento que verifique y corrija cualquier variación significativa. La configuración correcta de los relojes del computador es importante para garantizar la exactitud de los registros de auditoría.

11. Control de acceso

11.1 Requisitos del negocio para el control de acceso

El acceso a la información, a los servicios de procesamiento de información y a los procesos del negocio se debería controlar con base en los requisitos de la seguridad y del negocio.

11.1.1 Política de control de acceso

Se debería establecer, documentar y revisar controles para los accesos tanto físicos como lógicos, políticas para la distribución y autorización de la información, perfiles estándar de acceso de usuario para funciones laborales, distribución de funciones de control de acceso, la legislación pertinente y obligaciones contractuales y el retiro de derechos de acceso cuando sea necesario.

Se debería establecer claramente que normativas son obligatorias y cuales son opcionales y cuando realizar cambios en los permisos de usuarios cuando estos tienes parámetros iniciales.

11.2 Gestión del acceso de usuarios

Deberían establecerse procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

11.2.1 Registro de usuarios

Debería definirse un procedimiento formal para el registro y cancelación de concesiones y revocatorias del acceso a todos los sistemas y servicios de información. Debería verificarse que los usuarios tengan autorización del responsable del sistema y que los privilegios otorgados sean adecuados y consistentes con las políticas de seguridad, esta concesión de privilegios deberían ser declarados en forma escrita y deberían ser firmados para constancia de que los usuarios entienden las condiciones de acceso.

El retiro o bloqueo de privilegios deberían se inmediatos el momento de cambios en el perfil funcional del usuario o cuando a abandonado la institución, y dichos privilegios deberían ser verificados, retirados o bloqueados periódicamente de acuerdo a un monitoreo constante.

11.2.2 Gestión de privilegios

Se deberían controlar y restringir la asignación y el uso de privilegios a través de procesos formales de autorización.

Se deberían identificar los usuarios y sus privilegios de acceso al sistema operativo, al sistema de gestión de base de datos y aplicaciones, cuyos accesos deberían solo los necesarios para su función.

El uso no apropiado de los privilegios de administración del sistema puede ser un factor importante para fallas o vulnerabilidades del sistema.

11.2.3 Gestión de contraseñas para usuarios

La asignación de contraseñas se debería controlar a través de un proceso formal de gestión. Debería generarse un documento formal donde se indique explícitamente que los usuarios y contraseñas asignados son confidenciales y que las contraseñas que inicialmente son entregadas deben ser modificadas inmediatamente que se haga el primer acceso.

Se debería considerar otras tecnologías disponibles para la identificación y autenticación del usuario.

11.2.4 Revisión de los derechos de acceso de los usuarios

Debería existir un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios para garantizar que no se obtienen privilegios no autorizados, los cambios en las cuentas privilegiadas se deberían registrar para su revisión.

11.3 Responsabilidad de los usuarios

La cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad, se debería concientizar a los usuarios sobre sus responsabilidades y el uso de equipos, de debería crear una política de escritorio y pantalla despejados.

11.3.1 Uso de contraseñas

Se recomienda mantener la confidencialidad de las contraseñas, cambiarlas frecuentemente, seleccionar contraseñas de calidad que no sean vulnerables y que no contengan caracteres idénticos consecutivos, se recomienda también evitar la reutilización y no incluir el registro de contraseñas en ningún registro automatizado, no compartir las contraseñas se usuarios individuales y también se recomienda no utilizar la misma contraseña para el acceso a varios servicios, pero se lo puede permitir en el caso de que sea una contraseña altamente compleja.

11.3.2 Equipo de usuario desatendido

Es necesario establecer mecanismos que permitan terminar las sesiones activas cuando finalice, realizar registros de cierre de computadoras principales, servidores y computadores personales de oficina al terminar la sesión, asegurarse que cuando las computadoras no estén en uso se bloqueen con claves de bloqueo o un control equivalente.

11.3.3 Política de escritorio despejado y de pantalla despejada

Debería adoptarse políticas de escritorio despejado para reportes y medios de almacenamiento removibles, para lo cual es necesario realizar una clasificación de información sensible o crítica del negocio.

Se debería proteger los puntos de entrada y salida de correo y las máquinas de fascímil desatendidas, los documentos que contengan información sensible o clasificada se debería retirar inmediatamente de las impresoras.

Todas estas medidas reducen el riesgo de acceso no autorizados, pérdida y daño de la información durante y fuera de las horas laborables normales.

11.4 Control de acceso a redes

Es necesario controlar el acceso a los servicios de red tanto internos como externos, deberían existir interfaces apropiadas entre la red de la organización y las redes, mecanismos adecuados de autenticación para los usuarios y los equipos.

11.4.1 Política de uso de los servicios en red

Deberían establecerse políticas de control de acceso para poder identificar quién accede a los servicios y los medios utilizados para el acceso.

Las conexiones inseguras y no autorizadas a servicios de red pueden afectar a toda la información.

11.4.2 Autenticación de usuarios para conexiones externas

La autenticación de usuarios remotos debería realizarse a través de criptografía, tokens de hardware o protocolos de desafío/respuesta.

Deberían existir controles adicionales para controlar el acceso a redes inalámbricas.

Cada uno de los controles impuestos debe responder a una evaluación de riesgos.

11.4.3 Identificación de los equipos en las redes

Se debería autenticar conexiones de equipos y ubicaciones específicas, se suele utilizar un identificador en el equipo o acoplado a éste que verificará que el equipo esté autorizado para accesar a la red. Puede considerarse la protección física del equipo para mantener la seguridad del identificador de éste.

11.4.4 Protección de los puertos de configuración y diagnóstico remoto

Se deberían colocar bloqueos de clave y procedimientos de soporte para controlar el acceso físico al puerto.

Muchos sistemas de computador, sistemas de red y sistemas de comunicación se instalan en un sitio de configuración o de diagnóstico remoto para ser utilizados por los ingenieros de mantenimiento.

11.4.5 Separación de las redes

Las redes grandes deberían dividirse en dominios lógicos de red separados para poder colocar controles para los entornos de la seguridad basados en una evaluación de riesgos. Los puertos de enlace se deberían configurar para filtrar el tráfico entre los dominios y bloquear accesos no autorizados.

Las redes también se pueden separar utilizando la funcionalidad del dispositivo de red, toda esta separación debe basarse en una clasificación de la información almacenada o procesada en la red y los niveles de confianza.

La separación de las redes inalámbricas procedentes de redes internas y privadas debe también obedecer a una evaluación de riesgos y a la identificación de los controles adecuados.

11.4.6 Control de conexión a las redes

Para las redes compartidas se debería restringir la capacidad de los usuarios para conectarse a la red a través de puertos de enlace que filtren el tráfico en servicios como mensajería, transferencia de archivos, acceso interactivo o acceso a aplicaciones.

11.4.7 Control del enrutamiento en la red

Se deberían implementar controles de enrutamiento en las conexiones a las redes entre computadores y los flujos de información para validar la dirección fuente/destino en los puntos de control de las redes internas y externas.

Las redes compartidas pueden requerir controles adicionales de enrutamiento.

11.5 Control de acceso al sistema operativo

Es necesario crear políticas de autenticación de usuarios autorizados, registro de intentos exitosos y fallidos, registro del uso de privilegios especiales, emisión de

alarmas cuando se violen políticas de seguridad, suministrar medios adecuados para la autenticación y cuando sea necesario restringir el tiempo de conexión a usuarios.

11.5.1 Procedimientos de registro de inicio seguro

El procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado. No se debería mostrar identificadores de aplicación ni de sistema, y se debería mostrar advertencias de notificación general a usuarios autorizados, se debería validar la información del registro de inicio y limitar la cantidad de intentos permitidos, así como el tiempo máximo y mínimo permitido para el registro de inicio, no se debería mostrar la contraseña que se introduce considerando enmascararla y no se debería transmitir contraseñas en texto claro a través de la red.

11.5.2 Identificación y autenticación de usuarios

Todos los usuarios deberían tener un identificador único utilizando una técnica a apropiada para comprobar la identidad y poder rastrear las actividades de la persona.

Cuando se requiera verificación de identidad y autenticación sólidas, se debería utilizar métodos alternos como encriptación, tarjetas inteligentes, token o medios biométricos.

La fortaleza de la identificación y autenticación del usuario debería ser adecuada a la sensibilidad de la información a la que se tiene acceso, una combinación de tecnologías y mecanismos enlazados podría dar la fortaleza requerida.

11.5.3 Sistema de gestión de contraseñas

Se debería permitir al usuario la selección y el cambio de contraseñas ya que de la fortaleza de la misma dependerá el grado de responsabilidad del usuario frente a la información que debe manipular, se debería imponer el cambio periódico de las contraseñas y se debería conservar un registro de contraseñas para evitar su reutilización y dicho registro debe estar almacenado en otro lugar que el de la aplicación.

Si es requerido trasmitir las contraseñas, se las debería enviar en formatos protegidos.

Tanto el usuario como la contraseña deben estar bajo responsabilidad y custodia de cada usuario.

11.5.4 Uso de las utilidades del sistema

Debería restringirse y controlar estrictamente el uso de programas utilitarios que anulen los controles del sistema y de las aplicaciones.

Es necesario mantener un registro de las utilidades del sistema y llevar una documentación sobre los niveles de autorización así como de los retiros o inhabilitación de todas las utilidades.

11.5.5 Tiempo de inactividad de la sesión

La dilatación del tempo de inactividad debería reflejar los riesgos de la seguridad del área, la clasificación de la información que se maneja y las aplicaciones que se utilizan, para evitar el acceso de personas no autorizadas y negar ataques al servicio.

11.5.6 Limitación del tiempo de conexión

Se debería limitar el tiempo de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.

La limitación del periodo durante el cual se permite la conexión a los servicios de computador reduce las oportunidades de acceso no autorizado.

11.6 Control de acceso a las aplicaciones y a la información

El acceso lógico al software de aplicación y a la información se debería restringir a usuarios autorizados con el fin de no poner en peligro otros sistemas que comparten los recursos de información.

11.6.1 Restricción del acceso a la información

La restricción del acceso debe ser tanto a nivel usuario como a nivel de personal de soporte, se aconseja: proporcionar menús para controlar el acceso a las funciones del sistema y controlar los derechos de acceso a los usuarios.

11.6.2 Aislamiento de sistemas sensibles

Los sistemas sensibles deberían tener un entorno informático aislado y su grado de sensibilidad se debería documentar e identificar explícitamente por parte del usuario responsable, con mayor razón cuando comparta recursos con otras aplicaciones.

El aislamiento se puede lograr utilizando métodos físicos o lógicos.

11.7 Computación móvil y trabajo remoto

Cuando se usa la computación móvil, debería tomar en cuenta los riesgos de trabajar en un entorno sin protección y aplicar una protección adecuada para garantizar que se han establecido las disposiciones adecuadas para el trabajo remoto.

11.7.1 Computación y comunicaciones móviles

Se debería tener un cuidado especial para asegurarse de que la información no se pone en peligro con este modo de transmisión, se debería colocar controles físicos, técnicas criptográficas para acceso, copias de respaldo y protección contra virus.

Los servicios de computación móvil debería protegerse en forma física contra robo y peor aún si maneja información sensible y/o crítica, este equipo nunca se debería dejar desatendido sin usar cerraduras especiales.

Este tipo e equipos deben tener un tratamiento especial ya que los protocolos de seguridad inalámbrica son inmaduros y tienen debilidades conocidas.

11.7.2 Trabajo remoto

El trabajo remoto debe ser autorizado una vez que la persona encargada esté satisfecha con las disposiciones de la seguridad y los controles establecidos.

Es necesario tomar en cuenta las restricciones y vulnerabilidades de las redes domésticas y la configuración de servicios de la red inalámbrica, la protección antivirus y firewalls, el trabajo remoto en horas laborales.

Se debería prever soporte y mantenimiento de hardware y software para los equipos de trabajo remoto, así como auditoría y monitoreo de la seguridad.

12. Adquisición, desarrollo y mantenimiento de sistemas de información

12.1 Requisitos de la seguridad de los sistemas de información

El diseño y la implantación del sistema de información que da soporte a los procesos del negocio pueden ser cruciales para la seguridad, y todos estos aspectos deben ser tomados en cuenta en el desarrollo y/o implementación, lo que debe ser justificado, acordado y documentado.

12.1.1 Análisis y especificación de los requisitos de seguridad

Se deberían considerar los controles automatizados que se han incorporado en el sistema de información y la necesidad de controles manuales de apoyo. Los controles deberían reflejar el valor para el negocio de los activos de información involucrados.

Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Se debería tomar en cuenta los controles de los riesgos introducidos y asociados antes de adquirir productos desarrollados en forma externa.

12.2 Procesamiento correcto en las aplicaciones

Se debería validar los datos de entrada, del procesamiento interno y de los datos de salida, tomando en cuenta el grado de sensibilidad de la información que se maneja.

12.2.1 Validación de los datos de entrada

Se debería verificar las entradas de las transacciones del negocio, los datos permanentes y de las tablas de parámetros. Se debería inspeccionar los documentos de entrada impresos para determinar cambios no autorizados, la respuesta ante errores de validación, la definición de responsabilidades para todo el personal.

12.2.2 Control de procesamiento interno

Se debería incorporar verificaciones de validación para detectar cualquier daño o pérdida de información por errores de procesamiento o actos deliberados, lo cual minimizará los riesgos de falla.

Se deberían utilizar funciones para agregar, modificar y borrar para mantenimiento de datos, procedimientos para evitar que los programas se ejecuten en orden erróneo, utilización de programas adecuados para la recuperación después de fallas, protección

contra ataques empleando desbordamiento/exceso en el búfer, controles de sesión, controles de balance, validación de datos de entrada en su integridad o autenticidad, totales de verificación, creación de registro de actividades implicadas en el procesamiento.

12.2.3 Integridad del mensaje

Se debería velar por la autenticidad e integridad de los mensajes de las aplicaciones, colocando controles adecuados y basados en una evaluación de riesgos, talvez usando técnicas criptográficas o cualquier otro medio que lo valide.

12.2.4 Validación de los datos de salida

Es necesario validar los datos de salida de una aplicación para confirmar su correcto y adecuado procesamiento. Se deben definir procesos de conciliación para determinar exactitud, totalidad, precisión y clasificación de la información. También deben establecerse claramente las responsabilidades de cada persona.

Siempre debe recordarse que aún los sistemas sometidos a prueba pueden producir salidas incorrectas en algunas circunstancias.

12.3 Controles criptográficos

Si se considera necesario deberían establecerse controles criptográficos y establecer una gestión de claves con el uso de la criptografía.

12.3.1 Políticas sobre el uso de controles criptográficos

Se debería realizar una evaluación de riesgos para identificar el nivel requerido de protección teniendo en cuenta tipo, fortaleza y calidad del algoritmo de encriptación requerido. Se debería tener especial cuidado con la información sensible que es transportada a través de medios móviles o removibles y utilizar métodos criptográficos.

Para la aplicación de estos métodos se debería tomar en cuenta los reglamentos y las restricciones nacionales y los aspectos del flujo trans-fronterizo de la información encriptada.

Los controles criptográficos deben velar por la confidencialidad, integridad/autenticidad y el no-repudio, el tipo de control que se debería aplicar y para qué propósito y cuál proceso del negocio.

No se debe temer a buscar asesorías externas especializadas de ser necesario a un nivel apropiado de protección.

12.3.2 Gestión de claves

Todas las claves criptográficas deberían tener protección contra modificación, pérdida, destrucción y divulgación no autorizada, y el equipo donde se almacenas dichas claves debe estar protegido por medios físicos.

La institución debe contar con controles y procedimientos idóneos para la protección de la autenticidad de las claves públicas.

También se deberían considerar el uso de claves secretas y públicas para el uso de firmas digitales.

12.4 Seguridad de los archivos del sistema

Los accesos a los archivos del sistema y al código fuente del programa deberían estar protegidos.

12.4.1 Control de software operativo

La actualización del sistema operativo debería ser realizada por personal administrador autorizado, los sistemas operativos deberían contener ejecutables aprobados y se debería implantar políticas de estrategia de restauración al estado anterior antes de implementar cambios.

Las versiones antiguas del software se deberían archivar junto con toda la información requerida, la organización debería considerar los riesgos de depender de software de soporte.

Se debería implementar procedimientos de monitoreo para controlar y evitar cambios no autorizados que generen fallas de seguridad.

Las mejoras no deberían tener lugar sólo porque esté disponible una nueva versión, esta debería ser probada en el ambiente de la organización antes de su implantación.

12.4.2 Protección de los datos de prueba del sistema

Se debería evitar el uso de base de datos operativos que contienen información personal o cualquier otra información sensible con propósitos de prueba, se debería retirar o modificar antes del uso para evitar el reconocimiento.

Debería existir autorización separada cada vez que se copia la información operativa.

12.4.3 Control de acceso al código fuente de los programas

Se debería evitar la introducción de funcionalidades no autorizadas y evitar los cambios involuntarios, de igual forma controlar el acceso a bibliotecas para desarrollo.

Se debería conservar un registro de auditoría de todos los accesos a las bibliotecas fuentes de programas.

12.5 Seguridad en los procesos de desarrollo y soporte

Los entornos de soporte y de desarrollo deberían estar estrictamente controlados para garantizar que todos los cambios propuestos en el sistema se revisan para comprobar que no ponen en peligro la seguridad del sistema ni del entorno operativo.

12.5.1 Procedimiento de control de cambios

La introducción de sistemas nuevos y de cambios importantes en los sistemas debería seguir un proceso formal de documentación, especificación, prueba, control de

calidad e implementación con gestión. Los procesos de control existentes no deberían ponerse en peligro con la implantación de cambios sin control.

Antes de la implantación de cambios, estos deben ser autorizados por los usuarios antes de su aplicación con sus respectivos rastros de auditoría, se debe procurar que los cambios sean oportunos y no deberían perturbar los procesos del negocio involucrados.

Todos estos controles se logran teniendo en forma separada el entorno de producción y el de desarrollo.

12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo

La revisión de los procedimientos de integridad y control de la aplicación debe ser periódico y constante, debe haber la garantía de la notificación oportuna sobre los cambios en el sistema operativo, realización de pruebas y revisiones apropiadas antes de la implementación. De igual forma deberían existir personas responsables para el monitoreo de las vulnerabilidades y las nuevas versiones de parches y arreglos.

12.5.3 Restricciones en los cambios a los paquetes de software

En la medida de lo posible todo el software suministrado debería usarse sin modificaciones, debería tomarse muy en cuenta que el impacto de que la organización se haga responsable del mantenimiento de software con modificaciones es muy alto y debería ser tomado como un riesgo.

Si los cambios son necesarios, el software original debería conservarse y los cambios deberían aplicarse a una copia del mismo, todos los cambios se deberían probar y documentar en su totalidad de manera que se puedan volver a aplicar de ser necesario.

12.5.4 Fuga de información

Es necesario minimizar el riesgo de fuga de información, utilizando sistemas y software con alta integridad, monitorear regularmente las actividades del personal y del sistema, monitorear el uso de recursos en los sistemas de computador, evitar la existencia de posibles canales encubiertos, evitar la intromisión de códigos troyanos previniendo el acceso no autorizado a la red.

12.5.5 Desarrollo de software contratado externamente

El software que se adquiera en forma externa debe contar con certificación de calidad y exactitud del trabajo realizado, derechos de acceso para auditar, realización de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

12.6 Gestión de la vulnerabilidad técnica

Se debería implementar de forma eficaz, sistemática y repetible con toma de mediciones que confirme la eficacia de la gestión de vulnerabilidades.

12.6.1 Control de las vulnerabilidades técnicas

Se debería obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas con el fin de tomar las acciones apropiadas para tratar los riesgos asociados.

El inventario completo y actual de activos es un prerrequisito para la gestión eficaz de la vulnerabilidad técnica para tomar acciones oportunas y apropiadas.

Deberían existir funciones y responsabilidades bien definidas sobre los recursos de información y sobre los riesgos asociados y sus acciones inmediatas. Es conveniente probar y evaluar los parches antes su instalación y el monitoreo debería ser a intervalos regulares.

13. Gestión de los incidentes de la seguridad de la información

13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información

Es conveniente establecer el reporte formal del evento y los procedimientos de escalada, donde se listen los distintos tipos de eventos y las debilidades que puedan tener impacto en la seguridad de los activos de información.

13.1.1 Reporte sobre los eventos de seguridad de la información

Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible utilizando un formato aprobado para dicho acto, y debería establecerse un proceso disciplinario en el caso de incumplimiento de dicho procedimiento.

Para poder tratar apropiadamente los eventos e incidentes de seguridad podría ser necesario recolectar evidencia tan pronto como haya dado el suceso.

13.1.2 Reporte sobre las debilidades en la seguridad

Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre fallas de seguridad a su responsable inmediato, los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. La recomendación inmediata debería ser que no se trate de probar las debilidades encontradas.

13.2 Gestión de los incidentes y las mejoras en la seguridad de la información

Se debería aplicar un proceso de mejora continua a la respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes de seguridad de la información.

13.2.1 Responsabilidades y procedimientos

El reporte de los eventos y las debilidades debería emplearse para detectar los incidentes de seguridad.

Es necesario crear procedimientos para manejar los diferentes tipos de incidentes, planes normales de contingencia, crear pistas de auditoría, acciones para recuperación de las violaciones de seguridad y corrección de fallas y se deberían establecer en forma clara los responsables de esta actividad que comprendan las prioridades para el manejo de incidentes.

13.2.2 Aprendizaje debido a los incidentes de seguridad de la información

Deberían establecerse mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes, costos, recurrencia e impacto de los incidentes de seguridad de la información. La necesidad de mejorar o agregar controles debería limitar la frecuencia, daño y costo de futuras recurrencias.

13.2.3 Recolección de evidencias

Las evidencias deben recolectarse, retenerse y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente. Las evidencias deben cumplir con admisibilidad y peso (calidad y cabalidad).

Las evidencias en papel deben garantizar que los originales no han sido alterados, la evidencia digital debería ser un duplicado o copias y los originales deben conservarse intactos y en forma segura. Se recomienda la participación inicial de un abogado o un policía en cualquier acción legal contemplada y asesorarse sobre la evidencia requerida.

14. Gestión de la continuidad del negocio

14.1 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio

Se debería implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto y la recuperación por la pérdida de activos de información, se deberían identificar los procesos críticos e integrar los requisitos de la gestión de seguridad de la información de la continuidad del negocio y garantizar la restauración oportuna de las operaciones esenciales.

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

El primer paso es tener una comprensión real de los riesgos que enfrenta la organización, con su identificación y prioridad, para lo cual se debe realizar una identificación de todos los activos involucrados en los procesos críticos del negocio que puedan causar interrupciones; por lo que debería analizarse la adquisición de pólizas de seguros, controles preventivos y mitigantes adicionales, identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes, pruebas y actualización de los planes y procesos de gestión con sus respectivos responsables.

14.1.2 Continuidad del negocio y evaluación de riesgos

Se debería identificar los eventos que pueden ocasionar interrupciones con su ponderación de probabilidad e impacto, se debería realizar una evaluación de riesgos para determinar la probabilidad y el impacto, es primordial la participación de los responsables de los recursos y los procesos.

La evaluación debería identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización.

14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

Se debería desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, identificar y acordar todas las responsabilidades y los procedimientos para la continuidad del negocio, procedimientos para permitir recuperar y restaurar las operaciones del negocio y la disponibilidad de la información, procedimientos operativos que se han de seguir en espera de la terminación de la recuperación y restauración, formación apropiada del personal en los procedimientos y procesos acordados, pruebas y actualización de los planes.

Los servicios y recursos deberían identificar el personal y recursos no relacionados con el procesamiento de la información.

Los planes de continuidad del negocio deberían afrontar las vulnerabilidades de la organización especialmente en la información sensible, las copias de los planes de continuidad del negocio deben estar actualizadas y protegidas con el mismo nivel de la seguridad que se aplica en la sede principal.

14.1.4 Estructura para la planificación de la continuidad del negocio

Cada plan debería especificar el plan de escalada y las condiciones de activación, cuando se identifican nuevos requisitos se deberían modificar los planes apropiadamente, cada plan debería tener un responsable específico.

La estructura para la planificación de la continuidad del negocio debe contener las condiciones para la activación de los planes, procedimientos de emergencia, procedimientos de respaldo, procedimientos operativos temporales, procedimientos de reanudación, programación de mantenimiento, actividades de concientización, educación y formación diseñadas, responsabilidades de las personas y los activos y recursos críticos necesarios.

14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio

Deberían asegurar que todos los miembros del equipo de recuperación son conscientes de los planes y sus responsabilidades y cada uno de los elementos del equipo se deberían probar con frecuencia.

Existe una variedad extensa de pruebas que podrían funcionar como pruebas sobre papel de varios escenarios, simulaciones, pruebas de recuperación, en un lugar alterno, pruebas de recursos y servicios del proveedor, ensayos completos, etc.

Se deberían registrar los resultados de las pruebas y cuando sea necesario, el proceso formal de control de cambios debería garantizar la distribución y el refuerzo de los planes actualizados mediante revisiones regulares del plan completo.

15. Cumplimiento

15.1 Cumplimiento de los requisitos legales

El diseño, el uso, la operación y la gestión de los sistemas de información pueden estar sujetos a requisitos de la seguridad estatutaria, reglamentaria y contractual.

15.1.1 Identificación de la legislación aplicable

Los controles específicos y las responsabilidades individuales para cumplir estos requisitos se deberían definir y documentar de forma similar.

15.1.2 Derechos de propiedad intelectual (DPI)

Debería definirse claramente las reglas para el uso de material que puede tener derechos de propiedad intelectual y sobre el uso de productos de software patentado.

Debería publicarse una política de cumplimiento de los derechos de propiedad intelectual, para la adquisición de software a fuentes conocidas, sobre mantener pruebas y evidencias sobre la propiedad de licencias, discos maestros, manuales, etc., la verificación de software autorizado y productos licenciados que no supere el máximo de usuarios permitidos.

Hay que tener mucho cuidado con duplicar software que están bajo la ley de derechos de copia, y de no copiar ni total ni parciamente libros, artículos, informes ni otros documentos con dicho derecho de copia.

Los productos de software patentados usualmente se suministran bajo un acuerdo de licencia que especifica los términos y condiciones de la licencia. La violación de los derechos de copia puede conducir a acciones legales que pueden implicar procedimientos judiciales.

15.1.3 Protección de los registros de la organización

Todo material relacionado con claves criptográficos y programas asociados se debería almacenar para permitir el descifrado de los registros. Para un almacenamiento a largo plazo, se recomienda considerar el uso de papel y microfichas. Deberían establecerse procedimientos para la adecuada destrucción de los registros cuando ya no se los necesite.

Se recomienda llevar un inventarios de las fuentes de información calve e implementar controles apropiados para proteger los registros y la información contra pérdida, destrucción y falsificación.

Puede ser necesario retener algunos registros de manera segura para cumplir requisitos estatutarios, reglamentarios o contractuales, así como para dar soportes a las actividades esenciales del negocio.

15.1.4 Protección de los datos y privacidad de la información personal

Se debería desarrollar e implementar una política de protección y privacidad de los datos, con frecuencia esto se logra nombrando a una persona responsable en forma individual o con procedimientos específicos para el manejo de la información personal y de la concienciación sobre los principios de protección de datos, estos controles pueden imponer funciones sobre aquellos que recolectan, procesan y distribuyen información personal y pueden restringir la capacidad de transferencia de datos a otros países.

15.1.5 Prevención del uso inadecuado de los servicios de procesamiento de información

La dirección debería aprobar el uso de los servicios de procesamiento de información, si se identifica alguna actividad no autorizada por medio de monitoreo inmediatamente se debe identificar acciones legales y/o disciplinaria adecuada.

Todos los usuarios deberían conocer el alcance preciso de su acceso permitido y del monitoreo implementado para detectar el uso no autorizado.

Muchos países tienen legislaciones que protegen contra el uso inadecuado del computador, puede ser un acto criminal usar el computador con propósitos no autorizados.

15.1.6 Reglamentación de los controles criptográficos

Se deberían utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes, restricción al uso de encriptación con una adecuada asesoría legal.

15.2 Cumplimiento de las políticas y las normas de la seguridad y cumplimiento técnico

Se debería acostumbrar a auditar a intervalos regulares las plataformas técnicas y los sistemas de información evaluar controles y documentarles.

15.2.1 Cumplimiento con las políticas y las normas de la seguridad

Si se halla algún incumplimiento como resultado de la revisión, se debería determinar la causa del incumplimiento, las acciones que garanticen el cumplimiento, determinar e implementar las acciones correctivas apropiadas, revisar las acciones

correctivas que se ejecutaron. Los directores deberían informar los resultados de las revisiones periódicas independientes de ser necesarias.

15.2.2 Verificación del cumplimiento técnico

Se debería realizar verificaciones sea manualmente y/o con la ayuda de herramientas automáticas que generen un informe técnico. Deben existir evaluaciones de vulnerabilidades planificadas, documentadas y repetibles.

La verificación del cumplimiento debe revisar los controles de hardware y software que se han implementado en forma correcta, deberían realizarse pruebas de penetración y por ninguna razón se debe creer que las pruebas de vulnerabilidades reemplaza una evaluación de riesgos.

15.3 Consideraciones de la auditoría de los sistemas de información

Deberían existir controles para salvaguardar los sistemas operativos y las herramientas auditoría durante las auditorías de los sistemas de información, los controles deben salvaguardar la integridad y evitar el uso inadecuado de las herramientas de auditoría.

15.3.1 Controles de auditoría de los sistemas de información

Las verificaciones deben ser planificadas y acordadas para minimizar el riesgo de interrupciones de los procesos del negocio.

Las verificaciones deberían limitar el acceso de solo lectura del software y datos, identificar y acordar los requisitos para el procesamiento especial y adicional. Se recomienda documentar todos los procedimientos, requisitos y responsabilidades y que las personas que realicen las auditorías, en lo posible, sean independientes de las actividades auditadas.

15.3.2 Protección de las herramientas de auditoría de los sistemas de información

Se debería proteger el acceso a las herramientas de auditoría, separando los sistemas operativos de los de desarrollo.

1.1.3 GAP ANALYSIS

El GAP Analysis es una herramienta de análisis que nos permite comparar la situación actual de la empresa con los estándares que rigen en la industria, a través de lo cual se puede identificar las áreas débiles y aquellas que necesitan mejorar. Distinguir las áreas en las que el cumplimiento de normas necesita mayor atención. En este análisis se toma en cuenta los estándares internacionales porque el objetivo más usual de realizar un GAP Analysis es el de preparar el camino para una certificación.

Se pueden tomar en cuenta leyes y estándares vigentes en el lugar de análisis, como por ejemplo:

Leyes y regulaciones

- SOX - SarbanesOxley
- BASEL II - Administración de Riesgos Financieros
- HIPAA - Privacidad de la Información
- CNBV - Comisión Nacional Bancaria y de Valores
- CNSF - Comisión Nacional de Seguros y Fianzas
- CONSAR - Comisión Nacional del Sistema de Ahorro para el Retiro

Estándares y mejores prácticas

- COSO - Control Interno / Estimación de Riesgos
- COBIT - Objetivos de Control para la Información y Tecnologías
- ITIL - Modelo de Procesos de Control y Gestión de TI
- ISO-IEC 27000 - Estándar de Seguridad de la Información
- PCI - Industria de Pago Electrónico

Este análisis incluye determinación, documentación y aprobación de requisitos y capacidades actuales. Dentro de la documentación se analizará si los procedimientos tienen la suficiente información para que el personal operador pueda cumplirlos y que dichos procedimientos cumplan normas y políticas internacionales. También es necesario verificar si la documentación ha sido actualizada de acuerdo a la realidad de la institución y del resto de la industria.

Con el GAP Analysis se pretende responder preguntas como:

- ¿Dónde estamos?
- ¿Dónde deberíamos estar?

El Gap Analysis provee un indicativo del esfuerzo, tiempo, dinero y recursos humanos que van a ser requeridos para obtener ese objetivo deseado.

Para la implementación de esta actividad se prevé la realización de un relevamiento de información que se realiza a través de entrevistas al personal jerárquico involucrado.

El análisis de la brecha básicamente es beneficioso para:

- Cumplir con los estándares, leyes y regulaciones exigidos
- Proteger los activos de información

- Mejorar los procesos de gestión de tecnología de información

El producto final de esta evaluación será un informe donde se destaquen los puntos débiles de los procesos establecidos y que es necesario hacer para que la brecha entre lo real y lo que se espera sea mínima.

1.1.4 GESTIÓN DE RIESGOS

¿Por qué la evaluación y la gestión del riesgo son importantes?

La evaluación y gestión de riesgos son importantes porque nos ayudan a determinar los riesgos y las vulnerabilidades de nuestros principales activos, debiendo determinar los controles necesarios para hacerles frente.

Los riesgos se dividen en los siguientes tipos:

- Riesgo inherente: Es la posibilidad de que existan errores o irregularidades en la gestión administrativa y financiera, antes de verificar la eficiencia del control interno diseñado y aplicado por el ente a ser auditado, este riesgo tiene relación directa con el contexto global de una institución e incluso puede afectar a su desenvolvimiento.
- Riesgo de Control: Es la posibilidad de que los procedimientos de control interno incluyendo a la unidad de auditoría interna, no puedan prevenir o detectar los errores significativos de manera oportuna. Este riesgo si bien no afecta a la entidad como un todo, incide de manera directa en los componentes.
- Riesgo de detección: Se origina al aplicar procedimientos que no son suficientes para lograr descubrir errores o irregularidades que sean significativos, es decir que no detecten una representación errónea que pudiera ser importante

Para calificar los riesgos por componentes, se debe preparar una matriz que contenga, entre otros aspectos lo siguientes:

- Componente analizado
- Riesgos y su calificación
- Enfoque esperado de la auditoría
- Instrucciones para la ejecución de la auditoría

Las etapas básicas definidas para un Análisis de Riesgos son:

1. Estructurar la gestión de riesgos utilizando las estrategias de la organización, políticas y criterios de la empresa.
2. Identificar los riesgos para crear un inventario de riesgos a través de las preguntas ¿Qué puede suceder?, ¿Cómo? y ¿Por qué?

Para realizar el inventario se puede tomar en cuenta ciertos riesgos generales para la empresa que se presentan en la Tabla No. 1, pero también se deben tomar los criterios del personal involucrado en las áreas estratégicas de la empresa:

Tabla 1:
Riesgos generales

RIESGOS ESTRATÉGICOS	*RIESGOS DE OPERACIÓN*	*RIESGOS FINANCIEROS*
Reputación	Fallas en los sistemas	Riesgos de crédito
Imagen	Errores humanos	Riesgos de liquidez
Pérdida de oportunidad	Procedimientos inadecuados	Riesgos de mercado
	Controles inadecuados	
	Fraudes	
	Riesgos de desastre	
	Riesgos legal	
	Riesgos regulatorios (cambios)	

3. Evaluar los riesgos (probabilidad e impacto) tomando en cuenta las consecuencias, probabilidad, nivel de riesgos, priorización y el análisis de brechas y la posible aceptación por parte de la Dirección.

Para la evaluación de probabilidad e impacto se pueden establecer escalas con las cuales se puede identificar la importancia del impacto y el porcentaje del que suceda el riesgo. En el siguiente cuadro se grafica un ejemplo de valoración de impacto y probabilidad desde el 2 como menor valor hasta el 4 como mayor valor, las escalas que se escojan dependen del grado de detalle que se quiera reflejar y del grado de madurez de la institución para su descripción.

Tabla 2:
Escalas para valoración

IMPACTO	*Menor*	*Moderado*	*Mayor*
	2	*3*	*4*
PROBABILIDAD	*Improbable*	*Posible*	*Probable*
	2	*3*	*4*

Para poder ponderar los resultados se pueden utilizar mapas de calor donde los riesgos más preocupantes sean representados con colores rojos, así:

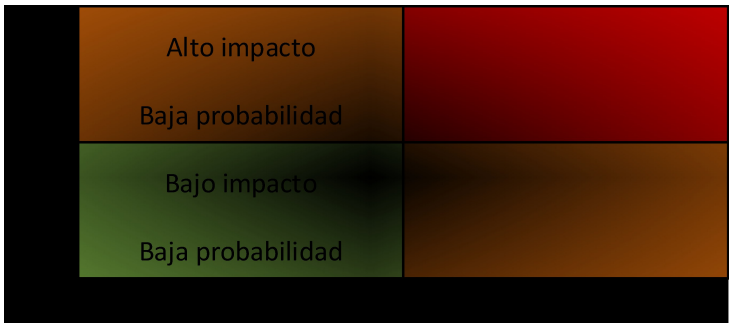

Gráfico 1: Mapa de calor para evaluar la respuesta a los riesgos
Fuente: COSO RM

4. Para el controlar los riesgos es necesario identificar, evaluar y seleccionar controles, crear un Manual de Control de riesgos e implementar dichos controles.
5. La Gestión de riesgos tiende a evitar, reducir, compartir o aceptar los riesgos que fueron descubiertos en las etapas anteriores.

Una vez que se pueden se han aclarado los conceptos básicos sobre la evaluación de riesgos, se analizarán dos herramientas que cumplen con los requerimientos necesarios para el estudio que está realizando:

1.1.5 NORMA ISO/IEC 27005:2008: TECNOLOGÍA DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD - GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN

Esta norma presenta lineamientos generales sobre la evaluación de riesgos prestando particular atención a los requisitos SGSI, pero el estándar no muestra una metodología específica ya que el análisis de riesgos depende de la institución y del alcance que el SGSI tiene en la empresa.

El análisis del estándar inicia en el punto 5 ya que los numerales del 1 al 4 solamente especifican términos generales sobre la estructura de la norma y consideraciones generales para su lectura y aplicación.

5. Información general

Los esfuerzos para la Seguridad de la Información deberían abordar los riesgos de una manera eficaz y oportuna donde y cuando sean necesarios. La gestión del riesgo de la seguridad de la información debería ser una parte integral de todas las actividades y se deberían aplicar tanto a la implementación como al funcionamiento continuo de un SGSI.

El proceso de evaluación de riesgo debería establecer un contexto global, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. Dicho proceso debería permitir a la institución identificar, valorar, comunicar, priorizar, informar a los interesados, aceptar, monitorear, revisar, capturar y educar a toda la empresa sobre los riesgos a los que está expuesta la organización. La evaluación de riesgos puede ser aplicada a toda la empresa o solo a una parte dependiendo de la estrategia de la Dirección.

6. Visión general del proceso de gestión del riesgo de la seguridad de la información

La normativa trata de definir un enfoque iterativo para realizar la valoración del riesgo que puede incrementar la profundidad y el detalle de la valoración en cada iteración. El enfoque iterativo suministra un buen equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, incluso garantizando que los riesgos altos se valoren de manera correcta. Si en cada iteración no se proporciona la valoración de riesgo suficiente se da otro bucle hasta llegar a un punto de equilibrio.

La eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo. Al terminar con el tratamiento del riesgo es necesario que los riesgos residuales sean aceptados por la alta gerencia y que dicha aceptación quede documentada para futuras evaluaciones.

Es importante que los riesgos y su tratamiento sean comunicados a los directores y al personal operativo correspondiente antes del tratamiento de los riesgos y toda acción debe ser documentada correctamente para evitar equivocaciones o errores de interpretación.

La aplicación de controles de Seguridad de la Información debe basarse en los riesgos detectados de la evaluación de riesgos.

En un SGSI, el establecimiento del contexto, la valoración del riesgo, el desarrollo del plan de tratamiento del riesgo y la aceptación del riesgo son parte de la fase de "planificar". En la fase de "hacer" del SGSI, se implementan las acciones y los controles que son necesarios para reducir el riesgo hasta un nivel aceptable, de acuerdo con el plan de tratamiento del riesgo. En la fase de "verificar" del SGSI, los directores determinarán la necesidad de revisiones de las valoraciones y del tratamiento del riesgo a la luz de los incidentes y los cambios en las circunstancias. En la fase de "actuar", se llevan a cabo todas las acciones que son necesarias, incluyendo la aplicación adicional del proceso de gestión del riesgo de la seguridad de la información.[1]

7. Establecimiento del contexto

7.1 Consideraciones generales

Para poder iniciar con una evaluación de riesgos es necesario recopilar la información suficiente sobre la empresa y delimitar el accionar de la evaluación; es decir, identificar claramente que áreas o procesos van a ser evaluados y que activos, sean personas o equipos, van a ser incluidos.

7.2 Criterios básicos

[1] ISO/IEC 27005:2008 Pág. 6

Es aconsejable seleccionar un enfoque adecuado para definir los criterios de evaluación de riesgos, de impacto y de aceptación del riesgo, es necesario realizar la valoración del riesgo y establecer un plan de tratamiento para el riesgo, definir e implementar políticas y procedimientos para implantar los controles necesarios, monitorear los controles y los procesos de gestión del riesgo de la seguridad de la información.

Criterios de evaluación del riesgo

- Determinar el valor estratégico del proceso de información del negocio
- La criticidad de los activos de información
- Requisitos legales y reglamentarios que afectan a la institución
- La importancia de la disponibilidad, confidencialidad e integridad para la institución
- Expectativas, percepciones y consecuencias negativas para el negocio
- Priorizar los criterios para el tratamiento de riesgos

Criterios de impacto

- Nivel de clasificación de los activos de información impactados
- Brechas de la seguridad de información
- Operaciones deterioradas
- Pérdida del negocio y valor financiero
- Daños para la reputación
- Incumplimiento de regulaciones legales de todo tipo

Criterios de la aceptación del riesgo: dependen de las políticas, metas, objetivos y partes interesadas

- Pueden incluir umbrales múltiples ya que se puede definir niveles de riesgos deseables y la alta dirección puede aceptar riesgos de un nivel superior dependiendo de las circunstancias
- Debe existir una relación entre el beneficio estimado y el riesgo estimado
- Deben existir distintos criterios de aceptación para distintas clases de riesgos
- Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional para el futuro

Los criterios de aceptación del riesgo pueden cambiar de acuerdo con la duración esperada del riesgo considerando los criterios del negocio, aspectos legales, operaciones, tecnología, finanzas y factores sociales y humanitarios.

7.3 Alcance y límites

Es necesario definir el alcance y límites con el fin de garantizar que todos los activos relevantes sean tomados en cuenta para la valoración del riesgo. Es necesario recolectar información para determinar el ambiente del que se generó y la pertinencia de la misma considerando los objetivos estratégicos, procesos del negocio, funciones y estructura de la organización, enfoque global de la organización, activos de información ubicación geográfica, restricciones de la organización, entorno socioculturales interfaces. Cualquier aspecto adicional debe ser justificado para su inclusión.

7.4 Organización para la gestión del riesgo de la seguridad de la información

Se debe establecer y mantener la organización con sus responsabilidades en el proceso de gestión del riesgo para desarrollar el proceso de gestión de la seguridad de la información, identificar y analizar las partes interesadas, definir responsabilidades internas y externas y establecer relaciones entre las partes interesadas y el alto nivel de la organización.

8. Valoración del riesgo de la seguridad de la información

8.1 Descripción general del la valoración del riesgo de la seguridad de la información

Un riesgo es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y se du probabilidad de ocurrencia, la valoración del riesgo puede ser cuantificada o cualificada dependiendo de los criterios establecidos. La valoración del riesgo determina el valor del activo de información, identifica las amenazas y vulnerabilidades, identifica los controles existentes y sus efectos, determina las consecuencias potenciales y prioriza los riesgos derivados y los clasifica de acuerdo a los criterios establecidos por la gestión de riesgos. Depende de la organización seleccionar los objetivos y metas de la valoración.

8.2 Análisis del riesgo

8.2.1 Identificación del riesgo

8.2.1.1 Introducción a la identificación del riesgo

Debe definirse qué podría suceder que cause una pérdida, el cómo, dónde y porqué podría ocurrir una pérdida.

8.2.1.2 Identificación de los activos

Un activo es todo aquello que tiene valor para la organización y que requiere de protección. La identificación de los activos debería tener un nivel de detalle suficiente

que proporcione información para la valoración del riesgo, se debe identificar al propietario de cada activo para asignarle la responsabilidad y rendición de cuentas, el propietario del activo con frecuencia es la persona más idónea para determinar el valor del activo para la organización.

8.2.1.3 Identificación de las amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas de origen natural o humano, accidental o deliberado dentro o fuera de la organización, ninguna amenaza debe ser pasada por alto.

La identificación de las amenazas se puede obtener de los propietarios o usuario de los activos de información, recursos humanos, área jurídica, expertos en seguridad, etc. tomando en cuenta aspectos ambientales y culturales. Se podría consultar otros catálogos de amenazas genéricos o estadísticas de incidentes disponibles en organismos de la industria, del gobierno, compañías, etc., pero es conveniente ser consciente que existe un cambio continuo en las amenazas importantes en especial si cambia el negocio.

8.2.1.4 Identificación de los controles existentes

Se debería realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios para verificar que dichos controles funcionen correctamente. Si el control no funciona como se espera, puede causar vulnerabilidades, una forma de estimar el efecto de control es ver la manera en que reduce la probabilidad.

Para la identificación de controles existentes o planificados se debe realizar una revisión de los documentos que contengan información sobre los controles, verificar con las personas responsables la eficacia de los controles implementados, efectuar una revisión en el sitio de los controles físicos y revisar los resultados de las auditorías internas.

8.2.1.5 Identificación de las vulnerabilidades

Existen vulnerabilidades en la organización, procesos, rutinas, personal, ambiente físico, configuraciones, hardware, software, equipos en general o dependencias externas.

La sola presencia de una vulnerabilidad no causa daño por sí misma, si no existe algo que la amenace tal vez no sea necesario aplicar controles, y en este caso no es un riesgo.

8.2.1.6 Identificación de las consecuencias

Las consecuencias pueden afectar a uno o más activos o a una parte del activo, es necesario tomar en cuenta el costo financiero consecuencia de dicha afectación. Para identificar las consecuencias se debe evaluar el tiempo de investigación y reparación, pérdida de tiempo, pérdida de oportunidad, salud y seguridad, costo financiero, imagen, y reputación de la organización.

8.2.2 Estimación del riesgo

8.2.2.1 Metodologías para la estimación del riesgo

Para la estimación del riesgo se deben tomar en cuenta diferentes grados de detalle dependiendo de la criticidad de los activos, la amplitud de las vulnerabilidades conocidas y los incidentes anteriores. La estimación del riesgo se puede medir en forma cualitativa o cuantitativa o una combinación de ambas, la estimación cualitativa proporciona una visión general del nivel del riesgo y el análisis cuantitativo proporciona niveles numéricos para poder generar gráficas, por lo general una evaluación cualitativa es menos costosa que una cuantitativa.

Estimación cualitativa: permite identificar la magnitud y la probabilidad. La ventaja de esta estimación es que facilita para la comprensión y la desventaja es la dependencia subjetiva hacia la escala escogida.

Estimación cuantitativa: Utiliza una escala con valores numéricos tanto para las consecuencias como para la probabilidad, la calidad del análisis depende de lo completo y exacto que sean los valores numéricos y de la validez de los modelos usados. La ventaja de esta estimación es que puede relacionarse directamente con los objetivos de seguridad y la desventaja es la falta de datos sobre riesgos nuevos o debilidades en la seguridad y cuando no se dispone de dichos datos crea una ilusión del valor y exactitud de la valoración del riesgo.

Las consecuencias y las probabilidades varían de acuerdo con el tipo de riesgo, la incertidumbre y la variabilidad tanto de las consecuencias deberían ser consideradas en el análisis.

8.2.2.2 Valoración de las consecuencias

El valor del impacto del negocio se puede expresar de manera cualitativa y cuantitativa expresado en valor monetario lo que proporciona más información para la toma de decisiones. La valoración de los activos debe iniciar con los de mayor

criticidad y debe ser analizados tomando en cuenta el valor de reemplazo del activo y las consecuencias para el negocio su perdida. Esta valoración se puede determinar a partir del análisis del impacto del negocio. La valoración de los activos es un factor clave en la valoración del impacto. Las consecuencias se pueden expresar en términos de criterios monetarios, técnicos o del impacto humano, u otros criterios pertinentes para la organización.

8.2.2.3 Valoración de los incidentes

Se deberían tomar en consideración la frecuencia con la que ocurren las amenazas y la facilidad con que las vulnerabilidades pueden ser explotadas teniendo en cuenta la experiencia y las estadísticas, fuentes de amenazas deliberadas, fuentes de amenazas accidentales, vulnerabilidades y controles existentes y su eficacia.

8.2.2.4 Nivel de estimación del riesgo

La estimación del riesgo asigna valores a la probabilidad y las consecuencias de un riesgo en forma cuantitativa o cualitativa. Se debe considerar el beneficio de los costos, los intereses de las partes involucradas y otras variables.

8.3 Evaluación del riesgo

Para evaluar los riesgos las organizaciones deberían compara los riesgos estimados con los criterios de evaluación del riesgo que se definieron. Las decisiones se basan principalmente en un nivel aceptable de riesgo, pero también es recomendable considerar las consecuencias, la probabilidad y el grado de confianza en la identificación y el análisis del riesgo, tomando en cuenta las propiedades de la seguridad de la información y la importancia de los procesos del negocio de la actividad sustentada por activos de información.

9. Tratamiento del riesgo de la seguridad de la información

9.1 Descripción general del tratamiento del riesgo

El tratamiento de riesgo tiene 4 opciones de elección: reducción de riesgo, retención del riesgo, evitación del riesgo y transferencia del riesgo. La elección depende del resultado de la valoración del riesgo. Las consecuencias adversas de los riesgos deberían ser bajas. Es conveniente definir un plan de tratamiento de riesgo donde claramente se identifique la priorización de los riesgos estableciendo diversas técnicas de clasificación de riesgos y análisis costo-beneficio.

La identificación de los controles existentes puede determinar que tales controles exceden la necesidad actuales pero puede resultar más económico dejar controles redundantes antes que eliminarlos. Siempre hay que tomar en cuenta los requisitos legales y reglamentarios que debe cumplir la organización.

Cuando ya se ha definido el tratamiento de riesgos es necesario determinar si los riesgos residuales satisfacen los criterios de aceptación del riesgo.

9.2 Reducción del riesgo

Se recomienda seleccionar controles adecuados y justificados, así como las regulaciones legales, reglamentarias y contractuales, los costos y el tiempo de implementación. Para la selección de controles es necesario identificar si son de protección, corrección, eliminación o prevención, así como los costos y el retorno de la inversión, y decidir si se implementan nuevos controles o se modifican los existentes. Se debe elaborar una lista de los controles posibles con sus costos, beneficios y prioridades de implementación. Existen restricciones de varios tipos: tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, personales, etc.

9.3 Retención del riesgo

Si el nivel de riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo puede retenerse.

9.4 Evitación del riesgo

Cuando los riesgos identificados se consideran muy altos o si los costos para implementar exceden los beneficios, es mejore retirar la actividad o conjunto de actividades que provocan el riesgo.

9.5 Transferencia del riesgo

Compartir riesgos con otras partes externas es una opción de transferencia de riesgo como contratando un seguro o subcontratación. Normalmente no es posible transferir la responsabilidad de un impacto.

10. Aceptación del riesgo de la seguridad de la información

En el caso de que el nivel de riesgo residual no satisfaga los criterios de aceptación del riesgo se puede tomar la decisión de tener que aceptar los riesgos que no satisfagan los criterios normales de aceptación con la debida justificación.

11. Comunicación de los riesgos de la seguridad de la información

La comunicación de los riesgos permite lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar y/o compartir la información con las personas involucradas. La comunicación debe ser bidireccional y debe proporcionar la seguridad del resultado, recolectar información del riesgo, compartir resultados de la valoración del riesgo, evitar o reducir la ocurrencia y las consecuencias, brindar soporte para la toma de decisiones, coordinar con las partes interesadas, dar la responsabilidad de la toma de decisiones, mejorar la toma de conciencia.

La comunicación del riesgo debe ser de forma continua y debe hacerse a través de las áreas de relaciones públicas o comunicaciones.

12. Monitoreo y revisión del riesgo de la seguridad de la información

12.1 Monitoreo y revisión de los factores de riesgo

Los riesgos no son estáticos, las amenazas, las vulnerabilidades, la probabilidad o las consecuencias puede cambiar abruptamente, por lo que es necesario monitorear en muchas ocasiones con servicios externos y dicho monitoreo debe ser continuo.

El monitoreo debe tomar en cuenta los activos nuevos, modificaciones en los valores de los activos, nuevas amenazas, nuevas vulnerabilidades o incremento de vulnerabilidades existentes, el incremento del impacto o de las consecuencias de las amenazas y los incidentes de la seguridad de la información.

Los cambios importantes que afectan a la organización deberían ser la razón para una revisión específica, las actividades de monitoreo se deberían repetir con regularidad y las opciones seleccionadas para el tratamiento del riesgo se deberían revisar periódicamente.

12.2 Monitoreo, revisión y mejora de la gestión del riesgo

El monitoreo y la revisión continua del tratamiento de riesgo debe ser pertinente y adecuada para las circunstancias. Todas las mejoras acordadas deberían ser notificadas a los directores para que se tomen las acciones necesarias y las decisiones. El monitoreo y revisión debe tomar en cuenta el contexto legal y ambiental, competencia del mercado, valoración del riesgo, categorías y valor de los activos, criterios de impacto, de evaluación del riesgo, de aceptación del riesgo, costo de la propiedad y los recursos necesarios. La organización debería garantizar que los recursos necesarios siempre estarán disponibles para revisar el riesgo, tratar las amenazas o vulnerabilidades y asesorar a la dirección según corresponda.

El monitoreo de la gestión de riesgo debe verificar los cambios identificados, la valoración del riesgo, el propósito de la gestión de riesgo y el objeto de la gestión de riesgos.

1.1.6 MAGERIT

Una de las metodologías más populares para el análisis de riesgos, especialmente en España, es MAGERIT con procesos específicos para los riesgos de TI (Tecnología de la Información).

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a riesgos que deben ser minimizados con medida de seguridad que generan confianza en el uso de tales medios.

MAGERIT fue publicado por primera vez en 1997, y desde allí el análisis de riesgos se ha convertido en un paso fundamental para la gestión de Seguridad de la Información.

Esta metodología es ideal cuando se trabaja con información mecanizada y sistemas informáticos y con mucha más razón cuando la información manipulada es valiosa y sensible para la empresa.

Los objetivos directos de la metodología son concientizar a los responsables de los sistemas de información de la existencia de riesgos y la necesidad de gestionarles a tiempo, ofrecer métodos sistemáticos para el análisis de riesgos y ayudar a descubrir y planificar medidas oportunas para mantener bajo control los riegos; y como objetivo indirecto el preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación según sea la necesidad de la empresa.

Esta metodología genera un Mapa de riesgos (relación de amenazas al que están expuestos los activos), Evaluación de controles (eficacia de los controles en relación al riesgo), Estado del riesgo (después de aplicar controles), Informe de insuficiencias (ausencia o debilidad de controles) y el Plan de Seguridad (conjunto de programas de seguridad que materialicen las decisiones de gestión de riesgos).

La metodología especifica dos tareas a realizarse:

- Determinar qué tiene la institución y estimar qué le podría pasar, elementos como activos, amenazas y controles. Se determina el impacto y el riesgo.
- Gestionar los riesgos: es decir, prepararse para emergencias, generar controles que minimicen los riesgos o los mitiguen o de ser el caso la Dirección los asume en cierto porcentaje.

Sus principales elementos son:

- Catálogo de activo de la información.
- Escala de valores cualitativos, cuantitativos y de indisponibilidad del servicio.
- Modelo de frecuencia de una amenaza como una tasa anual de ocurrencia.
- Escala alternativa de estimación del riesgo.
- Catálogos de amenazas.
- Catálogo de medidas de control.

Siendo de gran importancia, dentro de toda metodología de Gestión de Riesgos la definición de activos de la información, MAGERIT establece grupos de activos[2] a ser considerados para evitar que alguno se nos olvide, los grupos definidos son:

- Los servicios que ofrece la institución tanto al interior como al exterior.
- Los datos e información que se manipula al interior de la institución.
- Las aplicaciones de software.
- Equipos informáticos.
- Personal interno, externo, subcontratado, clientes, etc.
- Redes de comunicaciones propias o subcontratadas.
- Soportes físicos de información.
- Equipamiento auxiliar a los sistemas de información que no se han incluido en los otros grupos.
- Instalaciones físicas donde se alojen los sistemas de información.

1.1.7 NORMA ISO/IEC 27003:2012: TECNOLOGÍA DE LA INFORMACIÓN – TÉCNICAS DE SEGURIDAD – GUÍA DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Esta norma específica lineamientos generales para la creación de una Guía para la Implementación del SGSI.

El análisis del estándar inicia en el punto 5 ya que los numerales del 1 al 4 solamente especifican términos generales sobre la estructura de la norma y consideraciones generales para su lectura y aplicación.

5. Obtención de aprobación de la Dirección para iniciar un proyecto SGSI

5.1. Perspectiva general de la obtención de aprobación de la Dirección para iniciar un proyecto

Siendo la Seguridad de la Información un tema primordial para la empresa es necesario que la alta Dirección tome conciencia de su importancia y la necesitada imperiosa de iniciar tareas que salvaguarden y propicien los principios fundamentales

[2] Implantación de un SGSI en la empresa, INTECO (Instituto Nacional de Tecnologías de la Comunicación)

de la seguridad como son integridad, confidencialidad y disponibilidad. Tomando en cuenta estos criterios, se debe trabajar con la alta Dirección para que dé el apoyo necesario frente a un proyecto integral de SGSI donde se defina funciones y responsabilidades de cada uno de los integrantes de dicho proyecto así como el compromiso para la implementación y ejecución de las actividades planificadas.

5.2. Aclarar las prioridades de la organización para desarrollar un SGSI

Antes de iniciar con un proyecto de SGSI es necesario fijar las prioridades y requerimientos de seguridad de la institución ya que se corre el peligro de querer implantar ciertas medidas que la institución no necesita o que no tenga debilidad en el área en la que se colocan controles, para lo cual se debe recopilar la mayor cantidad de información que alimente una matriz de riesgos lo cual nos permita escoger los mejores controles para mitigar o reducir el riesgo en la institución y permitan la continuidad del negocio.

5.3. Definir el alcance preliminar del SGSI

En fundamental en este punto, definir claramente el alcance del SGSI ya que de eso depende el cronograma de actividades y el tiempo a invertir en su implementación; en el alcance deben constar todos los procesos de negocio, sistemas, activos de información, estructuras organizacionales y ubicaciones geográficas donde se pretende implantar el SGSI.

Parte de la definición del alcance es la definición de funciones y responsabilidades de todo el personal involucrado en el SGSI tanto del personal directivo como de los líderes de los procesos que alcanzará el SGSI propuesto. De igual forma, si es necesario se sugerirá la incorporación al grupo de trabajo de personal externo a modo de consultoría para temas que no sean del conocimiento del personal interno, siempre y cuando el número de participantes sea óptimo para que fluyan las ideas y toma de decisiones.

5.4. Crear el caso del negocio y el plan del proyecto para aprobación de la Dirección

El siguiente paso, es la creación de un perfil de proyecto donde consten todos los recursos necesarios para la implantación del mismo tanto material como humano, financiero y tecnológico. En dicho proyecto también se deben establecer las metas y objetivos, así como los beneficios y toda la información recolectada anteriormente como los roles y responsabilidades de cada involucrado y un cronograma con hitos claves para controlar el avance del proyecto. Este proyecto debe ser aprobado por la Dirección y debe proporcionar la confianza a la institución de que lo esperado beneficie a todos especialmente a la toma de decisiones directiva.

6. Definir el alcance del SGSI, límites y políticas del SGSI

6.1. Perspectiva general de la definición del alcance, límites y políticas del SGSI

Una vez que se cuente con el plan aprobado por parte de la Dirección, hay que continuar con el detalle de los límites y el alcance y comenzar con el desarrollo de la política del SGSI que debe incluir el alcance y los límites: organizacionales, de las Tecnologías de la Información y Comunicación y físicos.

6.2. Definir el alcance y límites organizacionales

Los límites organizacionales deben ser claramente establecidos, ya que si hay áreas que no van a formar parte del SGSI las razones de la no inclusión deben ser debidamente documentadas.

El foro de gestión del SGSI debe estar conformado por los directivos de las áreas involucradas y el responsable directo de la gestión del SGSI debe ser un miembro de la alta Dirección para representar los intereses de la seguridad de la información.

Los límites organizacionales debe también especificar a todo el personal de la empresa que va a afectar el SGSI.

6.3. Definir el alcance y límites de las Tecnologías de la Información y Comunicación (TIC)

Además de definir los límites organizacionales, también es necesario definir qué elementos de la TIC van a ser necesarios para desarrollar el SGSI, tomando en cuenta todos los sistemas de información que procesen y almacenen información crítica de toda la organización.

Dentro de los sistemas de información se debe tomar en cuenta la infraestructura de comunicaciones, software que se use dentro de la institución, hardware para todo el procesamiento de información, roles y responsabilidades de cada uno de los componentes de las TIC.

De ser el caso de que algunos de estos componente antes nombrados no son controlados por la organización, también se debe tomar en cuenta los servicios de terceros.

6.4. Definir el alcance y límites físicos

Después de tomar en cuenta el recurso humano y tecnológico es necesario establecer los límites físicos, ubicaciones, locales o instalaciones donde se proyecta implantar el SGSI dentro de la organización. Dentro de los límites físicos se debe

analizar las instalaciones remotas, interfaces remotas de los sistemas de información y los servicios provistos por terceros y niveles de servicio, sites alternos donde se almacenan hardware e información.

6.5. Integrar cada alcance y límites para obtener el alcance y límites del SGSI

Una vez detallados los límites organizacionales estos deben ser integrados y se debe especificar las configuraciones del equipamiento, listados de los activos de información incluidos en el alcance, mapas de la ubicaciones físicas, roles y responsabilidades y sus relaciones con la estructura organizacional, etc.

6.6. Desarrollar la política del SGSI y obtener la aprobación de la Dirección

Con todo el análisis realizado en los puntos anteriores, hay que comenzar a desarrollar la política de seguridad y debe ser aprobada por la Dirección. La política debe contener los objetivos del SGSI en base a los requerimientos de la organización y las prioridades de seguridad, debe especificarse el enfoque general y una guía de acción para su implantación, tomar en cuenta los límites regulatorios y obligaciones contractuales, un contexto de la gestión de riesgos y su evaluación, aclarar las responsabilidades de la alta Dirección.

El producto directo de esta etapa es un documento con la política del SGSI con su respectiva aprobación por parte de la Dirección.

7. Realizar el análisis de los requerimientos de seguridad de la información

7.1. Perspectiva general de la realización del análisis de los requerimientos de seguridad de la información

Para comenzar con el análisis de los requerimientos para la seguridad de la información es necesario identificar los activos de información e identificar el estado actual de la seguridad de la información que permita definir de mejor manera el alcance del proyecto.

La recopilación de información permitirá a la Dirección identificar el punto de inicio, identificar y documentar las condiciones para la implementación, conocer el nivel deseado de protección y establecer el alcance de los procesos o departamentos que serán tomados en cuenta.

7.2. Definir los requerimientos de seguridad de la información para el proceso del SGSI

Se debe definir y analizar los requerimientos detallados de la seguridad de la información en un documento donde debe constar:

- Resumen de los objetivos, prioridades y requerimientos de la seguridad de la información.
- Las restricciones regulatorias, contractuales y de la industria de la seguridad de la información.

El primer paso es recolectar toda la información de respaldo para el SGSI que permitirá establecer el nivel de protección que la institución requiere, para ello es necesario trabajar con una descripción muy básica de los procesos de la organización, adicionalmente información sobre los activos de información, formas actuales de procesamiento, requerimientos legales y organizacionales, nivel de concientización de la seguridad dentro de la empresa y las necesidades de capacitación y educación a corto y largo plazo.

La salida más importante de este punto es una lista de vulnerabilidades públicamente conocidas que serán consideradas en los requerimientos de seguridad. También podrán ser planificadas capacitación y educación a nivel de la organización.

7.3. Identificar los activos dentro del alcance del SGSI

Hay que identificar y listar los activos de información a ser respaldados con información sobre el proceso al cual pertenecen, ponderación del proceso (crítico, alto, medio, bajo), propietario del proceso, entradas y salidas del proceso, aplicaciones de TI que respalden el proceso, y la clasificación de la información (confidencialidad, integridad, disponibilidad, acceso, no repudio, etc.).

7.4. Realizar una evaluación de la seguridad de la información

Es necesario realizar una comparación entre la situación actual de la seguridad de la información y los objetivos deseados, identificar el nivel de madurez de la organización frente a los conceptos de seguridad de la información lo que se verá plasmado en las políticas y directrices que defina la SGSI.

Se podrá determinar el estado actual de la seguridad de la información y las vulnerabilidades estudiando hechos basados en procesos críticos, clasificando los activos y los requerimientos organizacionales de seguridad de la información.

La evaluación deberá realizarse tanto con recurso interno como externo para obtener cierto nivel de independencia en los criterios. El personal interno debe contar con un profundo conocimiento del entorno, condiciones actuales y conceptos básicos en términos de seguridad.

Las acciones importantes que se debe realizar para una correcta evaluación se deben identificar y enlistar en las normas de la organización, los requerimientos de control, los documentos de referencia, etc.

Es fundamental seleccionar los procesos organizacionales importantes de la institución, crear un flujo completo que cubra los principales procesos, discutir con personal clave para analizar la situación actual de la organización tomando en cuenta los requerimientos de seguridad, determinar las deficiencias de control comparando con controles existentes y completar y documentar el estado actual.

8. Realizar la evaluación del riesgo y la planificación del tratamiento del riesgo

8.1. Perspectiva general de la realización de la evaluación del riesgo y la planificación del tratamiento del riesgo

Un punto importante dentro de la gestión del SGSI es la identificación, evaluación y tratamiento de los riesgos de la seguridad de la información para poder escoger los controles más adecuados.

8.2. Realizar la evaluación del riesgo

La evaluación de riesgos debería identificar amenazas y sus fuentes, controles existentes y planificados, vulnerabilidades que pueden ser usada por amenazas y causar daños en los activos de la organización, las consecuencias de ver afectados los principios de la seguridad de la información, evaluar el impacto de los incidentes de seguridad de la información en forma anticipada o real, evaluar la probabilidad de incidentes, estimar el nivel del riesgo y comparar los niveles de riesgo frente a los criterios de evaluación del riesgo y los de aceptación del riesgo.

Las personas que forman parte de este proceso deben contar con profundos conocimientos de los objetivos de la organización y entendimiento de conceptos de seguridad.

8.3. Seleccionar los objetivos de control y los controles

El tratamiento de riesgos debe especificar la relación entre los riesgos y los controles seleccionados para su tratamiento o aceptación. Para facilitar las auditorías,

la organización debe seleccionar una lista de controles pertinentes y aplicables al SGSI. El resumen de los controles podría manejar información sensible como parte de los activos de la institución.

8.4. Obtener autorización de la Dirección para implementar y operar un SGSI

Como ya se había indicado, la documentación es una parte fundamental de la norma y es necesario documentar también la aceptación de los riesgos residuales para poder transmitir esta información en el caso del cambio de personal directivo.

Como en todo el proceso antes descrito es necesario contar con la aprobación de la Dirección sobre la decisión de acepar los riesgos residuales identificados y autorizar la operación real de la SGSI.

9. Diseño del SGSI

9.1. Perspectiva general del diseño del SGSI

Un diseño detallado del proyecto del SGSI y las actividades planificadas para su implementación deberían ser desarrollados en este punto, debe ser definida la estructura interna y los requerimientos del SGSI así como los acuerdos de gestión e infraestructura pre-existente.

El diseño de la seguridad organizacional tomando en cuenta el análisis de riesgos, los requerimientos de registro y documentación, diseño de controles, seguridad de las TIC, procesos físicos y organizacionales y el diseño de los requerimientos específicos del SGSI.

El diseño del SGSI debe enfocarse en los siguientes puntos específicos:

1. Seguridad Organizacional: cubre los aspectos administrativos, de operación, tratamiento del riesgo, procedimientos para manejar y mejorar la seguridad.
2. Seguridad de las TIC: cubre las responsabilidades de las operaciones de las TIC y implementación técnica de controles para reducir los riesgos.
3. Seguridad física: cubre las responsabilidades del manejo del ambiente físico e infraestructura para la reducción de riesgos.
4. Específicos del SGSI: cubre las actividades que deberían ejecutarse en la implementación para lograr operativizar el SGSI, tales como monitoreo, medición, auditoría interna del SGSI, entrenamiento y concientización, gestión de incidentes, revisión por parte de la Dirección y mejoramiento del SGSI incluyendo acciones correctivas y preventivas.

La seguridad de las TIC debe cubrir tanto los sistemas y redes de información como los requerimientos operacionales, la seguridad física trata con todos los aspectos del control de acceso, no repudio, protección física de los activos de la información y lo que está almacenado o guardado.

El plan de proyecto del SGSI debería detallar como manejar el riesgo con el fin de lograr los objetivos de control. El equipo de gestión de la seguridad de la información es responsable de la preparación de la implementación que constituye la parte final del proyecto del SGSI.

9.2. Diseñar la seguridad de la información organizacional

9.2.1. Diseño de la estructura organizacional final para la seguridad de la información

Las estructuras y procesos organizacionales deben estar alineados al tratamiento de riesgos integrándose con áreas pre-existentes, así mismo las estructuras y procesos organizacionales diseñados para el SGSI deben reflejar las actividades para la implementación y operación del SGSI.

La organización del SGSI debe tomar en cuenta que rol para la implementación necesita la operación del SGSI y si los roles definidos son diferentes para la implementación del SGSI.

9.2.2. Diseñar un marco referencial para la documentación del SGSI

La documentación del SGSI incluye las siguientes actividades:

- Un marco referencial que describa los principios para documentar el SGSI
- Diseño de los requerimientos de documentación
- Diseño de los requerimientos de registro

Se debe contar con un registro detallado de las decisiones de la Dirección y toda la documentación debe proveer la evidencia de que los controles son seleccionados en base a resultados de la evaluación del riesgo y su tratamiento. La documentación es esencial para la reproducción de los resultados y procedimientos.

La documentación del SGSI deben ser manejados y puestos a la disposición de todo el personal que lo requiera y debe incluir: los procedimientos administrativos de gestión de documentos del SGSI, aprobación formal de los documentos previa su emisión, los cambios y revisiones de los documentos deben estar plenamente

identificados y la debe existir una protección y control de dicha documentación como un activo de la institución.

La documentación debe ser legible, fácilmente identificable, transferidos, almacenados y dispuestos de acuerdo a los procedimientos aplicables para la clasificación. La documentación debe ser creadas, mantenida y controlada lo que demostrará la efectividad de las operaciones.

Las tareas que deben realizarse para el control de registro son:

- Documentar los controles requeridos para identificar, almacenar, proteger, buscar y descartar datos y documentar la duración de su almacenamiento.
- Definir que debería ser registrados y en qué medida.
- El periodo de retención de documentación debería ser establecido de acuerdo a los requerimientos legales.

9.2.3. Diseñar la política de seguridad de la información

Es necesario dejar documentada la posición estratégica de la Dirección y de la Administración en cuanto a los objetivos de la seguridad de la información. Lo que la Dirección ha identificado como importante en el análisis previo, debería hacerse evidente y enfatizarse en el diseño de la política, así como las acciones que se tomarán en el caso de no seguir la política establecida, los impactos legales y regulatorios también deben ser tomados en cuenta.

El diseño de la política debe ser lo suficientemente resumida para que todo el personal entienda la intención de dicha política. Se recomienda que para instituciones grandes se deba elaborar una norma general y varias normas subyacentes.

El proceso correcto para la aprobación es que el gerente de operaciones apruebe la política de seguridad de información y luego la comunique a todo el personal involucrado de tal manera que sea pertinente, accesible y comprensible.

9.2.4. Las normas o políticas establecidas deben ser dirigidas a toda la organización o a partes específicas.

Las normas para la seguridad de la información deben estar a disposición de aquellos que necesitan conocerlas.

Las personas que participen en la definición de normas y procedimientos deben tener autoridad y ser representantes de la organización, entre ellos deben ser: directores de la seguridad de la información, representantes de la seguridad física, propietarios de

sistemas de información y propietarios de procesos de áreas estratégicas y operacionales.

Las normas y procedimientos de seguridad deberían entonces ser usados como una base para diseñar procedimientos técnicos u operativos detallados. Las normas y procedimientos de seguridad de la información deberían aplicarse a toda la organización o aclarar que roles, sistemas y áreas están cubiertos incluyendo una línea base para la organización.

9.3. Diseñar la seguridad de la información de las TIC y física

El siguiente paso es realizar la documentación para cada control que debe formar parte del plan de proyecto del SGSI, la cual debe contar con:

- Nombre de la persona responsable de la implementación del control
- Prioridad del control para ser implementado
- Tareas o actividades para implementar controles
- Definición del tiempo en cual el control va a ser implementado
- Persona a quien se debería reportar la implementación del control
- Recursos para la implementación

El diseño real para la implementación de las mejores prácticas para la organización debe tomar en cuenta:

- Diseño de cada uno de los controles seleccionados para las TIC, áreas físicas y organizacionales a nivel operativo del sitio de trabajo.
- Ejemplificación de cada control de acuerdo con diseño acordado.
- Procedimientos e información de controles y cursos de capacitación para promover la conciencia de la seguridad.
- Asistencia e implementación de controles en el sitio de trabajo.

La implementación de controles requiere de la participación de diferentes roles de la empresa.

La seguridad de la información debería ser integrada en procedimientos y procesos de toda la organización, donde consten la re-asignación de roles y responsabilidades y la adaptación de procedimientos técnicos.

Los resultados de la implementación deben contener un plan de implementación que detalle los controles, y el registro y documentación de los resultados de la implementación.

9.4. Diseñar la seguridad de la información específica del SGSI

9.4.1. Plan para la prevención por parte de la Dirección

Se debe contar con un plan de revisión donde participe la Dirección y se comprometa en la revisión de la operación y mejoramiento continuo del SGSI. Esta participación provee un medio para validar el SGSI frente a las necesidades del negocio y para mantener el compromiso del negocio con el SGSI.

Dentro de la planificación de las revisiones periódicas debe especificarse que roles se deben involucrar y también debe contar que la información de las revisiones deben ser informadas lo más pronto posible.

De los resultados de las mediciones del SGSI se puede determinar el nivel de madurez y eficacia del SGSI.

Se debería planificar una Auditoría Interna del SGSI donde se evalúen los objetivos de control, controles, procesos y procedimientos del SGSI para poder saber si están efectivamente implementados, mantenidos y estén en conformidad con los requerimientos de normas internacionales, legislación y regulaciones y que este acorde a los requerimientos identificados en la seguridad de la información.

Las revisiones deberían contar con la siguiente información:

- Reportes de incidentes del último periodo de operación.
- Verificación de la efectividad del control y de no conformidades identificadas.
- Resultados de otras verificaciones regulares.
- Recomendación para mejorar el SGSI.

9.4.2. Diseñar el programa de concientización, capacitación y educación sobre la seguridad de la información

La Dirección es responsable de llevar a cabo la educación y capacitación con el fin de concientizar al personal y que este entienda el significado e importancia de las actividades de la seguridad de la información.

Es importante asegurarse de que todos los empleados dentro del alcance del SGSI reciban la capacitación y/o educación necesaria sobre seguridad. Un programa de concientización, capacitación y educación sobre la seguridad de la información debería asegurar que se generen los registros de esta capacitación y educación en seguridad. Los cursos de capacitación deben estar orientados a usuarios de los sistemas de TI.

El material de capacitación sobre seguridad de la información debe contener como mínimo datos sobre riesgos y amenazas, términos básicos, definición clara de un incidente (identificación y control), política de seguridad, responsabilidades, guía sobre cómo mejorar, guía sobre incidentes, y donde obtener información adicional.

Los materiales de capacitación deben ser revisados y actualizados continuamente.

9.5. Producir el plan final del proyecto del SGSI

Las actividades necesarias para implementar los controles seleccionados deben ser formalizadas en un plan de implementación detallado como parte del proyecto final del SGSI. Este plan involucra muchos roles diferentes en la organización, claramente designadas a las partes responsables, este plan debe ser comunicado a toda la organización contando con los recursos suficientes tanto materiales como recurso humano y financiero.

1.1.8 ANÁLISIS DEL CICLO DE DEMING PARA LA PLANIFICACIÓN E IMPLANTACIÓN DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (PHVA)

La ISO/IEC 27001:2005 es una norma internacional que proporciona especificaciones y orientación para realizar una implantación y mantenimiento apropiado del SGSI.

Por este motivo uno de los objetivos fundamentales de la norma es validar la mejora continua, y para ello propone el modelo definido por W. Edward Deming; el mismo que describe un modelo metodológico de procesos: Planificar-Hacer-Verificar-Actuar (PHVA). (Gráfico 1.2)

Tomando en cuenta este enfoque PHVA, se han encasillado cada uno de los apartados de la 27001 en cada uno de los procesos descritos, así:

- *Planificar*: Tiene por objetivo planificar la implantación y la provisión de la gestión del SGSI, contemplando aspectos como: el alcance de la norma, las políticas, normas y directrices del sistema, así como los controles establecidos y la Gestión de Riesgos, siendo importantes para velar por los principios fundamentales de la Seguridad de la Información como son: Confidencialidad, Integridad y Disponibilidad.

- *Hacer*: Existen actividades esenciales dentro de la implantación propiamente dicha del SGSI, como son la asignación de recursos tanto humanos como financieros y operativos, capacitación y concientización del personal involucrado, análisis y evaluación de riesgos y la implantación de los controles adecuados para la mitigación de riegos. En otras palabras, su misión es la de implantar los objetivos de gestión del SGSI y el plan definido.
- *Verificar*: Los procesos implementados, los recursos asignados y los controles establecidos siempre deben ser verificados en su eficacia y eficiencia tanto por personal interno (Auditoría Interna), como por persona externo (Consultorías o Asesorías), que a través de informes entregados en la dirección avalúe y recomiende mejoras y modificaciones de ser el caso. Dichas revisiones deben ser periódicas o solicitas en el momento de realizar cambios importantes en la institución que impacten en el SGSI.
- *Actuar*: El resultado de los procesos de verificación deben terminar en procesos de mejora continua y el establecimiento de medidas preventivas y correctivas, que eviten que el SGSI pierda su rumbo o se estanque volviéndose obsoleta.

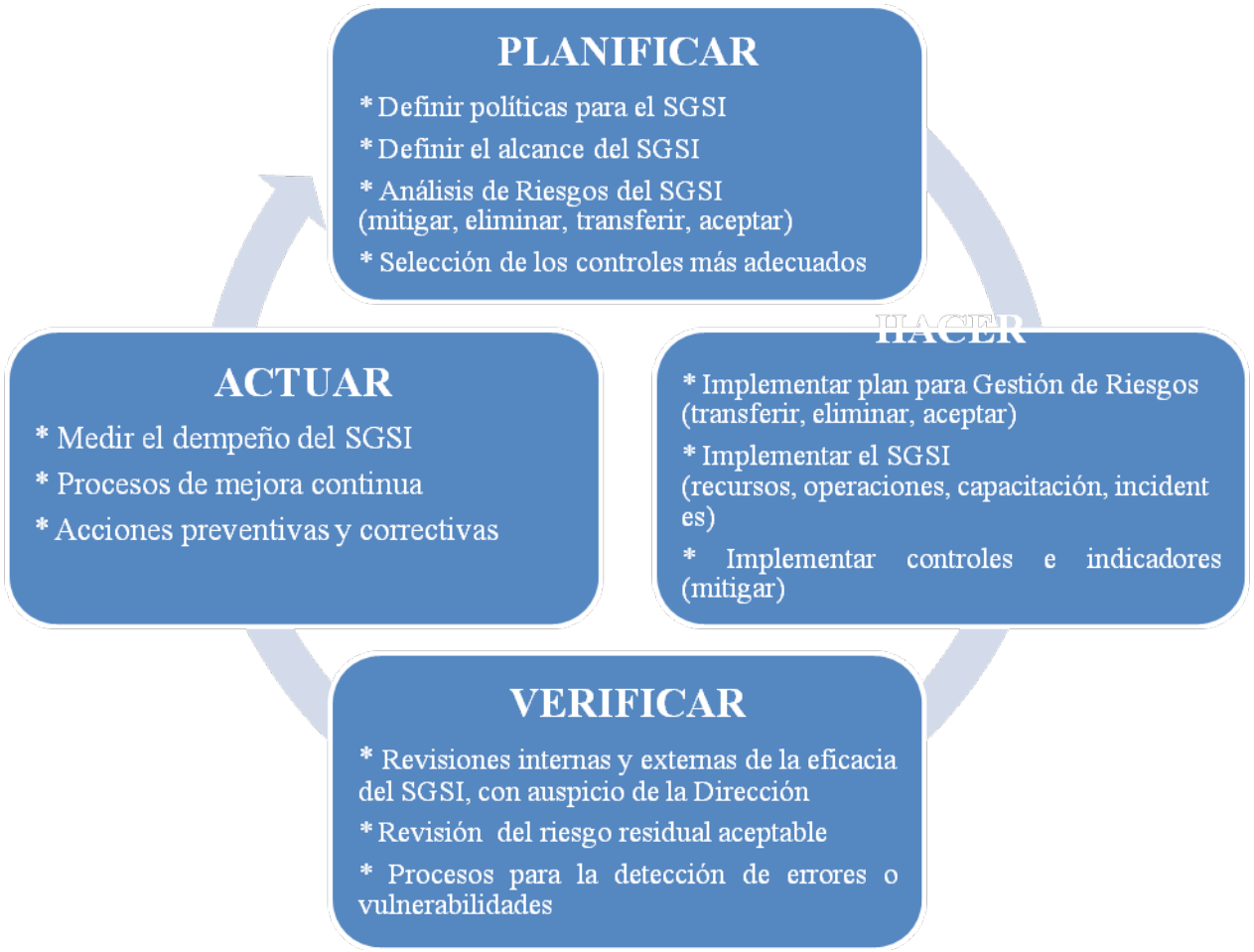

Gráfico 2: Ciclo de vida del SGSI

CAPÍTULO II

MARCO CONCEPTUAL

2.1 MAGERIT

No existe una metodología definida para la aplicación de los principios del GAP Analysis, sin embargo se han diseñado plantillas que permitan el análisis y evaluación de la información, como las siguientes:

- Listado de estándares: En esta plantilla se debe resumir todos los estándares internacionales que se aplican a nuestro caso de estudio así como el conjunto de buenas prácticas que deberían ser usadas para su implantación.

  Tabla 3:
  Formato para listado de estándares

Estándar	*Justificativo*	*Alcance*

- Evaluación de estándares: Una vez establecido los estándares a utilizar por la institución, se debe realizar una evaluación de los requerimientos básicos de cada estándar con el fin de definir el nivel de madurez de la empresa frente a estándares internacionales. La valoración del cumplimiento debe establecerse de acuerdo al nivel de detalle que se necesite, por lo general se colocan valores como **si** o **no**, o **alto**, **medio** o **bajo**.

  Tabla 4:
  Evaluación de estándares

Estándar	*Requerimient*	*Evaluació*

- Evaluación detallada de estándares: Dependiendo de las necesidades de la empresa se puede definir un detalle más particular en la evaluación de estándares, dependiendo del puntaje establecido con la evaluación anterior ya que si tenemos un nivel medio de madurez talvez se necesite aclarar más que nivel de detalle necesita control o revisión adicional, en el caso de tener un nivel bajo no es necesario este análisis.

  Tabla 5:
  Formato para listado de brechas

Estánda	*Requerimiento*	*Evaluació*

- Listado de estándares institucionales: Por último y con el fin de saber desde donde se debe arrancar, se debe realizar una lista de estándares institucionales que han sido implantados dentro de la empresa y que servirán de base para un análisis inicial y un análisis de mejora de ser necesario y poder así ubicar a la institución en el nivel de madurez en el que se encuentra para poder tomar las acciones más adecuadas.

Tabla 6:
Formato para evaluación de políticas

Políticas	*Fecha vigencia*	*Fecha actualización*	*Evaluación ?*

2.2 INVESTIGACIÓN SITUACIONAL DEL IGM

- El estudio que se llevará a cabo, permitirá identificar las brechas que tiene la institución en cuanto al conocimiento y aplicación de la seguridad de la información, de tal manera que se gpueda analizar con mayor profundidad aquellos aspectos que sean de interés institucional al momento en que se decida implantar el sistema de seguridad de la información.
- Además, la información que se pueda recopilar, a través de la encuesta, permitirá conocer las opciones y el porcentaje de seguridad que demanda la institución por parte del modelo ISO que se deberá cubrir de acuerdo a una acción estratégica.
- La encuesta piloto (Ver anexo 2), que tiene por objetivo el recopilar información sobre conocimientos y normativas básicas que los mandos medios de la Gestión Cartográfica poseen y han implantado, se llevará a cabo a través del correo electrónico. Con este instrumento de investigación se podrá obtener información sobre requerimientos, capacidades, voluntades y necesidades a fin de que la implantación del SGSI sea lo más objetivo posible.
- Entre las variables que se utilizarán para poder clasificar y ordenar la información, están: conocimiento general del SGSI, conocimiento específico del SGSI, requerimientos específicos o mejoras, interacción con el entorno y riesgos. El conocimiento general del SGSI permite conocer el nivel de madurez del personal frente a conceptos y controles de seguridad de la información, así como del grado de concientización frente a incidentes de seguridad.
- Los requerimientos específicos o mejoras buscan conocer las necesidades puntuales que puede tener la institución en su entorno, los conocimientos específicos

permitirán analizar el inteligenciamiento y aplicación que tiene la institución en relación a la seguridad de la información; la interacción con el entorno permite identificar las posibles vulnerabilidades a las que se enfrenta la institución y da la pauta para que los mismos usuarios puedan recomendar controles prácticos; y la identificación de riesgos busca situar al personal en la realidad de la institución y permite identificar, manejar, minimizar, aceptar y mitigar los riesgos asociados a los procesos normales de la institución.

- La encuesta se elaboró de acuerdo a las variables identificadas anteriormente, se utilizará una pregunta pivote, enfocada en la seguridad de la información, para poder determinar y relacionar los aciertos de esta encuesta, como son el conocimiento que tienen los encuestados del término seguridad de la información.
- La encuesta se encuentra formateada en el anexo 2 de este documento.
- El segmento objetivo de la encuesta son los funcionarios públicos de mandos medios de la institución castrense pertenecientes a la Gestión Cartográfica. Con la aplicación a este segmento institucional, se prevé tener contestaciones diversas, tomando en cuenta el enfoque de contestación que le brinde cada encuestado por su nivel de preparación y responsabilidad, esto de igual manera permitirá delinear estrategias de implantación.
- El tamaño del universo a consultar se definió a 11 personas, tomando en cuenta los mandos medios de los distintos departamentos de los procesos productivos de la Gestión Cartográfica.
- El procesamiento de los datos, codificación y tabulación se la realizará en una hoja de cálculo, tipo Excel. Luego de revisar y verificar los datos e información recopilada, se realizará cuadros estadísticos por cada pregunta a fin de facilitar la interpretación de la información resultante que ayude en la toma de decisiones estratégicas para el nuevo SGSI.

CAPÍTULO III

ESTUDIO DE LA ORGANIZACIÓN

El IGM es una institución de tipo militar, cuyas operaciones administrativas se encuentran en la ciudad de Quito, con una sucursal en Guayaquil; considerada por décadas como la empresa motor de la industria cartográfica y gráfica del país. Cuenta con un total de 572 empleados civiles y 98 empleados militares, de los empleados civiles se cuenta con un total de 200 personas con contrato temporal con lapsos de hasta 2 años. De los empleados militares asignados al IGM, 10 cumplen con funciones ejecutivas como Director, Subdirector y Jefes de área, el resto integra el personal operativo de las distintas áreas.

En la actualidad el IGM basa su operación en las directrices que establece el plan estratégico institucional vigente que fue elaborado y aprobado en el año 2007, el mismo establece directrices para los próximos 4 años.

El análisis de la situación actual conlleva la recopilación de la información de la institución en su establecimiento formal de organización y funciones que apalancan el tema de estudio que se está realizando, es por esta razón que se inicia con la documentación que muestra la Planificación Estratégica y los objetivos que persigue la institución y que dan su razón de existir, así:

3.1 ORGANIZACIÓN

Con el fin de poder determinar las acciones inmediatas que pueden ser tomadas, se analizará la base legal que rige el IGM y que podría apalancar las acciones inmediatas:

3.2 PLAN ESTRATÉGICO 2007-2010

3.2.1 MISIÓN

"Somos el organismo autorizado por el Estado Ecuatoriano para generar y regular la información y bases de datos Cartográfica Geográfica del país, proveer soluciones gráficas y de seguridad documentaria; extensión cultural en el campo científico de la astronomía y ciencias afines, que fortalecido con personal calificado, tecnología de vanguardia, procesos de mejoramiento continuo y respeto al medio ambiente, contribuye con el desarrollo nacional"

3.2.2 VISIÓN

"Satisfacer a los clientes a nivel nacional con proyección internacional, mediante soluciones integrales de cartografía, geografía, artes gráficas y seguridad documentaria, basados en una cultura de calidad y respaldados en la investigación técnica y científica"

3.2.3 OBJETIVOS ESTRATÉGICOS

1. *Mantener personal capacitado y motivado*: La capacitación para el personal debe ser considerada una inversión que mantendrá a los funcionarios motivados y actualizados en técnicas y herramientas para sus funciones específicas.
2. *Incrementar la productividad y el mejoramiento continuo*: Siempre debe ser una meta el mejorar a través de la retroalimentación continua.
3. *Incrementar los ingresos*: A pesar de que no es un objetivo dentro de las entidades pública, puede ser un índice de que las cosas van por buen camino.
4. *Unificación y aprobación de la normativa técnica*: Siendo una institución rectora de la normativa técnica para la elaboración de cartografía dentro del país, se debe contar con una normativa actualizada y aprobada.
5. *Aumentar la participación del mercado*: Siempre se debe trabajar por difundir los servicios de la institución.
6. *Mantener información actualizada*: Siempre acorde a los avances tecnológicos.
7. *Generar alianzas estratégicas*: Con instituciones que nos generen valor.
8. *Optimizar costos*: Siempre pensando en la naturaleza e incrementando el ahorro al estado.
9. *Mejorar el clima laboral*: Pensando siempre en el talento humano que sin él no se podría lograr los objetivos.
10. *Fortalecer la gestión del talento humano y la seguridad industrial*: Poniendo en primer plano la seguridad del talento humano.
11. *Posicionar la imagen institucional*: Colocándola en los mejores peldaños de la industria cartográfica y gráfica.
12. *Mejorar la satisfacción del cliente*: Satisfaciendo sus necesidades tanto en costos como en tiempos y calidad.
13. *Mejorar la relación con los proveedores:* Con el fin de lograr alianzas estratégicas para provisión de bienes y servicios en tiempos cortos.

14. *Implementar sistemas de seguridad integral*: Dentro de la Seguridad Integral se debe tomar en cuenta la Seguridad Informática, Salud Ocupacional y Seguridad Industrial, tomando en cuenta todas las normativas vigentes en el país y en la industria Cartográfica y Gráfica.
15. *Mejorar la comunicación interna*: Con una continua difusión de la normativas y políticas, así como de las mejoras que se van realizando.
16. *Optimizar las tecnologías de información*: Tomando en cuenta la tecnología de punta que hay en el mercado y que nos brinde las capacidades que necesitamos para la mejora de los productos y servicios que brinda el país.
17. *Contar con tecnología actualizada para generar y difundir información geoespacial*: Viene de la mano de objetivo estratégico 16.
18. *Provocar cambios y emisión de leyes*: Generando una normativa consistente y acorde a las necesidades de la institución, ésta tiene que siempre estar evaluada para poder ser actualizada de acuerdo a los cambios de la institución.
19. *Generar y mantener una cultura de calidad total / Mejorar la competitividad*: La calidad debe ser el valor agregado de todo producto y servicio dentro de la institución, y debe ser evaluada continuamente para ser actualizada y mantenida en los estándares esperados.
20. *Ser ambiental y socialmente responsables*: El incremento de ingresos no debe ser una excusa para irrespetar el ambiente o las normas sociales, siempre se debe tomar en cuentas la normativa vigente.
21. *Generar una adecuada difusión cultural*: Todo acorde a las necesidades del cliente externo especialmente los niños que son los usuarios frecuentes de los eventos del Centro Cultural.
22. *Definir la rentabilidad por producto*: Manejar una adecuado margen de utilidad y rentabilidad por la provisión de bienes y servicios.

Estos objetivos estratégicos buscan la sostenibilidad de la institución y el liderazgo en este nicho de mercado tan competitivo hoy en día. De igual manera, y como todo plan, la planeación marca la dirección institucional, reducción de incertidumbre y criterios de control.

Para que lo expuesto se alcance en el tiempo, cuenta con una estructura organizacional claramente definida.

3.3 ORGANIGRAMA ACTUAL

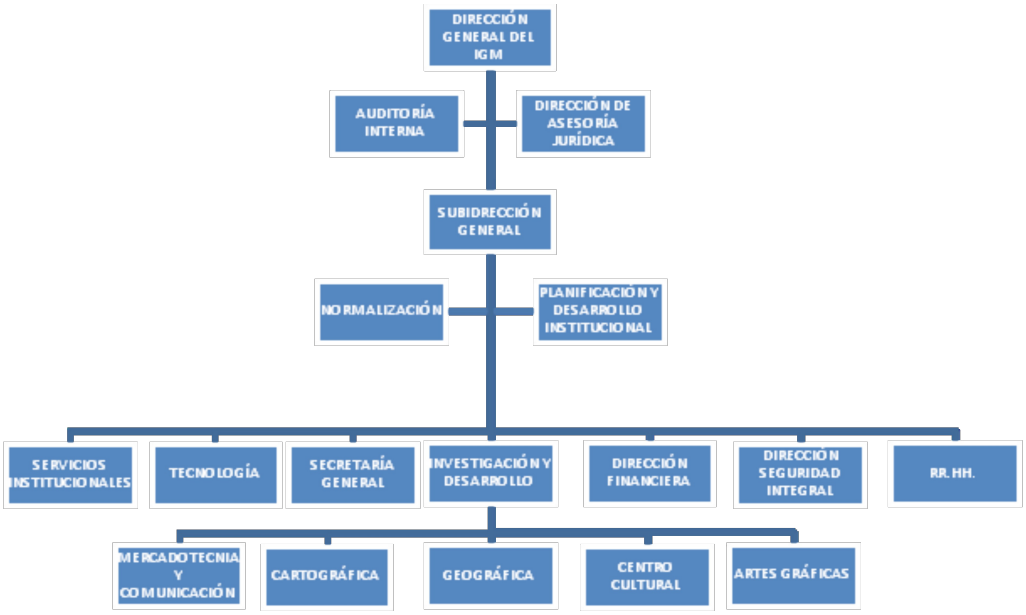

Gráfico 3: Organigrama Actual del IGM

En el organigrama se muestra que la institución es totalmente jerárquica donde las áreas directivas se encuentran en la cima, existen dos niveles de dirección general, cada una con sus áreas asesoras y al final se encuentran todas las áreas de apoyo.

Como aporte fundamental en la toma de decisiones y estructuración de procedimientos administrativos y operativos, en la institución se crean comités multidisciplinarios que aporten con ideas de mejora y creación de procesos para el manejo administrativo de la institución, así un ejemplo:

3.4 COMITÉ DE SEGURIDAD

Con resolución No. 2012-08-IGM-e del 14 de mayo del 2012 y firmada por el Tcrn. de CSM Ing. Milton Chamorro, Director del Instituto Geográfico Militar (E), se conformó el Comité de Seguridad integrado por: el Director quien presidirá dicho Comité, el Director de la Gestión de Seguridad Integral, el Jefe de la Gestión Tecnológica, el Jefe de la Gestión de Planificación y Desarrollo Institucional, el Jefe de la Gestión Cartográfica, el Jefe de la Gestión Geográfica, el Jefe de la Gestión de Artes Gráficas y el Jefe de Investigación y Desarrollo.

La primera sesión de Comité se celebró el 12 de junio del 2012 en el cual se tomaron ciertas decisiones, las cuales no fueron formalizadas por lo que nunca fueron implementadas, debido al cambio de autoridades no se han llevado a cabo más reuniones.

3.5 DEFINICIÓN DEL ALCANCE

Definir el alcance del SGSI es una de las más importantes decisiones que debe tomar cualquier institución que quiera implantar su propio sistema. En este sentido la ISO 27001, cláusula 4.2.1 literal a), es bastante precisa en dar las pautas a cualquier institución para definir su alcance.

En esencia, el alcance obedece a decisiones estratégicas de la institución. Siendo así y después de haber realizado el levantamiento y cruce de información con el personal directivo del instituto se determinó que el estudio deberá iniciar en la unidad de Gestión Cartográfica, la misma que decidió implantar el modelo en el proceso de "producción de la Gestión Cartográfica", debido a que en la actualidad está dando los primeros pasos hacia una certificación internacional ISO 9001, lo cual genera muchas ventajas para el IGM; además es el área que actualmente posee los procesos y proyectos documentados con proyección nacional como por ejemplo es la Cartografía integral del país.

Después de identificar la unidad funcional se procede a analizar los flujos de información para oportunamente identificar los activos de información los mismos que serán proporcionados por los usuarios a través de la encuesta generada.

3.5.1 FLUJOS DE PRODUCCIÓN DEL ÁREA CARTOGRÁFICA

Se anexan los flujos de los procesos cartográficos de producción, los cuales serán analizados para recomendar las mejoras más apropiadas. (ANEXO 3)

Como podemos apreciar en los flujos de los procesos de producción, cada uno genera un subproducto que alimenta al otro proceso, por ejemplo el subproceso "Restitución Fotogramétrica" genera el subproducto "Bloque fotogramétrico para CAD-SIG", el cual alimenta el subproceso "Estructuración CAD-SIG", así cada uno de ellos alimenta a otro hasta terminar con el "Almacenamiento en la base de datos", sea cual fuere su formato. Esta interrelación de los subprocesos podemos apreciarla de

mejor manera en el ANEXO 4. En cada uno de ellos podemos identificar los activos de información que intervienen, siendo éstos:

- Planificación y distribución de actividades (para cada proceso)
- Orden de producción
- Bloque fotogramétrico
- Bloque fotogramétrico restituido
- Directrices para restitución (para cada proceso)
- Corrección de errores (para cada proceso)
- Validación de la información (para cada proceso)
- Estructuración de la información
- Almacenamiento de información en proceso y terminal
- Modelo digital del terreno (MDT)
- Generación de curvas de nivel
- Migración del modelo a GBD (GeoDataBase)
- Catalogar el modelo en GDB
- Topología y criterios cartográficos
- Ortofotos (Mosaico de fotografías aéreas corregidas)
- Modelo semántico (pasos para un sistema informático SIG)
- Metadatos
- Generalizar hidrografía, vías, vegetación, planimetría, altimetría
- Base de datos Cartográfica
- Rectificación de fotografías
- Edición de zonas reservadas
- Información cartográfica, histórica, geográfica, fotográfica y legales
- Recopilar información en campo
- Estructuración de la información de acuerdo a las necesidades
- Features (clases geográficas como líneas, polígonos, etc.)
- Procesos de validación de la calidad

Es claro que en flujos de este tipo no se puede identificar todos los activos de información, porque su diseño ha sido elaborado para identificar procesos y almacenamientos y no lo correspondiente al talento humano y equipos o maquinaria, para ello se debe ahondar en entrevistas y cuestionarios directamente con el personal de mandos medios y personal operativo que son los que conocen lo necesario y lo indispensable.

Actualmente los procesos de producción de la Gestión Cartográfica se encuentran en proceso de certificación ISO 9001, por lo cual toda la documentación está bien sustentada y se han introducido mejoras en los flujos de los procesos normales de producción, se recomienda introducir procesos transversales de Seguridad de la Información con el fin de poder salvaguardar la información en sus distintas etapas, empezando por la información básica como es la fotografía aérea y terminando con los

mapas en sus distintos formatos. Es necesario establecer etapas de productos en proceso ya que muchos de dichos productos son vendidos o forman parte de la materia prima del siguiente proceso.

3.6 MÉTODO DE RECOPILACIÓN DE INFORMACIÓN

Tomando en cuenta que el objetivo básico de la Seguridad de la Información es salvaguardar la información crítica de la institución tanto física como la que viaja a través de la red, por lo cual el primer paso fue conocer la infraestructura física con la que cuenta el IGM y poder establecer recomendaciones a partir de lo recopilado, la Gestión de Tecnología proporcionó en esta etapa temprana del análisis un diagrama básico de la red interna del IGM (ANEXO 1).

El siguiente paso para poder tener un panorama de la situación actual de la institución es realizar encuestas abiertas al personal involucrado del área (ANEXO 2), e interpretar los resultados de acuerdo al objetivo de la encuesta.

3.7 ANÁLISIS DE LOS RESULTADOS DE LAS ENCUESTAS

PREGUNTA 1: *¿Conoce usted el término Seguridad de la Información?*

Tabla 7:
Tabulación de la pregunta No.1 - ¿Conoce usted el término Seguridad de la Información?

RESPUESTA	ENCUESTADOS	%
SI	6	55%
NO	0	0%
NO CONTESTO	5	45%
TOTAL	11	100%

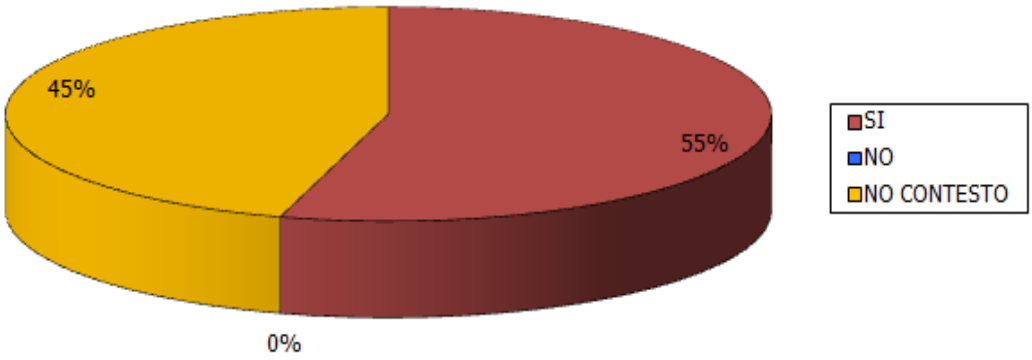

Gráfico 4: Tabulación de la pregunta 1 - ¿Conoce usted el término Seguridad de la Información?

Interpretación de los datos: La pregunta 1 fue una pregunta cerrada para conocer si las personas encuestadas conocían el término Seguridad de la Información; de 11 personas encuestadas, 6 respondieron que sí conocen del tema constituyendo el 55%, 0 contestaron que no conocen constituyendo el 45% y 5 prefirieron no responder constituyendo el 45%.

PREGUNTA 2: *Dé un breve concepto sobre Seguridad de la Información*

Tabla 8:
Tabulación de la pregunta No.2 - Dé un breve concepto sobre Seguridad de la Información

CONCEPTOS SEGURIDAD
Salvaguardar todo lo relacionado a información sea tecnológica o manualmente
Son todas las medidas que se toman para precautelar la confidencialidad de la información
Mecanismos para evitar acceso no deseado a información crítica
Medidas que se adoptan para la protección de la información: software especial a fin de evitar su fuga, su alteración, pérdida
Protección y prevención en caso de desastres informáticos los datos de una organización, empresa, usuario, etc.
Desarrollar y aplicar todas las medidas necesarias para proteger la fuga, plagio o pérdida de la información.

Interpretación de los datos: De los conceptos emitidos por los encuestados vemos que todos tienen una conceptualización del término que es la de proteger la confidencialidad, alteración o pérdida de la información sea a través de medios digitales o físicos. Esto nos permitirá tener un punto de partida en cuanto a lo que establece la norma.

PREGUNTA 3: *¿Ha tomado acciones para salvaguardar su información importante?*

Tabla 9:
Tabulación de la pregunta No.3 - ¿Ha tomado acciones para salvaguardar su información importante?

RESPUESTA	ENCUESTADOS	%
SI	6	55%
NO	0	0%
NO CONTESTO	5	45%
TOTAL	11	100%

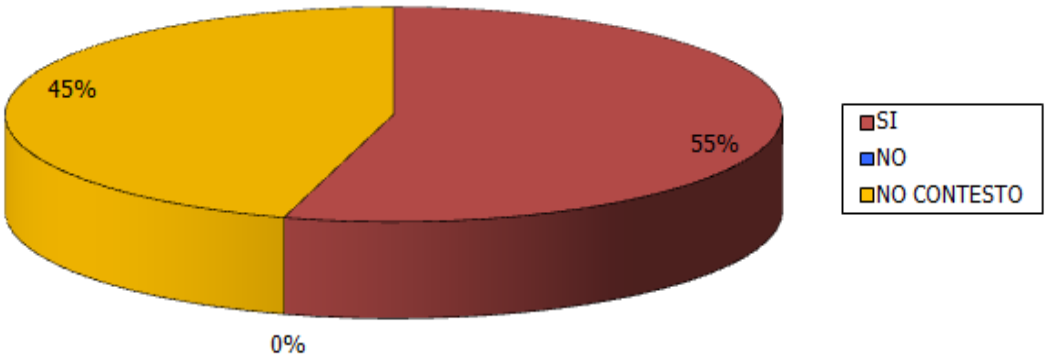

Gráfico 5: Tabulación de la pregunta 3 - ¿Ha tomado acciones para salvaguardar su información importante?

Interpretación de los datos: La pregunta número 3 fue una pregunta cerrada para conocer si las personas encuestadas han tomado acciones efectivas para proteger su información; de 11 personas encuestadas, 6 respondieron que SI han tomado previsiones para salvaguardar su información constituyendo el 55% y 5 encuestados no contestaron la pregunta.

PREGUNTA 4: *¿Qué acciones ha tomado en su trabajo?, enumere las 5 más importantes.*

Tabla 10:
Tabulación de la pregunta No.4 - ¿Qué acciones ha tomado en su trabajo?, enumere las 5 más importantes.

ACCIONES QUE SE HAN TOMADO
Respaldar en discos externos
Desinfectar los discos duros del computador
No mantener información delicada a la vista de todos
Pedir compartir información por usuarios
Acceso limitado a unidades de respaldo en cinta
Implementación de procedimientos para duplicación de información
Implementación de procedimientos para entrega de información a usuarios
No entregar claves de acceso
Cambiar claves permanentemente
Colocar clave a la máquina
Colocar clave en algunas carpetas
Bloquear el acceso a los puerto USB y grabador de CD
Evitar compartir las carpetas donde la información reside
Evitar el acceso de usuarios ajenos dentro de los equipos informáticos

Interpretación de los datos: Las acciones que los encuestados han tomado para la protección de su información en un porcentaje del 50%, es sacar respaldos en unidades

externas o a través de la red y almacenar su información sensible en forma segura. El otro 50% de las acciones no son particulares, son políticas que establece la Gestión de Tecnología como es el manejo de usuarios y control de accesos.

PREGUNTA 5: *¿Ha sufrido alguna pérdida o mal uso de su información por parte de terceros en su trabajo?*

Tabla 11:
Tabulación de la pregunta No.5 - ¿Ha sufrido alguna pérdida o mal uso de su información por parte de terceros en su trabajo?

RESPUESTA	ENCUESTADOS	%
SI	2	18%
NO	4	36%
NO CONTESTARON	5	46%
TOTAL	11	100%

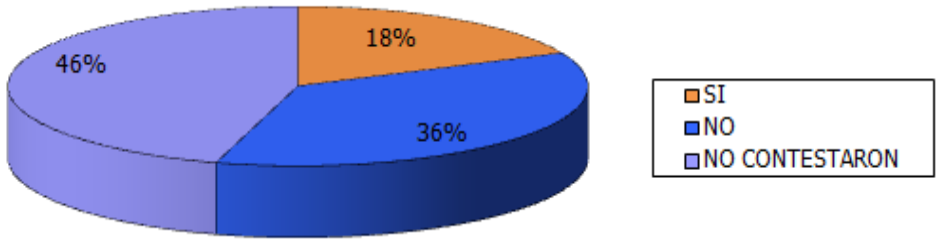

Gráfico 6: Tabulación de la pregunta 5 - ¿Ha sufrido alguna pérdida o mal uso de su información por parte de terceros en su trabajo?

Interpretación de los datos: Según las respuestas de los encuestados solo el 18% han sufrido incidentes de seguridad, el 36% NO ha sufrido incidentes de seguridad y el 45% NO respondieron la pregunta.

PREGUNTA 6: *¿Qué clase de incidentes ha sufrido?*

Tabla 12:
Tabulación de la pregunta No.6 - ¿Qué clase de incidentes ha sufrido?

RESPUESTA	ENCUESTADOS	%
Pérdida información importante	1	9%
Acceso no autorizado a su información	3	27%
No han sufrido incidentes	2	18%
No contestaron	5	45%
TOTAL	11	100%

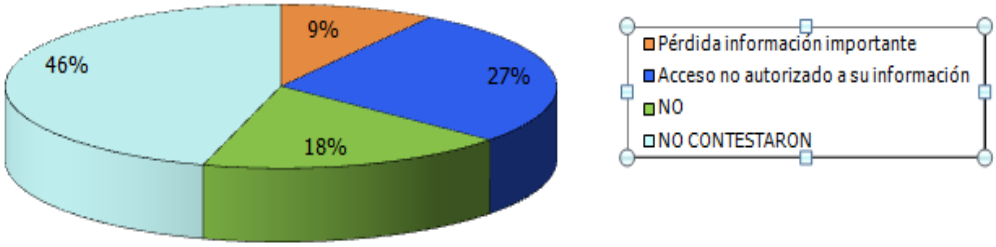

Gráfico 7: Tabulación de la pregunta 6 - ¿Qué clase de incidentes ha sufrido?

Interpretación de los datos: Se puede observar que el acceso no autorizado a información sensible representa el 27%, es el incidente más recurrente dentro del personal encuestado, el 9% responde a la pérdida de información importante como otro de los incidentes que ha sufrido, y el 18% de los encuestados responde que no ha sufrido incidentes.

PREGUNTA 7: *¿Ha recibido alguna capacitación interna o externa sobre Seguridad de la Información?*

Tabla 13:
Tabulación de la pregunta No.7 - ¿Ha recibido alguna capacitación interna o externa sobre Seguridad de la Información?

RESPUESTAS	ENCUESTADOS	%
SI	2	18%
NO	4	36%
NO CONTESTARON	5	46%
TOTAL	11	100%

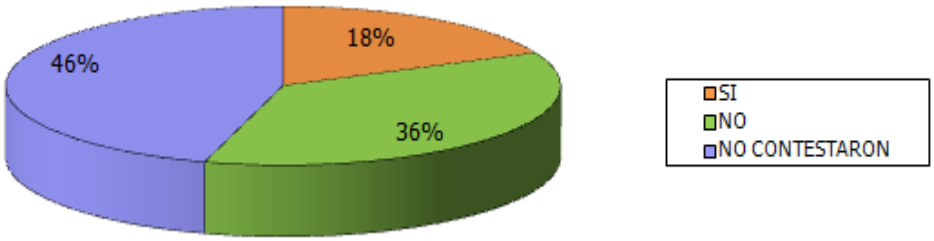

Gráfico 8: Tabulación de la pregunta 7 - ¿Ha recibido alguna capacitación interna o externa sobre Seguridad de la Información?

Interpretación de los datos: El no haber recibido capacitación formal o talleres de seguridad posee el mayor porcentaje con un 36%. El 36% contestó que no han tenido ninguna capacitación y el 45% decidió no contestar.

PREGUNTA 8: *¿Qué normativas internas conoce usted que ha difundido el IGM para salvaguardar su información tanto en forma física como lógica?*

Tabla 14:
Tabulación de la pregunta No.8 - ¿Qué normativas internas conoce usted que ha difundido el IGM para salvaguardar su información tanto en forma física como lógica?

NORMATIVA INTERNAS
Seguridad de hardware
Seguridad de software
Solicitar un espacio en servidores para guardar información importante
Seguridad de usuarios
Usos de internet
Uso de correo electrónico
No utilizar carpetas compartidas para mantener información confidencial
Cambiar claves permanentemente
No entregar claves de acceso
Bloqueo de los accesos a puertos de grabación
Suspender el uso de puerto USB
Suspender la grabación de CD

Interpretación de los datos: El momento de recopilar los resultados de la pregunta abierta, nos encontramos con una serie de normativas que no son generales para toda la institución, son normativas particulares para cada área y usuario dependiendo de sus necesidades y se redactan en forma general sin particularizar sus bondades como es el

caso de *Usos del Internet*, donde no se logran identificar lo razonable de dicha normativa.

PREGUNTA 9: *¿Aplica usted dichas normativas en su trabajo diario?*

Tabla 15:
Tabulación de la pregunta No.9 - ¿Aplica usted dichas normativas en su trabajo diario?

RESPUESTAS	ENCUESTADOS	%
SI	5	46%
NO	1	9%
NO CONTESTARON	5	45%
TOTAL	11	100%

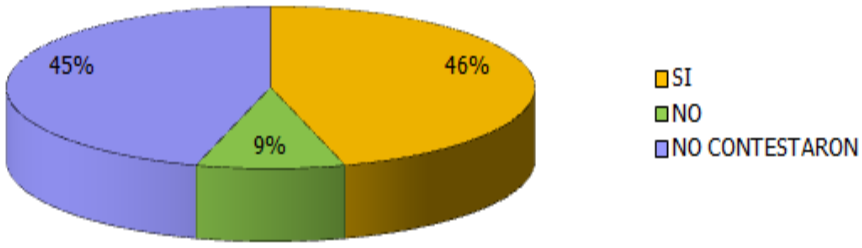

Gráfico 9: Tabulación de la pregunta 9 - ¿Aplica usted dichas normativas en su trabajo diario?

Interpretación de los datos: El 46% de personas afirman que usan las normativas internas, y el 9% no las usan.

PREGUNTA 10: *Indique las 3 más importantes normativas que usted aplica*

Tabla 16:
Tabulación de la pregunta No.10 - Indique las 3 más importantes normativas que usted aplica

NORMATIVA
No uso de carpetas compartidas
No entregar claves
Bloqueo de accesos a puertos de grabación
Seguridad de usuarios
Usos de internet
Uso de correo electrónico
Evitar la creación de carpetas compartidas con acceso a todos
Respaldo de información definitiva en servidor y equipo
Antivirus actualizado
Uso de cifrado y contraseñas de acceso a la información
Respaldo magnético de la información

Interpretación de los datos: Los encuestados detallan las normativas que posee la institución y el 60% de ellas son impuestas a través de software utilitario por parte de la Gestión de Tecnología, son pocas las normativas particulares que deberían ser evaluadas en su cumplimiento y eficacia.

PREGUNTA 11: *¿Qué seguridades físicas se han implantado en el IGM que usted considere importantes? Enumere las 5 más importantes.*

Tabla 17:
Tabulación de la pregunta No.11 - ¿Qué seguridades físicas se han implantado en el IGM que usted considere importantes? Enumere las 5 más importantes.

SEGURIDADES FISICAS
Revisiones por parte del personal militar
Asignación de cada computador a un usuario
Data Center
Cámaras de seguridad
Seguridad contra incendios
Acceso mediante tarjetas
Creación de la Unidad de Seguridad
Bloqueo de unidades de grabación
Deshabilitación de puertos USB
Acceso restringido a los servidores

Interpretación de los datos: De acuerdo a lo que establece la norma se considera que el 70% de las respuestas constituyen seguridades físicas, y el 30% son lógicas; en consecuencia, se debería concientizar al personal sobre los conceptos de seguridad de cada tipo para que el momento de detectar un incidente sepan a qué área funcional deben reportarla y evitar problemas peores por no solucionarlo por la persona competente con la premura necesaria.

PREGUNTA 12: *¿Qué seguridades lógicas se han implantado en el IGM que usted considere importantes? Enumere las 5 más importantes.*

Tabla 18:
Tabulación de la pregunta No.12 - ¿Qué seguridades lógicas se han implantado en el IGM que usted considere importantes? Enumere las 5 más importantes.

SEGURIDADES LOGICAS
Desconoce
Parches en programa de uso común
Regulaciones en uso del internet
Actualización del antivirus
Regulaciones en uso del correo electrónico
Instalación de software únicamente por personal autorizado
Bloqueo de puertos USB
Control de acceso mediante servidor de dominio cuentas de usuario

Interpretación de los datos: Las respuestas de esta pregunta abierta se orientan mejor a lo que son seguridades lógicas, pero una vez más el que exista personal que desconoce las normativas crea una brecha importante dentro del control de la seguridad de la información.

PREGUNTA 13: *¿Qué mejoras propondría usted para mejorar las seguridades físicas y lógicas del IGM.*

Tabla 19:
Tabulación de la pregunta No.13 - ¿Qué mejoras propondría usted para mejorar las seguridades físicas y lógicas del IGM.

MEJORAS
Control biométrico al data center
Limitaciones a ciertos servicios de aplicaciones

Interpretación de los datos: Debido a que no existe una capacitación formal sobre la seguridad de la información, las personas no sienten que la seguridad es tarea de todos y todos podemos recomendar medidas en virtud de los incidentes que se han sufrido dentro de la institución.

PREGUNTA 14: *¿Conoce usted a las personas responsables de cada proceso dentro de su área?*

Tabla 20:
Tabulación de la pregunta No.14 - ¿Conoce usted a las personas responsables de cada proceso dentro de su área?

REPUESTAS	ENCUESTADOS	%

SI	5	45%
NO	0	0%
NO CONTESTARON	6	55%
TOTAL	11	100%

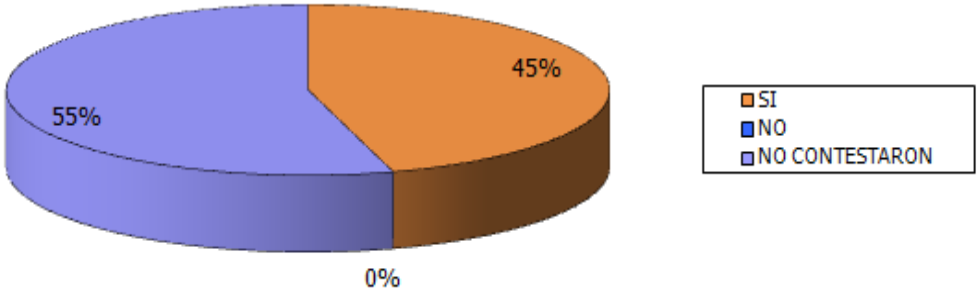

Gráfico 10: Tabulación de la pregunta 14 - ¿Conoce usted a las personas responsables de cada proceso dentro de su área?

Interpretación de los datos: Esta pregunta cambia el contexto en el que se estaba manejando las preguntas anteriores, ya que a partir de aquí se desea aclarar la confiabilidad de las respuestas anteriores donde se afirmaba que se usaban normativas y se conocía conceptos de seguridad. La pregunta 14 pretende establecer que además de conocer normativas también es necesario conocer a los dueños de procesos para poder informar con la premura del caso sobre incidentes de seguridad a las personas competentes y que la solución pueda fluir en forma más eficiente. El 45% afirmó que conoce los responsables de los procesos que interactúan directamente con sus actividades.

PREGUNTA 15: *¿Conoce que información le proporciona cada responsable de proceso para su trabajo?*

Tabla 21:
Tabulación de la pregunta No.15 - ¿Conoce que información le proporciona cada responsable de proceso para su trabajo?

RESPUESTAS	ENCUESTADOS	%
SI	4	36%
NO	1	9%
NO CONTESTARON	6	55%
TOTAL	11	100%

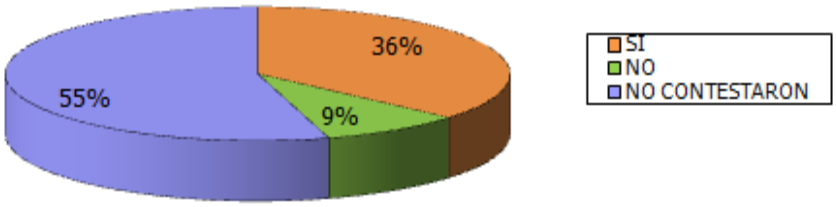

Gráfico 11: Tabulación de la pregunta 15 - ¿Conoce que información le proporciona cada responsable de proceso para su trabajo?

Interpretación de los datos: Es importante establecer con esta pregunta que el 36% de los encuestados conocen qué pedir y qué se puede obtener de cada fuente de información, no solo en forma digital sino también en forma impresa o manual que permita que fluyan sus actividades productivas y administrativas en forma normal, sin interrupción.

PREGUNTA 16: *Liste 3 responsables de proceso con la información que le proporciona*

Tabla 22:
Tabulación de la pregunta No.16 - Liste 3 responsables de proceso con la información que le proporciona

RESPONSABLES	*INFORMACIÓN*
Tecnología	Manejo de redes, antivirus, página web, correo electrónico, sistema interno
Alexis Bedón	Imágenes
Responsable Cartografía	Imágenes, restitución, archivos dgn, digitalización y ortofotos, archivos shape, geodatabase

Interpretación de los datos: El 20% de personas saben que necesitan de la ayuda de personal técnico para sus requerimientos de información, pero no están claros en que información proporcionan cada uno y por lo tanto no sabe cómo puede solventar sus problemas con incidentes de seguridad de la información, el 80% está claro en lo que necesita de cada dueño de proceso que le permita agilitar sus actividades normales en la institución.

PREGUNTA 17: *Liste los 5 elementos fundamentales que usa en su trabajo sin los cuales no podría cumplir sus funciones, sean tangibles o intangibles*

Tabla 23:
Tabulación de la pregunta No.17 - Liste los 5 elementos fundamentales que usa en su trabajo sin los cuales no podría cumplir sus funciones, sean tangibles o intangibles

ACTIVOS	*CLASIFICACION*
Computador, impresoras, medios de almacenamiento	EQUIPOS
Internet, red corporativa, privilegios de acceso	SERVICIOS
Paquetes informáticos	PAQUETES
Herramientas para mantenimiento, kit mantenimiento preventivo, Stock de repuestos	AUXILIAR
Archivos personales, reportes impresos o digitales	INFORMACION

Interpretación de los datos: El resultado de dicha pregunta se clasificó tomando en cuenta los conceptos de MAGERIT para su identificación, se puede apreciar que todo lo respecto a equipos y parcialmente información fue tomado en cuenta para la lista, pero no se listó como parte esencial al talento humano que en todas las actividades tiene una gran importancia.

PREGUNTA 18: *Enumere los 5 principales riesgos que usted considera pone en peligro la ejecución normal de su actividad*

Tabla 24:
Tabulación de la pregunta No.18 - Enumere los 5 principales riesgos que usted considera pone en peligro la ejecución normal de su actividad

RIESGOS	*VALORACIÓN*
Energía Eléctrica	ALTO
Red Corporativa, internet	ALTO
Falta de cuidado en revisión de documentos legales , enviar por escrito la solicitud de todas las revisiones	ALTO
Incendios, riesgos climáticos	ALTO
Robo o substracción de equipos e información reservada	ALTO

Interpretación de los datos: Una vez que se tabuló los resultados de la pregunta, se valoró su respuesta en cuanto a su probabilidad e impacto. Los resultados mostraron que el 75% de los riesgos son externos a la institución y estos deben ser aceptados o transferidos.

PREGUNTA 19: *¿Qué acciones ha tomado para evitar los riesgos anteriores?*

Tabla 25:
Tabulación de la pregunta No.19 - ¿Qué acciones ha tomado para evitar los riesgos anteriores?

ACCIONES PARA EVITAR RIESGOS
Mantenimiento físico y lógico permanente
Concientizar al usuario el buen uso de los equipos
Verificación de voltajes de alimentación
Comprobar la comunicación entre los puntos de red
Coordinación de instalaciones eléctricas
Extintores
Coordinación con el departamento de Seguridad Integral
Adoptar posturas correctas

Interpretación de los datos: El 65% de las acciones tomadas son controles que lo realiza personal técnico de mantenimiento general y de sistemas, y las acciones restantes son particulares.

PREGUNTA 20: *¿Qué acciones adicionales cree usted que son necesarias para evitar riesgos?*

Tabla 26:
Tabulación de la pregunta No.20 - ¿Qué acciones adicionales cree usted que son necesarias para evitar riesgos?

ACCIONES ADICIONALES
No utilizar dispositivos de almacenamiento masivo
Capacitación en cuanto a los riesgos laborales
Simulacro en caso de desastres ambientales e incendios
Capacitación a usuarios finales en el manejo de información reservada

Interpretación de los datos: Las acciones adicionales son fruto de incidentes de seguridad que sufrieron los encuestados en sus actividades diarias y recomiendan se tome en cuenta ciertos procesos que alguien más debería ejecutar a nivel de gestión directiva, lo preocupante es que son muy pocas las recomendaciones adicionales ya que solo el 20% de los encuestados respondieron a esta pregunta.

PREGUNTA 21: *¿Quién cree usted que debería gestionar las acciones adicionales?*

Tabla 27:
Tabulación de la pregunta No.21 - ¿Quién cree usted que debería gestionar las acciones adicionales?

ACCIONES ADICIONALES	*RESPONSABLE*
No utilizar dispositivos de almacenamiento masivo	Infraestructura
Capacitación en cuanto a los riesgos laborales	Jefe de Gestión, Responsable de cada área, todo el personal
Simulacro en caso de desastres ambientales e incendios	Jefe de Gestión, Responsable de cada área, todo el personal
Capacitación a usuarios finales en el manejo de información reservada	Jefe de Gestión, Responsable de cada área, todo el personal

Interpretación de los datos: Las actividades recomendadas deben tener como responsable un nivel directivo ya que de no contar con esa autoridad no se va a poder lograr el fin propuesto.

PREGUNTA 22: *¿Hay alguna inquietud adicional que no se ha preguntado en esta encuesta? Si es así, por favor, díganos de que se trata.*

Interpretación de los datos: A esta pregunta no respondió nadie.

Del análisis de las preguntas desde la No. 18 hasta la 20, de los riesgos encontrados por los usuarios se deben adicionar los riesgos propios de instituciones públicas cuyas políticas y presupuesto vienen directamente del Gobierno Central del país, como son:

- Recorte presupuestario

- Procedimientos establecidos para las adquisiciones a través del INCOP lo que produce, en muchos casos, demoras
- Regulaciones para pagos a través del eSigef
- Auditorías externas
- Respeto al medio ambiente
- Personal calificado acorde a los avances del medio
- Capacitación al personal en avances tecnológicos
- Competencia con costo y tiempo más bajos ya que la empresa privadas tiene menos restricciones
- Cambios en procesos acorde a nuevas ideologías, lo que deviene en cambios en las personas
- Avances tecnológicos costosos en la industria

El listado de riesgos se clasificará en altos, medios y bajos de acuerdo a su probabilidad e impacto y al apetito de riesgo que tenga la alta gerencia de acuerdo al nivel de madurez que tenga la institución frente a la gestión de riesgo.

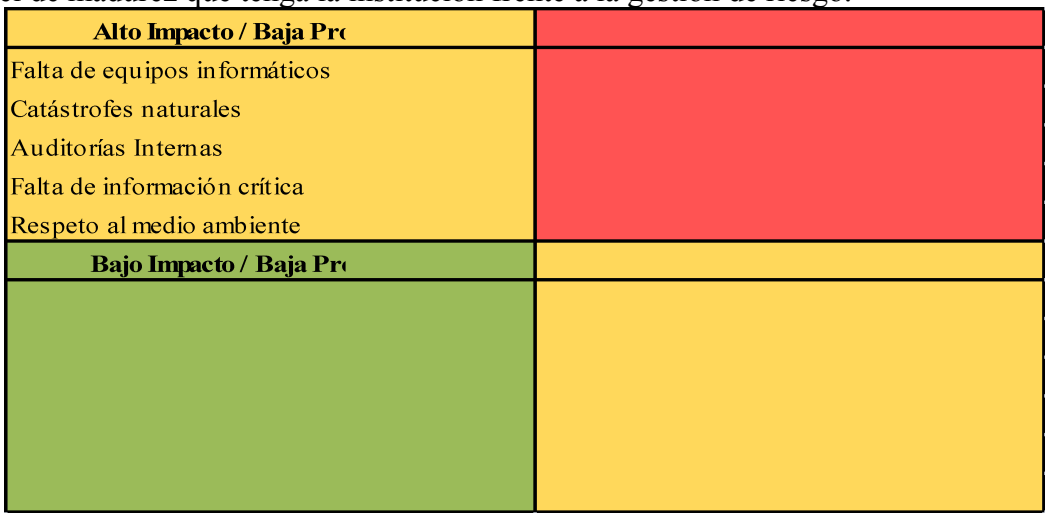

Gráfico 12: Resultado de la evaluación de riesgos
Fuente: COSO RM

Interpretación de los datos: La sección de color tomate identifica los riesgos que deben ser considerados a corto plazo para la generación de controles que permitan su mitigación y minimización del impacto y probabilidad. En el caso de la sección de color rojo, son riesgos que talvez no puedan ser extinguidos pero deberían ser tomados en cuenta para que en un porcentaje adecuado sean asumidos o transferidos de ser el caso, pero crear controles de forma inmediata que permita a la institución manejarlos y evitar que estos generen más problemas de los necesarios. Los riesgos del área verde pueden

ser asumidos sin causar mayores estragos porque no tienen ni gran impacto ni alta probabilidad de ocurrencia.

3.8 ANÁLISIS DE LA BRECHA

Una vez establecida la situación actual, el siguiente paso es definir a donde se quiere llegar, por lo cual es necesario analizar en qué contexto nacional nos encontramos y cuáles son los lineamientos básicos con los que debemos iniciar el proceso del Modelo de Gestión.

El primer paso es listar todos los estándares internacionales ISO 27000 que la institución deberá tomar en cuenta para el establecimiento del SGSI. Estándares que en forma posterior podrá garantizar una certificación.

Tabla 28:
Estándares internacionales

ESTÁNDAR	*JUSTIFICATIVO*	*ALCANCE*
ISO 27001	Requisitos para el SGSI	Gestión Cartográfica – proceso de producción
ISO 27002	Código de práctica para el SGSI	Gestión Cartográfica – proceso de producción
ISO 27005	Gestión de riesgos para el SGSI	Gestión Cartográfica – proceso de producción

Interpretación de los datos: Este cuadro resume los estándares internacionales ISO 27000 que van a formar parte del análisis a efectuar para evaluar el grado de madurez de la institución.

Una vez que se tiene claro que estándares deberán ser utilizados, se debe hacer un checklist para determinar el nivel de cumplimiento frente al estándar, donde la evaluación será valorada en una escala del 0 (deficiente) al 5 (óptimo); es decir, deficiente si no existe nada implantado y 5 si todos los requerimientos se cumplen, así:

Tabla 29:
Evaluación de cumplimiento de la ISO 27001

ESTÁNDAR	*REQUERIMIENTO*	*EVALUACIÓN*
ISO 27001	4 Creación y gestión del SGSI	0
	5 Responsabilidad de la Dirección	3
	6 Auditorías internas del SGSI	2
	7 Revisión del SGSI por parte de la Dirección	2

	8 Mejora del SGSI	0

Interpretación de los datos: Tomando en cuenta las encuestas realizadas se evaluó cada una de las secciones de la ISO 27001, colocando valores desde 0 a 5, siendo 0 el más bajo y 5 el valor más alto de cumplimiento frente a la norma, promediando un nivel bajo (ANEXO 5).

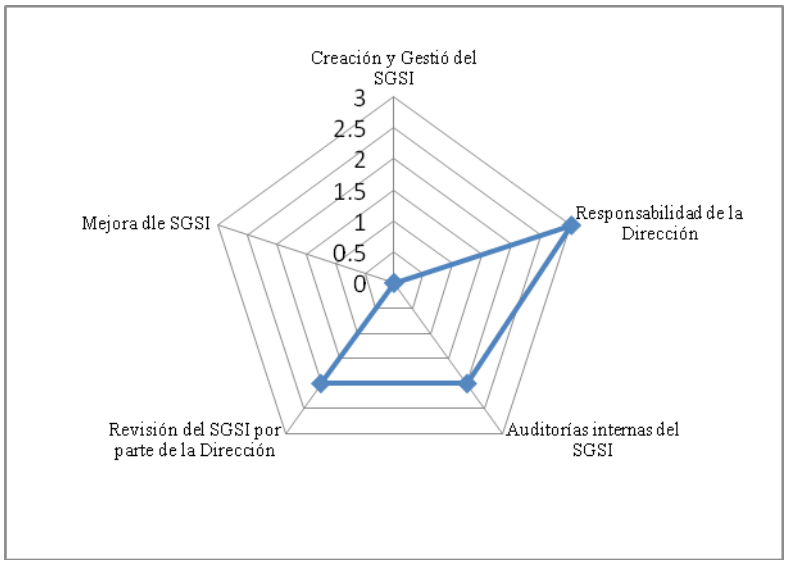

Gráfico 13: Evaluación de la ISO 27001

Tabla 30:
Evaluación de cumplimiento de la ISO 27002

ESTÁNDAR	*ESTÁNDAR*	*EVALUACIÓN*
ISO 27002	4 Evaluación y tratamiento del riesgo	no
	5 Políticas de Seguridad	no
	6 Organización de la Seguridad de la Información	no
	7 Gestión de Activos de Información	no
	8 Seguridad de los Recursos Humano	no

Interpretación de los datos: Tomando en cuenta las encuestas realizadas se evaluó cada una de las secciones de la ISO 27002, valorando con un SI o un NO, el cumplimiento o la falta de él, concluyendo que ninguna de las secciones fueron cumplidas.

Tabla 31:
Evaluación de cumplimiento de la ISO 27005

ESTÁNDAR	*ESTÁNDAR*	*EVALUACIÓ*

		N
ISO 27005	6 Visión general del proceso de gestión del riesgo de la Seguridad de la Información	no
	7 Establecimiento del contexto	no
	8 Valoración del riesgo	no
	9 Tratamiento del riesgo	no
	10 Aceptación del riesgo	no
	11 Comunicación de los riesgos	no
	12 Monitoreo y revisión del riesgo	no

Interpretación de los datos: Tomando en cuenta las encuestas realizadas se evaluó cada una de las secciones de la ISO 27005, valorando con un SI o un NO, el cumplimiento o la falta de él, concluyendo que ninguna de las secciones fueron cumplidas.

Al realizar el análisis global de los estándares escogidos se mostró que el nivel de madurez de la institución es bajo, por lo cual no es necesario realizar el análisis detallado de los requerimientos de los estándares.

Por último se recopilará toda la información sobre normativas o políticas que salvaguarden la Seguridad de la Información en el IGM, las mismas que han sido emitidas a través de resoluciones o simples documentos aprobados por la dirección que en algún momento entraron en vigencia y que a través del tiempo fueron olvidadas o reemplazadas por otras que generó una nueva dirección.

Una vez que se recopile dicha información, ésta deberá ser tabulada y analizada para evitar duplicaciones o posibles obsolescencias en el tiempo o por el cambio de normativas nacionales o internas. Esta lista también debe ser validada con las norma ISO 27001 para evitar contraposiciones y poder estandarizar los procedimientos internos con normas internacionales. Una vez depurada la lista y validada en Comité de Seguridad se deberá formalizar en un solo documento consolidado, el cual una vez aprobado será difundido en todo el IGM con el fin de poder verificar su eficiencia y oportunidad en los procesos normales del instituto.

Tabla 32:
Evaluación de controles implantados en el IGM

POLÍTICA	*FECHA VIGENCIA*	*FECHA ACTUALIZACIÓN*	*EVALUACIÓN ?*
Realizar actividades de mantenimiento preventivo de	2009	2011	SI

POLÍTICA	*FECHA VIGENCIA*	*FECHA ACTUALIZACIÓN*	*EVALUACIÓN ?*
equipos informáticos			
Instalación y actualización del antivirus corporativo	2009	2012	SI
Todo mantenimiento y reparación de equipos informáticos debe ser canalizadas a través de la Gestión de Tecnología	2009	2011	NO
Concientizar a todo el personal sobre la necesidad de crear usuarios y contraseñas y que éstas se cambien periódicamente	2009		SI
Clasificar la documentación crítica y crear lugares específicos para su almacenamiento	2009		NO
Realizar controles periódicos de las imágenes obtenidas desde las oficinas de seguridad	2009	2012	SI
Trasmisión de información con claves de seguridad	2009		NO
El personal que labore en el Centro de Comunicaciones debe ser personal idóneo con las capacidades necesarias para el manejo de comunicaciones	2009	2011	SI
Realizar mantenimiento periódicos en el Centro de Comunicaciones	2009		SI
Las actividades de cada persona del Centro de Comunicaciones deben estar perfectamente bien definidas para evitar superposición de funciones y responsabilidades	2009 2009	2011	NO
Debe realizar una instalación a tierra y darle mantenimiento para evitar descargas eléctricas y daños de equipos	2009		NO
Evitar el uso de software no confiables en los equipos de la red	2009	2012	NO
La manipulación de información cartográfica debe ser bajo procedimientos de seguridad para evitar fugas	2008	2012	NO SI
Mantener todos los equipos informáticos dentro de un dominio específico para poder colocar políticas de seguridad en forma conjunta	2008	2011	SI
Crear usuarios de acceso a la información compartida	2008	2011	SI
Crear usuarios de acceso a los	2008	2011	SI

Continua …

POLÍTICA	*FECHA VIGENCIA*	*FECHA ACTUALIZACIÓN*	*EVALUACIÓN ?*
servicios de la intranet			
Se bloqueará el acceso de cualquier usuario a cualquier equipo, cada usuario tendrá acceso solo al equipo que se le asigne y en casos especiales a otros previa autorización	2008	2011	SI
Eliminar en forma periódica la información almacenada en lugares públicos	2008	2012	NO
Determinación de sanciones acorde a las faltas cometidas	2008		NO
Los usuarios deben bloquear o cerrar la sesión en sus equipos cuando ya no se vaya a utilizar el equipo por un lapso de tiempo	2008		SI
Bloqueo de acceso a dispositivos de almacenamiento masivo como flash, cds o dvds	2009	2012	NO
La Gestión Tecnológica en coordinación con la Sección de Activos Fijos deben mantener un registro de los activos informáticos, así como su ubicación y actualización	2009		SI
Deben colocarse restricciones de acceso físico a las áreas críticas tales como Centro de Computo, Servidores, etc.	2009		SI
Las instalaciones de los Centros de Computo deben tener equipos de detección de humo y equipos de aire acondicionado	2009	2012	NO
Se debe mantener la documentación necesaria sobre las configuraciones básicas de los servidores por posibles incidentes	2009		NO
Debe crearse registros con las novedades del mantenimiento físico y lógico de los equipos informáticos	2009		SI
Mantener todos los servidores con los parches y actualizaciones que sean necesarios para evitar interrupción de servicios	2009		SI
Mantener un constante monitoreo de la red para identificar posibles ataques a través de equipos informáticos	2011		SI
Crear grupos para fijar cuotas de correo limitando el uso del mismo	2009	2011	SI

Continua …

POLÍTICA	*FECHA VIGENCIA*	*FECHA ACTUALIZACIÓN*	*EVALUACIÓN ?*
Bloquear el acceso de internet a páginas que se consideren peligrosas para la institución	2009	2012	SI
Negar el acceso de correos spam y que incluyan adjuntos peligrosos	2011	2012	SI
Crear usuarios especiales para accesos remotos	2011		NO

Interpretación de los datos: Se hizo una recopilación de las políticas de seguridad que el IGM ha implantado en los últimos 5 años, su fecha de actualización y evaluación de existir, y se llegó a la conclusión que muchas de ellas no han tenido revisión y casi ninguna ha formado parte de un análisis de evaluación o auditoría interna o externa.

Como es prudente, las normativas evaluadas y depuradas no englobarán todos los lineamientos de la ISO 27001, así que el siguiente paso constituye el análisis por etapas de la norma ISO 27001 para ir elaborando nuevas normativas y políticas que protejan el IGM, así como todos los posibles campos de acción. Se aclara que deberá irse ejecutando por etapas ya que resultará un trabajo bastante complejo y largo para querer proteger a todo el instituto en un solo paso, se deberá iniciar con las áreas productivas que se considera de mayor riesgo en fuga o inconsistencia de información, para después ir con las menos complejas como por ejemplo las áreas administrativas.

Para concluir el análisis de la situación actual, se verificará cuan apegados a la norma 27002 están los controles que actualmente están implantados en el IGM, y con este resultado se realizarán las recomendaciones pertinentes en el siguiente capítulo.

Tabla 33:
Evaluación de controles del IGM de acuerdo a lo que establece la ISO 27002

POLÍTICA	*CLÁUSULA*	*VALORACIÓN CUMPLIMIENTO*
Realizar actividades de mantenimiento preventivo de equipos informáticos	9.2.4	5
Instalación y actualización del antivirus corporativo	10.4	5
Todo mantenimiento y reparación de equipos informáticos debe ser canalizadas a través de la Gestión de Tecnología	6	3
Concientizar a todo el personal sobre la necesidad de crear usuarios y contraseñas y que éstas se cambien periódicamente	11.2.3	2
Clasificar la documentación crítica y crear lugares específicos para su almacenamiento	5.1.1	2

Continua …

POLÍTICA	CLÁUSULA	VALORACIÓN CUMPLIMIENTO
Realizar controles periódicos de las imágenes obtenidas desde las oficinas de seguridad	9.1.3	2
Trasmisión de información con claves de seguridad	11.6.1	1
El personal que labore en el Centro de Comunicaciones debe ser personal idóneo con las capacidades necesarias para el manejo de comunicaciones	8.1.2	3
Realizar mantenimiento periódicos en el Centro de Comunicaciones	9.2.4	4
Las actividades de cada persona del Centro de Comunicaciones deben estar perfectamente definidas para evitar superposición de funciones y responsabilidades	8.1.1	3
Debe realizar una instalación a tierra y darle mantenimiento para evitar descargas eléctricas y daños de equipos	9.1.4	4
Evitar el uso de software no confiables en los equipos de la red	15.1.2	2
La manipulación de información cartográfica debe ser bajo procedimientos de seguridad para evitar fugas	12.5.4	4
Mantener todos los equipos informáticos dentro de un dominio específico para poder colocar políticas de seguridad en forma conjunta	10.6	2
Crear usuarios de acceso a la información compartida	10.8	5
Crear usuarios de acceso a los servicios de la intranet	11.4	4
Se bloqueará el acceso de cualquier usuario a cualquier equipo, cada usuario tendrá acceso solo al equipo que se le asigne y en casos especiales a otros previa autorización	11.3	5
Eliminar en forma periódica la información almacenada en lugares públicos	11.3	4
Determinación de sanciones acorde a las faltas cometidas	8.2.3	2
Los usuarios deben bloquear o cerrar la sesión en sus equipos cuando ya no se vaya a utilizar el equipo por un lapso de tiempo	11.3	3
Bloqueo de acceso a dispositivos de almacenamiento masivo como flash, cds o dvds	11.4	4
La Gestión Tecnológica en coordinación con la Sección de Activos Fijos deben mantener un registro de los activos informáticos, así como su ubicación y actualización	7.1	4
Deben colocarse restricciones de acceso físico a las áreas críticas tales como Centro de Cómputo, Servidores, etc.	9.1	5
Las instalaciones de los Centros de Cómputo deben tener equipos de detección de humo y equipos de aire acondicionado	9.2	5
Se debe mantener la documentación necesaria sobre las configuraciones básicas de los servidores por posibles incidentes	10.1.1	
Debe crearse registros con las novedades del mantenimiento físico y lógico de los equipos informáticos	9.2.4	2
Mantener todos los servidores con los parches y	10.6	5

Continua …

POLÍTICA	*CLÁUSULA*	*VALORACIÓN CUMPLIMIENTO*
actualizaciones que sean necesarios para evitar interrupción de servicios		
Mantener un constante monitoreo de la red para identificar posibles ataques a través de equipos informáticos	10.2.2	4
Crear grupos para fijar cuotas de correo limitando el uso del mismo	10.8	3
Bloquear el acceso de internet a páginas que se consideren peligrosas para la institución	11.1.1	3
Negar el acceso de correos spam y que incluyan adjuntos peligrosos	11.1.1	3
Crear usuarios especiales para accesos remotos	11.7.2	4

Interpretación de los datos: Tomando en cuenta las políticas de la tabla anterior, se realizó un análisis frente a los controles de la norma ISO 27002, verificando que muchas de ellas se acoplan a alguna de las secciones de la ISO y se colocó un nivel de valoración de cumplimiento de 0 a 5 siendo 0 el valor más bajo y 5 el más alto, encontrando un valor de cumplimiento de 3 a 4.

3.9 APLICACIÓN DEL MODELO PHVA

En esta etapa se propondrán las pautas necesarias para generar una Guía para la implantación de un Modelo de Gestión de la Seguridad de la Información acorde a las necesidades y realidad del IGM que trabaje ligado a los principios de mejora continua.

El principal objetivo del Modelo de Gestión propuesto es el de crear concientización en el personal del instituto sobre como resguardar los activos de información que sustentan su trabajo diario, como tratarlos y manejarlos en la forma más eficiente, siempre con la mente abierta para los cambios necesarios de mejora.

Tanto en la Misión como en la Visión del IGM se nombra en forma prioritaria la seguridad por lo cual, es necesario tomar ciertas medidas inmediatas que permitan dar ese valor agregado en los productos del IGM en forma eficiente y basada en norma internacionales como las ISO 27000.

3.9.1 PLANIFICAR

Para iniciar con la etapa de Planificación lo primero que se debe realizar es la definición de los objetivos que se desea cumplir, orientados al problema que se quiere solucionar. Dichos objetivos deben ser específicos (correctamente formulados),

medibles (con indicadores definidos), comprendido (comunicados por todos los involucrados), realistas (alcanzable) y con un tiempo definido de cumplimiento (inicio y fin).

Una vez que los objetivos están correctamente definidos, difundidos y comprendidos, se deben definir los recursos necesarios para su cumplimiento, dichos recursos pueden ser financieros, materiales o recursos humanos, y se debe gestionar con la alta gerencia la asignación correcta de los recursos solicitados ya que la falta de ellos o su insuficiencia podrían provocar el fracaso del proyecto emprendido.

Para una correcta planificación además de definir los recursos necesarios, también es necesario definir el tipo de controles o políticas que se desea implementar, del éxito de los controles dependerá el cumplimiento de los objetivos establecidos. Las políticas deben ser lo suficientemente detalladas y documentadas como para ser aplicados por la persona responsable.

3.9.2 HACER

Constituye la ejecución o implantación de la planificación, de una buena planificación depende una buena ejecución.

La implantación debe iniciar con la implementación del Plan de Gestión de Riesgos, con el fin de transferir, eliminar y aceptar los riesgos encontrados, los cuales de acuerdo al apetito de riesgos de la institución se clasificarán para su correcto tratamiento. Dependerá de la dirección y de las decisiones del Comité de Seguridad, la clasificación de los riesgos, los cuales podrán ser transferidos a través de terceras empresas como brókers de seguros, pueden ser eliminadas a través de la implantación de los controles más adecuados, y aceptados en el caso de que la institución no pueda hacer nada que evite dichos riesgos tales como desastres naturales.

La implementación del SGSI debe estar directamente ligada a la planificación generada en la fase anterior, iniciando con las actividades planificadas, con los responsables asignados y los recursos necesarios para cumplir con dichas actividades, el éxito de esta etapa dependerá de las facilidades que se dé a los responsables para el cumplimiento de sus actividades y se les asigne los recursos, cualquiera que sea su tipo, en el momento oportuno y de las características solicitadas. Todo dependerá del apoyo que se tenga de la dirección para completar con cada una de las etapas planificadas en el tiempo adecuado para evitar retrasos innecesarios.

Para finalizar esta etapa, se deben implementar todos los controles o políticas necesarias que permitan mitigar todos los riesgos identificados para ser controlados, a través de acciones preventivas cuyos procesos tienen recursos y responsables asignados, ninguna acción puede ser reactiva, ya que ellos significaría que no hubo una planificación correcta.

3.9.3 VALIDAR

La solicitud de validaciones o auditorías sean internas o externas deben nacer de la dirección, ya que de no ser así no se contará con la colaboración de todo el personal y no se lograrán los resultados esperados.

La validación de los controles establecidos en la etapa de planificación debe ser en forma periódica, la validación debe verificar que se cumplan los resultados esperados. De ser necesario se debe contratar consultores externos que hagan las revisiones independientes. En el caso de ser revisiones de rutina se puede contar con el personal de Auditoría Interna para dichas auditorías.

Las evaluaciones deben estar orientadas a la revisión de los riesgos residuales, fracciones de riesgos que quedaron después de haber aplicado los controles planificados, así como a la detección de nuevos riesgos o vulnerabilidades a los que se enfrenta la institución frutos de procesos nuevos o cambios en los procesos establecidos.

La comunicación de los resultados y las posibles desviaciones debe ser inmediata a todo el personal involucrado y responsables, especialmente a la dirección para que en conjunto con el Comité de Seguridad establezcan los procesos y actividades adicionales para re-orientar los objetivos establecidos.

3.9.4 ACTUAR

El cuarto paso consiste en revisar y optimizar los procesos validados, considerando siempre actividades de mejora.

El objetivo de utilizar el ciclo de Deming como un medio para diseñar un Modelo de Gestión es el de evitar Reacción, a través de una adecuada planificación, la Reacción se desarrolla por incidentes y en pocas ocasiones soluciona los problemas, en muchas ocasiones genera más problemas que soluciones.

Una vez establecidos los problemas o desviaciones en la fase anterior se deben generar acciones preventivas y correctivas que evitarán el fracaso de la implantación del

SGSI, dichas acciones deben responder a los objetivos específicos que se plantearon inicialmente, ya que si ellos no se cumplen, el proyecto habrá fracasado, dichas acciones adicionales deben contar de igual manera con una planificación inicial y asignación de los recursos necesarios.

Se debe realizar un análisis de los activos de información tanto digital como impreso dentro de cada proceso y el análisis de riesgos de cada activo de información para colocar normativas y políticas de seguridad acorde a las necesidades del área, para que dichas normativas cumplan con el objetivo planteado de salvaguardar la información tanto en proceso como el producto terminado.

De igual forma, una vez definidos los activos de información, se debe asignar lugares lógicos y físicos para su almacenamiento con su respectivo control de acceso por usuario ya que deben existir usuarios responsables para su almacenamiento con el fin de evitar duplicaciones o almacenamiento de basura, de igual forma debe existir un administrador del servidor o servidores donde se va a almacenar la información para crear usuarios y asignar cuotas de espacio físico para poder limitar el almacenamiento y planificar su expansión de ser necesario, debe existir una coordinación permanente entre los administradores tanto de información como del servidor ya que cualquier ingreso de información errada o alteración de la misma sin la autorización correspondiente, así como la falta de espacio o usuarios válidos podría causar la paralización de los procesos de producción o peor aún generación de información falsa o errada. En el caso de los almacenamientos físicos deben existir responsables que guarden y organicen dicha información con el mismo objetivo, tener solo la información válida, disponible para cuando se necesite y ubicados en un lugar físico protegido que salvaguarde la información vital para los procesos de producción.

Documentar cada uno de los procesos es vital, ya que si no existen bitácoras de los almacenamientos y de todos los productos en procesos, éstas bitácoras permitirán discernir sobre qué información debe ser almacenada y cuál debe ser desechada con el fin de optimizar los espacios físicos y lógicos y evitar inversión en infraestructura que no se va usar en forma óptima.

Después de analizar los procesos de producción (ANEXO 4), se identifica que muchos de ellos interactúan entre sí, el producto terminado de un proceso es materia prima para el siguiente y en muchos casos esa materia prima también constituye información que puede ser vendida de acuerdo a la necesidad del usuario. En el caso de

que cualquier información sea mal utilizada o mal elaborada, el siguiente proceso puede resultar erróneo o el producto vendido puede causar pérdidas, por lo cual es necesaria una profunda coordinación entre los administradores de la información con el fin de almacenar y tener a la mano la información real para el momento en que cualquier proceso o persona lo necesite, y con toda la documentación actualizada que permite su ubicación con la premura del usuario o del cliente de ser necesario.

La administración física y lógica, como lo habíamos indicado antes, es un punto importante que tomar en cuenta ya que si no es suficiente puede causar pérdidas y de ser exagerada, puede ser considerada también una pérdida en inversión, siempre es necesario realizar análisis de optimización con el fin de explotar sus bondades al máximo.

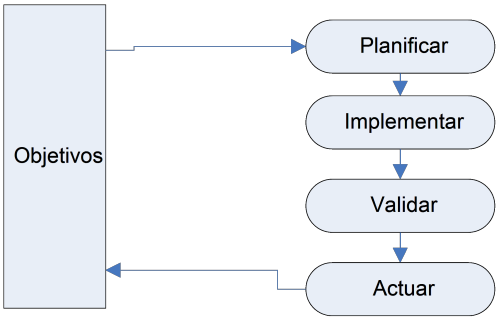

Gráfico 14: Flujo de ciclo de Deming

En el gráfico 13 se representa en forma gráfica la interacción de las fases establecidas en el ciclo de Deming frente al establecimiento de objetivos estratégicos en la institución, si no existen objetivos no se tiene donde cimentar la planificación y la evaluación posterior.

CAPÍTULO IV

DESARROLLO DE LA GUÍA PROPUESTA

Para poder realizar una adecuada Gestión de la Seguridad de la Información es necesario contar con estrategias a nivel de la Alta Dirección, para lo cual se recomienda reformar el organigrama actual con la inclusión directa de la Dirección de la Seguridad de la Información a nivel de asesoría, para que sea capaz de formular y apoyar en la toma de decisiones directivas claves, las mismas que tengan el apoyo directo de la Alta Dirección de la Institución.

4.1 ORGANIGRAMA PROPUESTO

Como se puede visualizar en el organigrama actual no se cuenta con una unidad especializada para la normalización y monitoreo de la Seguridad de la Información, por lo que se recomienda iniciar con la creación de una unidad específica de la Seguridad de la Información dentro de la institución, lo más recomendable sería crear una unidad asesora a nivel de la dirección con el personal técnico formado y capacitado en procesos y herramientas de seguridad.

La estructura propuesta quedaría de la siguiente manera:

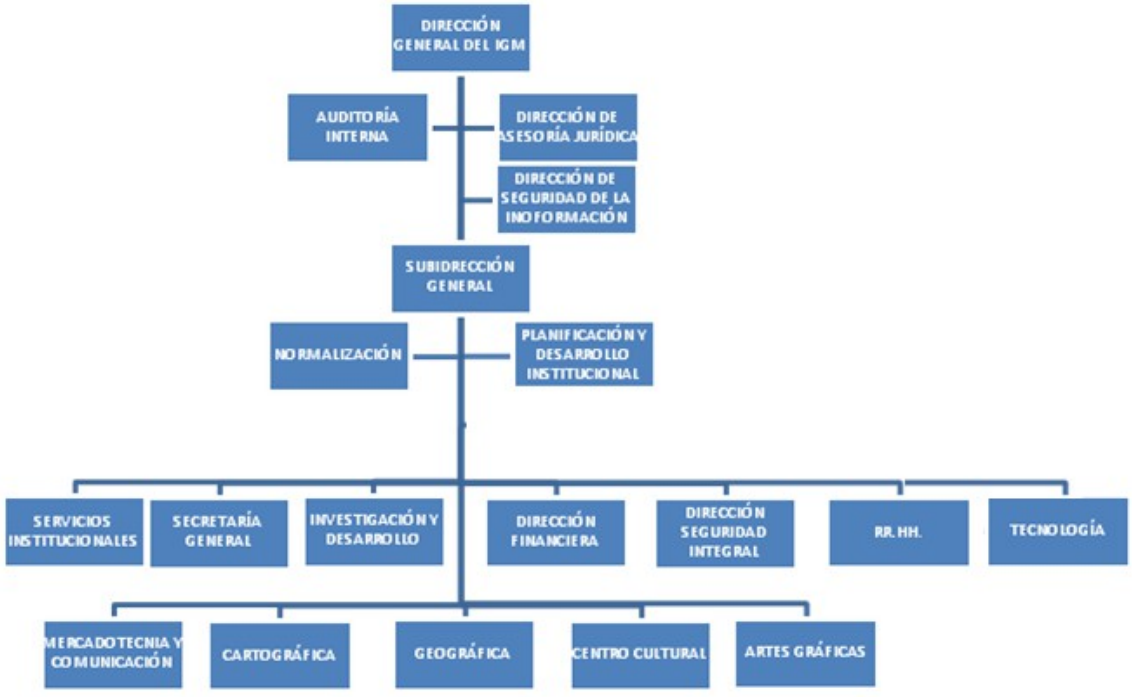

Gráfico 15: Organigrama propuesto para el IGM

4.2 ORGANIZACIÓN INTERNA DE LA DIRECCIÓN DE SEGURIDAD DE LA INFORMACIÓN

Esta unidad de asesoría recomendada, estaría conformada por el Director de Seguridad o el Oficial de Seguridad y uno o dos técnicos operativos que apoyen a la operativización de los procesos de Seguridad de la Información, todo dependería de la demanda de la institución y del grado de madurez que la institución desee alcanzar frente a la Seguridad de la Información.

Las funciones asignadas a cada rol serían claramente definidas y aplicadas.

4.2.1 Oficial de Seguridad de la Información

Las principales actividades que deberá cumplir, además de ser responsable de planear, coordinar y administrar los procesos de seguridad informática en la institución, son:

1. Definir la misión de seguridad informática de la institución en conjunto con las autoridades de la misma.
2. Elaborar y aplicar una metodología de análisis de riesgo para evaluar la seguridad informática en la institución.
3. Definir la Política de seguridad informática de la institución.
4. Definir los procedimientos para aplicar la Política de seguridad informática.
5. Seleccionar los mecanismos y herramientas adecuados que permitan aplicar las políticas dentro de la misión establecida.
6. Crear un grupo de respuesta a incidentes de seguridad, para atender los problemas relacionados a la seguridad informática dentro de la organización.
7. Promover la aplicación de auditorías enfocadas a la seguridad, para evaluar las prácticas de seguridad informática dentro de la organización.
8. Crear y vigilar los lineamientos necesarios que coadyuven a tener los servicios de seguridad en la organización.
9. Crear un grupo de seguridad informática en la organización.[3]
10. Planificar y administrar el presupuesto asignado para el área, tanto para adquisiciones como para recursos para la implementación, monitoreo y mejoras del SGSI.
11. Administración del personal a su cargo.
12. Monitoreo de las tareas permanentes de la Seguridad de la Información.

[3] http://rfc.cudi.edu.mx/drafts/draft2.pdf

13. Planificar y ejecutar charlas de concientización para el personal de la institución.

Las charlas informativas que se organizan para la concientización del personal antiguo y nuevo deben ser orientadas a las razones de la Seguridad y los planes de acción planificados para su mejora, deben tener secuencia periódica y en forma obligatoria al personal nuevo como parte de su inducción. Así como se van a informar sobre los planes de acción, también deben darse los avances de cada plan de acción ya que de no ser así las charlas terminan siendo algo teórico y utópico de lo cual nunca se podrán ver resultados ni mejoras.

Las charlas deben contener temas de actualidad, siempre mejorando con nuevas situaciones y nuevos procesos, o nuevas políticas y normativas de las nuevas directivas o fruto del Comité de Seguridad que debería tener una periodicidad mensual, siempre tratando de informar y tratando de que sean cortas y concisas para evitar dispersión de la gente y aburrimiento. Cuando se topen temas un poco teóricas, no acopladas a la realidad de la institución, inmediatamente incluir planes de acción a corto y largo plazo para poder inducir a la gente a la mejora y concientizarlos que la institución siempre está buscando el bienestar del personal.

Es siempre necesario poner mayor énfasis en la consecuencias de ciertas acciones en la Seguridad, los problemas que ocasionan y cómo prevenirlos, y especialmente la razón de colocar controles y que aunque muchas veces dichos controles son estorbosos, tienen su razón de ser y deben ser respetados.

Se debería considerar profundizar los conceptos sobre Seguridad de la Información con cursos de capacitación formal con empresas expertas en este tipo de formación para crear líderes que fomenten y velen por la Seguridad de la Información dentro de la institución.

4.2.2Técnico de Seguridad de la Información

Las responsabilidades que deberá cumplir son:

1. Implementación, configuración y operación de los controles de seguridad informática (Firewalls, IPS/IDS, antimalware, etc.)
2. Monitoreo de indicadores de controles de seguridad
3. Primer nivel de respuesta ante incidentes (típicamente a través de acciones en los controles de seguridad que operan)
4. Soporte a usuarios

5. Alta, baja y modificación de accesos a sistemas y aplicaciones
6. Gestión de parches de seguridad informática (pruebas e instalación)
7. Investigación de incidentes de seguridad y cómputo forense.
8. Atención de auditores y consultores de seguridad. [4]

Una vez establecida la estructura organizacional básica para la Gestión de la Seguridad de la Información se debe continuar con la formalización y estructuración del marco referencial para su implantación.

Después de haber realizado un levantamiento de las políticas implementadas en el IGM sobre Seguridad Informática de los últimos 5 años se pudo llegar a la conclusión que muchas de las políticas o normativas fueron fruto de incidentes de Seguridad, no fueron planificadas o consensuadas, y por lo tanto no fueron difundidas en forma adecuada o global. La estructuración de las políticas y normativas tampoco son adecuadas ya que no muestran el origen ni el fin de cada decisión.

Para la estructuración de las políticas y correcta estandarización se recomienda utilizar la norma ISO 27003 en el Anexo D, para su formalización correcta. En el Anexo D se especifica la siguiente estructura:

- Resumen de la política
- Introducción
- Alcance
- Objetivos
- Principios
- Responsabilidades
- Resultados Claves
- Políticas relacionadas

Lo que se recomienda es agrupar las políticas existentes por área relacionada y crean un documento global con objetivos y resultados comunes, y de aquí en adelante crear un documento similar por cada nueva política o normativa que sea consensuada en Comité se Seguridad y posteriormente dicho documento sea difundido a nivel global del IGM y cada una de estas políticas, de acuerdo a su alcance, sea suministrada a cada personal nuevo que ingresa en la institución.

El siguiente paso para la etapa de planificación se debe realizar también un diagnóstico de riesgos con lo cual se definirán objetivos adicionales que permitirán mitigar, eliminar, transferir o aceptar los riesgos encontrados en el análisis realizado.

[4] http://seguinfo.wordpress.com/2007/10/18/la-funcion-de-seguridad-informatica-en-la-empresa/

Para realizar el análisis de riegos se debe tomar como base la ISO 27005 donde se especifica que debe iniciarse con una valoración de los riesgos, continuar con el tratamiento de riesgos, aceptación, comunicación, monitoreo y revisión de los riesgos de la seguridad de la información.

Del análisis realizado en la sección de la situación actual se encontraron los siguientes riesgos como afectación moderada para la institución:

- Falta de equipos informáticos
- Catástrofes naturales
- Auditorías Internas
- Falta de información crítica
- Respeto al medio ambiente
- Avances tecnológicos
- Cambios en la ideología del Talento Humano
- Competencia empresa privadas
- Problemas del Talento Humano
- Regulación de pagos en eSigef
- Personal calificado

Y riesgos altamente preocupantes:

- Procesos demorosos de adquisiciones
- Recortes Presupuestarios

Muchos de los riesgos en los que se puede trabajar son aquellos que pueden ser transferidos, por ejemplo el tema de la capacitación y concientización del personal, pueden planificarse cursos de capacitación o adiestramiento en temas específicos que son necesarios para la institución de acuerdo al perfil del personal involucrado. El crear cursos de capacitación de temas que no competen a los perfiles profesionales del personal puede causar más riesgos que solucionar problemas porque mucha gente va a querer incursionar en actividades que no le competen y pueden crear brechas de seguridad tomándose atribuciones que no le competen. Es vital realizar un análisis profundo de las necesidades de capacitación del personal porque si no se realiza una planificación adecuada se puede gastar recursos y generar inconformidad en el personal con capacitación inútil.

Para una buena Gestión de Riesgos es necesario recordar que existen restricciones inherentes a la labor empresarial como:

- **Restricciones de tiempo**: siempre se cronograma el tiempo de ejecución de proyectos pensando que se va a tener el tiempo suficiente para las actividades planeadas, planificando ciertas brechas por si existen imprevistos, pero nunca se puede imaginar que los imprevistos sean más demorosos que las brechas planificadas.
- **Restricciones financieras**: dejando de lado los recortes presupuestarios por parte del gobierno, también existen problemas de inflación que elevan los precios de las adquisiciones planificadas y se escapan de los presupuestos realizados a inicios de año. La elevación de precios puede incidir en la cantidad y calidad de los productos adquiridos.
- **Restricciones técnicas**: pueden ser causadas por incompatibilidad entre productos adquiridos, es necesario tomar en cuenta para futuras adquisiciones.
- **Restricciones operativas**: estas restricciones pueden resultar por cambios en las condiciones iniciales de operación, como por ejemplo: horarios, equipos, procesos, etc.
- **Restricciones culturales**: para evitar estas restricciones es necesario tomar en cuenta el ambiente en el que se desarrolla la empresa: ubicación geográfica, creencias, nivel económico, etc.
- **Restricciones éticas**: para la colocación de cualquier control es necesario tomar en cuentas las normas éticas que rigen a la institución, no se puede pedir a nadie que incumpla sus normas éticas.
- **Restricciones ambientales**: para poder realizar cualquier inversión y definir cualquier actividad, es necesario tomar en cuenta el clima reinante, disponibilidad de espacio o desastres naturales comunes según la zona geográfica.
- **Restricciones legales**: en todo país o región se deben seguir normas o políticas regulatorias que deben ser respetadas, mucho más en el caso instituciones públicas.
- **Facilidades de uso**: para la implantación de cualquier control se debe tomar en cuentas las habilidades de las personas o la facilidad que tienen para adaptarse a nuevos procedimientos.
- **Restricciones de personal**: en muchas ocasiones los sueldos y las responsabilidades inherentes no van de la mano y es por esta razón que existe falta de personal idóneo para ocupar tanto cargos operativos como directivos.

- **Restricciones para integrar controles nuevos y existentes**: para la implantación de controles nuevos es necesario tomar en cuenta el personal adecuado, la infraestructura correcta y los espacios adecuados, por lo cual también es necesario planificar recursos extras para cubrir las nuevas necesidades.

Cuando se termine el proceso de planificación se debe conocer qué vamos a hacer, quién lo va a ejecutar, cuando se lo va a realizar y con qué recursos disponibles se cuenta.

4.3 GUIA PARA LA IMPLANTACION DEL SGSI

4.3.1 PLANIFICACIÓN

1. La Dirección, deberá emitir una resolución donde se crea el Comité de Seguridad, con el fin de poder iniciar con las reuniones y gestionar la Seguridad de la Información.
2. La Dirección debe apoyar e incentivar la difusión de la normativa de Seguridad en toda la institución, siendo la principal función permanente del Oficial de Seguridad.
3. Debe formar parte del Comité de Seguridad de la Información, los directivos de cada una de las áreas que conforman el Instituto, sean civiles o militares.
4. La Dirección, definirá las actividades del Comité de Seguridad, que entre las más generales estarán:
   - Definir y mantener las políticas, normas y procedimientos de la Seguridad de la Información, así como gestionar su aprobación y posterior puesta en vigencia y el cumplimiento de la misma por parte de la institución.
   - Monitorear y gestionar los riesgos significativos que amenacen la Seguridad de la Información.
   - Conocer y supervisar los incidentes de Seguridad de la Información.
   - Aprobar iniciativas para incrementar la Seguridad de la Información de acuerdo a las competencias y responsabilidades de cada área.
   - Evaluar y coordinar la implementación de controles específicos de la Seguridad de la Información para nuevos sistemas y servicios.
   - Promover la difusión de las políticas acordadas.
   - Coordinar y gestionar la continuidad del negocio frente a incidentes de Seguridad de la Información.
   - Designar los custodios de los activos de información de las diferentes áreas, esta designación debe ser formalizada en un documento físico o digital.

- Gestionar la provisión de recursos para la Gestión de la Seguridad de la Información.
- Velar por la aplicación de la NTE INEN ISO/IEC 27000 en la institución según el ámbito de acción.
- Designar formalmente al Oficial de Seguridad de la Información que reportará directamente a la máxima autoridad.
- Designar al responsable de la seguridad en el Área de Tecnología de la Información que coordinará con el coordinar o jefe del área.

5. Para la asignación del Oficial de Seguridad del IGM, se debe tomar en cuenta que debe ser un integrante del staff con suficientes privilegios para la toma de decisiones, y su perfil básico puede ser:
   - Ingeniero en Sistemas o carreras afines.
   - Mínimo 5 años de experiencia.
   - Experiencia en las distintas áreas de la Tecnología de la Información.
   - Conocimiento sobre los procesos del negocio, si es posible en forma detallada.
   - Conocimientos formales en normas ISO 27000, si es posible con certificaciones.
   - Tener conocimientos sobre herramientas de hackeo ético, informática forense, etc.
6. Las obligaciones básicas que debe cumplir el Oficial de Seguridad de la Información, entre las más generales puede ser:
   - Definir procedimientos para el control de cambios de procesos operativos, con el fin de que no afecten a la Seguridad de la Información.
   - Definir criterios de Seguridad de la Información para los nuevos sistemas, contemplando sus respectivas pruebas previas su implantación.
   - Definir procedimientos para el manejo de incidentes.
   - Definir procedimientos para la administración de medios de almacenamiento.
   - Definir mecanismos de distribución y difusión de información dentro y fuera de la institución.
   - Definir procedimientos para la detección y prevención del acceso no autorizado con el fin de garantizar la seguridad de los datos y los servicios conectados a la red.
   - Desarrollar charlas de concientización de usuarios en materia de Seguridad de la Información y control de accesos.
   - Verificar el cumplimiento de normas, procedimientos y controles de seguridad.
   - Coordinar la gestión de riesgos con cada una de las áreas del negocio.
   - Coordinar la gestión de eventos con otras entidades gubernamentales.
   - Convocar a Comité de Seguridad cuando se amerite llevando un control de asistencia y actas.

7. Asignar al responsable de Seguridad en el Área de Tecnología, quien deberá cumplir con las siguientes actividades básicas:
   - Controlar la existencia de documentación física y digital relacionado con los procedimientos relacionados con procesos operativos del área de Tecnología.
   - Evaluar los posibles impactos en la Seguridad de la Información, al realizar cambios de los sistemas y equipamientos, verificar su correcta implementación y sus responsabilidades.
   - Administrar los medios técnicos para la segregación de los ambientes de procesamiento.
   - Monitorear las necesidades de capacidad y las posibles amenazas de seguridad.
   - Controlar la obtención de copias de información y probar su restauración.
   - Asegurar el registro de las actividades realizadas por el personal operativo de la Seguridad de la Información para su posterior revisión.
   - Establecer procedimientos para la comunicación de fallas de procesamiento y para la toma de medidas correctivas.
   - Implementar controles de seguridad establecidos en Comité de Seguridad.
   - Definir procedimientos para la administración de medios digitales e impresos de almacenamiento de información y su correcta destrucción de ser necesario.
   - Gestionar incidentes de Seguridad de la Información.
   - Y demás actividades de la Gestión de la Seguridad de la Información que establezca el Comité de Seguridad.
8. Crear cronogramas para realizar talleres con las distintas áreas para definir los activos de información importantes para la institución y procesos actuales, así como los responsables de cada uno de ellos. También se debe proponer por parte de los responsables, el mejor trato a los activos y los posibles controles para su mantenimiento y revalorización de forma permanente. (ANEXO 5)
9. Crear el Plan de Gestión de Riesgos con aspectos generales sobre las novedades encontradas en los análisis detallados anteriormente, tomando en cuenta los activos de información levantados en el punto anterior, definiendo los prioritarios ya que al ser una institución tan grande, no se puede comenzar a colocar controles a todos los activos en una etapa inicial. (ANEXO 6)

   El Plan de Gestión de Riesgos debe contener en forma básica:

   - Diagnóstico Inicial
   - Actividades (prevención, mitigación, plan de contingencia)
   - Recursos

10. Como parte de las actividades del Plan de Gestión de Riesgos, deben definirse políticas generales para la Seguridad de la Información que sean aplicables a toda la institución aprobadas por el Comité de Seguridad, tomando en cuenta los activos prioritarios definidos en la etapa anterior.

    La estructura de las políticas desde las más generales hasta las más específicas deben tener un formato uniforme donde consten las siguientes partes:

    - Resumen de la política
    - Introducción
    - Alcance (partes o actividades de la institución)
    - Objetivos
    - Principios (reglas de las acciones y decisiones)
    - Responsabilidades (responsable de acciones)
    - Resultados claves para el negocio
    - Políticas relacionadas

11. Poner a discusión las políticas propuestas en Comité de Seguridad para su aprobación. (ANEXO 7)
12. Realizar cronogramas de análisis y evaluaciones a corto plazo de Gestión de Riesgos del resto de activos de información, para conocer las necesidades particulares de cada área en cuanto a Seguridad de la Información y poder generar políticas particulares. La Gestión de Riesgos debe enfocarse en los activos definidos y se deben tomar en cuenta los riesgos inherentes al sector público, como son:
    - Recorte presupuestario
    - Procedimientos establecidos para las adquisiciones a través del INCOP lo que produce, en muchos casos, demoras
    - Regulaciones para pagos a través del eSigef
    - Auditorías externas
    - Respeto al medio ambiente
    - Personal calificado acorde a los avances del medio
    - Capacitación al personal en avances tecnológicos
    - Competencia con costo y tiempo más bajos ya que la empresa privadas tiene menos restricciones
    - Cambios en procesos acorde a nuevas ideologías, lo que deviene en cambios en las personas
    - Avances tecnológicos costosos en la industria

    El detalle de riesgos también dependerá del nivel de madurez de la institución y del apetito de riesgos de la Dirección.

13. Tomando en cuenta las necesidades particulares de la institución, generar cronogramas a largo plazo definiendo secciones de aplicación de la norma y poder ir cerrando brechas por secciones, sin descuidar las evaluaciones globales.

14. Una vez realizadas las evaluaciones particulares, definir en Comité de Seguridad los controles más adecuados para cada riesgo encontrado, iniciando con los más generales y llegando a los más particulares, para esta definición debemos tomar en cuenta la NTE INEN-ISO/IEC 27002 con la definición de controles que posee. (ANEXO 8)

15. Para poder formalizar todas las actividades desarrolladas en los puntos anteriores y asegurar su implementación y seguimiento, se debe crear el documento del Plan de Gestión de Riesgos el cual debe contener:
    - Listado de los activos de información con su respectivo responsable
    - Listado de riesgos con sus respectivos plan de acción
    - Listado de controles por sus respectivos riesgos
    - Listado de recursos necesarios para cumplir con los controles planteados
    - Plan de contingencia donde se especifiquen las acciones inmediatas para mantener la continuidad de los servicios vitales, así como los responsables de cada actividad y tiempos máximos de ejecución.
16. Generar cronogramas para evaluar el cumplimiento de controles y su posible rectificación de ser necesario. Las evaluaciones tienen que orientarse a medir cumplimiento y efectividad para poder recomendar actualización o cambios en los controles.

4.3.2 HACER

1. La primera acción en la etapa de HACER es comenzar con las tareas planificadas en el Plan de Gestión de Riesgos con el fin de transferir, eliminar y aceptar los riegos establecidos, dependiendo del apetito de riesgo de la Dirección. Las tareas deben ser priorizadas y gestionadas por cada responsable, contando con los recursos necesarios y planificados en la etapa anterior. En esta etapa debe estar claro el completo compromiso por parte de la Dirección ya que de no existir la gestión de recursos, muchas de las tareas planteadas no se podrán cumplir, especialmente si no se cuenta con la gente y el financiamiento necesario. Para ello es necesario realizar

un cronograma de actividades para el cumplimiento del Plan de Riesgos de la institución, con actividades claras con sus respectivos responsables, ya que de no asignar responsabilidades claras con tiempos, no se van a cumplir los tiempos establecidos, de igual forma se debe especificar acciones claras para el momento de por cualquier razón no se cumplan las actividades en los tiempos solicitados.

2. Para la implementar del SGSI deben cubrirse las brechas que existen en cuanto a capacitación del personal de la institución, primero en cuanto a la concientización de todo el personal y en segundo lugar en conceptos más profundos sobre Seguridad de la Información para el personal asignado para estas tareas. La capacitación debe ser formal con empresa que tengan amplia experiencia en este tipo de instrucción, ya que los conocimientos deben ser reales y aplicables a la realidad de la institución.

   Se debe mantener una bitácora de incidentes de Seguridad de la Información generadas en cualquier área de la institución ya que de su retroalimentación se pueden generar nuevos controles o actualización de los existentes. La generación, actualización y control de dicha bitácora debe estar a cargo del Oficial de Seguridad de la Información y es responsabilidad de los dueños de los activos de información el informar en forma oportuna de incidentes ocurridos, cualquier omisión podría se causa de problemas mayores y sanciones a los responsables.

   Todos los recursos especificados en el Plan de Gestión de Riesgos deben ser solventados por los distintos estamentos de la institución; y de no ser así, deben darse los justificativos pertinentes y una solución sea en tiempo o reemplazo de recursos con el fin de no interrumpir la secuencia lógica de actividades en tiempo y eficacia.

   La operativización de las acciones que constan en el Plan de Gestión de Riesgos debe estar a cargo de los responsables de cada área en coordinación directa con el Oficial de Seguridad, y deben ser evaluadas en forma periódica con el fin de verificar su eficacia y poder realizar los afinamientos oportunos, con evaluaciones tanto internas como externas, dependiendo del grado de cumplimiento que tenga la Dirección.

3. Con el objetivo de mitigar los riesgos encontrados en etapas anteriores, es necesario la implementación de controles e indicadores de valoración que permitan establecer correcciones en el camino, ya que si existen controles que no cumplen con su objetivo o su implementación ha causado más problemas que soluciones, los riesgos en vez de bajar en su impacto, está creciendo en la probabilidad, o lo contrario. Las evaluaciones continuas son responsabilidad de los dueños de los procesos en coordinación con el Oficial de Seguridad. Todo control implementado tiene como objetivo el reducir o minimizar los riesgos encontrados en las etapas de evaluación, si el control no está sirviendo para este propósito, debe ser modificado o mejorado, en la etapa de retroalimentación.

4.3.3 VERIFICAR

1. La verificación de la eficacia y eficiencia de los controles implementados, debe iniciar con revisiones internas periódicas a cargo del Oficial de Seguridad y de los responsables de los procesos de la institución y con auspicio de la Dirección, generando bitácoras de incidentes encontrados y este reporte debe ser discutido en Comité de Seguridad con el fin de poder encontrar soluciones prácticas y a corto plazo para su mejora.

   De encontrar incidentes permanentes, que no pueda ser solventados por los controles colocados, es decir, que no se encuentra solución viable dentro de la institución, debe recurrirse a revisiones externas de la eficacia del SGSI, con auspicio de la Dirección, contratando consultorías externas que recomienden medidas eficaces para mitigar, transferir o aceptar los riesgos recurrentes.

2. Se deben realizar revisiones del riesgo residual aceptable con el fin de generar políticas para minimizarlo o aceptarlo, pero con continuas evaluaciones para evitar que aumente, evaluar la contratación de externos para poder transferir el riesgo y evitar que su impacto sea mayor.
3. Se deben crean procesos y procedimientos para la detección de errores o vulnerabilidades en forma permanente, creando técnicos capacitados en ethical hacking y técnicas de intrusión para poder detectar problemas de intrusión externa y

utilizar herramientas que disminuyan y eliminen los posibles riesgos a los que la institución se encuentra vulnerable.

4.3.4 ACTUAR

1. Para medir el desempeño del SGSI, es necesario realizar análisis y evaluaciones constantes de las políticas y reglamentos establecidos con el fin de mejorarlos y optimizarlos, ya que dicha documentación debe evolucionar de acuerdo a la modernización de la institución y acorde a las nuevas amenazas del mercado que podrían afectar a la información sensible de la institución. Toda la evaluación debe estar orientada a la razón de ser de la institución y hacia donde quiere ir, ya que la implementación de controles, la adquisición de software y hardware, contratar a expertos y consultorías, etc. debe obedecer a las necesidades particulares de la institución y al presupuesto que la institución logre para el proyectos de la implementación del SGSI.

   Todas las actividades deben estar orientadas a resolver problemas particulares que deben ser analizados en Comité de Seguridad con el asesoramiento particular del responsable de Seguridad de TI, ya que es la persona más idónea para identificar con más claridad las falencias técnicas de la institución, y es la personal que debe realizar la evaluación de herramientas técnicas y realizar informes de factibilidad para recomendar adquisiciones o consultorías.

2. Los procesos de mejora continua van de la mano con las evaluaciones expuestas en el literal anterior, pero toda mejora debe ir de la mano de la evolución de la institución.
3. Si las acciones preventivas y correctivas consisten en actualizaciones de los reglamentos y políticas establecidas, con ser tratadas en Comité de Seguridad y aprobadas es suficiente, pero de consistir en proyectos completos con acciones a corto y largo plazo deben ser planteadas a niveles directivos para su aprobación y apoyo, tanto económico como humano. De no existir el apoyo por varias razones, es mejor plantear actividades de organización que no implique la inversión de dinero, pero no se deben dejar vulnerabilidades sueltas que puedan afectar a la institución.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

El análisis situacional del IGM, desde el punto de vista de la Seguridad de la Información, constituye una base estratégica para la planificación e implantación del SGSI. A través de éste se puede identificar de manera cualitativa y cuantitativa las brechas y aspectos que generan impactos en la seguridad por las mismas actividades que lleva a cabo la institución.

La institución, y luego de una análisis riguroso de información estratégica se determinó que el estudio de seguridad deberá iniciar en la unidad de Gestión Cartográfica, la misma que decidió implantar el modelo para el proceso de "producción de la Gestión Cartográfica".

Fruto del análisis realizado dentro de la institución se ha concluido en que:

- Existe funciones y responsabilidades sobre Seguridad de la Información que no están claramente definidas en cada área, en los flujos examinados de la producción de la Gestión Cartográfica se puede determinar que en ningún momento de insertaron procesos adicionales para el control de la integridad, confidencialidad y disponibilidad de los productos terminados ni de los productos en proceso.
- Se estaría manejando el supuesto de que la Seguridad de la Información es competencia únicamente de TI o de Seguridad Integral. No se establecen claros procesos de seguridad de la información para cada responsable de los activos de información.
- No existe un departamento u oficial de Seguridad asignado en el IGM, lo que no permite que exista control o evaluación de las políticas establecidas, y crear nuevos procesos de acuerdo a los riesgos a los que se enfrenta la institución.
- La implantación de la Seguridad de la Información en el IGM se basa en una disposición de la Fuerza Terrestre, lo que conlleva a que no exista un completo comprometimiento de todas las partes dentro del instituto, llega a ser una obligación más que una necesidad real.
- La dirección del IGM ha delegado funciones sobre seguridad de la información, debido al hecho de que el Comité de Seguridad no se haya reunido, representando varias dificultades sobre las políticas implantadas.

- De los riesgos identificados a través de las encuestas llevadas a cabo, se concluye que el 75% constituyen riesgos externos frente a los cuales la institución no puede crear controles que logren mitigarlos o reducirlos.

5.2 RECOMENDACIONES

Implantar el SGSI propio del instituto, acogiendo como alcance el proceso crítico denominado "Producción de la Gestión Cartográfica"; así como procurando el mejoramiento continuo.

Es importante tomar en cuenta las siguientes recomendaciones para evitar fracasos en la implantación del SGSI dentro de la institución, que aunque parecen errores presumibles, es necesario reconocerlos para no pasarlos desapercibidos:

- La persona que lidere el proceso de implantación debe ser una persona que conozca del tema y que tenga la jerarquía necesaria para tomar decisiones, ya que de no ser así otras personas con jerarquía pueden tomar las decisiones equivocadas a falta del líder del proceso. El no escoger a la persona adecuada y no darle las atribuciones correspondientes puede causar demoras y errores en la implantación de la Seguridad de la Información dentro de la institución, la persona encarga a más de tener nociones básicas sobre el tema, debe estar en constante preparación e investigación sobre herramientas y nuevos controles que puedan ayudar a la institución.
- No siempre el adquirir una herramienta informática garantiza el éxito de la implementación, es necesario cumplir ciertos requisitos previos para su uso; se recomienda investigar en forma profunda lo disponible en el mercado y los pre-requisitos para su uso, porque de no ser así se puede generar una pérdida en vez de una inversión.
- La implantación de procesos de Seguridad de la Información debe ser el fruto de un análisis consensuado de todo el personal directivo de la empresa para dar soluciones reales a problemas de seguridad y proteger los activos sensibles de información de la institución, dicho análisis deben ser fruto de un análisis de brecha entre la situación actual y la deseada.
- El soporte y gestión de TI debe ir acorde a las necesidades de la institución y es TI quien debe proponer soluciones tecnológicas integrales como inversión a largo y corto plazo para la institución, siempre respetando las normativas vigentes tanto gubernamentales como institucionales.

- A pesar de que en muchas ocasiones, la mejor respuesta para una implantación de esta magnitud es contar con la ayuda de un consultor, no se debe creer que los consultores externos conocen más de la institución que el personal interno, el consultor debe retroalimentarse del personal de planta para sustentar sus comentarios y recomendaciones. El resultado final, el informe del consultor, debe ser evaluado y consensuado por personal interno para ver si ha cumplido con el objetivo propuesto y se acopla a las necesidades de la institución.
- Lo que se recomienda, en este punto, es retomar las reuniones de Comité de Seguridad que según el Artículo 3 se deberán llevar a cabo todos los meses durante la primera semana, y dicho Comité debería adicionarse la presencia del Jefe del Talento Humano ya que su presencia es vital en el momento de analizar casos extremos determinar sanciones y hasta multas en el caso de contravenir en alguna de los procedimientos de seguridad establecidos. Al Comité de Seguridad deberían asistir los jefes departamentales sin opción de delegación, ya que en muchas se debe contar con personal de toma de decisiones.
- Toda acción que se defina para poder normar procedimientos de Seguridad de la Información debe pasar por la aprobación del Comité de Seguridad y principalmente por la aprobación de la alta dirección ya que sin su apoyo o su conocimiento sería imposible implementar en forma adecuada y global.
- Es el Comité de Seguridad el que debe liderar todo lo concerniente a la Gestión del SGSI; debe dirigir, monitorear y completar las tareas que sean necesarias para su implementación y promover procedimientos adecuados para el manejo de los activos de información por parte de sus responsables directos.
- El Comité debe ser el encargado de consensuar políticas para su posterior implementación, y es el responsable de TI el que debe promover la compra de infraestructura y de determinar las acciones necesarias para minimizar los riesgos que puedan correr los activos de información.
- Una vez identificados los riesgos que afectan a la Gestión Cartográfica, es necesario que en Comité de Seguridad se creen las estrategias a corto y largo plazo para minimizar su impacto o reducir su probabilidad, existen riesgos externos que no pueden ser tratados con actividades internas, deben tomarse medidas a más alto nivel gerencial para poder minimizar su efecto dentro de la institución, por ejemplo para los problemas de procesos demorosos de adquisición lo que se debe es planificar

mejor las adquisiciones con el fin de reducir los procesos que son muy burocráticos, o realizarlos en forma distribuida todo el año para evitar que a fin de año se acumulen y causen problemas internos y externos en la institución; en el caso de los recortes presupuestarios se deben realizar gestiones a nivel directivo con el Ministerio de Finanzas para tratar de justificar los rubros que se colocan en el presupuesto anual y evitar en los posibles que dichos recortes sean lo menos posible. Cada una de las estrategias que sean escogidas para solventar cada uno de los riesgos, debe tener una documentación completa, seguimiento y monitoreo permanente para evitar que en vez de minimizarlos se agiganten y no puedan ser manejados de la manera adecuada, y poder reorientarlos si se están desviando del camino esperado.

- Es total responsabilidad de la Dirección el tomar las decisiones adecuadas para la implantación de la Seguridad de la Información y el delegar esta función en personal no jerárquicamente adecuado puede provocar un fracaso en el proceso de gestión e implantación. El éxito de este proyecto es involucrar totalmente a los líderes de los procesos quienes guiarán al resto de la institución a no tomar decisiones equivocadas y evitar el mal uso de recursos.
- Debido a que fruto de las encuestas verificamos que el 75% de los riesgos son externos, se recomienda trabajar en controles a niveles directivos o mandos medios que permitan transferir los riesgos a entidades externas como aseguradoras; o en el caso extremo aceptarlos, tomando en cuenta las consecuencias inherentes.

BIBLIOGRAFÍA

Referencias bibliográficas impresas

Contraloría General del Estado. (2009). Acuerdo No. 039-CG, Registro Oficial de la República del Ecuador No. 87. Quito-Ecuador.

Salgado, Francisco (2009). *Estándares y Protocolos de Seguridad Lógica en los Sistemas de Información*. Veracruz-México: Universidad Veracruzana

Norma ISO/IEC 27001 (2005). *Técnicas de Seguridad - Sistema de Gestión de la Seguridad de la Información - Requisitos*, International Standarization Organization.

Norma ISO/IEC 27005 (2008). *Técnicas de Seguridad - Gestión de Riesgos*, International Standarization Organization.

Norma ISO/IEC 27003 (2010). *Técnicas de Seguridad - Guía de Implementación del Sistema de Gestión de la Seguridad de la Información*, International Standarization Organization.

Instituto de Salud Carlos III (2009), Ministerio de Ciencia e Innovación, *Investigación en tecnologías de inteligencia ambiental para la salud del futuro*.

INTECO (Instituto Nacional de Tecnologías de la Comunicación) (2013), *Implantación de un SGSI en la empresa*.

José Antonio Pérez Fernández de Velasco. (2010). *Gestión por procesos*. España: Alfaomega.

Referencias WEB

Sergio Molanphy. (2008). *Gap Analysis*. Recuperado en el 2013. Sitio web: http://sergio.molanphy.net/category/gap_analysis/

Gie. (2004). *Gap analysis*. 2013. Sitio web: http://giemdp.com.ar/index.php?page=gap-analisys&hl=es_ES

ISO. (2005). *El portal de ISO 27001 en Español*. Recuperado en el 2013. Sitio web: www.iso27000.es/

BSI. (2013). *Gap Analysis*. Recuperado en el 2013, Sitio web: http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/Nuestros-servicios/Gap-Analysis/

Universidad Nacional Mayor de San Marcos. (2013). *Glosario de términos sobre administración pública*. Recuperado en el 2013. Sitio web: http://www.unmsm.edu.pe/ogp/archivos/glosario/indr.htm

GLOSARIO DE TÉRMINOS

Activo de Información: Se considera toda dato relacionado con las actividades y servicios de una organización, que tenga valor para ésta según estime su propietario, atendiendo a las escalas de valoración utilizadas, los requisitos legales, su sensibilidad y criticidad para la organización, cualquiera sea su forma y medio de comunicación y/o conservación.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. También se utiliza como sinónimo de salvaguarda o contramedida.

Estándar: es un modelo a seguir al hacer algo. Son documentos que dan los detalles técnicos y las reglas necesarias para que un producto o tecnología se use correctamente.

Herramientas informáticas: conjunto de instrumentos empleados para manejar información por medio de la computadora como el procesador de texto, la base de datos, graficadores, correo electrónico, hojas de cálculo, buscadores, programas de diseño, presentadores, redes de telecomunicaciones, etc.

Método: cada plan seleccionado para alcanzar un objetivo, medio que se utiliza para llegar a una cierta meta.

Metodología: es una pieza esencial de toda investigación, plan de investigación que permite cumplir ciertos objetivos en el marco de una ciencia. La metodología es normativa (valora), pero también es descriptiva (expone) o comparativa (analiza).

Norma: Una norma es una regla que debe ser respetada y que permite ajustar ciertas conductas o actividades.

Procedimiento: consiste en seguir ciertos pasos predefinidos para desarrollar una labor de manera eficaz. Su objetivo debería ser único y de fácil identificación, aunque es posible que existan diversos procedimientos que persigan el mismo fin, cada uno con estructuras y etapas diferentes, y que ofrezcan más o menos eficiencia.

Proceso: conjunto de acciones o actividades sistematizadas que se realizan o tienen lugar con un fin. Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

Regulación: consiste en el establecimiento de normas, reglas o leyes dentro de un determinado ámbito. El objetivo de la regulación es mantener un orden, llevar un control y garantizar los derechos de todos los integrantes de una comunidad.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Riesgo Residual: Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.

Técnica: tipo de acciones regidas por normas o un cierto protocolo que tiene el propósito de arribar a un resultado específico. Procedimiento o grupo de procedimientos que tienen el fin de obtener un resultado específico sin importar el campo en donde nos estemos desenvolviendo.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Vulnerabilidad: Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.