Universidad Nacional de Ingeniería

Facultad de ciencias y sistemas

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27001:2013 EN LA DGI"

Maestría en Gestión de la Seguridad de la Información

Ciclo académico 2013-2015

Tutor: Msc. Héctor Álvarez

Autor: José Antonio Herrera Palacios

Contenido

Agradecimientos.....vi
Presentación.....vii
Introducción.....viii
Presentación de la Problemática.....x
Definición de los Objetivos.....xii
Objetivo General.....xii
Objetivos Específicos.....xii
Justificación.....xiii
Hipótesis.....xiv
Metodología.....xv
Alcances o Metas.....xvi
Capítulo I Marco teórico conceptual.....1
Modelo del Sistema de Gestión de la Seguridad de la Información.....2
Principios:.....2
Importancia de la información:.....2
Enfoque de sistemas:.....2
Conceptos básicos.....2
Estructura del modelo.....3
Los ocho principios de gestión de la ISO.....5
Definición del SGSI.....5
Ciclo de mejora continua.....6
Definición del enfoque para la implementación del SGSI.....7
Madurez de un SGSI.....8
Evaluación de riesgos.....9
Metodologías de gestión de riesgo.....10
Ejemplo de formato de evaluación de riesgos.....10

Opciones de tratamiento de riesgos....11
Reducción....11
Retención....11
Transferencia....11
Evitar los riesgos....12
Identificación de los activos de soporte....12
Definición de declaración de aplicabilidad....12
Incidentes de seguridad de la información....13
Gestión de eventos....15
Sistemas de monitoreo....15
Proceso de monitoreo....16
Monitoreo de la Disponibilidad....16
Sistemas de Gestión Documental....18
Trabajo en grupo o workflow....18
Sistemas OpenSource....18
OpenKM....18
Eramba....19
Kimios....20
Alfresco....22
Roles y Responsabilidades....23
Naturaleza y funciones de la Dirección General de Ingresos....24
Visión....24
Misión....24

Objetivos institucionales....24

Marco Legal de la institución....25

Infraestructura y Descripción del Sistema "Ventanilla Electrónica Tributaria"....27
Objetivo general del sistema....27

Descripción General de la Operación del Sistema....28

Transacciones en línea realizadas....28

Infraestructura del Sistema....28

Descripción de los procesos....29
Declaraciones en línea....29

Pagos gestionados realizados en entidades bancarias....30

Generación de Estados de Cuenta....30

Emisión de solvencias....31

Consultas de documentos....31

Diagrama Lógico del Sistema....32

Personal involucrado con la gestión de la VET....32

Cargos relacionados con el SGSI....33

Capítulo II Desarrollo y justificación de la solución propuesta....35

Alcance de la implementación propuesta....36
Ruta de implementación....36
Diagnóstico de la situación actual de la institución....37

Entrevistas con los cargos claves....38

Análisis de la información....39

Estrategia de implementación....42

Plan de acción....44

Controles a implementar ISO 27001:2013....45
Control de la documentación (Políticas de seguridad)....47

Matriz Raci control de la documentación....48

Requerimientos de la implementación:....49

Requisitos de Hardware....49

Procedimiento de instalación....49

Organización lógica de la herramienta....50

Contenido de la herramienta....52

Ciclo de la información documentada....52

Control de incidentes....54

Nivel de escalamiento....58

Notificación de puntos débiles de la seguridad....58

Hardware y Software....59

Revisión de Logs de seguridad....59

Aprendizaje de los incidentes de seguridad de la información....60

Capítulo III Conclusiones y recomendaciones....61

Conclusiones....62
Recomendaciones....64

Bibliografía....67

Anexos....70

Modelo de entrevista para análisis del estado actual de la seguridad de la información....70

Anexo I.....71
Entrevista con Personal para diagnóstico de la situación actual de la seguridad en la DGI.....71

4. Contexto organizacional.....71

5. Gestión de Liderazgo.....74

6. Planificación.....75

7 Soporte.....76

Anexo II.....78
Formato de gestión de incidentes de seguridad.....78

Anexo III.....78
Presupuesto de implementación.....78

Agradecimientos

Me gustaría agradecer a todas las personas que me han apoyado en el proceso de la Maestría, especialmente a mi familia.

A la Dirección General de Ingresos por el apoyo incondicional brindado desde el comienzo de esta maestría.

Al tutor Héctor Álvarez por su apoyo incondicional.

Presentación

El proyecto iniciará con un análisis de la situación de la seguridad de la información institucional, políticas, planes y proyectos, así como los controles de seguridad existentes en el área de tecnología de la Dirección General de Ingresos, específicamente al área del Sistema de Ventanilla Electrónica Tributaria, que es la aplicación de mayor importancia de los sistemas tributarios de la institución.

Con base al análisis se creará el plan de acción para el proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2013, con un alcance al Sistema de Ventanilla Electrónica Tributaria (VET).

Se procederá a realizar un análisis de los principales hitos a tomar en cuenta y diseñar el plan para la implementación del Sistema de Gestión, para que en base a esto definir las políticas y objetivos de implementación del Sistema de Gestión.

Se identificarán los principales hitos para el proyecto de implementación del ISO 27001

Se diseñarán análisis para evaluar los controles de información adecuados, según el nivel de riesgo.

Se efectuará propuesta de implementación de los controles de la documentación, así como de la gestión de incidentes.

Introducción

La información, es un recurso que como el resto de los activos, tiene valor para la institución y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daños y contribuyendo de esta manera, a una mejor gestión de la Dirección General de Ingresos.

La información en todas sus formas, es uno de los principales activos de cualquier empresa, la cual es necesaria para normar el funcionamiento y la consecución de sus objetivos [ISO27001:2013]. Debido a esta importancia, las organizaciones necesitan proteger su información para asegurar que la misma esté disponible cuando se necesite (aseguramiento de que los usuarios autorizados tienen acceso a la información y sus activos asociados cuando lo requieran), que sea íntegra (garantía de la exactitud y completitud de la información y los métodos de sus procesamiento), que sea confiable (aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso), que mantenga la autenticidad (aseguramiento de la identidad u origen) y que pueda ser trazable (aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento).

La seguridad de la información se ha convertido en un tema dominante y es objeto de un enfoque renovado para todas las organizaciones a raíz del entorno de negocios actual, la economía mundial y competitividad en el mercado, por lo que la DGI no está exenta de esta realidad. Por la importancia que representa los activos de información que maneja la institución así como por la legislatura nicaragüense, se requiere que la información de los contribuyentes sea mantenido con sigilo.

Todo esto está soportado por una compleja plataforma tecnológica, que se debe ampliar continuamente, y debe estar acompañada de todas las directivas, estándares y mejores prácticas que existen hoy en día para brindar la calidad del servicio necesario para atender a los contribuyentes.

En este trabajo se pretende realizar un análisis del estado actual de la seguridad de la información en la institución, determinando el grado de madurez y el estado inicial.

Una vez determinado el estado se plantearán los proyectos (actividades) requeridas para implementar el SGSI basado en ISO 27001:2013, su estrategia de implementación.

Finalmente se realizarán implementaciones necesarias para el funcionamiento inicial del SGSI, principalmente en el control documental, que es lo más importante en las etapas iniciales del proyecto de implementación del SGSI.

Presentación de la Problemática

La problemática de la institución, es que no se ha efectuado un enfoque integral que aplica a la seguridad de la información institucional, principalmente en el área de tecnología.

Los enfoques actuales están diseñados en base a seguridad informática, con énfasis en ciertos puntos, que no representan un enfoque general, el cual se pueda medir y corregir, que además se haga énfasis en la seguridad de la información como tal, basada en análisis de riesgos.

El proceso de implementación de un sistema de gestión de seguridad de la información requiere de recursos, los cuales, no están disponibles para realizar una sola inversión, por la naturaleza de la institución (ente presupuestado), por tanto se debe dar un enfoque de implementación paulatina, primeramente con un alcance limitado, el cual se irá ampliando a medida que se tengan mayores recursos disponibles.

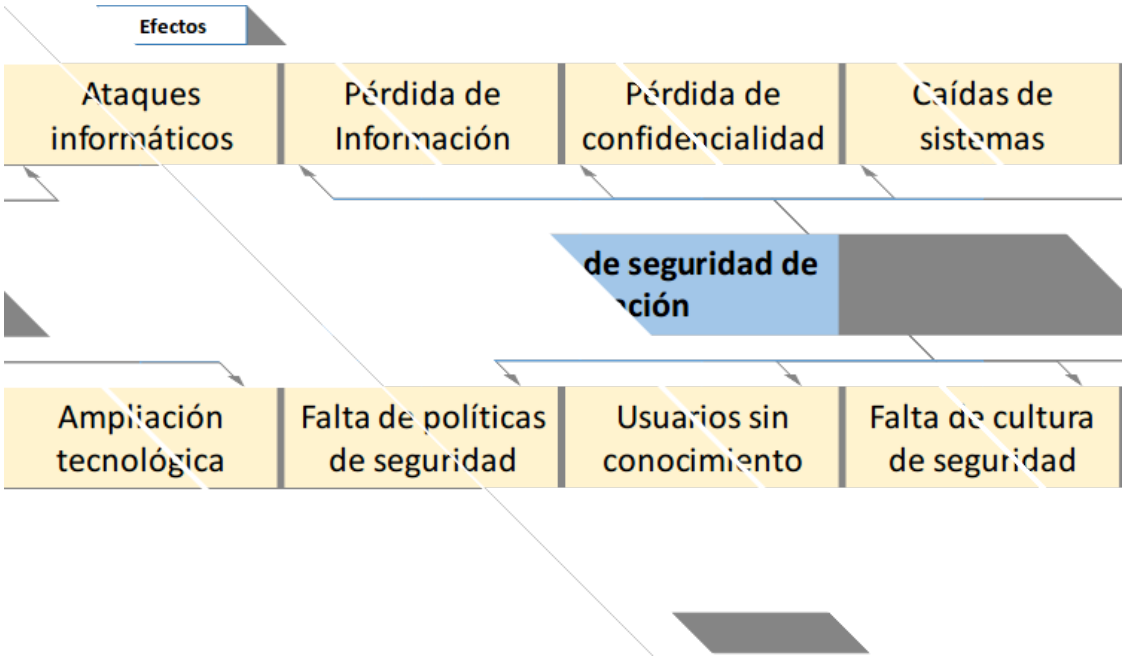


Ilustración 1: Causa y efecto

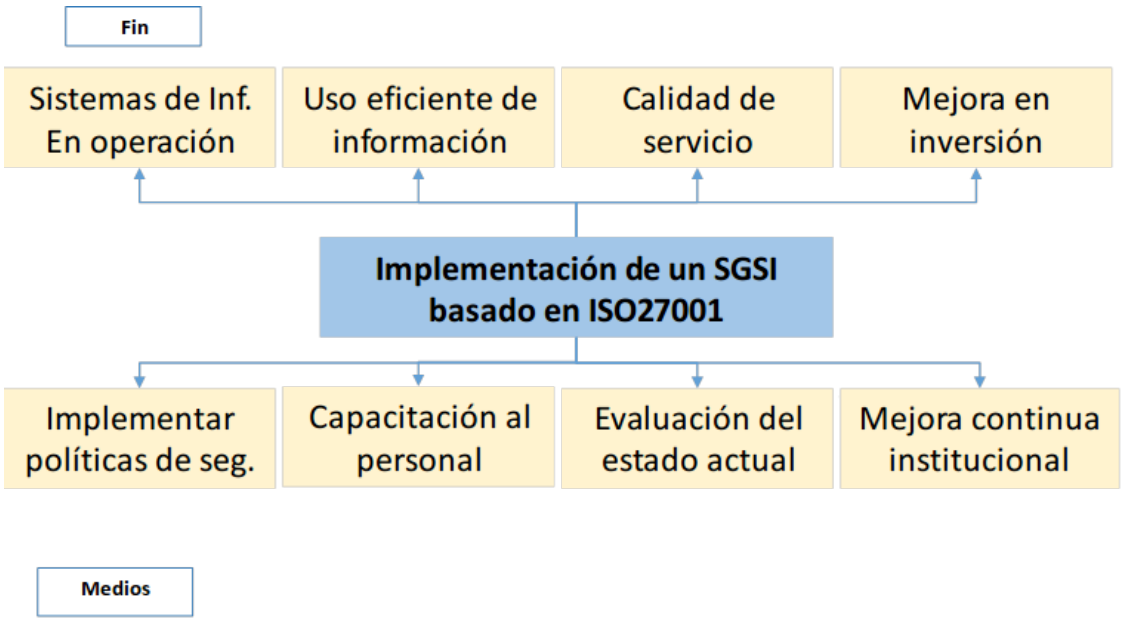


Ilustración 2: Fines y medios

Definición de los Objetivos

Objetivo General

- Implementar los controles relacionados con la gestión documental y control de incidentes de un sistema de gestión de la seguridad de la información la Ventanilla Electrónica Tributaria de la Dirección General de Ingresos basado en los estándares internacionales de la normativa ISO/IEC 27001:2013 y mejores prácticas.

Objetivos Específicos

- Diagnosticar la estructura y procedimientos que existen actualmente en la DGI para conocer el estado actual de la seguridad de la información institucional de la Ventanilla Electrónica.
- Diseñar un plan de acción para la implementación paulatina del Sistema de Gestión de Seguridad de la Información basado en los estándares internacionales de la normativa ISO/IEC 27001:2013 para la DGI.
- Definir los principales aspectos que la Dirección General de Ingresos debe tener en cuenta para implementar el Sistema de Gestión de Seguridad para identificar los riesgos asociados a la integridad, disponibilidad, confidencialidad y no repudio de la información, basado en la normativa ISO/IEC 27001:2013.
- Implementar los controles de seguridad ISO 27001:2013 al Sistema de Ventanilla Electrónica Tributaria (VET) relacionados con la gestión documental y gestión de incidentes.

Justificación

La Dirección General de Ingresos, dentro de sus planes institucionales tiene como base el uso y ampliación de la tecnología para mejorar la atención a los contribuyentes, esto permitirá ampliar servicios y facilitar el cumplimiento de las obligaciones tributarias de los contribuyentes, es por esta razón que está realizando inversiones en todo el aspecto tecnológico, por lo cual es necesario tener un enfoque integral de la tecnología y la seguridad dela información que es administrada por los sistemas tributarios.

Por este motivo el proyecto de investigación propondrá un modelo de implementación de un Sistema de Gestión de la Seguridad de la Información que esté a la medida de la institución y su importancia, a fin que sea revisado por la dirección superior de la institución y hacer un proceso de implementación paulatina de acuerdo a los intereses definidos institucionalmente.

Al desarrollar este Sistema de Gestión de la Seguridad de la Información (SGSI), implicará crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de la información, ayudando a la institución a cumplir con sus objetivos principales, que es obtener recursos necesarios para financiar los proyectos del Estado de Nicaragua, que beneficie a la población en general y ayude al desarrollo del país.

Hipótesis

Con la implementación de un SGSI basado en ISO 27001:2013 se podrán establecer mecanismos de control que mitiguen los riesgos de pérdida de información, confiabilidad, confidencialidad, disponibilidad y no repudio de la información en el Sistema de Ventanilla Electrónica Tributaria de la Dirección General de Ingresos, a un costo razonables, de acuerdo a los principales riesgos identificados.

Metodología

La investigación es de tipo documental y aplicada a una institución, mediante la recolección, revisión de información y documentos se pretende resolver un problema práctico en la seguridad de la información de la institución.

El proyecto iniciará con un análisis de la situación de la seguridad de la información institucional, políticas, planes y proyectos, así como los controles de seguridad existentes a todos los niveles de la DGI Central.

Se identificarán los principales activos de información y realizar los respectos análisis de riesgos de la información seleccionada, ponderando riesgos con probabilidad y obteniendo la matriz de riesgos.

Se procederán a efectuar análisis de los estándares y buenas prácticas a nivel internacional para la escogencia de los procesos más adecuados que se puedan aplicar a nivel de la institución.

La investigación no será experimental ya que es un estudio que no manipulará variables, sino que se observarán y analizarán los fenómenos en su ambiente de desarrollo.

Alcances o Metas

- Analizar la situación actual de la seguridad de la información en base a los 114 controles de la norma ISO/IEC 27002:2013.
- Desarrollar la propuesta hasta la fase de planeación de la norma ISO/IEC 27001:2013.
- Estimar los resultados esperados por la implementación de un subconjunto de controles de la norma ISO/IEC 27002:2013.

CAPITULO I

MARCO TEÓRICO CONCEPTUAL

Modelo del Sistema de Gestión de la Seguridad de la Información

Principios:

Del texto de la norma ISO 27001 pueden extraerse los siguientes elementos como principios básicos del modelo:

Importancia de la información:

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Enfoque de sistemas:

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Conceptos básicos

El concepto básico que sustenta el SGSI es, por supuesto, el de seguridad de la información. Aunque es un concepto difícil de precisar por todos los elementos que implica, generalmente se acepta que son tres los componentes de la seguridad la información: confidencialidad, integridad y disponibilidad.

Confidencialidad: “Asegurar que la información es accesible solo a las personas que están autorizadas para tener acceso.”

Integridad: “Salvaguarda de la precisión y totalidad de la información y los métodos de procesamiento”.

Disponibilidad: “Asegurar que los usuarios autorizados tienen acceso a la información y los activos asociados”.

Vulnerabilidad: La debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Amenazas: Causa potencia de un incidente no deseado, que puede resultar en daño a un sistema u organización.

Estructura del modelo

El modelo del sistema de gestión de la seguridad de la información ISO 27001 sigue la estructura del PHVA. La planificación inicia con la definición del alcance del SGSI, determinando las áreas o procesos de la organización en los que se va a aplicar el sistema. Generalmente se eligen las áreas más críticas o vulnerables en materia de gestión de la información. Luego de definido el alcance, se debe formular y divulgar una política de gestión de la seguridad de la información, que establezca los lineamientos generales que la organización debe tener en cuenta frente a los riesgos de la información, que establezca los lineamientos generales que la organización debe tener en cuenta frente a los riesgos de la información, considerando en ello los requisitos legales, contractuales y propios de la empresa.

El eje central de la planificación del SGSI consiste en identificar los riesgos de la información en relación con las posibles amenazas y los puntos vulnerables de la organización en cuanto a la confiabilidad, seguridad y disponibilidad de la información.

A partir de la identificación de estos riesgos, y de su análisis y valoración, se definirán los planes de control o tratamiento del riesgo, que pretenden llevarlo hasta un nivel aceptable o manejable por la entidad.

La implementación se fundamenta en poner en práctica estos planes de control o tratamiento del riesgo. Incluye también la documentación y la aplicación de los procedimientos necesarios para aplicar tales controles, así como la formación y la concienciación de los empleados respecto a la seguridad de la información y los controles que se han de aplicar. Un elemento importante es el de definir e implementar planes detección y respuesta ante incidentes de seguridad de la información, para reducir el impacto que tales incidentes puedan tener en la operación de la organización.

La fase de verificación incluye la medición del desempeño del SGSI, la evaluación de los riesgos y la eficacia de los controles implementados, la realización de auditorías internas al sistema y la revisión del mismo por parte de la dirección. De estas acciones se desprende el mejoramiento, que incluye la actualización de los planes de seguridad y la definición e implementación de las acciones correctivas y preventivas a que haya lugar.

((Federico Alonso Atehortua Hurtado, 2008))

Los ocho principios de gestión de la ISO

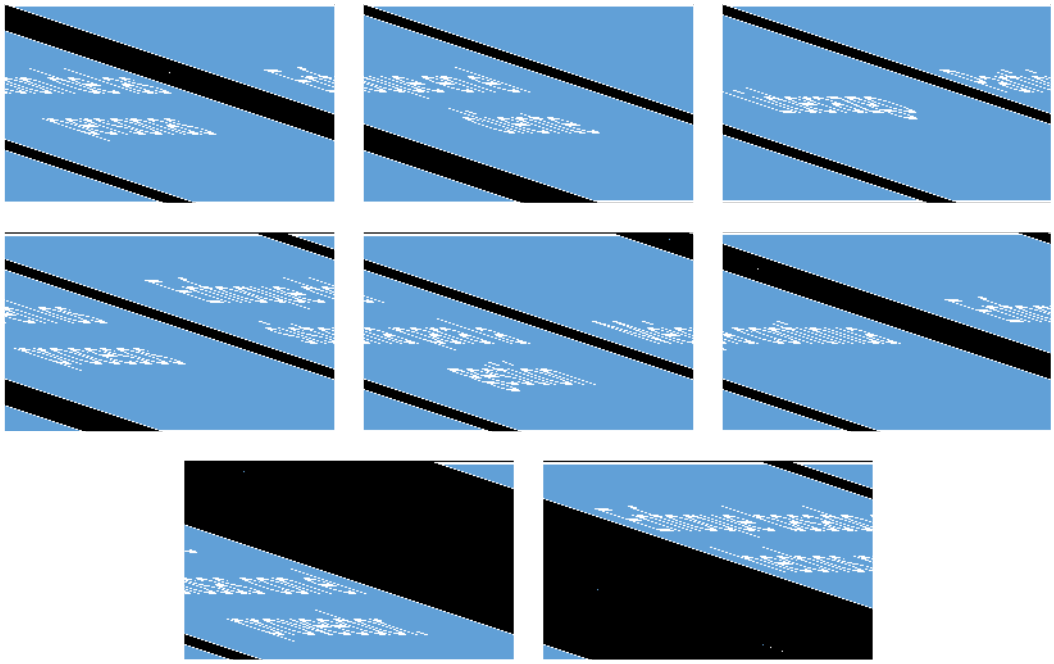


Ilustración 3: Principios de la gestión ISO 27001

Definición del SGSI

Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para conseguir los objetivos del negocio. Se basa en una evaluación del riesgo y de los niveles de aceptación de riesgo de la organización diseñados para tratar y gestionar los riesgos de manera eficaz. Analizar los requisitos para la protección de los activos de información y aplicar controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la aplicación de un SGSI.

(PECB, 2005)

Ciclo de mejora continua

El ciclo de Deming, conocido también como ciclo PDCA (Plan, Do, Check, Act), es un elemento fundamental en la gestión de las organizaciones innovadoras. Esta metodología puede ser utilizada tanto para la mejora reactiva, es decir, mediante decisiones profesionales frente a situaciones cambiantes, como para sistematizar reacciones y buscar soluciones racionales a los problemas.

La utilización del ciclo PDCA en la resolución de problemas permite conocer las causas que los generan, para después atacarlas y de esta forma disminuir o erradicar los efectos que incluyen de manera directa o indirecta en la ausencia de la calidad, obteniendo una mayor efectividad y eficiencia en el desempeño.

Cuando el enfoque del ciclo PDCA se dirige a los procesos, mejora la interpretación de la cadena cliente-proveedor, genera sinergias interdepartamentales y predispone y desarrolla las actitudes y habilidades en el manejo de técnicas de gestión en departamentos autónomos o departamentales.

El abordaje se realiza mediante una combinación de las fases del ciclo de Deming con el método de las 5 “w” y 1 “l”: what, why, who, when, where and how (qué, porqué, quién, dónde, cuándo y cómo).

(Mora Martínez, 2003)

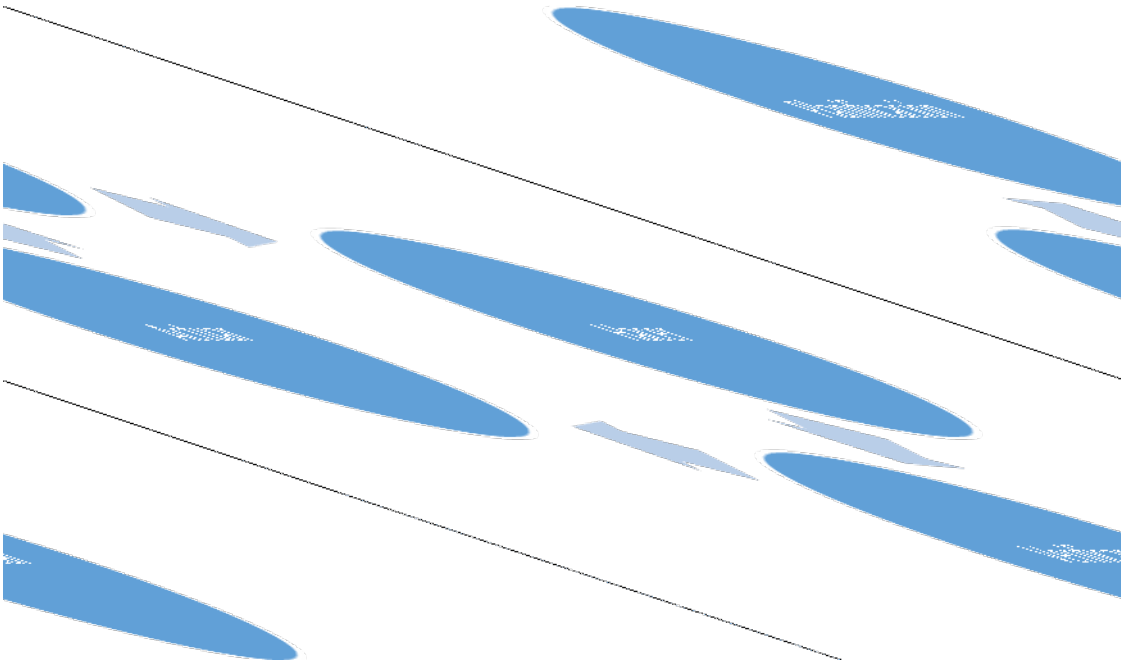


Ilustración 4: Ciclo de Demming

Definición del enfoque para la implementación del SGSI

Una organización que quiera cumplir con la norma ISO 27001 puede considerar varios enfoques sobre la base de:

- Velocidad de implementación
- El alcance
- Nivel de madurez del proceso y los controles de seguridad buscados (en comparación con el SGSI inicial).

Utilizando el enfoque racional, es razonable considerar un período de 6 – 12 meses para el proyecto, desde la concepción hasta la finalización del primer ciclo de auditorías y seguimiento del sistema.

Según una encuesta (“ISO 27001 Encuesta mundial 2008, Certificación europea) de 312 empresas certificadas con la norma ISO 27001, en el 60% de ellas, la propuesta de ejecución tomó menos de doce meses para implementar un SGSI y en el 20% menos de 6 meses. Es de destacar que todas las empresas que han tomado menos de seis meses para implementar un SGSI tenían otro sistema de gestión ya existente en la organización.

(PECB, 2005)

Madurez de un SGSI

Para validar la madurez del SGSI se basará en el método ISM3, este método establece que la seguridad como “El resultado de cumplir o exceder de forma continua un conjunto de objetivos”. Por la naturaleza de los objetivos del negocio difieren entre organizaciones, el enfoque de la seguridad es independiente.

Niveles de Madures:

- 0 No existentes
- 1 Inicial: Se ha efectuado un reconocimiento inicial pero no han procesos estandarizados.
- 2 Repetible: Se han desarrollado los procesos hasta el punto en que se siguen procedimientos
- 3 Definido: Los procedimientos del proceso se han estandarizado y documentado, y se han difundido a través de capacitación.
- 4 Administrado: Se puede administrar y monitorear el cumplimiento de los objetivos definidos.
- 5 Optimizado: Con todas las mejoras continuas establecidas después de revisiones efectuadas.

[1], 2011

Evaluación de riesgos

Una organización que quiera cumplir con la norma ISO 27001 ,deberá como mínimo:

1. Seleccionar y definir una metodología de evaluación de riesgos.
2. Demostrar que la metodología seleccionada proporciona resultados comparables y reproducibles.
3. Definir los criterios para la aceptación de riesgos y determinar los niveles de riesgo aceptables.

Toda organización debe hacer lo siguiente:

- Seleccionar las opciones de tratamiento de riesgos para la seguridad de la información, teniendo en cuenta los resultados de la evaluación de riesgos.
- Determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgos de seguridad de la información.
- Elaborar una declaración de aplicabilidad que contiene los controles necesarios.
- Formular un plan de tratamiento de riesgos de seguridad de la información.
- Obtener la aprobación de los propietarios del plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales para la seguridad de la información.

Evaluación cualitativa: La evaluación cualitativa utiliza una escala de atributos de clasificación para describir la magnitud de las posibles consecuencias (por ejemplo, baja, media y alta) y la probabilidad de que esas consecuencias se produzcan. Se desarrollan escenarios de riesgo mediante la asignación de un nivel de importancia a

las amenazas, vulnerabilidades y el impacto potencial para lograr un nivel de riesgo. Al final se calcula el riesgo y se recomiendan medidas de control adecuadas.

Evaluación cuantitativa: La evaluación cuantitativa utiliza una escala con valores numéricos (en lugar de escalas descriptivas) para las consecuencias como para la probabilidad, utilizando datos de una variedad de fuentes. Se utiliza análisis matemático y financiero mediante la asignación de un valor monetario a cada componente de la evaluación de riesgos y a las pérdidas potenciales.

Metodologías de gestión de riesgo

Método	Origen	Descripción
Octave	Estados Unidos	Perfil de necesidades de seguridad, el estudio de las vulnerabilidades y la estrategia de desarrollo y plan de seguridad.
CRAMM	Reino Unido	La definición de los activos que están en riesgo, análisis de riesgo y vulnerabilidad y la identificación y selección de controles de seguridad.
MICROSOFT	Estados Unidos	La evaluación de riesgos apoya a la decisión, el establecimiento de controles, medición de la eficiencia del programa
TRA	Canadá	Metodología usada por entidades de gobierno
NIST800-30	Estados Unidos	Guía de gestión de riesgo para sistemas de tecnología de la información del gobierno de Estados Unidos.
EBIOS	Francia	Estudio de contexto, definiendo necesidades de seguridad.
MEHARI	Francia	Análisis y clasificación de los activos críticos, el diagnóstico de los servicios de seguridad.

Ejemplo de formato de evaluación de riesgos

Donde el impacto se mide en base al promedio de impacto en los atributos de la seguridad de la información (C= Confidencialidad, I = Integridad, D = Disponibilidad).

Activo	Amenazas	Vulnerabilidades	Impacto			Probabilidad	Riesgo
			C	I	D		

		Probabilidad		
		Baja	Media	Alta
	Impacto	1	2	3
Alto	3	3	6	9
Medio	2	2	4	6
Bajo	1	1	2	3

La Dirección, debe establecer el apetito de riesgo para poder gestionar los riesgos, cuando definimos el apetito de riesgo debemos entender la tolerancia con la cual la institución está dispuesta a tolerar.

Opciones de tratamiento de riesgos

Reducción

Deberían ser seleccionados y justificados controles apropiados para satisfacer las necesidades identificadas en la evaluación de riesgos y el tratamiento de riesgos.

Retención

Es posible que haya ciertos riesgos cuyos controles la organización no será capaz de identificar o que el costo de estos sea mayor que la pérdida potencial, la institución decide vivir con el riesgo.

Transferencia

Se traslada los riesgos a terceros, tales como aseguradoras.

Evitar los riesgos

Cuando los riesgos identificados se consideran demasiado altos o los costos de aplicación de otras opciones de tratamiento exceden los beneficios, se puede tomar la decisión de evitar los riesgos por completo, retirándose de la actividad.

Identificación de los activos de soporte

Categoría	Definición	Ejemplos
Hardware	Elementos físicos de soporte de procesos	Servidores, laptops, impresoras.
Software	Código que soporta procesos	Sistemas operativos, procesadores de texto, bases de datos.
Redes	Todos los dispositivos de telecomunicaciones	Switches, Routers
Personal	Personas involucradas en los procesos	Propietarios, usuarios, programadores.
Sitios	Lugares físicos	Centros de datos, escritorios, oficinas
Estructura de la organización	Marco organizativo asignado para la realización de las actividades	Sede Central, divisiones, departamentos.

(PECB, 2005)

Definición de declaración de aplicabilidad

La declaración de aplicabilidad es más que una simple lista de verificación de los controles de seguridad del Anexo A que se aplicarán en el SGSI. Es un documento fundamental del SGSI que es una referencia para el auditor externo durante la auditoría en una certificación. Este es uno de los primeros documentos que se analizarán. También es uno de los documentos que la Dirección debe validar y aprobar antes del inicio de las operaciones del SGSI.

La declaración de aplicabilidad es la declaración documentada que describe los objetivos de control y los controles que son pertinentes y aplicables al SGSI de la organización.

La organización debe revisar los 114 controles de seguridad en el Anexo A para identificar los que no son aplicables y los que no se consideran en el contexto del SGSI. La mayoría de las organizaciones informa de más de 80 controles de seguridad implementados.

La organización debería justificar las razones de la exclusión de cada control de seguridad del Anexo A que no está incluido en el SGSI.

Los motivos más frecuentes de exclusión son:

- Violación de un requisito legal, estatutario o contractual (Ej. Investigación de antecedentes).
- No hay en la organización actividad relacionada con este control (Ej. Tele trabajo).

(PECB, 2005)

Incidentes de seguridad de la información

La Norma ISO /IEC TR 18044:2004 define incidente de seguridad de la información, como “un único evento o serie de eventos de seguridad de la información inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información”.

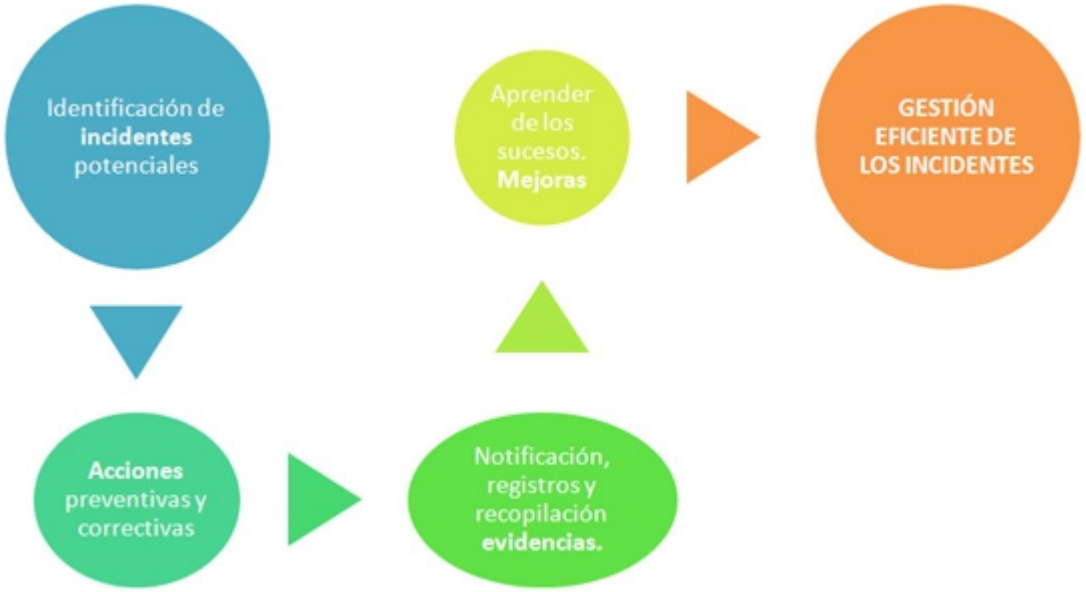


Ilustración 5: Proceso de gestión de incidentes

- El primer documento que recoge la gestión de las incidencias es la Política de Seguridad de la Información que indica los responsables y el método de comunicación de los incidentes a nivel de organización interna y a las autoridades competentes.
- La organización debe definir procesos generales supervisión y mecanismos de control para la identificación y detección temprana de los incidentes, definición de acciones que los prevengan y realizar revisiones periódicas de su eficiencia.
- Las actividades de coordinación interdepartamentales incluyen la propuesta de planes de tratamiento de los incidentes, su revisión y mejora de forma conjunta.
- Debe existir un plan de acción que minimice los efectos de los incidentes sobre el acceso a la información a clientes y terceros, además de existir

controles pertinentes que eviten las amenazas que estos mismo pueden provocar.

- El plan de formación debe incluir un apartado donde se informa sobre las acciones a llevar a cabo en caso de incidente y a quién y cómo comunicarlos.
- En las auditorías internas, se recopilarán todas las evidencias y registros de la gestión de incidentes.
- Durante la Revisión por la Dirección, se analizará la información del informe de incidentes de seguridad que recopile toda la información y los registros sobre el tratamiento de los incidentes, origen, causa, respuesta, soluciones, impacto, interacciones, acciones preventivas y de mejora…Si fuese preciso, la organización debería contratar asesoría externa para la actualización de la información del sector, en aras de prevenir nuevas amenazas.

(ISO 27001: Gestión de incidencias en los Sistemas de Seguridad de la Información, 2013)

Gestión de eventos

Uno de los procesos fundamentales que soportan la gestión de servicios de TI corresponde a la gestión de eventos, proceso que se encarga de monitorear todos los eventos que ocurren en la infraestructura de TI para permitir su operación normal a través de la detección y escalamiento de condiciones de excepción. En consecuencia, una gestión de eventos efectiva depende del conocimiento del estado de la infraestructura de TI a través de la detección oportuna de cualquier desviación de la operación normal o esperada.

Sistemas de monitoreo

Un sistema de monitoreo, es un sistema que censa y/o detecta alertas en la infraestructura de TI para determinar su estado y disponibilidad. Cualquier excepción generará una alerta que necesita ser comunicada a la herramienta o equipo adecuado para tomar acción correctiva o preventiva.

Proceso de monitoreo

El proceso de monitoreo de la infraestructura se realizará de la siguiente manera:

- Clasificación de los equipos y/o servidores de acuerdo a la función y servicio realizado.
- Creación de los grupos de seguimiento y respuesta, así como escalamiento.
- Habilitación del proceso de chequeo activo, consultando el estado de los servicios, equipos y servidores cada cierto tiempo, definido de acuerdo a la prioridad de los mismos.
- Seguimiento a los recursos de hardware, (memoria, disco, procesamiento, etc.).
- Plan de prevención, mediante la programación de mantenimientos periódicos de acuerdo a los parámetros de umbrales.

Monitoreo de la Disponibilidad

El monitoreo de la disponibilidad del servicio y la elaboración de los informes correspondientes son dos de las principales actividades de la Gestión de la Disponibilidad.

Desde el momento de la interrupción del servicio hasta su restitución o "tiempo de parada" el incidente pasa por distintas fases que deben ser analizadas de forma individual:

- Tiempo de detección: es el tiempo que transcurre desde que ocurre el fallo hasta que la organización TI tiene constancia del mismo.
- Tiempo de respuesta: es el tiempo que transcurre desde la detección del problema hasta que se realiza un registro y diagnóstico del incidente.
- Tiempo de reparación/recuperación: periodo de tiempo utilizado para reparar el fallo o encontrar una solución temporal al mismo y devolver el sistema a la situación anterior a la interrupción del servicio.

Es importante determinar métricas que permitan medir con precisión las diferentes fases del ciclo de vida de la interrupción del servicio. El cliente debe conocer estas métricas y dar su conformidad a las mismas para evitar malentendidos. En algunos casos es difícil determinar si el sistema está "caído o en funcionamiento" y la interpretación puede diferir entre proveedores y clientes, por lo tanto, estás métricas deben de poder expresarse en términos que el cliente pueda entender.

Algunos de los parámetros que suele utilizar la Gestión de la Disponibilidad y que debe poner a disposición del cliente en los informes de disponibilidad correspondientes incluyen:

- Tiempo Medio de Parada (Downtime): que es el tiempo promedio de duración de una interrupción de servicio, e incluye el tiempo de detección, respuesta y resolución.
- Tiempo Medio entre Fallos (Uptime): es el tiempo medio durante el cual el servicio está disponible sin interrupciones.
- Tiempo Medio entre Incidentes: es el tiempo medio transcurrido entre incidentes que es igual a la suma del Tiempo Medio de Parada y el Tiempo Medio

entre Fallos. El Tiempo Medio entre Incidentes es una medida de la fiabilidad del sistema.

(Fundamentos de gestión de ITIL, 2013)

Sistemas de Gestión Documental

Los sistemas de gestión documental se utilizan también para facilitar al usuario el acceso a la masa de información disponible en Internet, organizándola de distintas maneras. De hecho, la gestión documental está incorporando otras tecnologías como workflow, imaging, email, groupware y filtros. Algunos sistemas integran capacidades de workflow muy consistentes, incidiendo en la administración y re dirección de documentos compuestos que pueden contener imágenes, textos, hojas de cálculo, sonido o gráficos.

Trabajo en grupo o workflow

La gestión de flujos de trabajo o workflow se definen como la automatización de los procesos de negocio mediante la gestión de los movimientos de información, documentos y transacciones generados, a través de la secuencia de los pasos que forman los procedimientos de trabajo. Una aplicación de workflow considera, desde el principio hasta el final, todos los pasos de un proceso, incluyendo sus condiciones de excepción, generalmente basadas en las reglas de negocio ya establecidas. La llave en la gestión de workflow, es el seguimiento de los procesos, su información asociada y el estado en cada paso implicado en la organización.

(Llauger, 2001)

Sistemas OpenSource

OpenKM

OpenKM es una aplicación web de gestión documental que utiliza estándares y tecnologías OpenSource.

OpenKM proporciona capacidades completas de gestión de documentos incluyendo el control de versiones, metadatos, escaneo, comentarios, foros sobre el documento, workflow, etc. Esto permite que las actividades sociales en torno al contenido se utilicen para conectar a las personas a otras personas, la información a la información, y las personas a la información., ayudando a gestionar, de forma más eficiente, la inteligencia colectiva que reside en los recursos humanos de la compañía.

OpenKM integra en una sola aplicación fácil de usar todas las funcionalidades para colaborar, gestionar y buscar documentos.

(openkm, 2016)

Eramba

Construido por y para la seguridad, TI, profesionales de Auditoría y Cumplimiento que sólo están interesados en un valor tangible.

Algunos Módulos que ofrece:

- Programa
- Organización
- Gestión de Activos
- Catálogo de control
- Gestión de cumplimiento

- Operaciones de Seguridad
- Gestión del Sistema
- Programas de concientización

(eramba, 2016)

Kimios

http://www.kimios.com/

Kimios tiene como objetivo optimizar la cadena de producción de documentos y de ser una alternativa a los sistemas ECM pesados (Enterprise Content Management) que suelen ser de gran tamaño.

Una herramienta diaria

Kimios es el sistema de gestión de documentos (DMS) que tiene como objetivo ser el más potente entorno de producción de documentos más fácil, así como. Debido a que producen y acceso a los mismos son tareas muy frecuentes en las organizaciones modernas, Kimios ha hecho facilitando las operaciones de su principal objetivo.

Porque no sólo se trata de contenidos web

El modelo de producción real, donde los usuarios se ven obligados a utilizar diferentes tipos de aplicaciones web ya no es la única solución. Usando Kimios permite a los usuarios acceder a las funciones de colaboración directamente desde su escritorio y sus entornos de Microsoft Office.

Usted es el administrador

La estructura de un repositorio de documentos evoluciona constantemente, es por eso Kimios permite a los usuarios configurar embargo propia estructura de carpetas,

mapeo de metadatos y flujo de trabajo de arquitectura. ¡Olvídate de los archivos de configuración XML y convertirse en el administrador de su repositorio!

Buscar, encontrar

Kimios ha hecho su sistema de indexación y búsqueda de una característica clave del repositorio de documentos. Cada documento se indexa junto con su contenido y sus metadatos y se puede buscar con texto completo y consultas booleanas. Los usuarios pueden combinar varios criterios de búsqueda y luego hacer Kimios un poderoso motor de búsqueda.

Building un repositorio de documentos fiable ya no puede disociarse de una fuerte dimensión colaborativa. Kimios es el DMS de código abierto que ofrece un acceso único a las funciones de colaboración.

Control de versiones

El control de versiones es la base del sistema de la base Kimios. Cada usuario puede contribuir a un mismo documento, preservando su integridad y su reversibilidad. Contenido, metadatos y comentarios son partes del sistema de control de versiones lo que se garantiza la trazabilidad completa del ciclo de vida de los documentos.

Flujos de trabajo

Kimios hace que el diseño del flujo de trabajo más fácil. Los usuarios pueden emitir solicitudes de flujo de trabajo a grupos o usuarios autorizados. Cada paso de un flujo de trabajo es totalmente personalizable y se puede configurar para enviar notificaciones por correo electrónico.

Una Arquitectura Arquitectura Orientada a Servicios

Kimios se basa en una arquitectura totalmente orientada a servicios (SOA). Todas las aplicaciones (cliente Web, Kimios Explorer, Kimios para Office) son clientes de terceros conectados al servidor central Kimios que expone una capa de servicio web que cubre todas las funciones de DMS. Esta arquitectura ofrece sólidas capacidades de interoperabilidad que se pueden utilizar a través de diferentes APIs disponibles en dotNet, PHP y Java.

Un modelo abierto

El código fuente del servidor Kimios es completamente de código abierto y disponible bajo licencia GPL. Cualquier desarrollador puede acceder, modificar o mejorar las características del repositorio de documentos. Además, Kimios ofrece varias interfaces que se pueden implementar con el fin de personalizar el sistema de gestión de usuarios, el sistema de gestión de reglas, la estructura metadatos o el sistema de indexación.

(kimios, 2016)

Alfresco

https://www.alfresco.com/

ECM + BPM

Alfresco es líder en la convergencia de las ECM y BPM y ayudar a crear procesos eficientes, conectados que el contenido en su contexto actual. Más de 1,800 empresas en 195 países confían en Alfresco, incluyendo líderes en servicios financieros, salud y el sector público. Una red global de socios y muchos desarrolladores de código abierto están listos para ayudarle a utilizar para acelerar su transformación digital.

ECM y BPM plataforma abierta y altamente integrado de Alfresco es simple, elegante y seguro. Alinear las personas, el contenido y los procesos para recuperar el control

del contenido de crítica para el negocio, fortalecer el cumplimiento y optimizar los procesos, toma de colaboración fácil para los empleados, socios y clientes.

(Alfresco, 2016)

Roles y Responsabilidades

Las organizaciones bien estructuradas pueden tomar las decisiones correctas en poco tiempo y ejecutarlas con éxito. Para ello es fundamental que los roles y responsabilidades estén definidos con claridad, algo que también resulta esencial en el proceso de Diseño del Servicio. Uno de los modelos que pueden resultar útiles en este sentido es el modelo RACI. RACI es un acrónimo formado por las iniciales de los cuatro roles más importantes:

- Responsable de ejecutar (Responsible): La persona que es responsable de realizar la tarea.
- Alto responsable (Accountable): Aquella única persona que es responsable final de la tarea.
- Consultado (Consulted): Personas que asesoran.
- Informado (Informed): Personas que deben recibir información sobre el progreso del proyecto.
- Existe una variación adicional que es Support, que consiste en el personal de apoyo asignado para cumplir la actividad.

Para crear un sistema RACI son necesarios los siguientes pasos:

- Identificar actividades y procesos.
- Identificar y definir roles funcionales

- Llevar a cabo reuniones y delegar los códigos RACI
- Identificar carencias y posibles solapamientos
- Comunicar el esquema y tener en cuenta la retro alimentación.
- Comprobar que se siguen las asignaciones.

(Bon, 2010)

Naturaleza y funciones de la Dirección General de Ingresos

Visión

Ser una Administración Tributaria profesional, ágil y sencilla al servicio del pueblo Nicaragüense.

Misión

Recaudar los tributos internos con equidad, transparencia y eficiencia, promoviendo la cultura Tributaria y cumpliendo con el Marco Legal, aportando al Gobierno recursos para el desarrollo económico y social del país.

Objetivos institucionales

Los principales objetivos de la institución son:

- Crear un nuevo modelo de fiscalización que permita alcanzar un mayor control de los contribuyentes.
- Fortalecimiento de los servicios y atención por medios electrónicos: Para agilizar y trámites tributarios.
- Gestión efectiva del registro: Para mejorar e identificar los contribuyentes, como uno de los puntos de partida del ciclo de vida que es clave para formalizar los procesos tributarios.

- Generación efectiva de cuenta corriente, omisos y cobranzas: Con el objetivo de mantener actualizada la cuenta corriente y por ende los procesos de control de omisidad y morosidad.
- Refundación de Grandes contribuyentes: Como la oficina clave para la atención a los principales contribuyentes del país, que aportan más del 67% de la recaudación del país.
- Rediseño del proceso de devolución del IVA: Para integrarlo con los procesos de fiscalización para lograr un mayor control del proceso.
- Actualización y mantenimiento de las TICS: Como herramienta de apoyo para el cumplimiento de los objetivos de recaudación.
- Modernización de la gestión de recursos humanos: Que permitirá la obtención del personal necesario y con las competencias requeridas para cumplir los objetivos institucionales.

(http://www.dgi.gob.ni/interna.php?sec=11, 2016)

Marco Legal de la institución

Artículo 2.- Naturaleza La Dirección General de Ingresos (DGI) y la Dirección General de Servicios Aduaneros (DGA) son entes descentralizados con personalidad jurídica propia, que gozan de autonomía técnica, administrativa y e gestión de sus recursos humanos. Están bajo la rectoría sectorial del Ministerio de Hacienda y Crédito Público, al que le compete definir, supervisar y controlar la política tributaria del Estado y verificar el cumplimiento de las recaudaciones y de los planes estratégicos y operativos de la DGI y de la DGA.

Artículo 3.- Objetivos de la DGI: La DGI tiene a su cargo la administración de los Ingresos Tributarios y las relaciones jurídicas derivadas de ellos, así como los otros

Ingresos No Tributarios que se regulen a favor del Estado, exceptuando los Tributos Aduaneros, Municipales y las Contribuciones de Seguridad Social, que se rigen por sus leyes específicas.

Artículo 5.- Funciones de la DGI:

La Dirección General de Ingresos tendrá las siguientes funciones:

1) Cumplir y hacer cumplir las leyes, actos y disposiciones que establecen o regulan los ingresos a favor del Estado y que estén bajo su jurisdicción, a fin de que estos ingresos sean percibidos a su debido tiempo, con exactitud y justicia.

2) Requerir el pago y percibir de los contribuyentes y responsables los tributos adeudados y, en su caso, los intereses y multas previstos en las leyes tributarias.

3) Indicar las personas naturales o jurídicas que deben presentar las declaraciones tributarias dentro de los plazos o términos que señalan las leyes tributarias y brindarles asesoría para la formulación de dichas declaraciones.

4) Asignar el número RUC a contribuyentes y responsables.

5) Efectuar reparos conforme la ley para el efecto de liquidar el tributo.

6) Modificar las declaraciones, exigir aclaraciones y adiciones, y efectuar los cambios que estime convenientes de acuerdo con las informaciones suministradas por el declarante o las que se hayan recibido de otras fuentes.

7) Autorizar a determinados contribuyentes para que lleven una contabilidad simplificada.

8) Otorgar autorización, previa solicitud del contribuyente y responsable, para que los registros contables puedan llevarse por medios distintos al uso manual, incluso la emisión de factura.

9) Verificar y controlar el cumplimiento de las normas tributarias y aplicar las sanciones que legalmente correspondan a los infractores.

10) Requerir el auxilio de la fuerza pública cuando hubiere impedimento en el desempeño de las funciones y facultades que le confieren las leyes.

11) Establecer mediante disposición administrativa las diferentes clasificaciones de contribuyentes y responsables del sistema tributario a fin de ejercer un mejor control fiscal.

12) Solicitar a instancias e instituciones públicas extranjeras el acceso a la información necesaria para evitar la evasión fiscal, de conformidad con las leyes y tratados internacionales en materia fiscal.

13) Proporcionar bajo el principio de reciprocidad, la asistencia que le soliciten instancias supervisoras y reguladoras de otros países con los cuales se tengan firmados acuerdos o formen parte de convenciones internacionales de las que Nicaragua sea parte.

14) Requerir de todas las organizaciones del Estado las informaciones de carácter tributario que demande para el ejercicio de sus funciones.

(Ley creadora de la Dirección General de Servicios Aduaneros y de reforma de la ley creadora de la Dirección General de Ingresos, 2000)

Infraestructura y Descripción del Sistema "Ventanilla Electrónica Tributaria"

Objetivo general del sistema

- Permitir a los contribuyentes registrados realizar transacciones tributarias en línea.

Descripción General de la Operación del Sistema

La Ventanilla Electrónica Tributaria, es un sistema para uso de los contribuyentes registrados en la administración tributaria, en el cual realizan las principales transacciones tributarias en línea.

En la actualidad el sistema brinda servicio a más del 97% de las transacciones realizadas por la DGI, es decir, casi la totalidad de las operaciones realizadas de declaración, pagos, solvencias, etc. Son realizadas en línea, a excepción de ciertos servicios que están aún en proceso de desarrollo para su integración en la VET.

Los contribuyentes deben estar inscritos en las oficinas de la DGI, previo al uso del sistema y deben firmar contrato para el uso del mismo.

Este sistema es de alta criticidad, puesto que a través del mismo entra aproximadamente el 95% de la recaudación del país, con más de 115,000 usuarios registrados.

La población de Nicaragua es de aproximadamente 6.3 millones de personas, que es el segundo país menos poblado de Centroamérica.

Transacciones en línea realizadas

- Declaración en línea
- Pagos, gestionados a través de las instituciones bancarias.

- Generación de Estados de Cuenta
- Emisión de solvencias
- Consultas de documentos

Infraestructura del Sistema

El sistema es un sistema transaccional con arquitectura web.

Está basado en la siguiente plataforma LAMP (Linux, Apache, MySQL y PHP):

- Sistemas Operativos Linux SuSE Enterprise 11
- Apache 2.2
- MySQL 5.5,
- Adabas 6.3
- PHP 5.3
- Plataforma de Virtualización VMWare 5.5.
- Adicionalmente hace uso de servicios desarrollados en plataforma de .NET.

Descripción de los procesos

Declaraciones en línea

Las declaraciones en línea son los reportes de ingresos que deben presentar todos los contribuyentes inscritos en la administración tributaria, de acuerdo a sus obligaciones fiscales dispuestas por la Ley Tributaria Nicaragüense.

Estos se presentan utilizando una plantilla de Excel, con una estructura definida, indicando los ingresos, créditos fiscales, deducciones y otros rubros que se deben detallar en dicho archivo de Excel y para ciertos contribuyentes se presenta un

formulario electrónico donde son digitados los valores de las declaraciones a presentar.

Este se sube a la Ventanilla Electrónica Tributaria, indicando el RUC (NIT Número de Identidad Tributaria), período que se está declarando.

Según los impuestos a los cuales está obligado a declarar el contribuyente, se calculan los totales en base al documento que se carga, aplicando las respectivas validaciones de seguridad y de validación de negocio que permita confirmar que el documento es válido, que cumple con los requisitos de ley, y adicionalmente que los valores presentados no tengan errores y sean los correctos.

Una vez que se presente el reporte sumario de los datos presentados, el contribuyente confirma la presentación de la declaración, y si esta tiene saldo a pagar, se genera un documento con un número de identidad (BIT Boleta de Información Tributaria) para proceder a cancelar en cualquier oficina de la DGI o entidad bancaria autorizada.

Pagos gestionados realizados en entidades bancarias

Las transacciones de pagos no son realizadas directamente en la Ventanilla Electrónica Tributaria, estos pagos son realizados en los portales de las entidades bancarias, en las ventanillas de los bancos, o en las oficinas de la DGI. En la Ventanilla Se presentan los enlaces a los diferentes bancos autorizados a recibir pagos, una vez presentada la declaración.

Para realizar el pago se debe utilizar el número de BIT (Boleta de Información Tributaria) para identificar los montos, impuestos y períodos a los cuales se aplicará el pago.

Los bancos realizan el intercambio de información usando servicios web, disponibles a través de enlaces dedicados y/o VPNs.

Generación de Estados de Cuenta

Los estados de cuenta de los contribuyentes con consultas efectuadas a las diferentes transacciones realizadas. Estas se realizan en pantalla y se define un rango de fechas como datos de entrada.

En esta consulta se detallan las declaraciones, pagos, créditos y débitos efectuados por los contribuyentes en un rango de fecha determinado.

Adicionalmente permite consultar si un contribuyente se encuentra al día con sus obligaciones tributarias o si el mismo presenta morosidad u omisidad en las declaraciones a las cuales está obligado a presentar.

Emisión de solvencias

Las solvencias fiscales son documentos que la administración tributaria emite a solicitud de los contribuyentes certificando su solvencia en los tributos. Este documento es requerido por ley para efectuar diferentes trámites, tales como: Gestiones aduaneras, así como otros trámites expresos por ley.

Este documento se genera a través de la Ventanilla Electrónica Tributaria a los contribuyentes que estén al día con sus tributos en línea, en el cual se genera un documento PDF con los datos generales del contribuyente así como el período de vigencia del documento (es válido hasta la próxima fecha de vencimiento de sus tributos), así como un id que identifica de forma única el documento.

Este documento generado debe ser impreso por el contribuyente y adherirle un timbre fiscal.

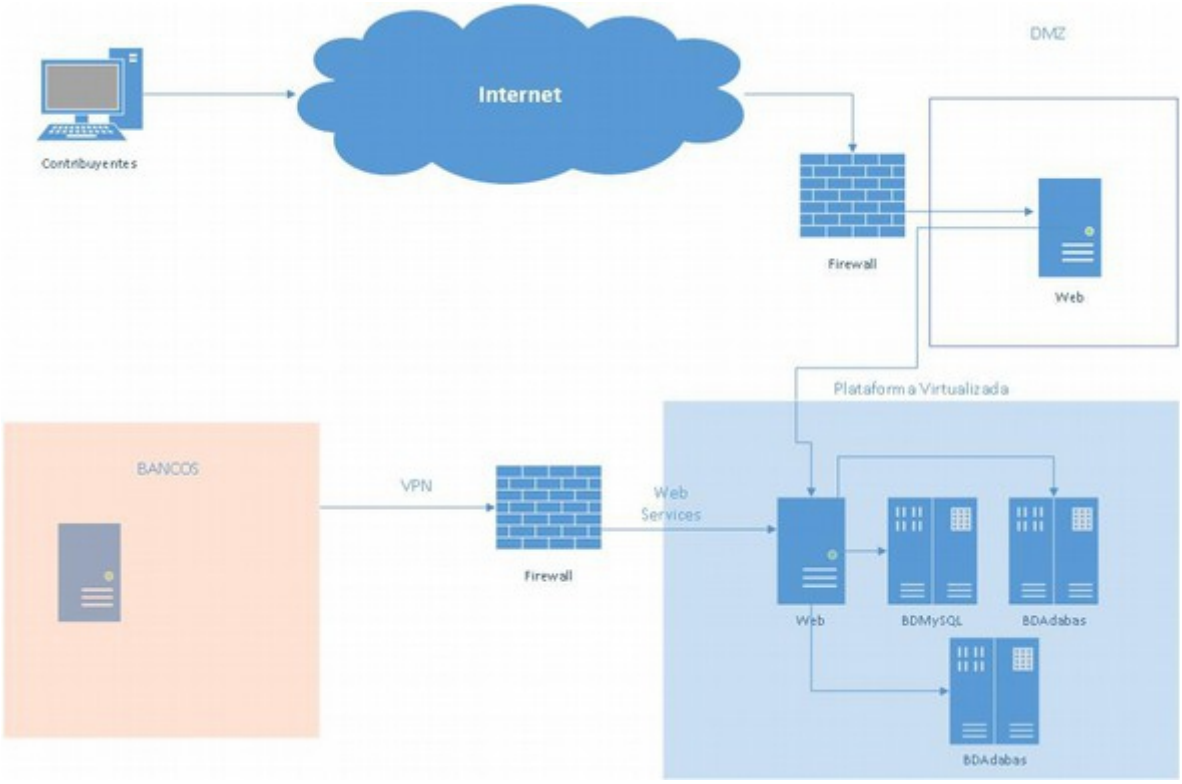
Adicionalmente existe una consulta pública donde se puede consultar en línea la validez del documento usando su id.

Consultas de documentos

Las consultas de los documentos son operaciones de consulta de los diferentes documentos generados por el contribuyente: pagos, solvencias. Estos datos se pueden consultar usando su número de identificación.

Adicionalmente existen consultas públicas de los documentos donde se puede validar la legitimidad de los documentos generados en la VET.

Diagrama Lógico del Sistema



Personal involucrado con la gestión de la VET

Artículo 10.- Organización de la DGI: La Dirección General de Ingresos (DGI) estará conformada por: la Dirección Superior, Sub Dirección General de Planes y Normas;

Sub Dirección General de Operaciones; Asesoría; División de Revisión de Recursos; División de Auditoría; División General de Recursos Humanos; División General de Administración Financiera; División de Planes y Control de Gestión; División Jurídico-Técnica; División de Información y Sistemas; División de Fiscalización; División de Administraciones de Rentas; División de Control de Exoneraciones, División de Catastro Fiscal y División de Asesoría al Contribuyente. Esta organización puede ser ampliada y modificada por el Reglamento de la presente Ley.

Cargos relacionados con el SGSI

Cargo	Rol	Descripción
Director General	Director.	Dirigir, coordinar, supervisar y evaluar el desarrollo de las actividades técnicas y administrativas de la institución a su cargo, así como su estructura orgánica y funcional
Director de Registro Recaudación y Cobranzas	Normativo	Establece los requerimientos del negocio y funcionalidad del sistema de Ventanilla Electrónica Tributaria
Director de Informática y Sistemas	Dirección Técnica	Gestiona los procesos automatizados del Sistema de Ventanilla Electrónica Tributaria.
Jefe de Sistemas	Gestión de Sistemas	Gestiona el desarrollo y pruebas de calidad del Sistema de Ventanilla Electrónica Tributaria. Subordinado al Director de Informática y Sistemas
Jefe de Tecnología	Gestión de infraestructura	Gestiona la infraestructura del Sistema de Ventanilla Electrónica Tributaria. Subordinado al Director de Informática y Sistemas
Director Administrativo Financiero	Gestión de las finanzas y administración	Gestiona los recursos financieros y administrativos (Finanzas y activos).
Servicios generales		Gestiona la administración y seguridad física de la institución y

		sus instalaciones.
Oficial de seguridad	Gestión y seguimiento del SGSI	Esta figura no existe actualmente en la institución, se propone la creación de la figura en dependencia directa del Director General.
Director de Recursos Humanos	Gestión y seguimiento del personal	Gestiona y administra los recursos humanos institucionales.
Director Jurídico Técnico	Gestión legal	Analiza y gestiona los requerimientos legales de la institución.
Director de planeación estratégica	Gestión y evaluación de estrategias institucionales	Controla y evalúa la gestión de institución relativa a los planes y metas propuestas. Controla documentación, manuales y procedimientos organizativos.

Capitulo II

DESARROLLO Y JUSTIFICACIÓN

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27001:2013 EN LA DGI

Alcance de la implementación propuesta

El alcance general es la implementación paulatina del SGSI en la DGI específicamente en el Sistema de Ventanilla Electrónica Tributaria, una vez alcanzado este objetivo se puede iterar y aumentar el alcance a otros sistemas y/o áreas críticas de la institución, siguiendo el plan de mejora continua que propone ISO27001:2013.

Se definirán iniciativas o proyectos que en su conjunto formarán parte del SGSI, esto a fin de gestionar eficientemente el proceso de implementación.

Se hará énfasis en el trabajo documental inicial, que es la base de planificación del SGSI para su alineación con las necesidades de seguridad del negocio.

Aunque los requisitos establecidos en la norma ISO 27001:2013 son genéricos, si una organización declara que cumple con la norma, no se deberá excluir ninguno de los requisitos definidos en los incisos 4, 5, 6, 7 , 8, 9 y 10.

Ruta de implementación

La implementación se hará mediante un proceso inicial de análisis que determine el estado actual de la seguridad de la información, determine la brecha entre los controles existentes con lo establecido en ISO 27001 y la creación de proyectos de implementación de controles, basado en un enfoque iterativo, que se irá incrementando una vez implementados los controles de forma exitosa. Esto en vista que pueden existir controles ya implementados que pueden ajustarse a ISO 27001, pero a la vez no existen definiciones básicas del contexto de un SGSI. “Cláusulas de la 4 a la 10” ISO 27001:

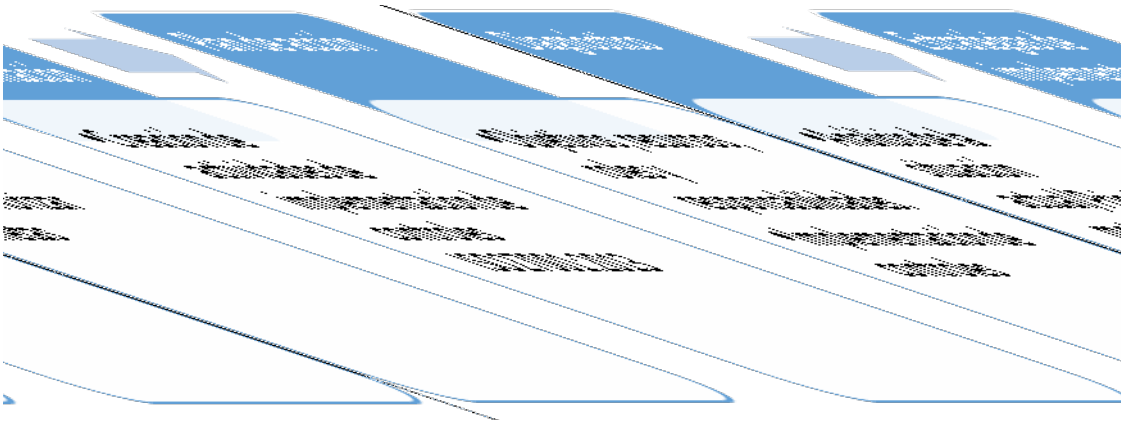


Ilustración 6: Estrategia de implementacikón

Diagnóstico de la situación actual de la institución

El diagnóstico de la situación actual se elaboró mediante la revisión de los controles y políticas existentes en la institución, relacionadas directamente con el Sistema de Ventanilla Electrónica Tributaria.

Siguiendo la siguiente metodología:

En el diagnóstico se contempla la evaluación de los diferentes aspectos de la ISO 27001:2013 que abarca las diferentes cláusulas de la norma:

Así como los controles detallados en el anexo ISO27002:2013.

Entrevistas con los cargos claves

El Método de entrevista se aplicó al personal clave en la definición de procesos y administración del Sistema de Ventanilla Electrónica Tributaria SIT. Comenzando con la Dirección Superior, la cual garantiza su compromiso con la implementación del

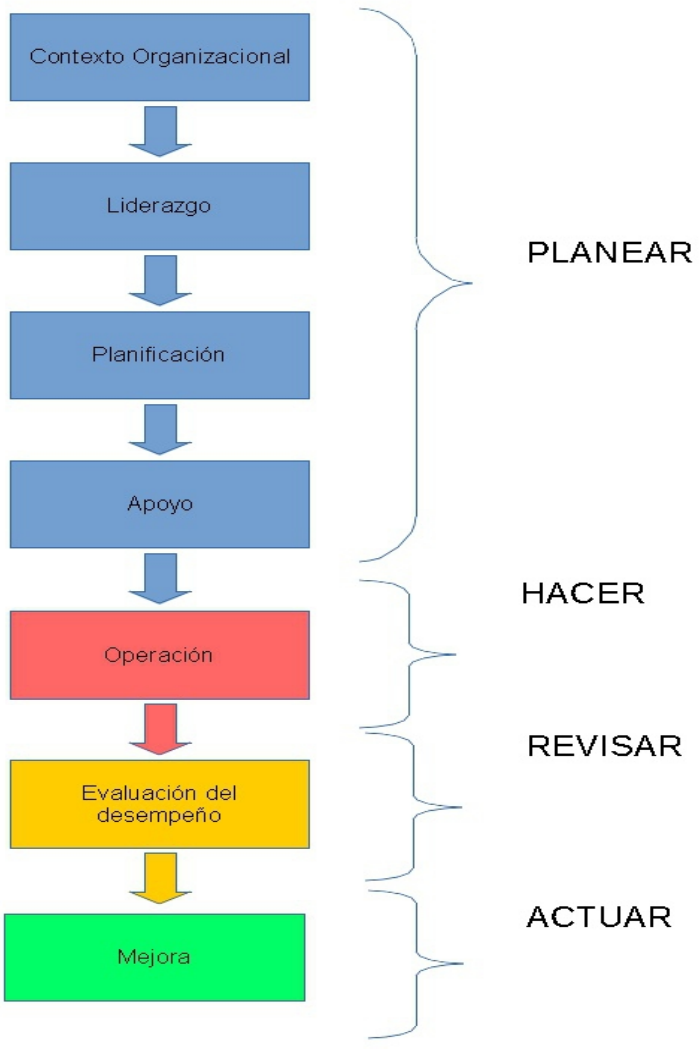


Ilustración 8: Ciclo de Demming con ISO 27001

SGSI mediante el patrocinio, impulso y evaluación del mismo. El detalle y formato de la entrevista puede verse en anexo I.

Se entrevistaron a los siguientes cargos, para determinar el nivel de madurez de los controles existentes:

- Director General
- Director de Informática y Sistemas
- Jefe de Sistemas
- Jefe de Tecnología

Análisis de la información

Es parte fundamental del SGSI basado en ISO 27001:2013 que la seguridad de la información debe estar alineada al negocio y no a lo inverso.

Conocer el contexto de la organización es fundamental, así como recibir el apoyo debido de la dirección, son pasos fundamentales en la implementación del SGSI.

Requisitos ISO27001	Definición	Observaciones
Clausula 4: Contexto de la Organización	Determinar los problemas externos e internos así como requisitos claros para considerar las partes interesadas. El contexto determina la política de SI, los objetivos y la forma en que la organización tendrá en cuenta el riesgo y el efecto del riesgo en su negocio y los requisitos de las partes interesadas pueden incluir los	No existe documentación definiendo alcance, objetivos, ni requerimiento de partes interesadas que se necesiten identificar. Existen requisitos legales que se deben cumplir (definido según las leyes de la

	requisitos legales, reglamentarios y las obligaciones contractuales	Contraloría General de la República).
Cláusula 5: Liderazgo	Resume los requisitos específicos para el papel de la alta dirección en el SGSI y delinea formas específicas para demostrar la gestión y su compromiso con el sistema.	Se revisión que existen planteamientos estratégicos para la creación del SGSI, que se está preparando presupuesto para su implementación. Pero no existe definida una política general de seguridad, solamente existen documentos normativos generales, pero que no comprenden todos los aspectos requeridos en una política. Se determinó que existe apoyo a la creación del SGSI de parte de la Dirección General.
Cláusula 6: Planificación	Establecimiento de objetivos y principios rectores para el SGSI y planificar el SGSI con base en el contexto de la organización debe ser tenido en cuenta a través de la consideración de los riesgos y oportunidades, los objetivos de la organización deben estar claramente definidos junto con los planes para alcanzarlos.	No están definidos los objetivos específicos del SGSI. No están definidas metodologías de análisis de riesgos que sirvan como base para la selección apropiada de controles.
Cláusula 7:	Lo necesario para establecer, implementar, mantener y	Existen recursos presupuestados para el

Soporte	mejorar continuamente un SGSI así como los requerimientos de recursos o competencias de las personas involucradas, conocimiento, comunicación y requisitos para la gestión de documentos donde se da más énfasis en el contenido en lugar del nombre.	inicio del proceso de implementación, pero no se han especificado las definiciones requeridas. No existe un sistema de gestión documental que sirva como medio para conocer, comunicar los registrar y controlar la documentación requerida del sistema de gestión de seguridad de la información.
Cláusula 8: Operaciones	Las organizaciones deben planificar, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad de la información se debe llevar a cabo valoraciones de riesgo de SI a intervalos planificados y la implementación de un Plan de Tratamiento de Riesgos de SI.	No se ha definido un proceso de control operativo de la seguridad ni se aplican evaluaciones periódicas de riesgo.
Cláusula 9: Evaluación del desempeño	Auditorías internas y revisión por la dirección de métodos claves de la revisión del rendimiento del SGSI y herramientas para su mejora continua.	Existen auditorías internas y revisión de los procesos claves de la institución, pero al no existir un SGSI no se aplica al mismo.
Cláusula 10: Mejora continua	Las no conformidades de los SGSI tienen que ser tratadas junto con las acciones correctivas para asegurarse de que no vuelvan a ocurrir.	No existe control de no conformidades en relación al ISO 27001. Existen procesos de revisión que se les efectúa mejora pero al no existir el SGSI no se

		aplica.

Con base al análisis efectuado se puede determinar que estado actual de la seguridad de la información de la institución es inicial.

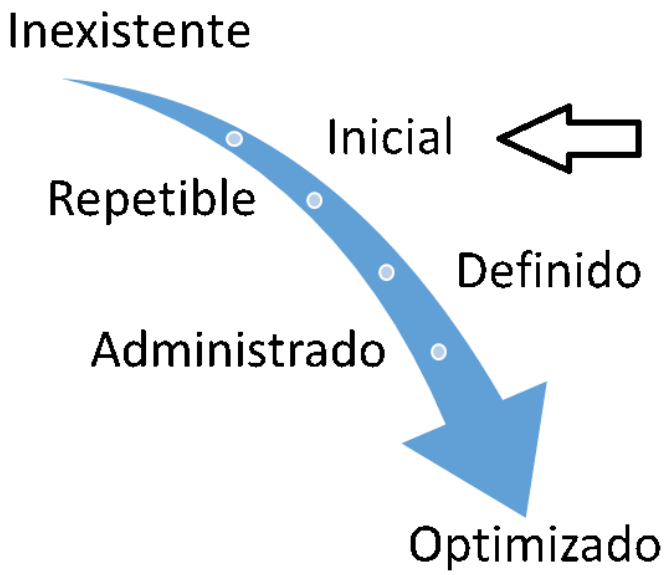


Ilustración 9: Estado de la seguridad

Como objetivo general nos concentramos en mantener el sistema en un estado 4 (Gestionado cuantitativamente), que es el paso previo para la mejora continua.

Estrategia de implementación

Para la implementación exitosa debe tomar en cuenta la complejidad de las operaciones, costos de implementación, personal y sobre todo las necesidades del negocio. La seguridad de la información debe estar alineada al negocio. En nuestro trabajo tomando en cuenta la importancia para el negocio del Sistema Ventanilla Electrónica Tributaria, se propondrá como la implementación de los controles documentales, puesto que estos servirán como base de los controles de sistemas que forman el SGSI basado en ISO 27001:2013, así como la gestión de incidentes.

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27001:2013 EN LA DGI

Tradicionalmente los sistemas se han implementado de forma secuencial, pero por lo general esto conlleva un gran consumo de recursos, tanto humanos como presupuestarios, por la planificación, aprobación o aplicación y tiende a agotar al equipo de trabajo involucrado, con un mayor riesgo de abandono del proyecto.

Por tal razón se propone un enfoque de implementación basado en los siguientes principios:

1. Enfocarse en el negocio, integrando en el entorno institucional, elegir los dominios relacionados con la actividad de la institución.
2. Enfoque sistemático, evitando la aplicación de procesos aislados.
3. Enfoque sistemático, mediante la aplicación de las mejores prácticas de gestión de proyectos.
4. Enfoque integrado, unificando la administración de seguridad, no teniendo diferentes sistemas, si no integrando con otros: (COBIT, etc.)
5. Enfoque iterativo, con un rápido establecimiento de un proceso mínimo y comenzar a mejorar a partir de este.

Es necesario identificar y nombrar formalmente a un Director de Proyecto del SGSI, en nuestro caso, el oficial de seguridad, sería la figura creada que tendrá a cargo el proyecto de implementación, una vez finalizado, gestionará y administrará el sistema.

Este Director de Proyecto deberá ser nombrado por el Director General de Ingresos, a fin que tenga las facultades necesarias para poder llevar a cabo la actividad.

Es importante dentro del proceso de implementación tomar en cuenta la participación de toda las personas, en todos los niveles, ya que su compromiso posibilita que sus habilidades se utilicen para el proceso del SGSI.

Plan de acción

El tiempo estimado de la implementación de forma iterativa, sistemática, integral y enfocado a la lógica del negocio, con el alcance de la Ventanilla Electrónica Tributaria, se estima en un plazo de 10 meses.

Como parte del proceso inicial e iterativo se comenzará a aplicar los dominios de forma paulatina enfocado en el Sistema de Ventanilla Electrónica.

Es necesario realizar etapas previas de capacitación al personal que se involucrará en las diversas herramientas necesarias para implementar de forma eficiente el SGSI.

Actividad	Tiempo de ejecución
Capacitación al personal involucrado	2 Meses
Creación de la figura de oficial de seguridad, con los recursos requeridos para la gestión del proyecto	1 Mes
Documentación de requisitos regulatorios y legales	1 Mes
Creación, actualización y revisión de las políticas de seguridad de la información, para alinearla con ISO27001:2013 Creación de política de Seguridad de la Información Creación de políticas de Seguridad de la Información por cada uno de los dominios que la Dirección estime se apliquen en el documento de aplicabilidad.	2 Meses
Gestión de acceso/Depuración de usuarios	1 Mes
Gestión de vulnerabilidades y parches para reducir los riesgos asociados con la explotación de vulnerabilidades técnicas publicadas de la plataforma	2 Meses
Gestión de eventos de seguridad, para monitorear en tiempo real.	3 Meses
Control de acceso a la red	3 Meses
Documentación de la arquitectura de seguridad	3 Meses
Implementación de herramientas de seguridad de la	4 Meses

información, para automatizar la gestión de la seguridad	
Análisis de la calidad del Software, para identificar y mejorar la calidad del software usado.	3 Meses

Controles a implementar ISO 27001:2013

Es importante tomar en cuenta que para que un SGSI sea auditable para la certificación ISO 27001, todos los controles deben estar implementados, salvo que exista un documento de aplicabilidad debidamente autorizado por la Dirección Superior.

Para efectos de realizar la implementación inicial de los primeros controles requeridos, se realizará desarrollo de la implementación de los controles relacionados con:

5 Políticas de seguridad

5.1 Directrices de la Dirección en seguridad de la información.

5.1.1 Conjunto de políticas para la seguridad de la información

5.1.2 Revisión de las políticas para la seguridad de la información

16. Control de Incidentes

16.1.1 Responsabilidades y procedimientos

16.1.2 Notificación de los eventos de seguridad de la información.

16.1.3 Notificación de puntos débiles de la seguridad.

16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones

16.1.5 Respuesta a los incidentes de seguridad.

16.1.6 Aprendizaje de los incidentes de seguridad de la información

16.1.7 Recopilación de evidencias.

La base del sistema de gestión de seguridad de la información, es la documentación, por tanto se implementará una herramienta para la gestión documental, que es indispensable para la implementación.

Adicionalmente se implementarán controles adicionales, de forma incremental. Estos controles se implementarán en base a la revisión de riesgos efectuada al Sistema de Ventanilla Tributaria VET, según se describe a continuación:

Activo	Amenazas	Vulnerabilidades	Impacto				Prob.	Riesgo
			C	I	D	Prom		
Servidores	Hackers Falla física Accesos no autorizados	Mala configuración Falta de protección Falta de redundancia Equipos obsoletos	3	2	3	3	2	6
Equipos de comunicación	Hackers Falla física Accesos no autorizados	Mala configuración Falta de protección Falta de redundancia Equipos obsoletos	2	2	3	2	3	6
Software	Hackers Virus	Software sin licencias Software sin parches Falta de respaldo	2	2	2	2	2	4
Servicios de interconexión	Servicio no disponible	Falta de redundancia	1	1	3	2	2	4
Servicios eléctricos	Falla eléctrica	Generador eléctrico antiguo Falta de mantenimiento	1	1	3	2	3	6
Personal	Servicio no disponible Errores Robo de información Malas prácticas	Personal nuevo Falta de capacitación Personal mal remunerado	3	3	2	3	2	6
Código Fuente	Hackers Accesos no autorizados Caídas de servicios Código no seguro	Códigos maliciosos Falta de documentación Falta de control de versiones Falta de respaldo	3	3	3	3	3	9

Control de la documentación (Políticas de seguridad)

Para esto usaremos una herramienta de gestión documental: Alfresco Community.

La razón de implementar esta herramienta tiene que ver directamente con el manejo de gestión documental que es indispensable tal como es indicado en las cláusulas 5.2 que nos indican lo siguiente:

1. La alta dirección debe establecer una política de seguridad de la información que:
    1. Sea apropiada para los fines de la organización
    2. Proporcione un marco para establecer objetivos de seguridad de la información.
    3. Incluya un compromiso de cumplir los requisitos aplicables.
    4. Incluya un compromiso de mejora continua del SGSI.
2. La política del SGSI deberá:
    1. Estar disponible como información documentada.
    2. Ser comunicada dentro de la organización
    3. Estar a disposición de todas las partes interesadas, según corresponda.

Al crear la documentación, la DGI debe garantizar lo siguiente:

1. Identificación y descripción.

2. Formato y medios de comunicación (correo, etc.)

3. La revisión y aprobación de idoneidad y suficiencia.

Con la implementación de la herramienta, se tendrá la base requerida para ir gestionando las políticas que vayan siendo creadas por la institución y gestionada para el personal.

Adicionalmente las políticas deberán tener en cuenta la estructura establecida en ISO 27003, Anexo D

1. Resumen
2. Introducción
3. Ámbito de aplicación
4. Objetivos
5. Principios
6. Responsabilidades
7. Resultados importantes
8. Políticas relacionadas.

Matriz Raci control de la documentación

Matriz Raci ISO/IEC 27002:2013 R = Responsible A = Accountable S = Supportive C = Consulted I = Informed		Prop. Activos Inform.	Director General	Ofic. Seg. Información RRHH		Dir. Jurídico Técnico	Dir. Adm. Financiero	Servicios Generales	Dir. Inform. Sist	Equip. trabajo/ Staff
5 Políticas de seguridad										
5.1	**Directrices de la Dirección en seguridad de la información.**									
5.1.1	Conjunto de políticas para la seguridad de la información	C	C	R	C	C	C	C	S	I
5.1.2	Revisión de las políticas para la seguridad de la información	C		S	S	S	S	C	S	

6 Aspectos organizativos de la seguridad de la información										
6.1	**Organización interna.**									
6.1.1	Asignación de responsabilidades para la segur. de la información.	A		C	C	C			C	I

Requerimientos de la implementación:

- Servidor Linux Centos 7
- JDK 6U45
- Apache tomcat 7 o superior
- PostgreSQL 9.4
- openldap (Para validación de usuarios / Integración)
- Libreoffice 4.4 o Superior

Requisitos de Hardware

- 8 GB Memoria
- 250 GB de Espacio en disco
- 4 Procesadores

Técnicamente esta herramienta se adapta fácilmente a la plataforma existente en la institución, con la ventaja de ser opensource, con el sistema operativo actualizado (Centos 7).

Procedimiento de instalación

La instalación se realizará sobre el servidor base con todos los parches y actualizaciones disponibles y realizando hardening:

- Instalación mínima de paquetes en modo texto

- Habilitación de IPTables con los accesos mínimos a los puertos de la aplicación (8080).
- Configuración con cliente de NTP al servidor de hora institucional.
- Paquetes de monitoreo (snmp).

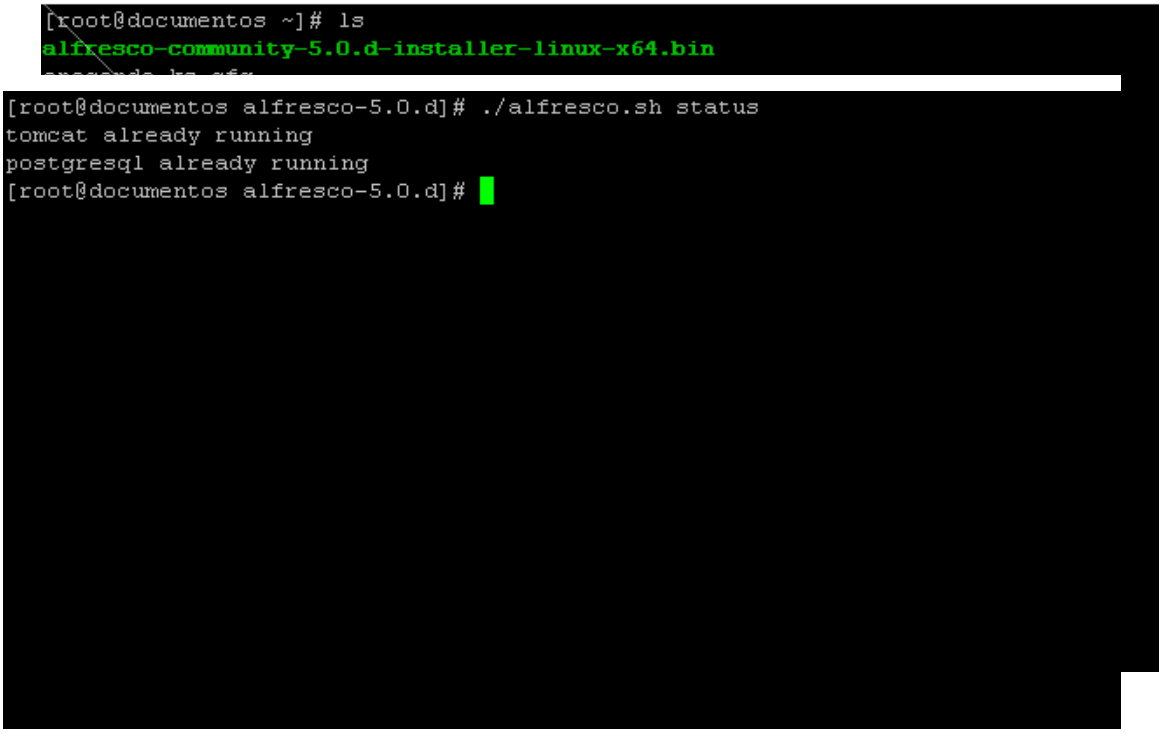


Ilustración 10: Instalación alfresco

Organización lógica de la herramienta

Se organizará lógicamente mediante la creación de usuarios con los roles indicados en cuadro de cargos relacionados con el sistema de gestión de la seguridad de la información:

- Administrador del Sistema: Gestionará la creación de usuarios inicial y operaciones de administración general del servidor.

- Director General de Ingresos: Aprueba los procedimientos, políticas y normas institucionales.
- Director de Informática: Gestionará creará los usuarios del área informática, autorizará procedimientos del área, administrará usuarios del área.
    - Jefe de apoyo tecnológico: Gestiona procedimientos relativos a los controles tecnológicos de hardware/software.
    - Jefe de Sistemas: Gestiona los procedimientos relativos a los diferentes sistemas desarrollados, manuales de sistemas, etc.
- Director de Registro Recaudación y Cobranzas: Gestionará creará los usuarios del área informática, autorizará procedimientos del área, administrará usuarios del área.
- Director Administrativo financiero: Gestiona la documentación, procesos relacionados con el área financiera, autorizará a usuarios del área.
- Servicios generales: Gestiona la documentación y procesos relacionados con la seguridad física de la institución.
- Oficial de seguridad: Gestionará la documentación, procesos y creará políticas relacionadas con la seguridad de la información para que puedan ser autorizadas por la Dirección General.
- Dirección de Recursos Humanos: Gestionará los procedimientos de RRHH, políticas de RRHH para su autorización por parte de la Dirección General.
- Dirección Jurídica Técnica: Gestionará los procedimientos, políticas relacionadas con los asuntos jurídicos institucionales. Gestionará la documentación legal que será dada a conocer a los contribuyentes y a la institución.

- Dirección de planificación estratégica: Gestionará la documentación general de la institución, revisará métodos y procedimientos institucionales, revisará la redacción de las políticas redactadas para su aprobación por parte de la Dirección General. Dará a conocer la documentación a los demás usuarios.
- Usuario General/Invitado: Tiene acceso a toda la documentación de carácter público que ha sido compartida por la Dirección y/o áreas.

Contenido de la herramienta

Se procederá a alimentar la herramienta con las políticas y procedimientos que se hayan redactado y estén actualizados, manteniendo el control de las versiones que han estado activas por un período de tiempo.

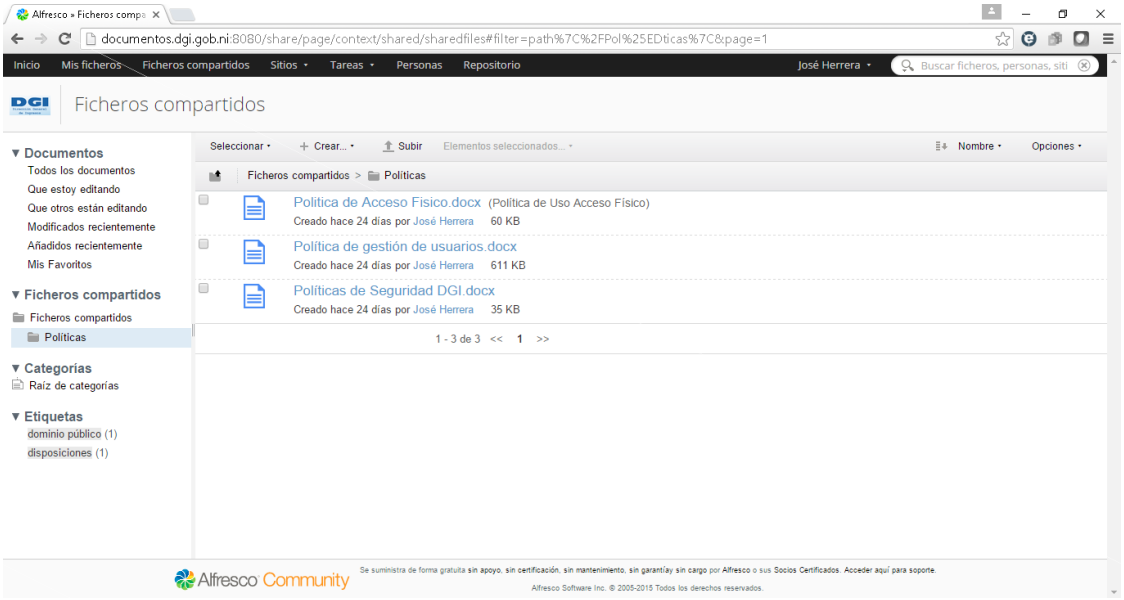
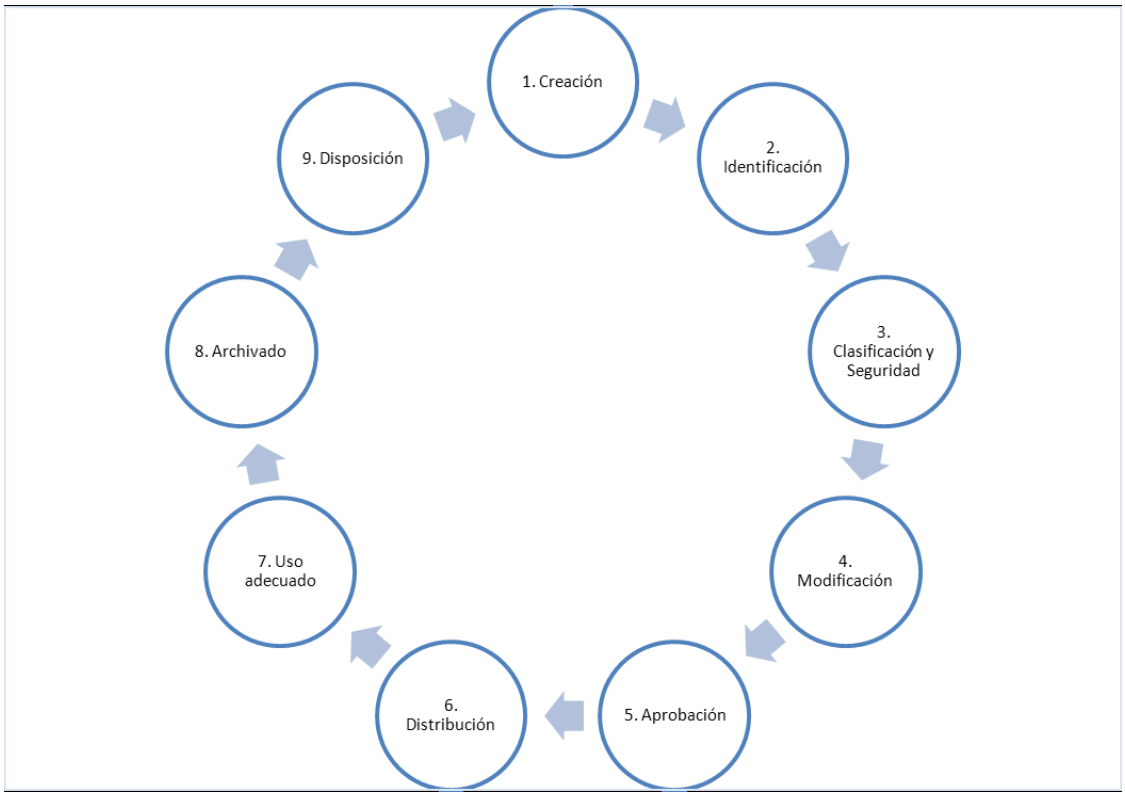


Ilustración 11: Detalle de Alfresco

Ciclo de la información documentada

Según ISO27001:2013 cláusula 7.5 Información documentada, al crear y actualizar la información se deberá garantizar:

- Identificación y protección
- Formato (idioma, versión, gráficos).
- Revisión y aprobación de idoneidad y suficiencia.
- Se debe comprobar que la información está disponible y apta para su uso, cuándo y dónde sea necesario.
- Está protegida adecuadamente.
- Deberá abordar las actividades de distribución, acceso, recuperación y uso; almacenamiento y conservación, incluida la conservación de la legibilidad.
- Control de cambios.
- Retención y disposición.



Control de incidentes

Matriz Raci ISO/IEC 27002:2013 R = Responsible A = Accountable S = Supportive C = Consulted I = Informed		Prop. Activos Inform.	Director General	Ofic. Seg. Información	RRHH	Dir. Jurídico Técnico	Dir. Adm. Financiero	Servicios Generales	Dir. Inform. Sist	Equip. trabajo/ Staff
16	**Gestión de incidentes en la seguridad de la información**									
16.1	**Gestión de incidentes de seguridad de la información y mejoras**									
16.1.1	Responsabilidades y procedimientos	A		S	S	C		S	S	
16.1.2	Notificación de los eventos de seguridad de la información.	A		R				S	S	I
16.1.3	Notificación de puntos débiles de la seguridad.	A		R				S	S	I
16.1.4	Valoración de eventos de seguridad de la información y toma de Decisiones.	A		S		C		S	S	
16.1.5	Respuesta a los incidentes de seguridad.	A		R		C		S	S	
16.1.6	Aprendizaje de los incidentes de seguridad de la información	A		S	C		C	C	C	
16.1.7	Recopilación de evidencias.	A		R		C		S	S	

Una de las herramientas fundamentales de la institución es la Ventanilla Electrónica Tributaria y por ende, su monitoreo y revisión es indispensable para su adecuado funcionamiento, de forma que se puedan corregir impactos que puedan afectar la VET y proponer acciones correctivas para futuras amenazas.

Para realizar un proceso efectivo de gestión de eventos debe automatizar por lo menos las actividades que se mencionan enseguida. Las dos primeras son responsabilidad del personal encargado de la infraestructura tecnológica, mientras que las demás recaen más del lado del sistema de monitoreo seleccionado, de ahí que su selección adecuada sea crucial para el éxito de la automatización del proceso de gestión de eventos:

- Ocurrencia del evento: Los eventos ocurren constantemente, pero no todos son registrados, por lo que los responsables de la infraestructura de TI deben tener muy claro qué tipos de eventos necesitan ser detectados.
- Notificación del evento: Consiste en habilitar la infraestructura de TI para comunicar información de su estado, permitiendo que ésta permita ser censada o que genere notificaciones cuando ciertas condiciones se cumplen. Las notificaciones puede ser propietarias o basadas en estándares abiertos como SNMP o TL1.
- Detección del evento: La notificación del evento debe ser detectada por el sistema de monitoreo, por lo que es muy importante que éste cuente con una amplia variedad de sondas y/o agentes que soporten los distintos tipos de notificaciones tanto estándares como propietarias, éstas últimas según las distintas marcas de los proveedores.
- Filtrado y deduplicación de eventos: El filtrado consiste en decidir cuáles eventos serán notificados y detectados por el sistema de monitoreo. La deduplicación consiste en la agrupación de múltiples eventos similares y recurrentes en uno mismo. Por tanto, el sistema de monitoreo debe contar con ambas capacidades.
- Asignación de significado: Consiste en la categorización de los eventos en base a su tipo de afectación e impacto en eventos informativos, avisos y excepciones, por lo que es muy importante que el sistema de monitoreo soporte por lo menos las severidades estándares: crítica, mayor, menor, aviso, indeterminada y resolutiva.
- Correlación de eventos: Consiste en la comparación de los eventos con un conjunto preestablecido de criterios llamados “reglas de negocio” con el objeto

de identificar algún impacto en el negocio a través de la búsqueda de causas raíz. Por tal motivo, es indispensable que el sistema de monitoreo seleccionado cuente con motores de correlación poderosos y fáciles de programar que realicen correlaciones de manera automática.

- Acciones automáticas: Si la actividad de correlación reconoce un evento de impacto para el negocio, una respuesta automática podría ser requerida, pudiendo ser de distintos tipos, por ejemplo, la creación de un registro en el sistema de gestión de incidentes, el registro histórico del evento para su posterior análisis, la ejecución de un script que lleve a cabo acciones particulares como el reinicio de un dispositivo o de un servicio, la notificación del evento a una persona o equipo vía correo electrónico o un mensaje de texto vía celular, etcétera. Es por tanto indispensable que el sistema de monitoreo permita una gran versatilidad para la ejecución de acciones automáticas.
- Acciones de revisión: Con miles de eventos generados cada día, es imposible revisar cada uno de ellos de manera individual. Sin embargo, es necesario asegurarse que aquellos eventos significativos hayan sido tratados de manera apropiada, dando seguimiento a tendencias y cuenta de ocurrencia de eventos, lo cual también puede ser hecho de manera automático por el sistema de monitoreo.
- Cierre del evento: Consiste en la resolución de un evento cuando éste ha sido solucionado. Esto se puede dar de manera automática a través del “clear” o solución generada por la infraestructura o de manera manual.

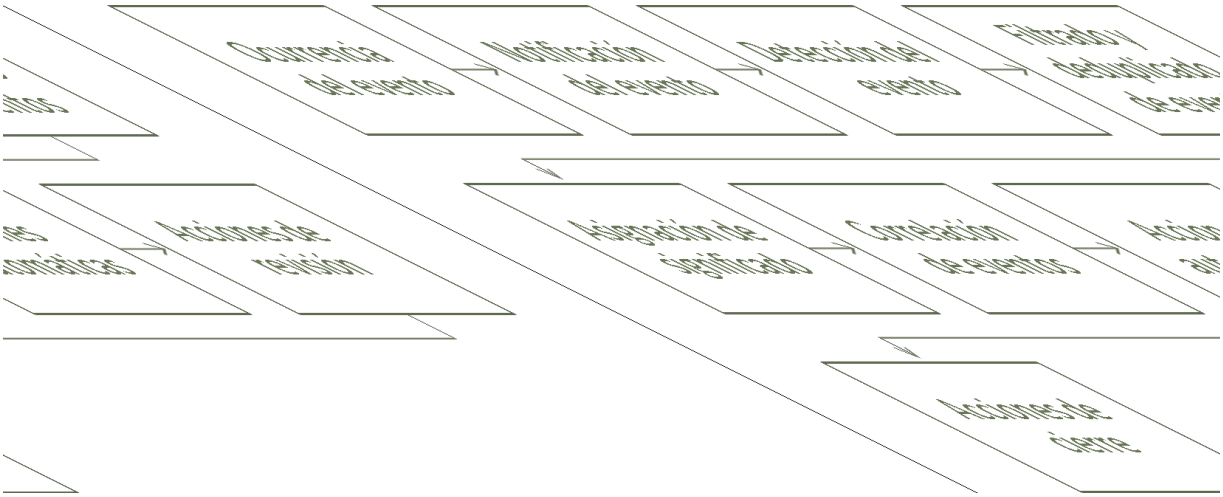


Ilustración 12: Proceso de eventos monitoreo

Nivel de escalamiento

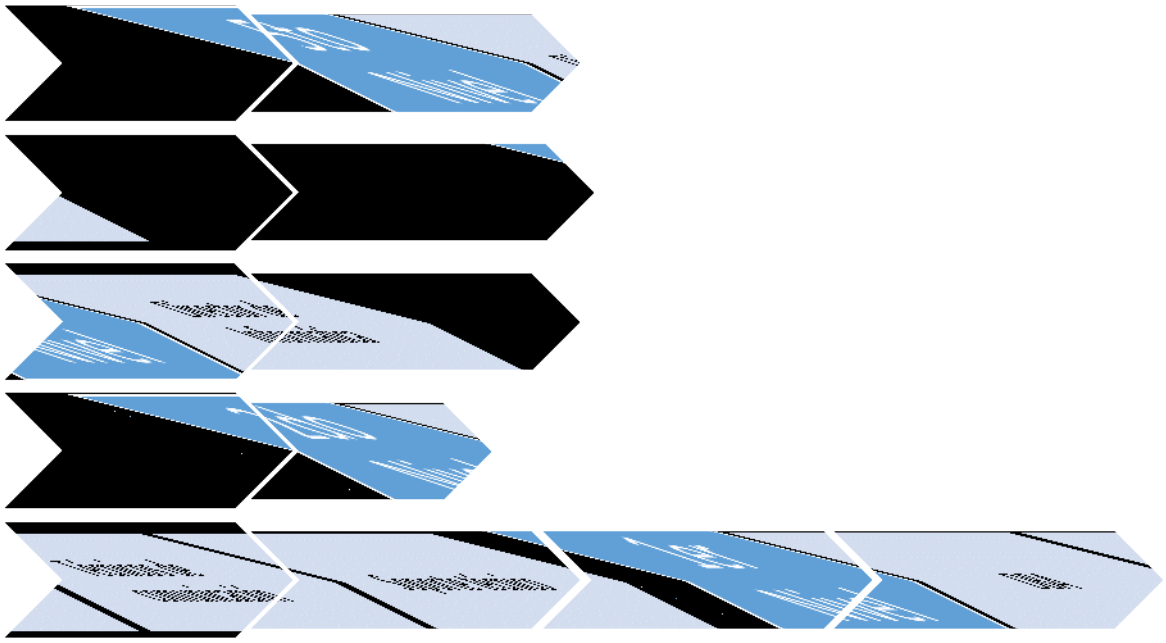


Ilustración 13: Niveles de escalamiento

Para el procedimiento de monitoreo se debe establecer un procedimiento de escalamiento que atienda los eventos de seguridad, teniendo en cuenta que el tiempo entre escalamientos no debería superar 30 minutos.

Notificación de puntos débiles de la seguridad.

Para poder tener en cuenta los puntos débiles de la seguridad de la información se debe hacer una preparación adecuada de los equipos mediante las siguientes actividades:

- Gestión de parches de seguridad: (Bases de datos, sistemas operativos, web servers).
- Aseguramiento de la plataforma: Configuración de servidores con principios de hardening que deben incluir habilitación mínima de servicios y privilegios,

mejorar configuraciones predeterminadas, contraseñas, recursos que son accedidos.

- Prevención de código malicioso: Habilitación de antivirus / antimalware.
- Sensibilización y entrenamiento a usuarios: Se debe sensibilizar a los administradores de equipos para la gestión de seguridad.

Cualquier debilidad encontrada deberá ser notificada al Jefe de Oficina de apoyo tecnológico.

Hardware y Software

Para una correcta y eficiente gestión de incidentes la entidad debería tener en cuenta los siguientes elementos:

- Portátiles Forenses:
- Analizadores de protocolos.
- Software de adquisición.
- Software para recolección de evidencia.
- Kit de respuesta a incidentes.
- Software de análisis forense.
- Medios de almacenamiento

Revisión de Logs de seguridad

Se debe realizar análisis sistemático de los diferentes logs de seguridad, tanto a nivel de aplicaciones, como servidores y equipos de comunicación.

Los administradores deben realizar la evaluación de los diferentes comportamientos y debe mantenerse en un repositorio centralizado.

Aprendizaje de los incidentes de seguridad de la información

Es importante que en todo evento de seguridad se realice una evaluación de la causa raíz del incidente para efectos de tomar las medidas respectivas para evitar la reincidencia del evento. Este análisis debe llevarse a cabo por parte del personal involucrado con la ayuda de otras áreas.

Una vez determinada la causa raíz del evento, se debe documentar y se debe definir cual sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.

CAPITULO III

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

La Dirección General de Ingresos es una institución con una gran importancia para el país, en vista de los recursos recaudados, así como la cantidad de contribuyentes que hacen uso de su plataforma de declaraciones y pagos en línea (Ventanilla Electrónica Tributaria).

Por esta razón es importante que la institución cuente con un SGSI que gestione la seguridad de la información que le ayude a cumplir con sus objetivos de negocio.

La base del SGSI que se debe implementar en la DGI es la definición de los objetivos de seguridad de la información así como gestión de las políticas y documentos, que es una de las funciones que tiene que fortalecer a fin de que los procedimientos existentes sean alineados con ISO 27001:2013 y las políticas, procedimientos, documentos requeridos.

Al no existir en la institución un SGSI, es necesario realizar cambios en la organización, a fin de crear la figura encargada de la gestión de la seguridad de la información, la cual debe responder directamente al Director General de Ingresos, a fin que tenga el nivel de empoderamiento necesario para cumplir eficientemente con sus funciones.

Es muy importante resaltar el papel del liderazgo de la Dirección Superior, podemos afirmar categóricamente que sin el apoyo de la Dirección no será posible lograr la implementación del SGSI, su papel es indispensable por los cambios que se deberán llevar a cabo, así como el patrocinio requerido, tanto a nivel de recursos humanos como financieros.

El Director General como conocedor de las necesidades institucionales tiene una visión clara del futuro y los objetivo institucionales.

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27001:2013 EN LA DGI

El papel de la Dirección Superior debe comenzar con la fijación de los objetivos del SGSI, su papel en la aceptación de los riesgos (definición del apetito de riesgos) así como en la definición de los controles que se deben aplicar en base al giro de la DGI (Documento de aplicabilidad).

Se debe realizar un proceso de capacitación al personal, para definir las evaluaciones de riesgos de forma periódica, ya que un sistema de SGSI es más efectivo si su selección de controles se hace en base al riesgo.

Así mismo el Director General de Ingresos debe incentivar un cambio en la cultura institucional que de mayor importancia a la seguridad de la información, para que todo el personal comprenda la importancia de los controles y cambios que se deben implementar.

El proyecto de implementación del SGSI se debe gestionar tomando en cuenta las mejores prácticas de gestión de proyectos, y sugerimos que sea tomando en cuenta la metodología de PMBOK, por ser un método establecido y ampliamente divulgado. El proyecto debe ser liderado por la nueva figura creada (Oficial de Seguridad de la Información), a fin que el mismo conozca todos los detalles y se empape en el SGSI desde un inicio.

Para ayudar en el desarrollo del trabajo inicial relativo a la gestión documental y como implementación de las secciones 4 a la 10 de la norma ISO 27001:2013, se implementó la herramienta alfresco, que es un software opensource, que serviría como herramienta para el manejo de la documentación del proyecto, políticas, procedimientos, control de versión de documentos, distribución y básicamente para todo el ciclo de vida documental requerido por el SGSI; también se efectuó la implementación de los controles relativos a los procedimientos de gestión de incidentes de seguridad de la información.

Estos incidentes de seguridad deben tomarse como base para efectuar análisis de causa raíz, y poder tomar las acciones respectivas para evitar que sean recurrentes y cumplir con la mejora continua del SGSI.

Una vez establecida, aprobada, divulgada las políticas, se debe efectuar el proceso de análisis de los demás controles que sean aprobados en el documento de declaración de aplicabilidad, siguiendo el enfoque iterativo.

Finalmente es necesario establecer los parámetros de medición del SGSI para comprobar su efectividad y ejecutar las medida correctivas necesarias para cumplir con los objetivos propuestos del SGSI, además de acompañarlos con procesos de revisión externo, el cual una vez dadas las revisiones satisfactorias, se puede proceder a realizar la certificación.

Con estos indicadores de medición basados, en los objetivos del SGSI, el cual se encuentra alineado a los objetivos del negocio, nos permite comprobar que al implementar el Sistema basado en ISO 27001:2013 se establecerán controles que permitirán mitigar los riesgos de pérdida de información, confiabilidad, confidencialidad, disponibilidad y no repudio de la información en el Sistema de Ventanilla Electrónica Tributaria de la Dirección General de Ingresos, a un costo razonables, de acuerdo a los principales riesgos identificados, dando por probada la hipótesis.

Recomendaciones

- Implementación paulatina tomando como inicio del proyecto la documentación, y los controles que tengan mejor complejidad y proporcionen mayor integración y/o valor a los procesos de negocio.
- Crear la figura de Oficial de seguridad con todas las facultades para la implementación del proyecto.

- Es necesario integrar a todo el personal involucrado a todos los niveles y capacitarlo para aprovechar las habilidades y comprometerlos al uso y gestión del SGSI. Al personal se le debe preparar, realizar concientización sobre el uso del SGSI y sobre la seguridad en general, así como evaluar el grado de compromiso.
- Crear un SGSI básico e ir agregando mayor funcionalidad con las mejores prácticas y necesidades basadas en los análisis de riesgos continuos. Se debe asegurar la formación del personal de dirección ante de comenzar los procesos de implementación y operación.
- Se debe evitar la aplicación de demasiados procesos nuevos al mismo tiempo.
- Un sistema que no se mide, no se puede gestionar efectivamente, por tanto hay que realizar mediciones y evaluaciones de desempeño de forma periódica para evaluar los objetivos.
- Realizar evaluaciones periódicas de riesgo, usando las metodologías fijadas que permitan obtener un mapa de riesgos apropiados para diseñar y controlar los riesgos residuales, y que permita a la Dirección General definir su apetito de riesgo de forma efectiva.
- Realizar evaluaciones periódicas del SGSI, por parte del personal involucrado así como la Dirección. Previo al proceso de evaluación se deben definir los indicadores y medidas necesarias para evaluar objetivamente el SGSI y posteriormente realizar los cambios de mejoras continuas.
- Se recomienda Implementar el proyecto usando metodologías PMBOK. La Guía PMBOK está basada en procesos, lo que significa que ésta describe el trabajo aplicado en los procesos en sí. Este enfoque es coherente, y muy similar, al mismo usado en otros estándares de gestión (Por ejemplo ISO 9000

y CMMI). Los procesos se superponen e interactúan a lo largo de la realización de las fases del proyecto. Los procesos están descritos en términos de:

- Entradas (documentos, planes, diseños, etc.)
- Herramientas y técnicas (mecanismos aplicados a las entradas)
- Salidas (documentos, planes, diseños, etc.)

- Se recomienda realizar auditorías externas de evaluación y seguimiento, para asegurar el cumplimiento de objetivos y efectividad del SGSI.
- Una vez que se tenga el SGSI en un nivel optimizado, se recomienda realizar la certificación del SGSI, esto en vista que puede ayudar a la institución en el cumplimiento de sus objetivos por medio de lo siguiente:
  - Mejora de la seguridad de la información
  - Mejora en la gobernanza de TI
  - Conformidad a los estándares internacionales y legislación nacional.
  - Reducción de costos por incidentes de seguridad
  - Mejora de la confianza y la imageninstitucional ante los contribuyentes.

Bibliografía

- Alfresco. (17 de febrero de 2016). Alfresco. Obtenido de https://www.alfresco.com/
- Bon, J. v. (2010). Fundamentos de ITIL® V3. En J. v. Bon, Fundamentos de ITIL® V3 (pág. 87). Amersfoort: Van Haren Publishing.
- eramba. (15 de febrero de 2016). Eramba. Obtenido de http://www.eramba.org/
- Federico Alonso Atehortua Hurtado, R. E. (2008). Sistema de gestión integral, Una sola gestión un solo equipo. Antioquía: Editorial Universidad de Antioquía.
- kimios. (17 de febrero de 2016). kimios. Obtenido de http://www.kimios.com
- Llauger, M. B. (2001). Hacia una economía del conocimiento. En M. B. Llauger. Madrid: ESIC-EDITORIAL-PricewaterhouseCoopers.
- openkm. (15 de febrero de 2016). openkm. Obtenido de http://openkm.org
- ISO IEC 27001:2013 British Standard Institute Second Edition 2013-10-01
- Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013 British Standard Institute
- Information technology — Security techniques — Code of practice for information security controls Second Edition 2013-10-01
- Nine Steps to Success: An ISO27001 2013 Implementation Second Edition Alan Carter 2013 it gp.
- Contents BSI - Standard 100 - 1: Information Security Management Systems (ISMS)

- [1], 2011 Van Haren Publishing
- ISO PECB – Implementador Lider Certificado en la Norma ISO/IEC 27001:2013, PECB 2005 -2013, versión 4.7
- ISO 27001: Gestión de incidencias en los Sistemas de Seguridad de la Información, url https://www.isotools.org/2013/12/11/gestion-de-incidencias-de-seguridad-de-la-informacion/, 2013
- ITIL V3: Fundamentos de gestión de itil.
- URL:http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_la_disponibilidad/proceso_gestion_de_la_disponibilidad/monitorizacion_de_la_disponibilidad.php., 2013
- Dirección General de Ingresos, Página Web, http://www.dgi.gob.ni, 2016

Índice de ilustraciones

Ilustración 1: Causa y efecto.....xi

Ilustración 2: Fines y medios.....xi

Ilustración 3: Principios de la gestión ISO 27001.....5

Ilustración 4: Ciclo de Demming.....7

Ilustración 5: Proceso de gestión de incidentes.....14

Ilustración 6: Estrategia de implementacikón.....37

Ilustración 7: Proceso de entrevistas.....38

Ilustración 8: Ciclo de Demming con ISO 27001.....38

Ilustración 9: Estado de la seguridad.....42

Ilustración 10: Instalación alfresco.....50

Ilustración 11: Detalle de Alfresco.....52

Ilustración 12: Proceso de eventos monitoreo.....57

Ilustración 13: Niveles de escalamiento.....58

Anexos

Modelo de entrevista para análisis del estado actual de la seguridad de la información

Entrevistado: Director General de Ingresos

No	Pregunta
1.	¿Cuál es la situación actual de la seguridad de la información en la institución?
2.	¿Cuál es el objetivo de la seguridad de la información que se pretende aplicar?
3.	¿Cuál es la diferencia entre la situación actual y el objetivo?
4.	¿Existen procesos estándarizados en la institución?
5.	¿Son los procesos seguidos por los usuarios relevantes?
6.	¿Están los procesos documentados?
7.	¿Hay un responsable designado para la eficacia del proceso?
8.	¿Están determinadas las funciones y responsabilidades?
9.	¿Se han comunicado a todas las personas involucradas en los procesos sus funciones y responsabilidades?
10.	¿Se dan capacitaciones sobre los procesos?
11.	¿Se controlan y miden los procesos existentes?
12.	¿Los procesos institucionales son automatizados?, ¿Se utilizan herramientas?
13.	¿Existen metodologías para actualizar procesos?
14.	¿El rendimiento de los procesos son comparados con las prácticas de instituciones similares?

Anexo I

Entrevista con Personal para diagnóstico de la situación actual de la seguridad en la DGI

Entrevistado: Director General de Ingresos

Objetivo: Determinar el grado de madurez del sistema, liderazgo y patrocinio del sistema de gestión de la seguridad de la información existente.

ANÁLISIS DEL SGSI	Hallazgos
4. Contexto organizacional	
4.2.1 a) Revisar la documentación del alcance y límites del SGSI, particularmente las exclusiones. ¿En qué medida el SGSI coinciden con la organización? ¿Hay razones justificadas para excluir cualquier elemento?	
4.2.1b) Revisar la política SGSI de la organización. ¿Refleja adecuadamente las características generales de la organización y su enfoque estratégico de gestión de riesgos? ¿Incorpora los requisitos de negocio de la organización, además de las obligaciones legales o reglamentarias de seguridad de la información? Confirmar que ha sido aprobado formalmente por la dirección y establece criterios significativos para la evaluación de los riesgos de seguridad de la información. [Nota: en el contexto de la norma ISO / IEC 27001, "Política SGSI" se refiere a la declaración de la gestión de los objetivos o requisitos de seguridad de la información, los principales principios básicos generales de seguridad de la información. Los más detalladas políticas de seguridad de la información, normas, procedimientos y directrices serán revisados en los puntos 4.2.1 y 4.2.2].	
4.2.1c) Determinar y revisar la organización de la(s) elección(es) de evaluación de riesgos del método / s (ya sea a medida o un método generalmente aceptado - véase la norma ISO / IEC 27005, cuando se emitan, para mayor información). Son los resultados de las evaluaciones de riesgo comparables y reproducibles? Busque ejemplos de resultados anómalos para determinar la forma en que fueron abordados	

y resueltos. Fue el método de evaluación de riesgos actualizada como resultado? También revisar la definición de gestión de los criterios para aceptar o mitigar los riesgos (el "apetito de riesgo"). Es la definición razonable y posible en relación con los riesgos de seguridad de la información?	
4.2.1d) y e) Revisar los riesgos de inventario de activos de información y la información de seguridad identificados por la organización. Son relevantes dentro del alcance activos de información está incluido? Se identificaron los propietarios responsables de todos los activos? Examinar el análisis / evaluación de amenazas, vulnerabilidades e impactos, la documentación de los escenarios de riesgo más la priorización o clasificación de los riesgos. Busque riesgos que sean sustancialmente mal-definidos o subestimados, por ejemplo aquellos en los que los controles correspondientes son caros o difíciles de aplicar, tal vez en que se han entendido mal los riesgos.	
4.2.1f) Revisión del plan de tratamiento del riesgo de la organización. Son apropiados los "tratamientos" (es decir, la mitigación mediante la aplicación de controles adecuados, evitando el riesgo, transfiriendo el riesgo a terceros o aceptar a sabiendas de los riesgos si están dentro de tolerancia al riesgo de gestión) especificado para todos los riesgos identificados? Busque lagunas y otras anomalías. Compruebe también si los cambios recientes (por ejemplo, nuevos sistemas o procesos de negocio) se han incorporado de manera adecuada, en otras palabras, es el plan de tratamiento del riesgo se utilizan y actualizan de forma proactiva como una herramienta de gestión de seguridad de la información?	
4.2.1g) Para los riesgos de seguridad de la información que van a ser mitigados, revisar los objetivos de control definidos y controles seleccionados mediante muestreo adecuado, por ejemplo, muestreo estratificado por tipos de control (técnicos, físicos, de procedimiento o jurídica), por clasificación de riesgos (unidades de negocios, sitios / edificios, etc.) (alta, media o baja), por ubicación o por otros criterios de muestreo de auditoría. Comparación de los objetivos de control y en contra de los sugeridos por la norma ISO / IEC 27002 y que se resumen en el Anexo A de la norma ISO / IEC 27001, en particular, identificar y revisar cualquier discrepancia significativa con respecto a las normas (por ejemplo, objetivos comunes o los controles de las normas que no son utilizados por el organización, o cualquiera que pueda haber sido añadido). Compruebe también que los requisitos de seguridad de la información impuestas explícitamente por las políticas corporativas, regulaciones de la industria, las leyes o contratos, etc. se	

reflejan adecuadamente en los objetivos de control y controles documentados.	
4.2.1h) Evaluar brevemente los riesgos de seguridad de la información residuales. La gerencia ha considerado formalmente y los aprobó? Están dentro del apetito de riesgo definido de la organización?	
4.2.1i) Confirmar si la administración ha autorizado la implementación y operación del SGSI, por ejemplo a través de un memorándum formal, la aprobación del proyecto, carta de apoyo de la Dirección, etc. Es esta una mera formalidad o hay evidencia de que la gestión realmente entiende y soportes SGSI?	
4.2.1 j) Revisar documentación de la Declaración de aplicabilidad y justificar los objetivos de control y controles, de la organización, tanto los que son aplicables y las que han sido excluidos / sin seleccionar. Confirmar que existen entradas adecuadas para todos los objetivos de control y controles enumerados en el anexo A de la norma ISO / IEC 27001. ¿Se ha examinado y aprobado la Declaración de aplicabilidad / autorizado por un nivel apropiado de la Dirección?	
4.2.2 Revisión del SGSI tal como se aplica y operados en contra de los requisitos del SGSI documentado mediante el muestreo (véase 4.2.1g y el anexo A de la norma ISO / IEC 27001). Buscar evidencia para apoyar o refutar la correlación entre los riesgos y los controles documentados y los realmente en funcionamiento.	
4.2.3 Revisar en el SGSI el monitoreo y procesos de revisión utilizando pruebas tales como planos, actas de las reuniones de revisión, informes de revisión de la gestión / auditoría interna, informes de incumplimiento / incidentes etc. Evaluar el grado en el que se detectan los errores de procesamiento, las brechas de seguridad y otros incidentes, informado y dirigida. Determinar si y cómo la organización está revisando efectiva y proactiva la implementación del SGSI para asegurar que los controles de seguridad identificadas en el plan de tratamiento del riesgo, políticas, etc. se aplican realmente y de hecho son en funcionamiento. revisar también de ISMS métricas y su uso para impulsar mejoras continuas del SGSI.	
4.2.4 Revisar los medios por los cuales la necesidad de mejoras del SGSI se determinan y se implementan las mejoras. Buscar evidencia en forma de notas, informes de gestión, correos electrónicos, etc. que documentan la necesidad de mejoras, se autoriza a ellos y hacer que sucedan.	
4.3.1 Revisión del SGSI documentación incluyendo: • **SGSI declaraciones de políticas, objetivos de control, procedimientos, normas, guías, etc.** • **Alcance del SGSI**	

• **Gestión de la elección del método de evaluación de riesgos / s, más la evaluación de los riesgos informe / s surgir y el Plan de tratamiento del riesgo** • **Otros procedimientos relacionados con la planificación, operación y revisión del SGSI** • **Registros de SGSI (véase 4.3.3)** • **La Declaración de aplicabilidad**	
4.3.2 Comprobar la presencia de, y el cumplimiento de un procedimiento documentado para el control de cambios a ISMS documentación, políticas, procedimientos, registros, etc. Determinar si los cambios en la documentación del SGSI se controlan formalmente por ejemplo, cambios son revisados y aprobados previamente por la administración, y se promulgan a todos los usuarios de la documentación SGSI por ejemplo, mediante la actualización de un conjunto de referencia definitiva de material mantenido en la intranet corporativa y / o explícitamente notificar a todos los usuarios aplicables.	
4.3.3 Evaluar los controles que protegen importantes registros del SGSI tales como evaluación y de auditoría informes diversos seguridad de la información, planes de acción, documentos formales del SGSI (incluyendo cambios a igual), libros de visitantes, la autorización de acceso / formularios de cambio etc. Revisar la adecuación de los controles sobre la identificación, almacenamiento, protección, recuperación, tiempo de retención y la disposición de tales registros, sobre todo en situaciones en las que hay obligaciones legales, reglamentarias o contractuales para implementar un SGSI según la norma ISO / IEC 27001 (por ejemplo, para proteger los datos personales).	
5. Gestión de Liderazgo	
5.1 Revisar el grado de compromiso de la dirección de seguridad de la información, utilizando pruebas tales como: **· Aprobación de la dirección formal del manual de políticas SGSI** **· Gestión de la aceptación de los objetivos del SGSI y planes de ejecución, además de la asignación de recursos y asignación de prioridades adecuadas a las actividades asociadas adecuadas (véase la sección 5.2.1)** **· Funciones y responsabilidades claras para la seguridad de la información, incluyendo un proceso para la asignación y la aceptación de la responsabilidad por la protección adecuada de los valiosos activos de información**	

· Gestión de orden, correos electrónicos, presentaciones, sesiones de información, etc. que expresan el apoyo y compromiso de los ISMS **· Criterios de aceptación del riesgo, el apetito de riesgo, etc. relativas a los riesgos de seguridad de la información** **· La determinación del alcance, asignación de recursos y el inicio de las auditorías y revisiones internas de gestión del SGSI**	
5.2.1 Revisión de los recursos asignados a los SGSI en términos de presupuesto, mano de obra, etc., en relación con los objetivos declarados de la organización para el SGSI y (en su caso) en comparación con otras organizaciones similares (benchmarking). Es el SGSI financiado adecuadamente en la práctica? Son suficientes fondos asignados por la administración para hacer frente a los problemas de seguridad de información en un tiempo razonable y con un adecuado nivel de calidad?	
5.2.2 revise la Capacitación de los involucrados específicamente en la operación del SGSI, y las actividades de sensibilización información general de seguridad dirigidas a todos los empleados. Son competencias necesarias y los requisitos de formación / sensibilización para los profesionales de la seguridad de la información y otros con funciones y responsabilidades específicas identificadas explícitamente? Son los presupuestos de formación / sensibilización adecuada para financiar las actividades de formación y sensibilización asociados? Examinar los informes de evaluación de la formación, etc., y buscar pruebas para confirmar que efectivamente se han adoptado medidas de mejora necesarias. Comprobar mediante el muestreo de ese empleado registros de recursos humanos en cuenta la formación relacionada con SGSI etc. (en su caso). Evaluar el nivel general de conocimiento seguridad de la información mediante una encuesta de muestreo / o revisar los resultados de encuestas / muestras llevadas a cabo como parte del SGSI.	
6. Planificación	
6.1 Asegurarse que el SGSI pueda lograr los resultados previstos, prevenir o reducir efectos no deseados y lograr mejoras continuas. **6.2 Se deben planificar acciones para hacer frente a los riesgos y oportunidades, ponerlos en práctica y evaluar su eficacia.** **6.3 Establecer y mantener criterios de riesgos, asegurarse de que las evaluaciones de riesgo repetidas producen resultados consistentes, válidos y comparables, identificar los riesgos, analizar los riesgos y evaluar los riesgos.**	

7 Soporte	
7.1 La organización deberá determinar y proporcionar los recursos necesarios para el SGSI, se debe buscar evidencia de presupuestos y asignación de personal para el SGSI.	
7.2 La organización deberá asegurar que las personas competentes realicen las tareas relacionadas con el SGSI.	
7.3 Las personas que realicen el trabajo en el marco del control de organización deberán estar conscientes de las políticas de la Seguridad de la Información. Se deberá buscar evidencias de programas de concienciación de las personas involucradas en el SGSI.	
7.4 Se deberá buscar evidencia de documentación que se haya organizado y que sea necesaria para el SGSI.	
8. Operaciones	
8.1 Se deberá analizar la documentación donde esté la planificación, ejecución y control de los procesos necesarios para cumplir con los requisitos de la seguridad de la información y aplicar las medidas determinadas para hacer frente a los riesgos y oportunidades. **8.2 Se deberá buscar evidencia de que los procesos tercerizados son determinados y controlados.**	
9. Evaluación de desempeño	
9.1 Se deberá analizar el seguimiento y revisión de los procesos de detección y prevención de incidentes de seguridad. **9.2 Se deberá buscar evidencia de lo siguiente:** • **Revisión de parte de la Dirección y actualización de planes de seguridad.** • **Revisión periódica de la eficacia del SGSI teniendo en cuenta las proposiciones de las partes interesadas.** • **Medición de la eficacia de los procedimientos y controles** • **Revisión de las evaluaciones del riesgo y tratamiento de riesgos.** • **Realización de auditorías internas.**	
10. Mejora continua	
10.1 Se deberá buscar evidencia de que la organización está mejorando continuamente la conveniencia, adecuación y eficacia del SGSI.	

10.2 Se deberá analizar si la entidad realiza las siguientes acciones: • **Reacciona a las no conformidades.** • **Evalúa la necesidad de adoptar medidas para eliminar las causas de no conformidades, a fin que no se repita o se produzca en otros lugares.** • **Aplicar medidas necesarias.** • **Revisar la eficacia de las medidas correctivas adoptadas.** • **Realizar cambios en el SGSI.**	

Anexo II

Formato de gestión de incidentes de seguridad

Fecha	Hora	Tipo de incidente	Servidores Afectados	Servicios afectados	Persona que atiende	Observaciones

Anexo III

Presupuesto de implementación

Descripción	Monto
Salarios Consultores 3 personas x 10 meses	C$ 1.018.800,00
Adquisición de equipos de cómputo, impresoras	113.200,00
Papelería y artículos de oficina, adquisición normativas	45.000,00
Licenciamientos de Software (Linux)	84.900,00
Licenciamientos de Software (Windows, office)	33.960,00
Licenciamientos para análisis de seguridad	141.500,00
Total	C$ 1.437.360,00
Tipo de cambio estimado US$1 x 1	C$ 28,30
Total en Dólares	USD $50.790,11