# ESTUDIO PARA LA IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA SECRETARIA DE EDUCACION DEPARTAMENTAL DE NARIÑO BASADO EN LA NORMA ISO/IEC 27001

RICARDO ANDRÉS AGUIRRE TOBAR
ANDRÉS FERNANDO ZAMBRANO ORDOÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD PASTO
2015

# ESTUDIO PARA LA IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA SECRETARIA DE EDUCACION DEPARTAMENTAL DE NARIÑO BASADO EN LA NORMA ISO/IEC 27001

RICARDO ANDRÉS AGUIRRE TOBAR
ANDRÉS FERNANDO ZAMBRANO ORDOÑEZ

Trabajo de Grado presentado como requisito para optar el título de Especialista en Seguridad Informática

ASESOR:
HENRY FERNANDO RODRÍGUEZ HERNÁNDEZ
ESPECIALISTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CEAD PASTO
2015

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE GRÁFICOS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

“Los conceptos, afirmaciones y opiniones contenidas en el presente trabajo son responsabilidad única y exclusiva de los autores y no compromete a la Universidad”

NOTA DE ACEPTACION:

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma jurado

_____
Firma jurado

San Juan de Pasto, junio de 2015

DEDICATORIA

Dedicada a esas personas importantes en mi vida, que siempre están ahí para brindarme toda su ayuda, apoyo y amor de manera incondicional, por sacrificar parte de su tiempo para que yo alcanzara esta meta, ahora puedo decir que ésta tesis lleva mucho de ellos, se las dedico con AMOR.

Mi Esposa Milena
Mis Hijos Anabelen y Manuel

RICARDO ANDRÉS AGUIRRE TOBAR

# DEDICATORIA

Dedico este trabajo de grado a mi esposa Claudia Susana, quien es mi apoyo incondicional y mi inspiración. A mis padres Segundo y Evila por ser los cimientos de mi formación.

ANDRÉS FERNANDO ZAMBRANO ORDOÑEZ

# AGRADECIMIENTOS

Los autores expresan su agradecimiento:

A la Universidad Nacional Abierta y a Distancia UNAD por la formación personal y profesional ofrecida en esta especialización.

A los tutores y orientadores de cada una de las materias vistas en esta especialización.

A los compañeros de especialización por sus aportes valiosos en este proceso de aprendizaje virtual y colaborativo.

A la Secretaría de Educación de Nariño por permitirnos realizar el trabajo de grado, especialmente al área financiera.

A todas aquellas personas que de una u otra manera aportaron con un granito de arena para que esta formación y este trabajo se hayan llevado a cabo.

# INTRODUCCION

Realizar un diagnóstico de la seguridad informática en el área financiera de la Secretaría de Educación Departamental de Nariño es un proceso que adquiere importancia y relevancia dado el continuo desarrollo de la tecnología y del acceso a los diferentes canales de comunicación.

Así las cosas es de mucha relevancia para el área financiera y para la entidad en general contar con una herramienta que le aporte para la toma de decisiones tendientes a ajustar o eliminar las falencias que se puedan estar presentando tanto en el sistema que soporta los procesos como en el manejo mismo de la información al interior del área y de la entidad.

El problema principalmente radica en que en la Secretaría de Educación del Departamento de Nariño no se tiene implementado un Sistema de Gestión de la Seguridad de la Información (SGSI), hasta el momento no se ha realizado un proceso de auditoría de los sistemas de información en general, que permita establecer los riesgos que se presentan en cuanto a la seguridad informática y de la información, y el sistema de control es incipiente para la mitigación de las eventuales amenazas y riesgos que puedan presentarse.

Así las cosas la presente investigación busca minimizar el impacto y la probabilidad de las amenazas y riesgos potenciales a que ve expuesta el área financiera mediante un diagnóstico de la seguridad informática y de la información que ayude a la implementación de un SGSI basado en la norma ISO/IEC 27001 en la Secretaría de Educación de Nariño.

Para tal propósito el presente trabajo se divide en seis capítulos. En un primer capítulo se define la línea de investigación, el nombre del proyecto y el tema, posteriormente el segundo capítulo se encarga de encauzar los elementos propios del problema de investigación así como también propone el marco referencial del proyecto; el capítulo tercero delimita la investigación en su enfoque metodológico; el capítulo cuarto se encarga de distribuir la presentación de resultados en atención al cumplimiento de cada uno de los objetivos específicos del proyecto y posteriormente las capítulos quinto y sexto se dedican a formular las conclusiones y recomendaciones obtenidas con base en los hallazgos proyectados en el trabajo de campo de la investigación.

# 1. LÍNEA DE INVESTIGACIÓN

## 1.1 NOMBRE DEL PROYECTO

Estudio para la implementación del sistema de gestión de seguridad de la información para la secretaria de educación departamental de Nariño basado en la norma ISO/IEC 27001

## 1.2 LÍNEA DE INVESTIGACIÓN

El proyecto se encuentra definido en la Línea de investigación de **Gestión de Sistemas** de la Cadena de Formación de Ingeniería de Sistemas. Ya que con este proyecto se profundizará en conocimientos de administración de tecnología y sobre todo de auditoría de sistemas, ya que se incluirá el control de la información, la calidad de los procesos y seguridad informática, componentes vitales para asegurar la validez y veracidad de la información.

## 1.3 TEMA

**AUDITORÍA DE SISTEMAS.** El proyecto incluye el diagnóstico del área financiera de la Secretaria de Educación Departamental (SED) Nariño, análisis del sistema de información que soporta la actividad financiera (software PCT) y al manejo y control que se le está dando a la información.

# 2. PROBLEMA

## 2.1 DESCRIPCIÓN DEL PROBLEMA

El problema principalmente radica en que en la Secretaría de Educación del Departamento de Nariño no se tiene implementado un Sistema de Gestión de la Seguridad de la Información (SGSI), hasta el momento no se ha realizado un proceso de auditoría de los sistemas de información en general, que permita establecer los riesgos que se presentan en cuanto a la seguridad informática y de la información, y el sistema de control es incipiente para la mitigación de las eventuales amenazas y riesgos que puedan presentarse.

La falta de un SGSI y la implementación de controles le han traído a la Secretaría de Educación un sin número de inconvenientes derivados del desconocimiento por parte de los usuarios de la importancia de la información del personal que labora en la entidad, la normatividad vigente sobre el tema y las políticas existentes en cuanto a la seguridad y protección de los activos informáticos y de la misma información.

En este sentido el área financiera no ha sido ajena a esta situación, está área cuenta con un software de la firma PCTG LTDA de la ciudad de Bogotá, el sistema es administrado directamente por el área de Sistemas de la entidad, instalado en un servidor local de aplicaciones y operado por toda el área financiera, este software presenta una serie de inconvenientes entre los cuales tenemos:

- En cuanto a seguridad el sistema no es exigente a la hora de conformar claves de acceso a los módulos lo que ha resultado en accesos no autorizados y en manipulación de información por parte de personas ajenas al área financiera y que nada tienen que ver con el proceso.
- El sistema no garantiza integridad de la información ya que se presentan continuas fallas y el sistema es continuamente parchado por el proveedor, generando cierta desconfianza por parte del operador o usuario final.
- La administración del sistema no es sencilla, intuitiva para el administrador, es confusa y cada parche viene acompañado de un manual de como ejecutarlo.
- El mecanismo de copias de seguridad se lo realiza con una rutina propia del sistema, pero estas copias no son custodiadas o no existe una cadena de custodia acorde a la entidad.
- Para corregir muchas de las fallas del sistema existe la necesidad de enviar copia de la Base de Datos a la firma proveedora del sistema para que haga

pruebas y corrija los errores, lo que no es prudente hacerlo debido a que en algún momento se puede atentar contra la confidencialidad de la información.

- En términos generales no se trata de un sistema estable al cual haya que hacerle los mantenimientos de rigor necesarios sino que deja la sensación de que es un sistema que se está construyendo con el ejercicio diario de la entidad y que al proveedor le ha servido para mejorarlo en muchos aspectos.
- En muchas oportunidades para corregir un error hay necesidad de esperar a que el proveedor envíe la solución y esto retrasa las tareas diarias de la oficina financiera ya que por ese error de debe parar todo, atentando contra la disponibilidad de la información.
- Por último sobre este sistema no se ha realizado ninguna revisión o auditoría a la seguridad informática o de la información.

Por otra parte dentro del área financiera y del área de sistemas tampoco están establecidos sistemas de control informáticos y de seguridad de la información efectivos que permitan controlar el acceso a la información, o si estos existen no se están aplicando de manera adecuada.

De seguir funcionando así, la SED y el área financiera de la misma entidad pueden estar expuestas a amenazas o ataques al sistema que ocasionaría múltiples inconvenientes como pérdida total de la información, fuga de recursos económicos, filtración de información importante que no es de público conocimiento y por tratarse de una entidad del estado puede derivar en procesos de investigación disciplinarios, fiscales y penales por los órganos de control.

La entidad debe procurar no depender del proveedor ya que en muchas ocasiones se ha manifestado que el sistema se cambiará por uno que de mejores garantías y tranquilidad pero desafortunadamente el proveedor ha manejado los procesos de cierre de vigencias contables y apertura de las nuevas de tal forma que se hace ver como un proceso traumático y caótico para la entidad.

## 2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo un diagnóstico de la seguridad informática y de la información ayudará a la implementación de un SGSI basado en la norma ISO/IEC 27001, que minimice el impacto y la probabilidad de las amenazas y riesgos potenciales a que ve expuesta el área financiera de la Secretaría de Educación de Nariño?

## 2.3 JUSTIFICACIÓN

Realizar un diagnóstico de la seguridad informática en el área financiera de la Secretaría de Educación Departamental de Nariño es un proceso que adquiere importancia y relevancia dado el continuo desarrollo de la tecnología y del acceso a los diferentes canales de comunicación, es de mucha importancia para el área financiera y para la entidad en general contar con una herramienta que le servirá para la toma de decisiones tendientes a ajustar o eliminar las falencias que se puedan estar presentando tanto en el sistema que soporta los procesos como en el manejo mismo de la información al interior del área y de la entidad.

Por otra parte los usuarios que operan el sistema y para el área financiera como tal, contar con un documento que les orientará y guiará para la implementación de mejoras y ejercer control sobre aspectos que se consideran secundarios ayudará a que ellos le den el verdadero valor a los sistemas y a la información como tal, que este activo sea visto como el más importante y se cree esa conciencia del manejo de la información.

Debido a las constantes fallas que se presentan en el sistema, para el área de sistemas que soporta y administra el software este documento será un soporte fundamental para la planeación interna en el sentido de llevar los ajustes a una propuesta de mejora global del área de sistemas, con el ánimo de proteger y salvaguardar la información y garantizar que los sistemas en este caso el financiero, den un verdadero soporte y ofrezcan las garantías que la entidad necesita, más aun tratándose de una entidad oficial adscrita a la Gobernación de Nariño y que maneja recursos públicos.

La información hoy por hoy se constituye en un activo vital para el éxito y la continuidad de cualquier entidad por eso es necesario buscar el aseguramiento de la misma con la implementación de estándares actuales y reconocidos a nivel internacional como lo es ISO/IEC 27001, a través de este documento que será una guía dinámica donde se mostrara los objetivos claros que se persiguen frente a la seguridad y evolución de riesgos a los cuales está sometida la información de la entidad.

Para la entidad contar con este tipo de estudios y pretender una posterior certificación de la misma en ISO 27001trae para la ella muchas ventajas entre las que podemos encontrar son:

- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de su actividad diaria.
- Demuestra que al interior de la entidad se respetan las leyes y normas que son de aplicación.
- Proporciona una ventaja competitiva y posicionamiento frente a otras de sus mismas características al demostrar a los usuarios que la seguridad de su información es primordial.
- Formaliza unos procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la directiva de la entidad con la seguridad de la información.
- El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora.

## 2.4 OBJETIVOS DEL PROYECTO

### 2.4.1 OBJETIVO GENERAL

Minimizar el impacto y la probabilidad de las amenazas y riesgos potenciales a que ve expuesta el área financiera mediante un diagnóstico de la seguridad informática y de la información que ayude a la implementación de un SGSI basado en la norma ISO/IEC 27001 en la Secretaría de Educación de Nariño.

### 2.4.2 OBJETIVOS ESPECÍFICOS

- Recolectar, clasificar y analizar información sobre las normas y estándares de seguridad de la información para definir los objetivos de la auditoria.
- Reconocer el funcionamiento del área financiera de la Secretaría de educación departamental de Nariño y su proceso Tesorería para verificar su estado actual respecto a los controles de la norma ISO/IEC 27001.
- Basados en ISO/IEC 27002, elaborar el plan de auditoría que incluya todos los aspectos auditables en cuanto a la seguridad informática, los recursos necesarios y el cronograma de actividades y pruebas a desarrollarse en el proceso de tesorería del área financiera de la Secretaría de Educación Departamental de Nariño.
- Ejecutar el plan de trabajo diseñado anteriormente, aplicar los instrumentos diseñados para recolectar la información, y ejecutar las pruebas necesarias

que permitan establecer el estado actual de la seguridad informática y de la información en el área financiera de la SED.

- Elaborar el informe final de los resultados obtenidos en la auditoria, para determinar los posibles controles que apliquen en cada caso y el tratamiento de los mismos que permitan mitigar las amenazas y riesgos encontrados.
- Entregar documento guía para la implementación de un SGSI acorde a las necesidades de la SED Nariño, en especial al área financiera que determinen las políticas y procedimientos de seguridad informática y de la información frente a las posibles amenazas y riesgos donde además se incluirá un plan de mejora continua.

## 2.5 MARCO REFERENCIAL

### 2.5.1 Antecedentes

*"LLERENA RIASCOS Rafael Esteban, GUERRA ERASO José Daniel, Diagnóstico del estado de los sistemas de gestión de seguridad de la información (SGSI), con la aplicación de un software, en las instituciones de educación superior de San Juan de Pasto, 2009, Proyecto de grado (Ingeniero de Sistemas), Institución Universitaria CESMAG, FACULTAD DE INGENIERÍA".*[1]

A través de este proyecto los autores buscan en primer lugar estudiar las características de la norma ISO/IEC 27001 contra las características informáticas de algunas de las más importantes instituciones de educación superior de San Juan de Pasto y con todo ello desarrollar una aplicación que permita realizar una evaluación que muestra el estado general de estas instituciones y promover al mismo tiempo el acogimiento de la norma.

Uno de los autores del proyecto en cuestión hace parte del proyecto actual por lo cual este antecedente ha sido tenido en cuenta desde los momentos iniciales de la propuesta y ayudó a promover la idea de una auditoría. Entre las características más relevantes que convierten el proyecto nombrado en un antecedente están el uso de la norma ISO/IEC 27001 y la exposición de indicadores que dejan en evidencia los puntos más débiles de algunas instituciones frente a los controles de la norma.

- *"ERAZO ARCINIEGAS Andrea, MORAN BRAVO Carmen, Políticas de seguridad para el área de sistemas del instituto Colombiano de bienestar familiar regional Nariño, San Juan de Pasto, Proyecto de grado, IU CESMAG".*[2]

En este estudio, basado en el Instituto Colombiano de Bienestar Familiar se demostró la existencia de algunas deficiencias en el manejo de los recursos informáticos y en especial deficiencias en la seguridad de acceso físico a las instalaciones del área de sistemas y acceso lógico a la información.

[1] LLERENA RIASCOS Rafael Esteban y GUERRA ERASO José Daniel. Diagnóstico del estado de los sistemas de gestión de seguridad de la información (SGSI), con la aplicación de un software, en las instituciones de educación superior de San Juan de Pasto. Pasto: I. U CESMAG, 2009. p 15.
[2] ERAZO ARCINIEGAS, Andrea, MORAN BRAVO Carmen, Políticas de seguridad para el área de sistemas del instituto Colombiano de bienestar familiar regional Nariño. Pasto: I. U CESMAG. p. 18

Es relevante porque determina las políticas de seguridad informática de una institución pública frente a un conjunto de deficiencias y que pueden ser comunes y que están contenidas en la norma ISO/IEC 27001 como el acceso a recursos físicos, lógicos y a la información.

- *"PATIÑO ALPALA Luis Olmedo, Propuesta De Actualización, Apropiación Y Aplicación De Políticas De Seguridad Informática En Una Empresa Corporativa, Propolsinecor, San Juan de Pasto, Proyecto de grado, UNAD"*[3]

En este proceso de investigación, basado en Propolsenicor, se pudo establecer que hace falta una estructura jerárquica dedicada exclusivamente al manejo de la seguridad de la información, como también herramientas que permitan monitorear la red y probar la vulnerabilidad de los aplicativos.

Por otra parte se estableció que la compañía tiene un sistema de seguridad informática que contempla algunos apartes de la norma estándar ISO NTC 27001, implementada como controles de seguridad de la información en los procesos de calidad de la ISO NTC 9001, con unas políticas de seguridad informática llamados controles, encontrándose debilidades en cuando a la poca difusión y capacitación en la implementación del sistema de seguridad informática.

### 2.5.2 Marco Teórico

**2.5.2.1 Auditoria.** Es principalmente, estudiar y analizar toda la documentación y sistemas de información relativos a una empresa, institución u organismo, esta auditoría ayuda a determinar si la información que ofrece la entidad u área objeto de estudio esta correlacionada con la situación real de la misma, y para determinar si sus sistemas de información son los correctos para el funcionamiento de la misma y la consecución de sus objetivos.

Las auditorias se llevan a cabo por empresas independientes y son una herramienta muy útil para saber que una entidad funciona correctamente, por ejemplo, al presentar resultados ante la administración central o para suministrar

[3] PATIÑO ALPALA Luis Olmedo, Propuesta De Actualización, Apropiación y Aplicación de Políticas de Seguridad Informática en una Empresa Corporativa, Propolsinecor. Pasto: UNAD. p. 34.

información a las directivas para una correcta toma de decisiones. Algunas auditorias están reguladas por Ley y las empresas e instituciones deben someterse a ellas de manera obligatoria, por lo general estas están establecidas cada cierto período de tiempo. Pero las directivas de las entidades públicas o privadas pueden encargar en una firma auditora que estudie los planes, objetivos, sistemas de información, sistemas de producción, etc. de la entidad a fin de identificar y corregir posibles ineficiencias o errores que se estén cometiendo.

**2.5.2.2 Estándares de Auditoria. "**Una auditoria se realiza con base en un patrón o también llamado conjunto de directrices o buenas prácticas sugeridas, dando lugar a los estándares los cuales sirven como base para las auditorías informáticas"[4] en este caso, los estándares como ISO 27002 el cual es un código de buenas prácticas para la seguridad de la información, al igual que 27001 que es un estándar de seguridad de información en el cual se definen los requisitos de auditoría y sistemas de gestión de seguridad.

**2.5.2.3 Auditoría Informática.** Universalmente la auditoría es comprendida como un proceso de examen realizado por un auditor ("*todo aquel que tiene la virtud de oír*"[5]) y que tiene como resultado un conjunto de indicadores que determinan el estado y confiabilidad de un sistema.

En la actualidad existen muchos tipos distintos de auditoría que plantean diferentes finalidades. En el caso de la auditoría informática se trata del estudio que se realiza sobre los recursos informáticos de una organización para emitir un informe de la situación actual de los mismos y que posteriormente la organización encargada pueda usarla como una herramienta de mejora.

**2.5.2.4 Etapas de una Auditoría Informática. "**El proceso de auditar los sistemas informáticos cuenta por supuesto con una secuencia ordenada de actividades que deben planearse correctamente antes de iniciar este proceso y teniendo en cuenta las necesidades específicas de la empresa donde será aplicada.

[4] WIKIPEDIA. Auditoría de seguridad de sistemas de información. [en línea]. [consultado el 22 de mayo de 2015]. Disponible en http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3

[5] REAL ACADEMIA ESPAÑOLA. Auditoría Informática. [en línea]. [consultado el 02 de mayo de 2015]. Disponible en http://www.rae.es/rae.html.

Las actividades de una auditoría informática no se imponen sino que se adaptan de acuerdo al tipo de auditoría y los objetivos planteados por la organización y el equipo de auditores. La metodología de una auditoría informática tiene tres etapas generales: Planeación, Ejecución y Dictamen como se puede observar en la siguiente tabla[6]:

**Tabla 1. Etapas de una auditoría informática**

| ETAPAS | PASOS A REALIZAR |
|---|---|
| **Planeación de la Auditoria de Sistemas** | 1. Identificar el origen de la auditoría. |
| | 2. Realizar una visita preliminar al área que será evaluada. |
| | 3. Establecer los objetivos de la auditoría. |
| | 4. Determinar los puntos que serán evaluados en la auditoría. |
| | 5. Elaborar planes, programas y presupuestos para realizar la auditoría. |
| | 6. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría. |
| | 7. Asignar los recursos y sistemas computacionales para la auditoría. |
| **Ejecución de la Auditoria de Sistemas** | 1. Realizar las acciones programadas para la auditoría. |
| | 2. Aplicar los instrumentos y herramientas para la auditoría. |
| | 3. Identificar y elaborar los documentos de oportunidades de mejoramiento encontradas. |
| | 4. Elaborar el dictamen preliminar y presentarlo a discusión. |
| | 5. Integrar el legajo de papeles de trabajo de la auditoría |
| **Dictamen de la Auditoria de Sistemas** | 1. Analizar la información y elaborar un informe de situaciones detectadas. |
| | 2. Elaborar el Dictamen final. |
| | 3. Presentar el informe de auditoría. |

Fuente: BENAVIDES RUANO, M. C. SOLARTE SOLARTE, F. N. J. (2013). MODULO GUÍA: RIESGOS Y CONTROL INFORMÁTICO. Pasto: Universidad Nacional Abierta y a Distancia

[6] BENAVIDES RUANO, M. C. SOLARTE SOLARTE, F. N. J. MÓDULO GUÍA: RIESGOS Y CONTROL INFORMÁTICO. Pasto: Universidad Nacional Abierta y a Distancia, 2013. p. 34.

**2.5.2.5 La Serie ISO 27000. "**A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.
Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- **ISO 27000:** En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma está previsto que sea gratuita, a diferencia de las demás de la serie que tendrían un coste.

- **ISO 27001:** Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en AENOR"[7]

Otros países donde también está publicada en español son, por ejemplo, Colombia y Venezuela. El original en inglés y la traducción al francés pueden adquirirse en ISO.org.

El estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) fue aprobado y publicado como estándar internacional en Octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

[7] ISO 27000. El portal de ISO 27001 en Español. [en línea]. [consultado el 05 de mayo de 2015]. Disponible en http://www.iso27000.es/iso27000.html.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la revisión de la norma británica British Standard BS 7799-2:2002.

Actualmente el ISO-27001 es el único estándar aceptado internacionalmente (Certificable) para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad.

- **ISO 27002:** "Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.

- **ISO 27003:** En fase de desarrollo; su fecha prevista de publicación es Mayo de 2009.

Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación"[8].

- **ISO 27004: "**En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles

[8] GESTION – CALIDAD.COM. La Serie ISO 27000. [en línea]. [consultado el 05 de mayo de 2015]. Disponible en http://www.gestion-calidad.com/iso-27000.html.

relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA”.[9]

- **“ISO 27005:** En fase de desarrollo; su fecha prevista de publicación es mayo de 2008.

Consistirá en una guía de técnicas para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI. Recogerá partes de ISO/IEC TR 13335.

- **ISO 27006:** Publicada el 1 de Marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSI's) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSI's. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.

- **ISO 27007:** En fase de desarrollo; su fecha prevista de publicación es mayo de 2010”[10].

Consistirá en una guía de auditoría de un SGSI.

- **ISO 27011:** En fase de desarrollo; su fecha prevista de publicación es Enero de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

[9] LINA, Andrea. Norma ISO 27000. [en línea]. [consultado el 05 de mayo de 2015]. Disponible en http://linaandrea2-mantenimientodepc.blogspot.com/2010/09/norma-iso-27000.html.
[10] LINA, Andrea. Óp., Cit., p. 28

- **“ISO 27031:** En fase de desarrollo; su fecha prevista de publicación es mayo de 2010.

  Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones”[11].

- **“ISO 27032:** En fase de desarrollo; su fecha prevista de publicación es febrero de 2009. Consistirá en una guía relativa a la ciberseguridad.

- **ISO 27033:** En fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y renumeración de ISO 18028”.

#### 2.5.2.6 Objetivos de control de la Norma ISO/IEC 27001

- **“Política de seguridad:** Una política de seguridad es un enunciado formal de las reglas y procedimientos que los usuarios que acceden a los recursos de la organización deben cumplir, para prevenir, proteger y manejar los riesgos, y su objetivo es de informar al mayor nivel de detalle a los usuarios, empleados y gerentes, de las normas y mecanismos que deben cumplir y utilizar para proteger los componentes de los sistemas de la organización” [12]

- **“Organización de la seguridad de la información:** La organización de la seguridad está orientada a administrar la seguridad de la información dentro del organismo y establecer un marco gerencial para controlar su implementación, así como para la distribución de funciones y

[11] CONISEC. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. LINA, Andrea. Norma ISO 27000. [en línea]. [consultado el 07 de mayo de 2015]. Disponible en http://www.conisec.com/file3.html.

[12] ICONTEC. COMPENDIO: Sistema de gestión de la seguridad de la información. LINA, Andrea. Norma ISO 27000. [en línea]. [consultado el 03 de mayo de 2015]. Disponible en http://www.Icontec.org.co.

responsabilidades. Además de fomentar la consulta y cooperación con organismos especializados para la obtención de asesoría en materia de seguridad de la información y garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

- **Gestión de activos:** La gestión o administración de activos está destinada a mantener una adecuada clasificación y protección de los activos del organismo, en esta también se clasifica la información para señalar su sensibilidad y criticidad. Además de definir niveles de protección y medidas de tratamiento especial acordes a su clasificación"[13].

- **Seguridad de los recursos humanos:** La seguridad de los recursos humanos este orientado a reducir los riesgos de error humano, robo, fraude, o uso inadecuado de las instalaciones, además de definiciones de puestos de trabajo y asignación de recursos. Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

  La seguridad de los recursos humanos también debe garantizar que los usuarios estén al tanto de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la política de seguridad de la información de la organización en el transcurso de sus tareas normales.

- **Seguridad física y del entorno:** La seguridad física y del entorno está destinada a impedir accesos no autorizados, daños e interferencia a las dependencias e información de la organización. Proteger el equipamiento de procesamiento de información crítica del organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

  Además debe controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo. Y también debe implementar medidas para

[13] ICONTEC. Óp., Cit., p. 29

proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

- **"Gestión de comunicación y operaciones:** La gestión de comunicación y operaciones está dirigida a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información, y establecer responsabilidades y procedimientos de gestión y operación para todas las instalaciones. Además de una implementación de separación de funciones cuando corresponda.

- **Control de acceso:** Un sistema de control de acceso es el que impide el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. También Implementa seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

  Además debe registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas y concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

- **Adquisición, desarrollo y mantenimiento de sistemas de información:** El desarrollo y mantenimiento de sistemas de información está orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento. Además de definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan y también determina los métodos de protección de la información crítica o sensible"[14].

- **Gestión de los incidentes de la seguridad de la información:** La gestión de los incidentes de la seguridad de la información está orientada a minimizar el daño producido por incidentes y anomalías en materia de seguridad, donde también se determina como monitorear dichos incidentes y aprender de los mismos, para no repetir fallos o interrupciones del mismo tipo.

[14] ICONTEC. Óp., Cit., p. 29

- **“Gestión de la continuidad del negocio:** La gestión de la continuidad del negocio está orientada a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres. Además de asegurar la coordinación con el personal de la organización y los contactos externos que participaran en las estrategias de planificación de contingencias y asignarles funciones para cada actividad definida.

- **Cumplimiento:** El cumplimiento está destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal, de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos, y de los requisitos de seguridad.

  Además de revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información”[15]

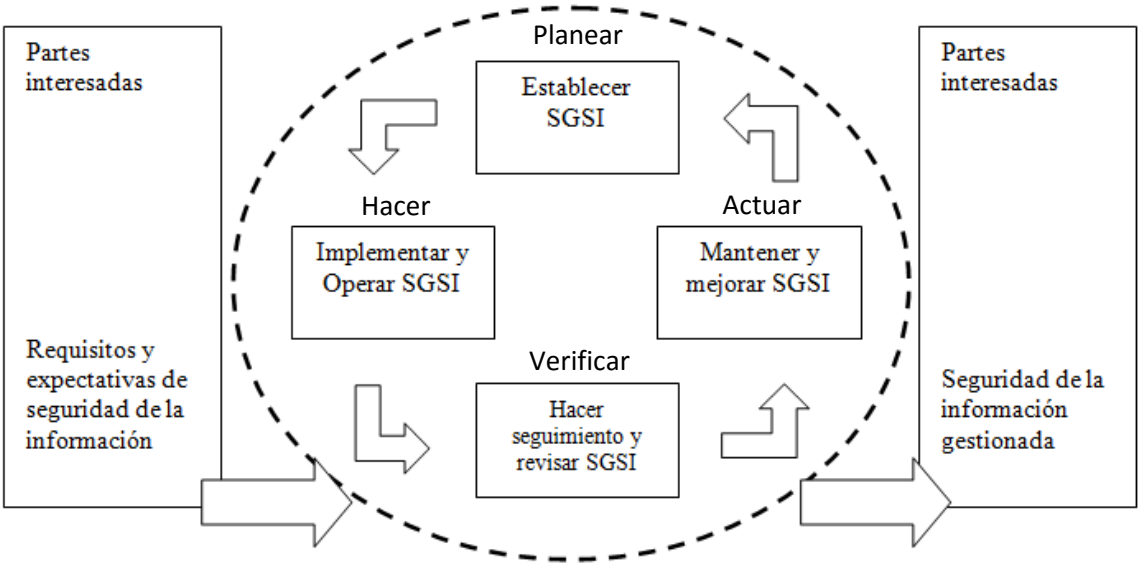
**2.5.2.7 Modelo de procesos “*Planear-Hacer-Verificar-Actuar*”. “**Esta norma adopta el modelo de procesos “Planear-Hacer-Verificar-Actuar” (PHVA) que se aplica para estructurar los procesos del SGSI, este toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas y, a través de acciones y procesos necesarios produce resultados de seguridad de la información que cumplen con dichos requisitos y expectativas.

La adopción del modelo PHVA refleja los principios establecidos en las directrices OCDE para la seguridad de sistemas y redes de información, esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad”[16]

[15] ICONTEC. Óp., Cit., p. 29

[16] BUITRAGO ESTRADA, Johanna Carolina; BONILLA PINEDA, Diego Hernando y MURILLO VARON, Carol Estefanie. DISEÑO DE UNA METODOLOGIA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI, EN EL SECTOR DE LABORATORIOS DE ANALISIS MICROBIOLOGICOS, BASADO EN ISO 27001. [en línea]. [consultado el 05 de mayo de 2015]. Disponible en http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1.

**Figura 1. Modelo PHVA aplicado a los procesos de SGSI**




Fuente: ICONTEC. COMPENDIO: Sistema de gestión de la seguridad de la información (SGSI), Colombia. 2006. Disponible en www.Icontec.org.co

**Tabla 2. Descripción del modelo PHVA**

| Proceso PHVA | Descripción |
|---|---|
| Planificar: **Establecer el SGSI** | Establecer la politica, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información con el fin de entregar resultados acordes con las politicas y objetivos globales de una organización. |
| Hacer: **Implementar y operar el SGSI** | Implementar y operar la politica, los controles, procesos y procedimientos del SGSI |
| Verificar: **hacer seguimiento y revisar el SGSI** | Evluar, y, en donde sea apliucable, medir el desempeño del proceso contra la politica y los objetivos de seguridad y la experiencia practica y reportar los resultados a la direccion para su revisión. |
| Actuar: **Mantener y mejorar el SGSI** | Emprender acciones correctivas y |

| | |
|---|---|
| | preventivas con base en los resultados de la auditoria interna del SGSI y la revision por la direccion para lograr la mejora continua. |

Fuente: ICONTEC. COMPENDIO: Sistema de gestión de la seguridad de la información (SGSI), Colombia. 2006. Disponible en www.Icontec.org.co

**2.5.2.8 ISO/IEC 27002. "**Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

Al igual que ISO 17799 tampoco es una norma certificable sino que recomienda a las organizaciones una serie de medidas que les ayuden a mejorar la seguridad de la información y generar políticas para su esquema de seguridad cobijando todos los aspectos básicos"[17]

La ISO/IEC 27002 cuenta con 11 dominios, 39 objetivos de control y 133 controles descritos en la siguiente tabla:

**Tabla 3. Dominios, objetivos de control y controles ISO/IEC 27002**

| DOMINIOS | OBJETIVOS DE CONTROL | CONTROLES |
|---|---|---|
| **1. POLÍTICA DE SEGURIDAD.** | **1.1.** Política de seguridad de la información. | **1.1.1.** Documento de política de seguridad de la información.<br>**1.1.2.** Revisión de la política de seguridad de la información. |

[17] ALTAGRACIA, Arelys. DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. CASO: DIRECCIÓN DE INFORMÁTICA DE LA ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL ESTADO LARA. [en línea]. [consultado el 06 de mayo de 2015]. Disponible en: http://bibcyt.ucla.edu.ve/Edocs_Bciucla/Repositorio/TGMQA76.9.A25L662011.pdf.

| | | |
|---|---|---|
| **2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN** | **2.1.** Organización interna | **2.1.1.** Compromiso de la Dirección con la seguridad de la información.<br>**2.1.2.** Coordinación de la seguridad de la información.<br>**2.1.3.** Asignación de responsabilidades relativas a la seg. de la información.<br>**2.1.4.** 6.1.4 Proceso de autorización de recursos para el tratamiento de la<br>**2.1.5.** información.<br>**2.1.6.** 6.1.5 Acuerdos de confidencialidad.<br>**2.1.7.** 6.1.6 Contacto con las autoridades.<br>**2.1.8.** Contacto con grupos de especial interés.<br>**2.1.9.** Revisión independiente de la seguridad de la información. |
| | **2.2.** Tratamiento | **2.2.1.** Identificación de los riesgos derivados del acceso de terceros.<br>**2.2.2.** Tratamiento de la seguridad en la relación con los clientes.<br>**2.2.3.** Tratamiento de la seguridad en contratos con terceros. |
| **3. GESTIÓN DE ACTIVOS** | **3.1.** Responsabilidad sobre los activos. | **3.1.1.** Inventario de activos.<br>**3.1.2.** Propiedad de los activos.<br>**3.1.3.** Uso aceptable de los activos. |

| | | |
|---|---|---|
| | **3.2.** Clasificación de la información. | **3.2.1.** Directrices de clasificación.<br>**3.2.2.** Etiquetado y manipulado de la información. |
| **4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS** | **4.1.** Antes del empleo. | **4.1.1.** Funciones y responsabilidades.<br>**4.1.2.** Investigación de antecedentes.<br>**4.1.3.** Términos y condiciones de contratación. |
| | **4.2.** Durante el empleo. | **4.2.1.** Responsabilidades de la Dirección.<br>**4.2.2.** Concienciación, formación y capacitación en seg. de la informac.<br>**4.2.3.** Proceso disciplinario. |
| | **4.3.** Cese del empleo o cambio de puesto de trabajo. | **4.3.1.** Responsabilidad del cese o cambio.<br>**4.3.2.** Devolución de activos.<br>**4.3.3.** Retirada de los derechos de acceso. |
| **5. SEGURIDAD FÍSICA Y DEL ENTORNO.** | **5.1.** Áreas seguras. | **5.1.1.** Perímetro de seguridad física.<br>**5.1.2.** Controles físicos de entrada.<br>**5.1.3.** Seguridad de oficinas, despachos e instalaciones.<br>**5.1.4.** Protección contra las amenazas externas y de origen ambiental.<br>**5.1.5.** Trabajo en áreas seguras.<br>**5.1.6.** Áreas de acceso público y de carga y descarga. |
| | **5.2.** Seguridad de los equipos. | **5.2.1.** Emplazamiento y protección de equipos.<br>**5.2.2.** Instalaciones de suministro. |

| | | |
|---|---|---|
| | | **5.2.3.** Seguridad del cableado.<br>**5.2.4.** Mantenimiento de los equipos.<br>**5.2.5.** Seguridad de los equipos fuera de las instalaciones.<br>**5.2.6.** Reutilización o retirada segura de equipos.<br>**5.2.7.** Retirada de materiales propiedad de la empresa. |
| **6. GESTIÓN DE COMUNICACIONES Y OPERACIONES.** | **6.1.** Responsabilidades y procedimientos de operación. | **6.1.1.** Documentación de los procedimientos de operación.<br>**6.1.2.** Gestión de cambios.<br>**6.1.3.** Segregación de tareas.<br>**6.1.4.** Separación de los recursos de desarrollo, prueba y operación. |
| | **6.2.** Gestión de la provisión de servicios por terceros. | **6.2.1.** Provisión de servicios.<br>**6.2.2.** Supervisión y revisión de los servicios prestados por terceros.<br>**6.2.3.** Gestión del cambio en los servicios prestados por terceros. |
| | **6.3.** Planificación y aceptación del sistema. | **6.3.1.** Gestión de capacidades.<br>**6.3.2.** Aceptación del sistema. |
| | **6.4.** Protección contra el código malicioso y descargable. | **6.4.1.** Controles contra el código malicioso.<br>**6.4.2.** Controles contra el código descargado en el cliente. |
| | **6.5.** Copias de seguridad. | **6.5.1.** Copias de seguridad de la información. |
| | **6.6.** Gestión de la seguridad de las redes. | **6.6.1.** Controles de red.<br>**6.6.2.** Seguridad de los servicios de red. |

| | | |
|---|---|---|
| | **6.7.** Manipulación de los soportes. | **6.7.1.** Gestión de soportes extraíbles.<br>**6.7.2.** Retirada de soportes.<br>**6.7.3.** Procedimientos de manipulación de la información.<br>**6.7.4.** Seguridad de la documentación del sistema. |
| | **6.8.** Intercambio de información. | **6.8.1.** Políticas y procedimientos de intercambio de información.<br>**6.8.2.** Acuerdos de intercambio.<br>**6.8.3.** Soportes físicos en tránsito.<br>**6.8.4.** Mensajería electrónica.<br>**6.8.5.** Sistemas de información empresariales. |
| | **6.9.** Servicios de comercio electrónico. | **6.9.1.** Comercio electrónico.<br>**6.9.2.** Transacciones en línea.<br>**6.9.3.** Información públicamente disponible. |
| | **6.10.** Supervisión. | **6.10.1.** Registros de auditoría.<br>**6.10.2.** Supervisión del uso del sistema.<br>**6.10.3.** Protección de la información de los registros.<br>**6.10.4.** Registros de administración y operación.<br>**6.10.5.** Registro de fallos.<br>**6.10.6.** Sincronización del reloj. |
| **7. CONTROL DE ACCESO.** | **7.1.** Requisitos de negocio para el control de acceso. | **7.1.1.** Política de control de acceso |
| | **7.2.** Gestión de acceso | **7.2.1.** Registro de usuario. |

| | | |
|---|---|---|
| | de usuario. | **7.2.2.** Gestión de privilegios.<br>**7.2.3.** Gestión de contraseñas de usuario.<br>**7.2.4.** Revisión de los derechos de acceso de usuario. |
| | **7.3.** Responsabilidades de usuario. | **7.3.1.** Uso de contraseña.<br>**7.3.2.** Equipo de usuario desatendido.<br>**7.3.3.** Política de puesto de trabajo despejado y pantalla limpia.<br>**7.3.4.** |
| | **7.4.** Control de acceso a la red. | **7.4.1.** Política de uso de los servicios en red.<br>**7.4.2.** Autenticación de usuario para conexiones externas.<br>**7.4.3.** Identificación de los equipos en las redes.<br>**7.4.4.** Protección de los puertos de diagnóstico y configuración remotos.<br>**7.4.5.** Segregación de las redes.<br>**7.4.6.** Control de la conexión a la red.<br>**7.4.7.** Control de encaminamiento (routing) de red.<br>**7.4.8.** |
| | **7.5.** Control de acceso al sistema operativo | **7.5.1.** Procedimientos seguros de inicio de sesión.<br>**7.5.2.** Identificación y autenticación de usuario.<br>**7.5.3.** Sistema de gestión de contraseñas.<br>**7.5.4.** Uso de los recursos del sistema.<br>**7.5.5.** Desconexión automática de sesión.<br>**7.5.6.** Limitación del tiempo |

| | | |
|---|---|---|
| | | de conexión. |
| | **7.6.** Control de acceso a las aplicaciones y a la información. | **7.6.1.** Restricción del acceso a la información.<br>**7.6.2.** Aislamiento de sistemas sensibles. |
| | **7.7.** Ordenadores portátiles y teletrabajo. | **7.7.1.** Ordenadores portátiles y comunicaciones móviles.<br>**7.7.2.** Teletrabajo. |
| **8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN** | **8.1.** Requisitos de seguridad de los sistemas de información. | **8.1.1.** Análisis y especificación de los requisitos de seguridad.<br>**8.1.2.** |
| | **8.2.** Tratamiento correcto de las aplicaciones. | **8.2.1.** Validación de los datos de entrada.<br>**8.2.2.** Control del procesamiento interno.<br>**8.2.3.** Integridad de los mensajes.<br>**8.2.4.** Validación de los datos de salida. |
| | **8.3.** Controles criptográficos. | **8.3.1.** Política de uso de los controles criptográficos.<br>**8.3.2.** Gestión de claves. |
| | **8.4.** Seguridad de los archivos de sistema. | **8.4.1.** Control del software en explotación.<br>**8.4.2.** Protección de los datos de prueba del sistema.<br>**8.4.3.** Control de acceso al código fuente de los programas. |
| | **8.5.** Seguridad en los procesos de desarrollo y soporte. | **8.5.1.** Procedimientos de control de cambios.<br>**8.5.2.** Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.<br>**8.5.3.** Restricciones a los cambios en los paquetes de software. |

| | | |
|---|---|---|
| | | **8.5.4.** Fugas de información.<br>**8.5.5.** Externalización del desarrollo de software. |
| | **8.6.** Gestión de la vulnerabilidad técnica. | **8.6.1.** Control de las vulnerabilidades técnicas. |
| **9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN** | **9.1.** Notificación de eventos y puntos débiles de seguridad de la<br>**9.2.** información. | **9.2.1.** Notificación de los eventos de seguridad de la información.<br>**9.2.2.** Notificación de puntos débiles de seguridad. |
| | **9.3.** Gestión de incidentes y mejoras de seguridad de la información. | **9.3.1.** Responsabilidades y procedimientos.<br>**9.3.2.** Aprendizaje de los incidentes de seguridad de la información.<br>**9.3.3.** Recopilación de evidencias. |
| **10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.** | **10.1.** Aspectos de seguridad de la información en la gestión de la<br>**10.2.** continuidad del negocio. | **10.2.1.** Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.<br>**10.2.2.** Continuidad del negocio y evaluación de riesgos.<br>**10.2.3.** Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.<br>**10.2.4.** Marco de referencia para la planificación de la cont. del negocio.<br>**10.2.5.** Pruebas, mantenimiento y reevaluación de planes de continuidad. |
| **11. CUMPLIMIENTO.** | **11.1.** Cumplimiento de los requisitos legales. | **11.1.1.** Identificación de la legislación aplicable.<br>**11.1.2.** Derechos de propiedad intelectual (DPI). |

| | | |
|---|---|---|
| | | **11.1.3.** Protección de los documentos de la organización.<br>**11.1.4.** Protección de datos y privacidad de la información de carácter personal.<br>**11.1.5.** Prevención del uso indebido de recursos de tratamiento de la información.<br>**11.1.6.** Regulación de los controles criptográficos. |
| | **11.2.** Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico. | **11.2.1.** Cumplimiento de las políticas y normas de seguridad.<br>**11.2.2.** Comprobación del cumplimiento técnico. |
| | **11.3.** Consideraciones sobre las auditorías de los sistemas. de información. | **11.3.1.** Controles de auditoría de los sistemas de información.<br>**11.3.2.** Protección de las herramientas de auditoría de los sistemas de información. |

Fuente: ISO/IEC 27002:2005. Dominios, Objetivos de Control y Controles. Disponible en http://www.iso27000.es/download/ControlesISO27002-2005.pdf

**2.5.2.9 Administración de Riesgos. "**La administración de riesgos es el proceso continuo basado en el conocimiento, evaluación, manejo de los riesgos y sus impactos que mejora la toma de decisiones organizacionales.
Es entonces la administración de riesgos el término asociado al conjunto de pasos secuenciales, lógicos y sistemáticos que debe seguir el analista de riesgos para identificar, valorar y manejar los riesgos asociados a los procesos de la Organización, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados minimizando las pérdidas o maximizando las oportunidades"[18].

[18] DNP. LINEAMIENTOS PARA LA ADMINISTRACION DE RIESGOS EN LOS PROCESOS DEL DNP. [en línea]. [consultado el 06 de mayo de 2015]. Disponible en https://colaboracion.dnp.gov.co/CDT/DNP/AR-L02%20Lineamientos%20Administracion%20Riesgos.Pu.pdf.

- **Análisis de riesgos**

"El análisis de riesgo es el estudio de las causas de las posibles amenazas y, los daños y consecuencias que éstas puedan producir. Este tipo de análisis es ampliamente utilizado como herramienta de gestión en estudios financieros y de seguridad para identificar riesgos (métodos cualitativos) y otras para evaluar riesgos (generalmente de naturaleza cuantitativa).

El primer paso del análisis es identificar los activos a proteger o evaluar. La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente.

La función de la evaluación consiste en ayudar a alcanzar un nivel razonable de consenso en torno a los objetivos en cuestión, y asegurar un nivel mínimo que permita desarrollar indicadores operacionales a partir de los cuales medir y evaluar"[19].

Los resultados obtenidos del análisis, van a permitir aplicar alguno de los métodos para el tratamiento de los riesgos, que involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos.

- **Evaluación de riesgos**

En la evaluación de riesgos se compara el nivel de riesgo encontrado durante el proceso de análisis contra el criterio de riesgo establecido previamente, y decidir si los riesgos pueden ser aceptados.

El análisis de riesgos y los criterios contra los cuales los riesgos son comparados en la valoración deben ser considerados sobre la misma base. Así, evaluaciones cualitativas incluyen la comparación de un nivel cualitativo de riesgo contra criterios cualitativos, y evaluaciones cuantitativas involucran la comparación de niveles estimados de riesgo contra criterios que pueden ser expresados como números específicos, tales como fatalidad, frecuencia o valores monetarios.

[19] DNP. Óp., Cit., p. 43.

El resultado de una evaluación de riesgos es una lista priorizada de riesgos para definirles acciones de tratamiento posteriores.

- **Gestión de riesgos**

"La Gestión de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Algunas veces, el manejo de riesgos se centra en la contención de riesgo por causas físicas o legales (por ejemplo, desastres naturales o incendios, accidentes, muertes o demandas). Por otra parte, la gestión de riesgo financiero se enfoca en los riesgos que pueden ser manejados usando instrumentos financieros y comerciales"[20]

El objetivo de la gestión de riesgos es reducir diferentes riesgos relativos a un ámbito preseleccionado a un nivel aceptado por la sociedad. Puede referirse a numerosos tipos de amenazas causadas por el medio ambiente, la tecnología, los seres humanos, las organizaciones y la política. Por otro lado, involucra todos los recursos disponibles por los seres humanos o, en particular, por una entidad de manejo de riesgos (persona, staff, organización).

**2.5.2.10 Sistema de Gestión de la Seguridad de la Información SGSI. "**El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información"[21].

[20] DNP. Óp., Cit., p. 43.
[21] INSOR. PLAN DE SEGURIDAD. [en línea]. [consultado el 08 de mayo de 2015]. Disponible en http://www.insor.gov.co/descargar/plan_de_seguridad.pdf.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

**2.5.2.11 Establecimiento y Gestión del SGSI.** La organización es la principal protagonista y a través de su junta directiva designar él o los responsables del control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos, además deberá:

a) "Definir el alcance y límites del SGSI en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.
b) Definir una política de SGSI en términos de las características del negocio, la organización, su ubicación, los activos y tecnología.
c) Definir el enfoque organizacional para la valoración del riesgo.
d) Identificar los riesgos.
e) Analizar y evaluar los riesgos.
f) Identificar y evaluar las opciones para el tratamiento de los riesgos.
g) Seleccionar los objetivos de control y los controles para el tratamiento de los riesgos.
h) Los objetivos de control y los controles se deben seleccionar e implementar de manera que cumplan los requisitos identificados en el proceso de valoración y tratamiento de riesgos.
i) Obtener la aprobación de la dirección sobre los riesgos residuales propuestos.
j) Obtener autorización de la dirección para implementar y operar el SGSI.
k) Elaborar una declaración de aplicabilidad que incluya:

- Los objetivos de control y los controles seleccionados y las razones para su selección.
- Los objetivos de control y controles implementados actualmente.
- La exclusión de cualquier objetivo de control y controles y la justificación para su exclusión" [22]

[22] ICONTEC. COMPENDIO: Sistema de gestión de la seguridad de la información (SGSI), Colombia, 2006. p. 21.

**2.5.2.12 Implementación y Operación del SGSI.** La organización debe:

a) "Formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información.
b) Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados que incluyen considerar la financiación y la asignación de funciones y responsabilidades.
c) Implementar los controles seleccionados para cumplir los objetivos de control.
d) Definir cómo medir la eficacia de los controles o grupos de controles seleccionados y especificar como se van a usar estas mediciones con el fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles.
e) Implementar programas de formación y de toma de conciencia.
f) Gestionar la operación del SGSI.
g) Gestionar los recursos del SGSI.
h) Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad"[23]

**2.5.2.13 Seguimiento y Revisión del SGSI.** La organización debe:

a) "Ejecutar procedimientos de seguimiento y revisión y otros controles para:
   - Detectar rápidamente errores en los resultados del procesamiento;
   - Identificar con prontitud los incidentes e intentos de violación a la seguridad que tuvieron éxito como los que fracasaron;
   - Posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada.
   - Ayudar a detectar eventos de seguridad y de esta manera impedir incidentes de seguridad mediante el uso de indicadores y
   - Determinar si las acciones tomadas para solucionar un problema de violación de seguridad fueron eficaces.
b) Emprender revisiones regulares de la eficacia del SGSI teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia, sugerencias y retroalimentación de todas las partes interesadas.
c) Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.

[23] ICONTEC, Ibíd., p. 46

d) Revisar las valoraciones de los riesgos a intervalos planificados y revisar el nivel de riesgo residual y riesgo aceptable identificado teniendo en cuenta cambios en:
   - La organización,
   - La tecnología,
   - Los objetivos y procesos de negocio, las amenazas identificadas, la eficacia de los controles implementados y eventos externos tales como cambios en el entorno legal o reglamentario en las obligaciones contractuales y en el clima social.

e) Realizar auditorías internas del SGSI a intervalos planificados.
f) Emprender una revisión del SGSI realizada por la dirección en forma regular para asegurar que el alcance siga siendo suficiente y que identifiquen mejoras al proceso de SGSI.
g) Actualizar los planes de seguridad para tener en cuenta las conclusiones de las actividades de seguimiento y revisión.
h) Registrar acciones y eventos que podría tener impacto en la eficacia o el desempeño del SGSI"[24]

**2.5.2.14 Mantenimiento y Mejora del SGSI.** La organización debe, regularmente:

a) "Implementar las mejoras identificadas en el SGSI;
b) Emprender las acciones correctivas y preventivas adecuadas. Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización.
c) Comunicar las acciones y mejoras a todas las partes interesadas con un nivel de detalle apropiado a las circunstancias y en donde sea pertinente llegar a acuerdos sobre cómo proceder.
d) Asegurar que las mejoras logran los objetivos previstos"[25]

### 2.5.3 Marco Conceptual

**2.5.3.1 Activo.** Finney – Miller (1975, p.5) afirma que: "El activo está constituido por las cosas de valor que se poseen; Tracy (1979, p.25) indica que los activos representan "los recursos económicos que son propiedad de la empresa"; Myron, Gordon y Gordon (1981, p.48) establecen que: "Todo activo es el derecho que tiene valor para su dueño"; y por último, para López de Sá (citado por Hernández,

[24] ICONTEC, Óp., Cit., p. 46
[25] ICONTEC, Ibíd., p. 46

1992, p.14) el activo representa “las aplicaciones del capital”[26]. Vemos que lo común entre estas apreciaciones es que relacionan al activo con la propiedad que tiene una entidad sobre los mismos.

- **Análisis del riesgo: “**El análisis del riesgo, también es conocido como evaluación de riesgo o PHA por sus siglas en inglés (Process Hazards Analysis) es el estudio de las causas de las posibles amenazas, y los daños y consecuencias que éstas puedan producir”[27]

- **Confidencialidad: “**La confidencialidad se entiende como la propiedad de la información mediante la cual se garantizará el acceso a la misma solo por parte de las personas que estén autorizadas.

  Es de alguna manera lo que se dice o hace en confianza y con seguridad recíproca entre dos o más individuos”.[28]

- **Disponibilidad: “**El concepto de disponibilidad se utiliza en diversos ámbitos y esferas para hacer referencia a la posibilidad de que algo, un producto o un fenómeno, en este caso la información esté disponible de ser realizado, encontrado o utilizado”[29]. La disponibilidad significa que esa información está disponible para ser usada. Que esté disponible quiere decir a su vez que uno puede disponer de ella ya que es asequible, está al alcance de la mano o simplemente porque es posible hacerlo.

- **Evaluación del riesgo: “**Es el proceso de estimar la probabilidad de que ocurra un evento no deseado con una determinada severidad o consecuencias en la seguridad de los sistemas de información. A partir de este, se deberá elaborar un Plan de Emergencia y Contingencia que permita prevenir y mitigar riesgos, atender los eventos con la suficiente

[26] MARCOTRIGIANO, Laura. Discusión del concepto de “activo” dentro del Marco Conceptual de las Normas Internacionales de Información Financiera. Disponible en: http://www.saber.ula.ve/bitstream/123456789/34234/3/articulo5.pdf. Citado (09/05/2015)

[27] HERNANDEZ, Adriana. Análisis de Riesgo. [en línea]. [consultado el 09 de mayo de 2015]. Disponible en http://adrianajhdez.blogspot.com/2013/05/analisis-e-l-analisis-del-riesgo-es-un.html.

[28] CALAMEO. Manual de procesos y procedimientos. [en línea]. [consultado el 09 de mayo de 2015]. Disponible en: http://es.calameo.com/books/0009207604661982da885.

[29] BLAZQUEZ, Florentino. Sociedad de la información y la educación. [en línea]. [consultado el 09 de mayo de 2015]. Disponible en http://es.calameo.com/books/0009207604661982da885.

eficacia, minimizando los daños y recuperarse en el menor tiempo posible"[30].

- **Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de negocio y amenazar la seguridad de la información. [ISO/IEC TR 18044:2004]

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad. [NTC-ISO/IEC 17799:2006]

- **Sistema de gestión de seguridad de la información SGSI: "**Parte del sistema de gestión global basada en un enfoque hacia los riesgos globales de un negocio cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información"[31]

- **Amenazas o ataques (Threats): "**Posible peligro del sistema. Pueden provenir de personas (hackers, crackers), de programas, de sucesos naturales. Equivalen a los factores que se aprovechan de las debilidades del sistema"[32].

### 2.5.3.2 Tipos de Controles

- **"Controles Preventivos.** Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.

[30] SIRE. METODOLOGÍAS DE ANÁLISIS DE RIESGO. [en línea]. [consultado el 09 de mayo de 2015]. Disponible en http://www.sire.gov.co/documents/13276/69801/A.3.4+Metodologias+AR.pdf/288b65be-c4d8-4d3f-a5f6-51942324e699

[31] UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS. Subsistema de Seguridad de la Información (SGSI). [en línea]. [consultado el 09 de mayo de 2015]. Disponible en http://comunidad.udistrital.edu.co/sigud/subsistema-de-seguridad-de-la-informacion-sgsi/

[32] ROMERO, Luis Alfonso. Seguridad Informática Conceptos Generales. [en línea]. [consultado el 09 de mayo de 2015]. Disponible en http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf.

Ejemplos: Letrero "No Fumar" para salvaguardar las instalaciones Sistemas de claves de acceso.

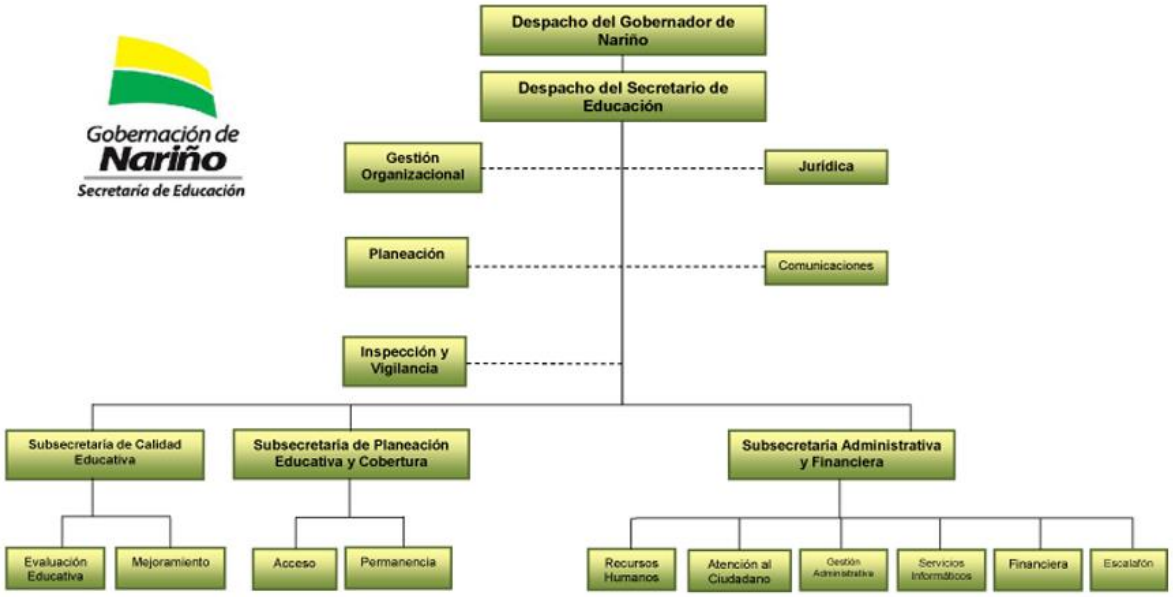
- **Controles Detectivos.** Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos. Ejemplo: Archivos y procesos que sirvan como pistas de auditoría, procedimientos de validación.

- **Controles Correctivos.** Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores".[33]

[33] GERENCIE.COM Auditoría de Sistemas. [en línea]. [consultado el 06 de mayo de 2015]. Disponible en http://www.gerencie.com/tipos-de-riesgos-de-auditoria.html.

### 2.5.4 Marco Contextual

**Figura 2. Organigrama de la Secretaria de Educación Departamental[34]**




Fuente: Ministerio de Educación Nacional. Proyecto de Modernización de Secretarías de Educación: Estructura. Disponible en www.modernizacionsecretarias.gov.co

### 2.5.5 Marco Legal

- **Ley 527 de 1999 - COMERCIO ELECTRÓNICO.** "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"[35].

- **Ley 962 de 2005.** "Con esta Ley invita a los organismos, que ejercen funciones públicas a utilizar medios tecnológicos integrados con el apoyo

[34] MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA. Proyecto de Modernización de Secretarías de Educación: Estructura. [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.modernizacionsecretarias.gov.co.

[35] ALCALDÍA DE BOGOTA. LEY 527 DE 1999. [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276.

del ministerio de comunicaciones, para disminuir tiempos y costos en la realización de gestiones administrativas, aplicando los principios de igualdad, economía, celeridad, imparcialidad, publicidad, moralidad y eficacia en la función administrativa y deberá garantizar los principios de autenticidad, disponibilidad e integridad. Para el efecto, podrán implementar las condiciones y requisitos de seguridad informática que para cada caso sea procedentes, sin perjuicio de las competencias que esta materia tengan algunas entidades especializadas. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos".[36]

- **Ley 1273 de 2009.** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones, como penas de prisión de 120 meses y multa de hasta 1500 salarios mínimos legales mensuales vigentes. La ley castiga los atentados contra la confidencialidad, la integridad y la confidencialidad de los datos y de los sistemas informáticos, entre otras infracciones como hurto por medios informáticos y semejantes, transferencia no consentida de activos y circunstancias de mayor unidad".[37]

- **Ley 1581 de 2012 y del Decreto 1377 de 2013.** "Por la cual se dictan disposiciones generales para la protección de datos personales. La información es el activo más importante en el mundo actual, es por ello que el 17 de octubre de 2012 el Gobierno Nacional expidió la Ley Estatutaria 1581 de 2012 mediante la cual se dictan disposiciones generales para la protección de datos personales, en ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo tal como lo corrobora la Sentencia de la Corte Constitucional C–748 de 2011 donde se estableció el control de constitucionalidad de la Ley en mención. La nueva ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión, en adelante tratamiento por parte de entidades de naturaleza pública y privada. Como Ley Estatutaria

[36] SENADO DE LA REPÚBLICA. LEY 962 DE 2005. . [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_0962_2005.html.
[37] ALCALDÍA DE BOGOTA. LEY 1213 DE 2009. . [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

(ley de especial jerarquía), tiene como fin esencial salvaguardar los derechos y deberes fundamentales, así como los procedimientos y recursos para su protección".[38]

- **Decreto 1151 de 2008.** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005 y se dictan otras disposiciones.

- **Ley 115 del 8 de febrero de 1994.** Ley general de educación.[39]

- **Ley 715 del 21 de diciembre de 2001.** Por la cual se dictan normas orgánicas en materia de recursos y competencias de conformidad con los artículos 151, 288, 356 y 357 (Acto Legislativo 01 de 2001) de la Constitución Política y se dictan otras disposiciones para organizar la prestación de los servicios de educación y salud, entre otros.[40]

- **Decreto 1151 del 14 de Abril de 2008.** Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la ley 962 de 2005 y se dictan otras disposiciones[41].

- **Norma ISO-IEC/27001.** Define como organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información[42].

[38] ALCALDÍA DE BOGOTA. LEY 1581 DE 2012. . [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.
[39] MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA. Ley 115 del 8 de febrero de 1994. [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.mineducacion.gov.co.
[40] ALCALDÍA DE BOGOTÁ D.C. Ley 715 del 21 de diciembre de 2001. . [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.alcaldiabogota.gov.co.
[41] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1151 del 14 de Abril de 2008. [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://programa.gobiernoenlinea.gov.co/
[42] ACADEMY. ¿Qué es norma ISO 27001? [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.iso27001standard.com/es/que-es-iso-27001/.

# 3. DISEÑO METODOLÓGICO

## 3.1 RESUMEN

Para el desarrollo de este proyecto, el grupo de trabajo basará su análisis en el enfoque definido por el estándar COBIT (Control Objectives for Information and related Technology) en su versión 4.1, debido a que está ampliamente aceptado por la comunidad internacional, y en los controles de la norma ISO/IEC 27001.

## 3.2 CONCEPTOS CLAVE

Estándar, ISO/IEC 27001, ISO/IEC 27001, Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento, Confiabilidad, Datos, Aplicaciones, Tecnología, Instalaciones, Personal.

## 3.3 DESCRIPCIÓN GENERAL DE ACTIVIDADES

El desarrollo de este proyecto se regirá según el orden de actividades, tareas y tiempo descrito en la siguiente tabla:

**Tabla 4. Descripción general de actividades del presente proyecto**

| ACTIVIDADES | TIEMPO |
|---|---|
| 1. Recolección de Información | **12 Semanas** |
| **a)** Búsqueda de Información | 4 Semanas |
| **b)** Clasificación de la Información | 3 Semanas |
| **c)** Estudio y Análisis del estándar ISO 27000 | 2 Semanas |
| **d)** Determinar Características Mínimas Rumbo a la Certificación | 3 Semanas |
| 2. Visita Preliminar al Área de Sistemas | **3 Semanas** |
| **e)** Delimitar el problema buscando las áreas y los procesos de información que serán objeto de estudio, realizar su comparación con los controles de la norma ISO/IEC 27001 para verificar su existencia por medio de listas de chequeo | 3 Semanas |
| 3. ISO/IEC 27002 | **9 Semanas** |
| **f)** Política de seguridad de la información<br>Aspectos organizativos de la seguridad de la información | 2 Semanas |
| **g)** Gestión de activos<br>Seguridad ligada a los recursos humanos | 2 Semanas |

| | |
|---|---|
| Seguridad física y del entorno | |
| **h)** Gestión de comunicaciones y operaciones<br>Control de acceso<br>**i)** Adquisición, desarrollo y mantenimiento de sistemas de información | 2 Semanas |
| j) Gestión de incidentes en la seguridad de la información<br>Gestión de la continuidad del negocio<br>Cumplimiento | 3 Semanas |
| 4. Documento Final | **5 Semanas** |
| **k)** Elaboración del documento Final | 4 Semanas |
| **l)** Presentación del documento a directivos | 1 Semana |

Fuente: la presente investigación – Año 2015

### 3.3.1 Fase 1: recolección de información.

- Búsqueda de documentación de riesgo informático, ISO 27000 y las leyes del gobierno Colombiano que hablen de certificación de procesos.
- Clasificación de información recolectada en grupos de importancia o relevancia para el proyecto.
- Determinar las características mínimas de calidad de un proceso informático, para facilitar la decisión de certificarse ante ISO.

### 3.3.2 Fase 2: vista preliminar del área de sistemas.

- Delimitar el problema buscando las áreas y los procesos de información que serán objeto de estudio, realizar su comparación con los controles de la norma ISO/IEC 27001 para verificar su existencia por medio de listas de chequeo.

### 3.3.3 Fase 3: ISO/IEC 27002.

- Política de seguridad de la información.
- Aspectos organizativos de la seguridad de la información.
- Gestión de activos.
- Seguridad ligada a los recursos humanos.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.

- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de incidentes en la seguridad de la información.
- Gestión de la continuidad del negocio.
- Cumplimiento.

### 3.3.4 Fase 4: Documentación Final.

- Elaborar el documento que describa desde el análisis realizado y los resultados obtenidos del estado actual hasta los procesos descritos por ISO/IEC 27002 para establecer el SGSI en la Secretaría de Educación de Nariño.

## 3.4 RECURSOS

Con el fin de ejecutar la propuesta del proyecto presente, se hacen necesarios los recursos nombrados a continuación:

### 3.4.1 Recursos Humanos

**Tabla 5. Descripción de recursos humanos**

| NOMBRE | CARGO |
|---|---|
| Mónica Lucia Meneses | Coordinadora Área de Sistemas SED |
| Fredy Díaz | Ingeniero de Soporte Área de Sistemas SED |
| Andrés Zambrano | Ingeniero de Soporte Área de Sistemas SED y ejecutor del proyecto |
| Omar Muñoz | Ingeniero de Soporte Área de Sistemas SED |
| Andrés Aguirre Tobar | Ejecutor del Proyecto |
| Henry Rodríguez | Asesor del Proyecto |

Fuente: Secretaría de Educación Departamental de Nariño – Año 2015

Además de los anteriormente nombrados y directos responsables en la ejecución del proyecto se requiere el compromiso del Comité Directivo de la SED con quien se socializará el proyecto al inicio y al final con el producto que resulte del estudio.

### 3.4.2 Recursos físicos y tecnológicos

Para apoyar las actividades del proyecto se requiere de los siguientes elementos físicos:

**Tabla 6. Descripción de recursos físicos y tecnológicos**

| TIPO | INVENTARIO DE RECURSOS | DESCRIPCIÓN |
|---|---|---|
| Infraestructura | • Oficinas de la SED | El lugar donde se desarrollará el proyecto en primera instancia son las oficinas de la Secretaría de Educación Departamental de Nariño de donde se obtiene la información necesaria y donde se ubican parte del recurso humano. |
| Hardware | • 2 Equipos portátiles de gama media<br>• 1 equipo de sobremesa de gama media<br>• Modem – Router<br>• Impresoras | Equipos de cómputo de escritorio y portátiles personales de los ejecutores del proyecto con prestaciones básicas y capacidad de navegación. |
| Software | • Software de ofimática OpenOffice, Office 2013<br>• Navegadores Google Chrome, Mozilla Firefox, Internet Explorer<br>• GanttProject | Programas básicos de ofimática como procesadores de texto y hoja de cálculo, navegadores y programas de gestión de proyectos y calendarización. |
| Documentación | • Sitios web nombrados en bibliografía<br>• Material en formato PDF<br>• Libro: COMPENDIO, Sistema de Gestión de la seguridad de la información.<br>• Libro: Las nueve claves del éxito explicación de la 27001<br>• Manuales de funciones y procesos de la | Nombrada en la bibliografía, en su mayoría puede conseguirse en formato digital. |

| | | |
|---|---|---|
| | SED | |
| Servicios | • Internet 1Mb/s como mínimo. | Internet para la comunicación, consulta y trabajo síncrono y asíncrono durante la ejecución del proyecto. |

Fuente: la presente investigación – Año 2015

# 4. PRESENTACION DE RESULTADOS

## 4.1 RECOLECCIÓN, CLASIFICACIÓN Y ANÁLISIS DE LAS NORMAS ISO/IEC 27001 Y 27002

Mediante la aplicación de la técnica de recolección de información denominada revisión documental se recurrió al análisis de las siguientes normas:

NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001 - TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS

NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27002 - TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Como producto de dicho análisis a continuación se presenta un resumen de los contenidos de las citadas normas y sus ventajas y desventajas en términos de implementación:

**Tabla 7. ISO/IEC 27001**

| **ASPECTOS DE LA NORMA** | **NTC-ISO/IEC 27001** |
|---|---|
| **OBJETO** | Esta norma específica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización. |
| **CAP 4. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | La organización debe establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado, en el contexto de las actividades globales del negocio de la organización y de los riesgos que enfrenta. |

| | |
|---|---|
| **CAP 5. RESPONSABILIDAD DE LA DIRECCIÓN** | La dirección debe brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI: |
| | a) mediante el establecimiento de una política del SGSI; |
| | b) asegurando que se establezcan los objetivos y planes del SGSI; |
| | c) estableciendo funciones y responsabilidades de seguridad de la información; |
| | d) comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información y de la conformidad con la política de seguridad de la información, sus responsabilidades bajo la ley, y la necesidad de la mejora continua; |
| | e) brindando los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI; |
| | f) decidiendo los criterios para aceptación de riesgos, y los niveles de riesgo aceptables; |
| | g) asegurando que se realizan auditorías internas del SGSI; |
| | h) efectuando las revisiones por la dirección del SGSI. |
| **CAP 6. AUDITORIAS INTERNAS DEL SGSI** | La organización debe llevar a cabo auditorías internas del SGSI a intervalos planificados, para determinar si los objetivos de control, controles, procesos y procedimientos de su SGSI: |
| | a) cumplen los requisitos de la presente norma y de la legislación o |
| | reglamentaciones pertinentes; |
| | b) cumplen los requisitos identificados de seguridad de la información; |

| | |
|---|---|
| | c) están implementados y se mantienen eficazmente, y |
| | d) tienen un desempeño acorde con lo esperado. |
| | Se debe planificar un programa de auditorías tomando en cuenta el estado e importancia de los procesos y las áreas que se van a auditar, así como los resultados de las auditorías previas. |
| | Se deben definir en un procedimiento documentado las responsabilidades y requisitos para la planificación y realización de las auditorías, para informar los resultados, y para mantener los registros. |
| **CAP 7. REVISIÓN DEL SGSI POR LA DIRECCIÓN** | La dirección debe revisar el SGSI de la organización a intervalos planificados (por lo menos una vez al año), para asegurar su conveniencia, suficiencia y eficacia continuas. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del SGSI, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar claramente y se deben llevar registros. |
| **CAP 8. MEJORA DEL SGSI** | La organización debe mejorar continuamente la eficacia del SGSI mediante el uso de la política de seguridad de la información, los objetivos de seguridad de la información, los resultados de la auditoría, el análisis de los eventos a los que se les ha hecho seguimiento, las acciones correctivas y preventivas y la revisión por la dirección. |

Fuente: Adaptación de la edición hecha por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) – Año 2015

**Tabla 8. ISO/IEC 27002**

| ASPECTOS DE LA NORMA | NTC-ISO/IEC 27002 |
|---|---|
| **OBJETO** | Esta norma puede servir como guía práctica para el desarrollo de normas de seguridad de la organización y para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones. |
| **CAP. 5 POLÍTICAS DE SEGURIDAD** | El contenido de las políticas se basa en el contexto en el que opera una organización y suelen ser considerados en su redacción los fines y objetivos de la organización, las estrategias adoptadas para alcanzar sus objetivos, la estructura y los procesos adoptados por la organización, los objetivos generales y específicos relacionados con el tema de la política y requisitos de las políticas procedentes de niveles más superiores relacionadas. Una estructura típica de las documentos de políticas podría ser: |
| | Resumen: Política Resumen - Visión general de una extensión breve; una o dos frases y que pueden aparecer fusionadas con la introducción. |
| | Introducción: Breve explicación del asunto principal de la política. |
| | Ámbito de aplicación: Descripción de los departamentos, áreas o actividades de una organización a las que afecta/aplica la política. Cuando es relevante en este apartado se mencionan otras políticas relevantes a las que se pretende dar cobertura desde ésta. |
| | Objetivos: Descripción de la intención de la política. |
| | Principios: Descripción de las reglas que conciernen a acciones o decisiones para |

| | |
|---|---|
| | alcanzar los objetivos. En algunos casos puede ser de utilidad identificar previamente los procesos clave asociados con el asunto principal de la política para pasar posteriormente a identificar las reglas de operación de los procesos. |
| | Responsabilidades: Descripción de quién es responsable de qué acciones para cumplir con los requisitos de la política. En algunos casos, esto puede incluir una descripción de los mecanismos organizativos, así como las responsabilidades de las personas con roles designados. |
| | Resultados clave: Descripción de los resultados relevantes para las actividades de la organización que se obtienen cuando se cumplen los objetivos. |
| | Políticas relacionadas: Descripción de otras políticas relevantes para el cumplimiento de los objetivos, usualmente se indican detalles adicionales en relación a temas específicos. |
| | La política de alto nivel (más genérica) habitualmente relacionada con el sistema de gestión para la seguridad de la información (SGSI) suele estar apoyada por políticas de bajo nivel, específicas a aspectos concretos en temáticas como el control de accesos, la clasificación de la información, la seguridad física y ambiental, uso aceptable de activos, escritorio y pantallas libres de información sensible, dispositivos móviles y teletrabajo, backups, protección contra el malware |
| **CAP. 6 ASPECTOS ORGANIZATIVOS SI** | Su objetivo es establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la |

| | |
|---|---|
| | organización. |
| | Para ello se debe definir formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de las políticas de seguridad, la coordinación de la implementación de la seguridad y la asignación de funciones y responsabilidades. |
| | Para una actualización adecuada en materia de seguridad se debe contemplar la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información. |
| **CAP. 7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS** | Su objetivo parte de la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. |
| | Es necesario reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento. |
| | Se requiere explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado, así como, garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la |

| | |
|---|---|
| | organización en el transcurso de sus tareas normales. |
| | El Responsable del Área Jurídica participa en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de las Políticas en seguridad y en el tratamiento de incidentes de seguridad que requieran de su intervención. |
| **CAP. 8 GESTIÓN ACTIVOS** | El objetivo de este capítulo es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos. |
| | Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información. |
| **CAP. 9 CONTROL DE ACCESOS** | El objetivo del capítulo es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática. |
| | Para impedir el acceso no autorizado a los sistemas de información se debe implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento. |
| | Los procedimientos comprenden todas las etapas del ciclo de vida de los |

| | |
|---|---|
| | accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso. |
| **CAP. 10 CIFRADO** | El objetivo de este capítulo es el uso de sistemas y técnicas criptográficas para la protección de la información con base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad. |
| | La aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas. |
| **CAP. 11 SEGURIDAD FÍSICA Y AMBIENTAL** | El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización. |
| | El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados. |
| | El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. |
| **CAP 12. SEGURIDAD OPERATIVA** | El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada. |
| | Adicionalmente, se debe evaluar el posible impacto operativo de los |

| | |
|---|---|
| | cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento. |
| | Con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario, es necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad. |
| | El control de la realización de las copias de resguardo de información, así como la prueba periódica de su restauración permite garantizar la restauración de las operaciones en los tiempos de recuperación establecidos y acotar el periodo máximo de pérdida de información asumible para cada organización. |
| | Se deben definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización. |
| | Finalmente, se deben verificar el cumplimiento de las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas (logs) como base para la monitorización del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos. |
| **CAP 13. SEGURIDAD EN LAS TELECOMUNICACIONES** | El objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte. |

| | |
|---|---|
| | La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección. |
| | La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección. |
| | Los intercambios de información por parte de las organizaciones se deberían basar en una política formal de intercambio y en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante. |
| **CAP 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN** | El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información. |
| | Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan. |
| | Definir los métodos de protección de la información crítica o sensible. |
| | Aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los ambientes administrados por la organización en donde residan los desarrollos mencionados. |
| **CAP 15. RELACIONES CON PROVEEDORES** | El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros. |
| | La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para |

| | |
|---|---|
| | asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas. |
| **CAP 16. GESTIÓN DE INCIDENTES** | El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno. |
| | Las organizaciones cuentan con innumerables activos de información, cada uno expuesto a sufrir incidentes de seguridad. Resulta necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares. |
| **CAP 17. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO** | El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad. |
| | Se debe integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativos y/o que estén dispuestos de un modo distinto a la operativa habitual. |
| | Se debe analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la |

| | |
|---|---|
| | información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos. |
| | Deben llevarse a cabo las pruebas pertinentes (tales como pruebas sobre el papel, simulacros, pruebas de failover, etc.) para (a) mantener los planes actualizados, (b) aumentar la confianza de la dirección en los planes y (c) familiarizar a los empleados relevantes con sus funciones y responsabilidades bajo condiciones de desastre. |
| | Minimizar los efectos de las posibles interrupciones de las actividades normales de la organización asociadas a desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos, protegiendo los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación. |
| | Instruir al personal involucrado en los procedimientos de reanudación y recuperación en relación a los objetivos del plan, los mecanismos de coordinación y comunicación entre equipos (personal involucrado), los procedimientos de divulgación en uso, los requisitos de la seguridad, los procesos específicos para el personal involucrado y responsabilidades individuales. |
| **CAP 18. CUMPLIMIENTO** | El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos. |

| | |
|---|---|
| | Se debe revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información. |

Fuente: Adaptación de la edición hecha por el portal Iso27000.es. Disponible en http://iso27000.es/iso27002.html

**Tabla 9. Ventajas y Desventajas ISO/IEC 27001, ISO/IEC 27002**

| NORMA | VENTAJAS | DESVENTAJAS |
|---|---|---|
| **ISO/IEC 27001** | Facilita la integración de los sistemas de gestión, debido a que es una estructura de alto nivel, donde los términos y definiciones ayudan a implementar | Es una abstracción y es un nivel alto, no es tan detallado |
| | Todas las definiciones vienen del estándar ISO 27000 y las inconsistencias se han removido. | Los requisitos son un tanto más difícil para interpretar, debido a los nuevos conceptos. |
| | Los riesgos en la seguridad de la información en su conjunto deben ser abordados. | No se menciona el enfoque PDCA. |
| | Los documentos requeridos están claramente establecidos, hace referencia al tamaño y complejidad. | No se menciona las políticas del SGSI. |
| | Menciona que las acciones preventivas no van. | No hay una descripción detallada de la identificación del riesgo. |
| **ISO/IEC 27002** | Aumento de la seguridad efectiva de los sistemas de información | El proyecto de implantación de la norma puede tener una extensa duración dependiendo del grado de madurez en seguridad de la información de la empresa |

| | | |
|---|---|---|
| | Correcta planificación y gestión de la seguridad | Por lo general, el proyecto de implantación de la norma requiere consultores externos lo que eleva el costo |
| | Garantías de continuidad del negocio | Se requiere conformar equipos interdisciplinares que no hablan un mismo idioma en términos del SGSI |
| | Mejora continua a través del proceso de auditoría interna | |
| | Incremento en los niveles de confianza en la cadena de valor | |

Fuente: la presente investigación – Año 2015

## 4.2 MACROPROCESO GESTIÓN FINANCIERA

Con base en los lineamientos contenidos en el manual de procesos y procedimientos de la Secretaría de Educación Departamental de Nariño se pudo identificar que el proceso de **Tesorería** corresponde a un proceso contenido en el macroproceso ***J. Gestión Financiera*****,** y dentro del cual se identifica con la denominación J02 Tesorería.

**Tabla 10. Procesos del macroproceso J. Gestión Financiera**

| PROCESO | SUBPROCESO |
|---|---|
| J01. Presupuesto | J01.01. Elaborar presupuesto |
| | J01.02. Ejecutar presupuesto |
| | J01.03. Realizar seguimiento al presupuesto |
| | J01.04. Elaborar y realizar seguimiento al plan anualizado y mensualizado de caja PAC |
| J02. Tesorería | J02.01 Elaborar flujo de caja |
| | J02.02. Efectuar pagos |
| | J02.03. Realizar conciliaciones |
| | J02.04. Administrar inversiones |
| J03. Contabilidad | J03.01. Realizar procesos contables |

| | |
|---|---|
| | J03.02. Efectuar cierre contable |
| | J03.03. Generar informes y estados financieros |
| | J03.04. Verificar y consolidar información de las instituciones educativas (Fondos de Servicios Educativos) |

Fuente: Manual de Procesos y Procedimientos SED – Año 2015

Como puede observarse el macroproceso de Gestión Financiera contiene a los procesos de J01 Presupuesto, J02 Tesorería y J03 Contabilidad. Específicamente dentro del proceso de Tesorería se manejan a su vez 4 subprocesos relacionados con la elaboración de flujo de caja, la realización de pagos, la realización de conciliaciones y la administración de inversiones.

### 4.2.1 Flujograma SIPCO del proceso Tesorería

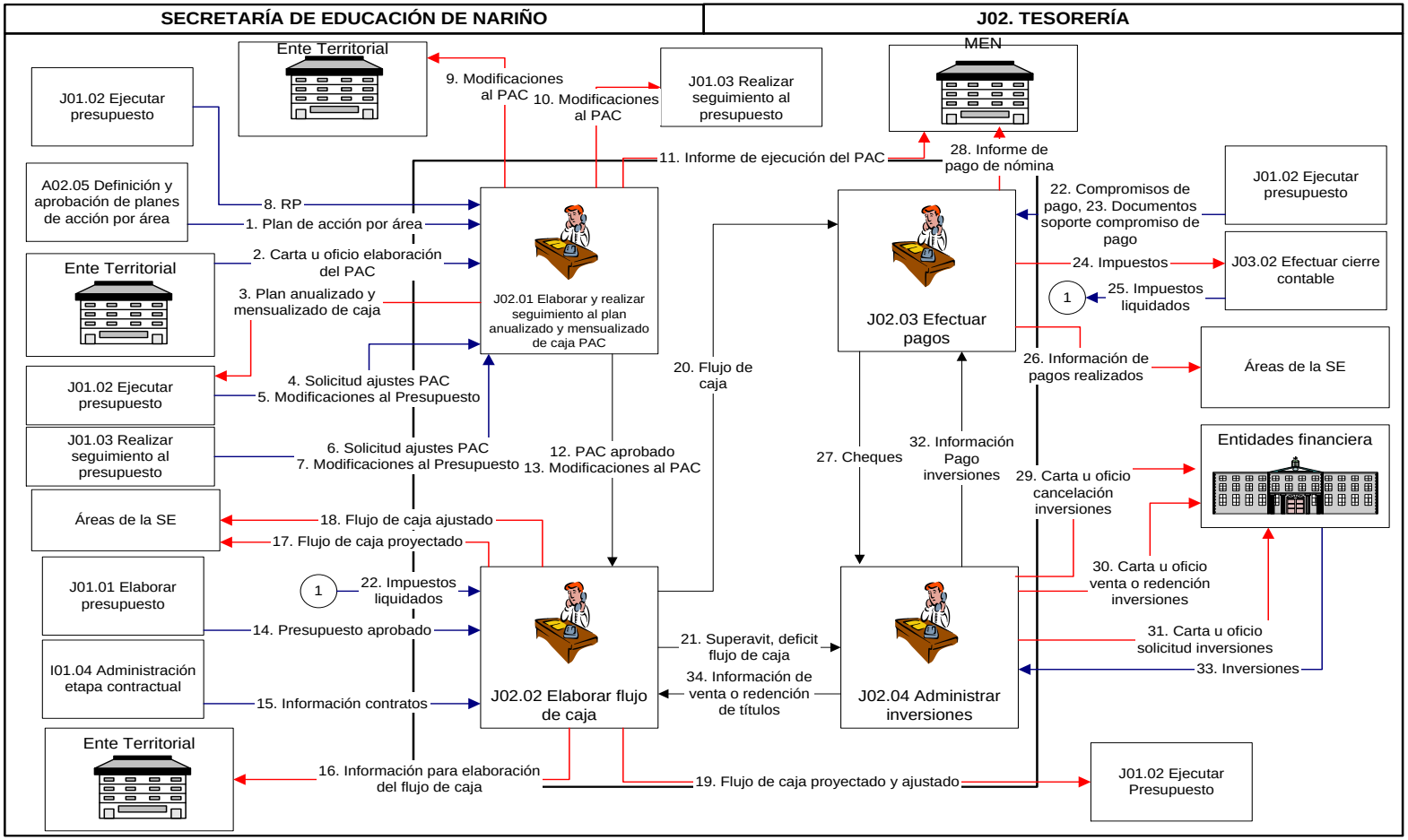
Para una mayor entendimiento tanto de los procesos, subprocesos como actividades que se realizan en el área de tesorería de la Secretaría de Educación Departamental de Nariño a continuación se presente en forma gráfica y descriptiva la composición de dicho proceso.

Para un mayor entendimiento de la sigla SIPCO, a continuación la desagregamos:

**S**: Supliré, Proveedores del proceso.
**I**: Input, Entradas al proceso.
**P**: Process, Proceso.
**C**: Customer, Cliente del proceso.
**O**: Output, Salidas del proceso.

- **Diagrama “SIPCO” del proceso**

**Figura 3. Diagrama SIPCO del Macroproceso de Gestión Financiera y del Proceso de Tesorería**




Fuente: Manual de Procesos y Procedimientos SED – Año 2015

- **Caracterización del proceso de Tesorería**

Como complemento al diagrama anterior, a continuación se detallan los subprocesos que conforman el proceso de tesorería y a través de los cuales se ejecutan las actividades con las que se da cumplimiento a la normatividad, determinando el origen (proveedores e insumos que alimentan el proceso) y el destino (clientes y productos del proceso) de la información.

De igual manera se determina quién debe asegurar, "líder y/o responsable del proceso", que lo descrito en la caracterización corresponda con la realidad. Por otra parte, se establecen los indicadores que permitirán hacer seguimiento a la evolución del proceso a fin de identificar mejoras.

**Tabla 11. Caracterización del proceso de Tesorería**

| **OBJETIVO** |
|---|
| Optimizar el manejo de los ingresos para la vigencia fiscal de la SE proporcionando la liquidez necesaria en todo momento, con el fin de garantizar el pago de los compromisos de manera transparente y oportuna para lograr un manejo eficiente de los recursos de acuerdo con la normatividad vigente proporcionando un soporte de apoyo a todas las áreas. |
| **ALCANCE** |
| El proceso de tesorería inicia con la elaboración del flujo de caja, contiene el pago de los compromisos; la constitución, administración y cancelación de títulos valores e inversiones, su resguardo y custodia y finaliza con el registro de las operaciones en el sistema de información. |
| **NORMATIVIDAD Y POLÍTICAS** |
| **NORMATIVIDAD.**<br><br>• Ley 38 de abril 21 de 1989. Normativo del Presupuesto General de la Nación.<br>• Ley 100 de 23 de diciembre de 1993. Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones.<br>• Ley 80 de 28 de octubre de 1993. Por la cual se expide el Estatuto General de Contratación de la Administración Pública.<br>• Ley 152 de 15 julio de 1994. Ley Orgánica del Plan de Desarrollo. Donde se define la planeación como un proceso constituido por la formulación, la ejecución, |

el seguimiento y la evaluación de los planes.

- Decreto 630 de 2 de abril 1996. Por el cual se establecen los lineamientos del Programa Anual Mensualizado de Caja PAC.

- Ley 734 de 5 de febrero del 2002. Por la cual se expide el Código Disciplinario Único. Art. 35. Prohibiciones, a todo servidor público le está prohibido: 16. Asumir obligaciones o compromisos de pago que superen la cuantía de los montos aprobados en el Programa Anual Mensualizado de Caja (PAC). Art. 48. faltas gravísimas. Son faltas gravísimas las siguientes: 23. Ordenar o efectuar el pago de obligaciones en excesos del saldo disponible en el Programa Anual Mensualizado de Caja (PAC).

- Ley 789 del 27 de diciembre del 2002. Por la cual se dictan normas para apoyar el empleo y ampliar la protección social y se modifican algunos artículos del Código Sustantivo de Trabajo.

- Ley 819 de 8 de julio del 2003. Normas orgánicas en materia de presupuesto, responsabilidad y transparencia fiscal.

- Ley 863 de 29 de diciembre del 2003. Por la cual se establecen normas tributarias, aduaneras, fiscales y de control para estimular el crecimiento económico y el saneamiento de las finanzas públicas.

- Ley 828 del 10 de julio de 2003. Normas para el control a la evasión del Sistema de Seguridad Social.

- Decreto 1222 de 6 de junio de 1986. Por el cual se expide el Código de Régimen Departamental. Art. 170. Autorizase a las Asambleas para ordenar la emisión de estampillas “Pro desarrollo Departamental”, cuyo producido se destinará a la construcción de infraestructura educativa, sanitaria y deportiva.

- Decreto 111 de 15 de enero de 1996. Por el cual se compilan la Ley 38 de 1989, la Ley 179 de 1994 y la Ley 225 de 1995 que conforman el Estatuto Orgánico del Presupuesto.

- Decreto 2170 de 30 de septiembre del 2002. Reglamentario de la ley 80.

- Decreto 1465 de 10 de mayo del 2005. Por medio del cual se reglamentan los artículos 9 de la Ley 21 de 1982, el parágrafo 1 del artículo 1 de la Ley 89 de 1988, 287 de Ley 100 de 1993, el numeral 4 del artículo 30 de la Ley 119 de 1994, 15 de la Ley 797 de 2003 y 10 de la Ley 828 de 2003.

- .Circular externa 033 de 2 agosto del 2002. Por la cual se definen la práctica de valoración de los portafolios de inversiones. Emitida por la Superintendencia de valores.

- Ordenanza 138 de 1995. Art. 2 Pago estampillas Pro desarrollo. Conceptos: Contratos escritos con personas naturales y jurídicas, pliegos para licitación

pública, adición de contrato escrito (sobre valor de adición), cuentas u órdenes de pago a favor de proveedores, reconocimiento de prestación de servicios que no requiere contrato escrito.

- Ordenanza 218 de 1997 Art. 5 Pago estampillas pro hospital. Conceptos: Todo contrato escrito o adición celebrado con personas naturales o jurídicas.

- Ordenanza 252 de 1998 Art. 4 Pago estampillas Pro universidades. Conceptos: Todo contrato escrito entre departamentos, municipios, entidades descentralizadas, asamblea, concejos, contralorías y personerías con personas naturales o jurídicas. Toda adición de contrato escrito (sobre valor de adición).

- Guía No. 8 Vigente, guía para la administración de los recursos del sector educativo.

- Guías emanadas por el MEN para la vigencia en curso.

- Plan General de Contabilidad Publica vigente.

**POLÍTICAS.**

- La definición, medición y seguimiento de los indicadores asociados a los procesos de la cadena de valor, como herramienta de apoyo para el mejoramiento continuo y al logro de los objetivos definidos dentro de la Secretaría, debe ser desarrollado por los responsables de cada proceso. La definición de los responsables se encuentra en la hoja de vida de cada indicador.

- El formato hoja de vida es el instrumento que se debe utilizar para la definición y seguimiento de los indicadores asociados a los procesos, en ésta se especifica la información, periodicidad y la formula requerida para la medición de los mismos, así como los rangos de evaluación necesarios para establecer el porcentaje de logro de las mediciones realizadas y las acciones requeridas sobre los resultados obtenidos. Existe una hoja de vida por proceso con todos los indicadores relacionados con el mismo, incluyendo los indicadores del Tablero de Indicadores. Las actividades detalladas para la definición, medición y seguimiento de indicadores se encuentran descritas en el numeral 8 del manual de calidad.

- Toda correspondencia, peticiones, quejas, reclamos, sugerencias, tutelas y trámites, verbales y escritos, que ingresen a la Secretaría de Educación se reciben y radican en el área encargada de Atención al Ciudadano y Correspondencia, por medio de los subprocesos del proceso E01. Gestionar solicitudes y correspondencia. Así mismo, las respuestas a las solicitudes y la correspondencia externa que generan las áreas de la Secretaría de Educación. Por otro lado todas las comunicaciones institucionales de la Secretaría se planean, desarrollan, y evalúan a través del proceso G02. Gestionar comunicaciones institucionales.

- Todos los registros que se generen en cada uno de los subprocesos deben ser archivados de acuerdo con lo definido en la tabla de registros del numeral 6 del documento “diseño detallado del subproceso” y teniendo en cuenta los lineamientos del subproceso N0201 Archivo de gestión.
- Cuando se identifiquen problemas reales o potenciales ya sea durante la ejecución de los diferentes subproceso o debido al análisis de los resultados de los indicadores asociados al proceso, el dueño del proceso debe generar acciones correctivas o preventivas, las cuales deben ejecutarse de acuerdo con lo estipulado en los subprocesos N01.02 Acciones correctivas y N01.03 Acciones preventivas.
- Dar cumplimiento ágil y oportuno a todos los pagos y obligaciones que se generen en la Secretaría de Educación, en forma eficaz de acuerdo a las disposiciones legales y términos establecido.
- Mantener continua comunicación con la Entidades Financieras en lo relacionado con el cobro y reintegro de comisiones bancarias, impuestos, contribución económica y rechazos de nómina.
- Garantizar que las erogaciones correspondan a lo definido en la respectiva cuenta de acuerdo con su rubro presupuestal.
- El Ente Territorial no provee políticas para el subproceso J02 Tesorería.

**RESPONSABLE / LÍDER DEL PROCESO**

- Profesional Universitario de Financiera de la SE

**SUBPROCESOS**

J02.01 Elaborar flujo de caja.

J02.02 Efectuar pagos.

J02.03 Realizar Conciliaciones.

J02.04 Administrar inversiones.

**PROVEDORES E INSUMOS (INFORMES /REGISTROS /DOCUMENTOS)**

| Subproceso / dependencia / área origen | Insumos (entradas) |
|---|---|
| Ente Territorial | Carta u oficio elaboración del PAC. |
| Entidades | Inversiones. |

| | |
|---|---|
| Financieras | |
| A02.05 Definición y aprobación de planes de acción por área | Plan de acción por área. |
| J01.02 Ejecutar presupuesto | RP.<br>Solicitud ajustes PAC.<br>Modificaciones al presupuesto.<br>Compromisos de pago.<br>Documentos soporte compromisos de pago. |
| J01.03 Realizar seguimiento al presupuesto | Solicitud ajustes PAC.<br>Modificaciones al presupuesto. |
| J01.01 Elaborar presupuesto | Presupuesto aprobado. |
| I01.04 Administración etapa contractual | Información contratos. |
| J03.02 Efectuar cierre contable | Impuestos liquidados. |
| **CLIENTES Y PRODUCTOS (INFORMES / REGISTROS / DOCUMENTOS)** | |
| Subproceso / dependencia / área destino | Productos (Salidas) |
| Ente territorial | Información para elaboración del flujo de caja.<br>Modificaciones al PAC. |
| MEN | Informe de ejecución del PAC.<br>Informe de pago de nómina. |
| Áreas de la SE | Flujo de caja ajustado.<br>Flujo de caja proyectado.<br>Información de pagos realizados. |

| | |
|---|---|
| J01.02 Ejecutar presupuesto | Plan anualizado y mensualizado de caja.<br>Flujo de caja proyectado y ajustado. |
| Entidades financieras | Carta u oficio cancelación inversiones.<br>Carta u oficio venta o redención inversiones.<br>Carta u oficio solicitud inversiones. |
| J01.03 Realizar seguimiento al presupuesto | Modificaciones al PAC. |
| J03.02 Efectuar cierre contable | Impuestos. |
| **INDICADORES DE GESTIÓN / SEGUIMIENTO** | |
| **CÓDIGO DEL INDICADOR** | **NOMBRE DEL INDICADOR** |
| **J02.001** | **CUMPLIMIENTO AL PAC** |
| **J02.002** | **CUMPLIMIENTO AL FLUJO DE CAJA** |
| **J02.003** | **TIEMPO PROMEDIO DE PAGO** |
| **J02.004** | **PORCENTAJE DE INVERSIÓN** |
| **J02.005** | **TIEMPO DE ENTREGA DE TÍTULOS VALORES EN CUSTODIA** |

Fuente: Manual de Procesos y Procedimientos SED – Año 2015

### 4.3 PLAN DE AUDITORÍA

Para efectos de la realización del plan de auditoría en cuanto a la seguridad informática del proceso de tesorería en la SED, se ha dispuesto el seguimiento formato de lista de chequeo el cual verifica uno a uno los aspectos auditables Basados en ISO/IEC 27002, así:

## Tabla 12. Lista de chequeo del Plan de Auditoría

| Capítulo de la norma ISO/IEC 27002:2005 | Numeral de la norma ISO/IEC 27002:2005 | Actividades a Auditar | Verificación | Calificación de Verificación | | | Recursos | Aplicación o revisión (Tiempo) |
|---|---|---|---|---|---|---|---|---|
| | | | | Aplica | No Aplica | En proceso | | |
| 5. POLÍTICAS DE SEGURIDAD | 5.1 Directrices de la Dirección en seguridad de la información | 5.1.1 Políticas para la seguridad de la información | La entidad cuenta con conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes | | | | | |
| | | 5.1.2 Revisión de las políticas para la seguridad de la información | Las políticas para la seguridad de la información se planifican y revisan con regularidad; si ocurren cambios significativos se adecuan para garantizar su idoneidad y efectividad. | | | | | |
| 6. ASPECTOS ORGANIZATIVOS SI | 6.1 Organización interna | 6.1.1 Asignación de responsabilidades para la SI | Se definen y asignan claramente todas las responsabilidades para la seguridad de la información. | | | | | |
| | | 6.1.2 Segregación de tareas | Se segregan tareas y áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización. | | | | | |
| | | 6.1.3 Contacto con las autoridades | Se mantienen los contactos apropiados con las autoridades pertinentes. | | | | | |
| | | 6.1.4 Contacto con grupos de interés especial | Se mantiene el contacto con grupos o foros de seguridad especializados y asociaciones profesionales. | | | | | |
| | | 6.1.5 Seguridad de la información en la gestión de proyectos | Se contempla la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización. | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 6.2 Dispositivos para movilidad y teletrabajo | 6.2.1 Política de uso de dispositivos para movilidad | Se establece una política formal y se adopta las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones. | | | | | |
| | | 6.2.2 Teletrabajo | Se desarrolla e implanta una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo. | | | | | |
| 7. Seguridad Ligada a los recursos humanos | 7.1 Antes de la contratación | 7.1.1 Investigación de antecedentes | Se realizan revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. | | | | | |
| | | 7.1.2 Términos y condiciones de contratación | Como parte de su obligación contractual, empleados, contratistas y terceros, se aceptan y firman los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información. | | | | | |
| | 7.2 Durante la contratación | 7.2.1 Responsabilidades de gestión | La Dirección requiere a empleados, contratistas y usuarios de terceras partes para aplicar la seguridad en concordancia con las políticas y los procedimientos. | | | | | |
| | | 7.2.2 Concienciación, educación y capacitación en SI | Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros reciben entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | procedimientos organizacionales como sean relevantes para la función de su trabajo. | | | | | |
| | | 7.2.3 Proceso disciplinario | Existe un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad. | | | | | |
| | 7.3 Cese o cambio de puesto de trabajo | 7.3.1 Cese o cambio de puesto de trabajo | Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste están claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente. | | | | | |
| 8. Gestión Activos | 8.1 Responsabilidad sobre los activos | 8.1.1 Inventario de activos | Todos los activos están claramente identificados, confeccionando y manteniendo un inventario con los más importantes. | | | | | |
| | | 8.1.2 Propiedad de los activos | Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información pertenecen a una parte designada de la Organización. | | | | | |
| | | 8.1.3 Uso aceptable de los activos | Se identifican, documentan e implantan regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información. | | | | | |
| | | 8.1.4 Devolución de activos | Todos los empleados y usuarios de terceras partes devuelven todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo. | | | | | |
| | 8.2 Clasificación de la información | 8.2.1 Directrices de clasificación | La información se clasifica en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización. | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 8.2.2 Etiquetado y manipulado de la información | Se desarrolla e implanta un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización. | | | | | |
| | | 8.2.3 Manipulación de activos | Se desarrolla e implanta procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización. | | | | | |
| | 8.3 Manejo de los soportes de almacenamiento | 8.3.1 Gestión de soportes extraíbles | Se establecen procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización. | | | | | |
| | | 8.3.2 Eliminación de soportes | Se eliminan los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales. | | | | | |
| | | 8.3.3 Soportes físicos en tránsito | Se protegen los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización. | | | | | |
| 9. Control de Accesos | 9.1 Requisitos de negocio para el control de accesos | 9.1.1 Política de control de accesos | Se establece, documenta y revisa una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización. | | | | | |
| | | 9.1.2 Control de acceso a las redes y servicios asociados | Se provee a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar. | | | | | |
| | 9.2 Gestión de acceso de usuario | 9.2.1 Gestión de altas/bajas en el registro de usuarios | Existe un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso. | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 9.2.2 Gestión de los derechos de acceso asignados a usuario | Se implementa un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios. | | | | | |
| | | 9.2.3 Gestión de los derechos de acceso con privilegios especiales | La asignación y uso de derechos de acceso con privilegios especiales es restringida y controlada. | | | | | |
| | | 9.2.4 Gestión de información confidencial de autenticación de usuarios | La asignación de información confidencial para la autenticación es controlada mediante un proceso de gestión controlado. | | | | | |
| | | 9.2.5 Revisión de los derechos de acceso de los usuarios | Los propietarios de los activos revisan con regularidad los derechos de acceso de los usuarios. | | | | | |
| | | 9.2.6 Retirada o adaptación de los derechos de acceso | Se retiran los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o son revisados en caso de cambio. | | | | | |
| | 9.3 Responsabilidades del usuario | 9.3.1 Uso de información confidencial para la autenticación | Se exige a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación. | | | | | |
| | 9.4 Control de acceso a sistemas y aplicaciones | 9.4.1 Restricción del acceso a la información | Se restringe el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida. | | | | | |
| | | 9.4.2 Procedimientos seguros de inicio de sesión | Cuando sea requerido por la política de control de accesos se controla el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 9.4.3 Gestión de contraseñas de usuario | Los sistemas de gestión de contraseñas son interactivos y aseguran contraseñas de calidad. | | | | | |
| | | 9.4.4 Uso de herramientas de administración de sistemas | El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas está restringido y estrechamente controlado. | | | | | |
| | | 9.4.5 Control de acceso al código fuente de los programas | Se restringe el acceso al código fuente de las aplicaciones software. | | | | | |
| 10. Cifrado | 10.1 Controles criptográficos | 10.1.1 Política de uso de los controles criptográficos | Se desarrolla e implementa una política que regule el uso de controles criptográficos para la protección de la información. | | | | | |
| | | 10.1.2 Gestión de claves | Se desarrolla e implementa una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida. | | | | | |
| 11. Seguridad física y Ambiental | 11.1 Áreas seguras | 11.1.1 Perímetro de seguridad física | Se definen y utilizan perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica. | | | | | |
| | | 11.1.2 Controles físicos de entrada | Las áreas seguras están protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso. | | | | | |
| | | 11.1.3 Seguridad de oficinas, despachos y recursos | Se diseña y aplica un sistema de seguridad física a las oficinas, salas e instalaciones de la organización. | | | | | |
| | | 11.1.4 Protección contra las amenazas externas y ambientales | Se diseña y aplica una protección física contra desastres naturales, ataques maliciosos o accidentes. | | | | | |
| | | 11.1.5 El trabajo en áreas seguras | Se diseña y aplica procedimientos para el desarrollo de trabajos y actividades en áreas seguras. | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 11.1.6 Áreas de acceso público, carga y descarga | Se controlan puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información. | | | | | |
| | 11.2 Seguridad de los equipos | 11.2.1 Emplazamiento y protección de equipos | Los equipos son emplazados y protegidos para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado. | | | | | |
| | | 11.2.2 Instalaciones de suministro | Los equipos son protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo. | | | | | |
| | | 11.2.3 Seguridad del cableado | Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se protegen contra la intercepción, interferencia o posibles daños. | | | | | |
| | | 11.2.4 Mantenimiento de los equipos | Los equipos se mantienen adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas. | | | | | |
| | | 11.2.5 Salida de activos fuera de las dependencias de la empresa | Los equipos, la información o el software no se retiran del sitio sin previa autorización. | | | | | |
| | | 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones | Se aplica la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos | | | | | |
| | | 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento | Se verifican todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | hayan sobrescrito de manera segura antes de su eliminación o reutilización. | | | | | |
| | | 11.2.8 Equipo informático de usuario desatendido | Los usuarios aseguran de que los equipos no supervisados cuentan con la protección adecuada. | | | | | |
| | | 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla | Se adopta una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información. | | | | | |
| 12. Seguridad en la Operativa | 12.1 Responsabilidades y procedimientos de operación | 12.1.1 Documentación de procedimientos de operación | Se documentan los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten. | | | | | |
| | | 12.1.2 Gestión de cambios | Se controlan los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información. | | | | | |
| | | 12.1.3 Gestión de capacidades | Se monitorea y ajusta el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas. | | | | | |
| | | 12.1.4 Separación de entornos de desarrollo, prueba y producción | Los entornos de desarrollo, pruebas y operacionales permanecen separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional. | | | | | |
| | 12.2 Protección contra código malicioso | 12.2.1 Controles contra el código malicioso | Se implementan controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios. | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 12.3 Copias de seguridad | 12.3.1 Copias de seguridad de la información | Se realizan pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida. | | | | | |
| | 12.4 Registro de actividad y supervisión | 12.4.1 Registro y gestión de eventos de actividad | Se producen, mantienen y revisan periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información. | | | | | |
| | | 12.4.2 Protección de los registros de información | Se protegen contra posibles alteraciones y accesos no autorizados la información de los registros. | | | | | |
| | | 12.4.3 Registros de actividad del administrador y operador del sistema | Se registran las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular. | | | | | |
| | | 12.4.4 Sincronización de relojes | Se sincronizan los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad y en relación a una fuente de sincronización única de referencia. | | | | | |
| | 12.5 Control del software en explotación | 12.5.1 Instalación del software en sistemas en producción | Se implementan procedimientos para controlar la instalación de software en sistemas operacionales. | | | | | |
| | 12.6 Gestión de la vulnerabilidad técnica | 12.6.1 Gestión de las vulnerabilidades técnicas | Se obtiene información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados. | | | | | |
| | | 12.6.2 Restricciones en la instalación de software | Se establece e implementa las reglas que rigen la instalación de software por parte de los usuarios. | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 12.7 Consideraciones de las auditorías de los sistemas de información | 12.7.1 Controles de auditoría de los sistemas de información | Se planifican los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio. | | | | | |
| 13. Seguridad en las Telecomunicaciones | 13.1 Gestión de la seguridad en las redes | 13.1.1 Controles de red | Se administra y controla las redes para proteger la información en sistemas y aplicaciones. | | | | | |
| | | 13.1.2 Mecanismos de seguridad asociados a servicios en red | Se identifica e incluye en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados. | | | | | |
| | | 13.1.3 Segregación de redes | Se segregan las redes en función de los grupos de servicios, usuarios y sistemas de información. | | | | | |
| | 13.2 Intercambio de información con partes externas | 13.2.1 Políticas y procedimientos de intercambio de información | Existen políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación. | | | | | |
| | | 13.2.2 Acuerdos de intercambio | Los acuerdos abordan la transferencia segura de información comercial entre la organización y las partes externas. | | | | | |
| | | 13.2.3 Mensajería electrónica | Se protege adecuadamente la información referida en la mensajería electrónica. | | | | | |
| | | 13.2.4 Acuerdos de confidencialidad y secreto | Se identifica, revisa y documenta de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información. | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 14. Adquisición, desarrollo y Mantenimiento de los sistemas de información | 14.1 Requisitos de seguridad de los sistemas de información | 14.1.1 Análisis y especificación de los requisitos de seguridad | Los requisitos relacionados con la seguridad de la información se incluyen en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes. | | | | | |
| | | 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas | La información de los servicios de aplicación que pasan a través de redes públicas se protege contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada. | | | | | |
| | | 14.1.3 Protección de las transacciones por redes telemáticas | La información en transacciones de servicios de aplicación se protege para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción. | | | | | |
| | 14.2 Seguridad en los procesos de desarrollo y soporte | 14.2.1 Política de desarrollo seguro de software | Se establecen y aplican reglas para el desarrollo de software y sistemas dentro de la organización. | | | | | |
| | | 14.2.2 Procedimientos de control de cambios en los sistemas | En el ciclo de vida de desarrollo se hace uso de procedimientos formales de control de cambios. | | | | | |
| | | 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo | Las aplicaciones críticas para el negocio se deben revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización. | | | | | |
| | | 14.2.4 Restricciones a los cambios en los paquetes de software | Se evitan modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente. | | | | | |
| | | 14.2.5 Uso de principios de ingeniería en protección de sistemas | Se establecen, documentan, mantienen y aplican los principios de seguridad en ingeniería de sistemas para cualquier labor de | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | implementación en el sistema de información. | | | | | |
| | | 14.2.6 Seguridad en entornos de desarrollo | La organización establece y protege adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema. | | | | | |
| | | 14.2.7 Externalización del desarrollo de software | La organización supervisa y monitorea las actividades de desarrollo del sistema que se hayan externalizado. | | | | | |
| | | 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas | Se realizan pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo. | | | | | |
| | | 14.2.9 Pruebas de aceptación | Se establecen programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones. | | | | | |
| | 14.3 Datos de prueba | 14.3.1 Protección de los datos utilizados en prueba | Los datos de pruebas se seleccionan cuidadosamente y se deberían proteger y controlar. | | | | | |
| 15. Relaciones con Suministradores | 15.1 Seguridad de la información en las relaciones con suministradores | 15.1.1 Política de seguridad de la información para suministradores | Se documentan adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas. | | | | | |
| | | 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores | Se establecen todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización. | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones | Los acuerdos con los proveedores incluyen los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones. | | | | | |
| | 15.2 Gestión de la prestación del servicio por suministradores | 15.2.1 Supervisión y revisión de los servicios prestados por terceros | Las organizaciones monitorean, revisan y auditan la presentación de servicios del proveedor regularmente. | | | | | |
| | | 15.2.2 Gestión de cambios en los servicios prestados por terceros | Se administran los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos. Se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos. | | | | | |
| 16. Gestión de Incidentes | 16.1 Gestión de incidentes de seguridad de la información y mejoras | 16.1.1 Responsabilidades y procedimientos | Se establecen las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. | | | | | |
| | | 16.1.2 Notificación de los eventos de seguridad de la información | Los eventos de seguridad de la información se informan lo antes posible utilizando los canales de administración adecuados. | | | | | |
| | | 16.1.3 Notificación de puntos débiles de la seguridad | Se anota e informa sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización. | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones | Se evalúan los eventos de seguridad de la información y decidir su clasificación como incidentes. | | | | | |
| | | 16.1.5 Respuesta a los incidentes de seguridad | Se responde ante los incidentes de seguridad de la información en atención a los procedimientos documentados. | | | | | |
| | | 16.1.6 Aprendizaje de los incidentes de seguridad de la información | Se el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro. | | | | | |
| | | 16.1.7 Recopilación de evidencias | Se define y aplica los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia. | | | | | |
| 17. Aspectos de la SI en la Gestión de la Continuidad de Negocio | 17.1 Continuidad de la seguridad de la información | 17.1.1 Planificación de la continuidad de la seguridad de la información | La organización determina los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre. | | | | | |
| | | 17.1.2 Implantación de la continuidad de la seguridad de la información | La organización establece, documenta, implementa y mantiene los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas. | | | | | |
| | | 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información | La organización verifica regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas. | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 17.2 Redundancias | 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información | Se implementa la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad. | | | | | |
| 18. Cumplimiento | 18.1 Cumplimiento de los requisitos legales y contractuales | 18.1.1 Identificación de la legislación aplicable | Se identifica, documentar y mantiene al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos. | | | | | |
| | | 18.1.2 Derechos de propiedad intelectual (DPI) | Se implementa procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software originales. | | | | | |
| | | 18.1.3 Protección de los registros de la organización | Los registros se protegen contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales. | | | | | |
| | | 18.1.4 Protección de datos y privacidad de la información personal | Se garantiza la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan. | | | | | |
| | | 18.1.5 Regulación de los controles criptográficos | Se utilizan controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes. | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 18.2 Revisiones de la seguridad de la información | 18.2.1 Revisión independiente de la seguridad de la información | Se revisa el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización. | | | | | |
| | | 18.2.2 Cumplimiento de las políticas y normas de seguridad | Los gerentes revisan regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente. | | | | | |
| | | 18.2.3 Comprobación del cumplimiento | Los sistemas de información se revisan regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización. | | | | | |
| **TOTAL** | | | | | **0** | **0** | **$ -** | |

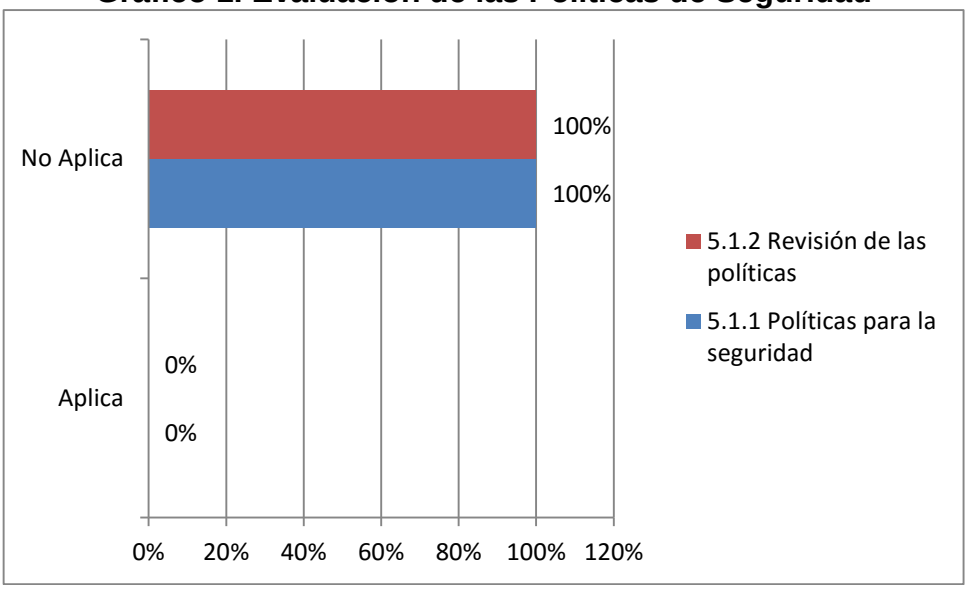
Fuente: la presente investigación – Año 2015

## 4.4 ANÁLISIS DE LOS RESULTADOS DE LA LISTA DE CHEQUEO

Con el fin de soportar el proceso de verificación y auditoría a los sistemas de información del área financiera de la SED se aplicó una lista de chequeo que contempló desde el capítulo 5 hasta el capítulo 18 de la norma ISO/IEC 27002:2005. Este formato de lista de chequeo fue aplicado a los 11 colaboradores del área financiera de la SED, obteniendo los siguientes resultados:

- **Capítulo 5. Políticas de Seguridad**

**Gráfico 1. Evaluación de las Políticas de Seguridad**




Fuente: la presente investigación – Año 2015

Según la opinión del 100% de la muestra, al interior del área financiera de la SED no se cuenta con políticas para la seguridad de la información, aprobadas por la dirección, publicadas y comunicadas a los empleados y a todas las partes externas relevantes. En el mismo sentido se pudo constatar que no se hace revisión de dichas políticas actualmente.

Lo anterior sugiere la necesidad de formular la política de seguridad del área financiera de la SED, entendiendo la importancia de la información que se maneja y el riesgo que supone no contar con claras directrices en este sentido.

- **Capítulo 6. Aspectos Organizativos de los Sistemas de Información**

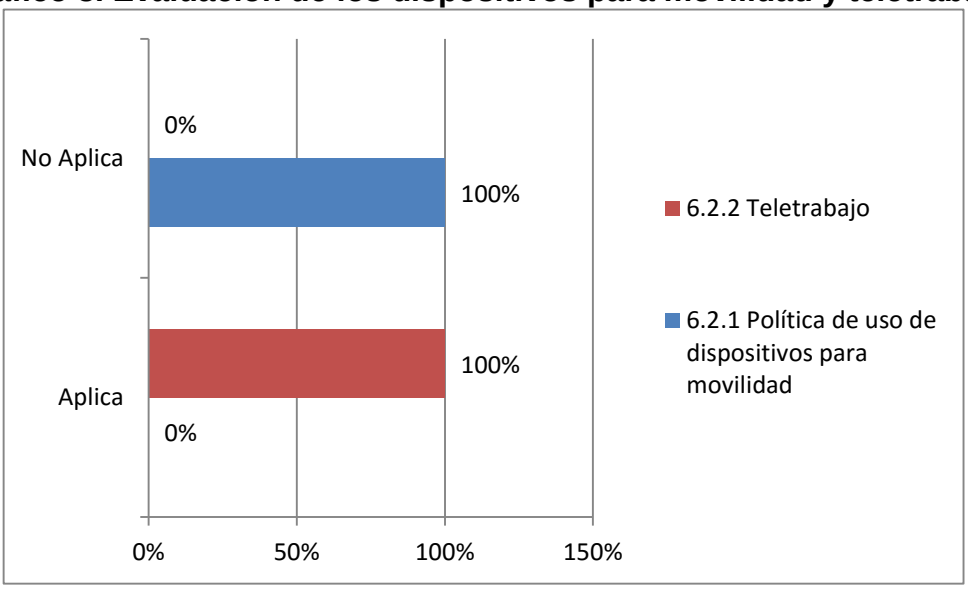
**Gráfico 2. Evaluación de la Organización interna**


Fuente: la presente investigación – Año 2015

Con respecto a los aspectos organizativos de los SI en la parte interna pudo determinarse que según el 100% de la muestra, no existe una gestión eficiente en este aspecto al interior del área financiera de la SED.

Lo anterior se soporta en la carencia en la asignación de las responsabilidades para la seguridad de la información, deficientes políticas de segregación de tareas y escaso relacionamiento con grupos o foros de seguridad especializados entre otros aspectos.

**Gráfico 3. Evaluación de los dispositivos para movilidad y teletrabajo**



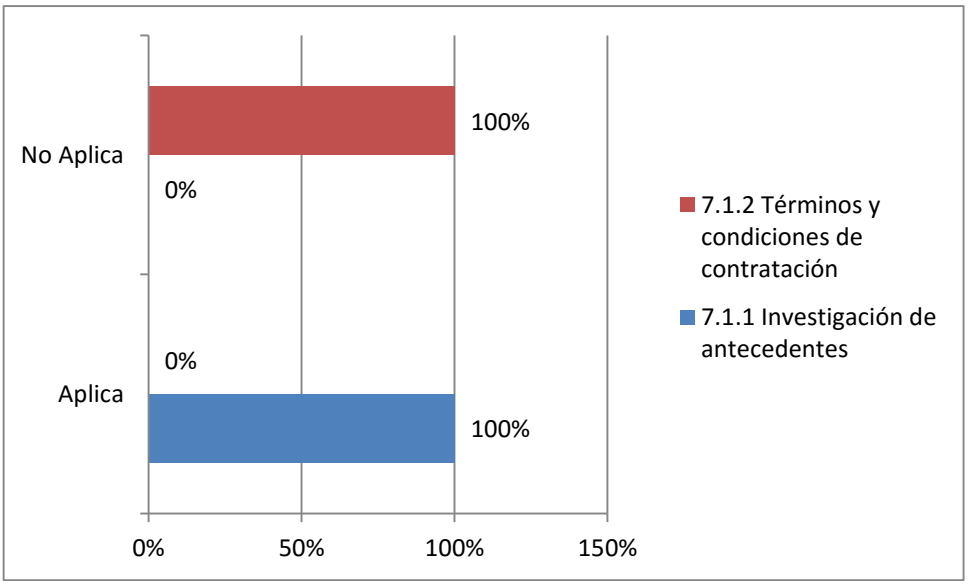

Fuente: la presente investigación – Año 2015

Frente a los dispositivos para movilidad y teletrabajo se encontraron opiniones divididas entre la muestras consultada, pues el 100% considera que existe una adecuada gestión para promover el teletrabajo soportada en una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas para tal fin, mientras que un 100% opina que son escasas las políticas para el uso de dispositivos de movilidad.

Lo anterior induce a pensar que las políticas de organización de los sistemas de información en el área financiera de la SED en el tema de los dispositivos para movilidad y teletrabajo se encuentran en una fase temprana de estructuración y aplicación.

- **Capítulo 7. Seguridad Ligada a los recursos humanos**

**Gráfico 4. Evaluación Antes de la contratación**

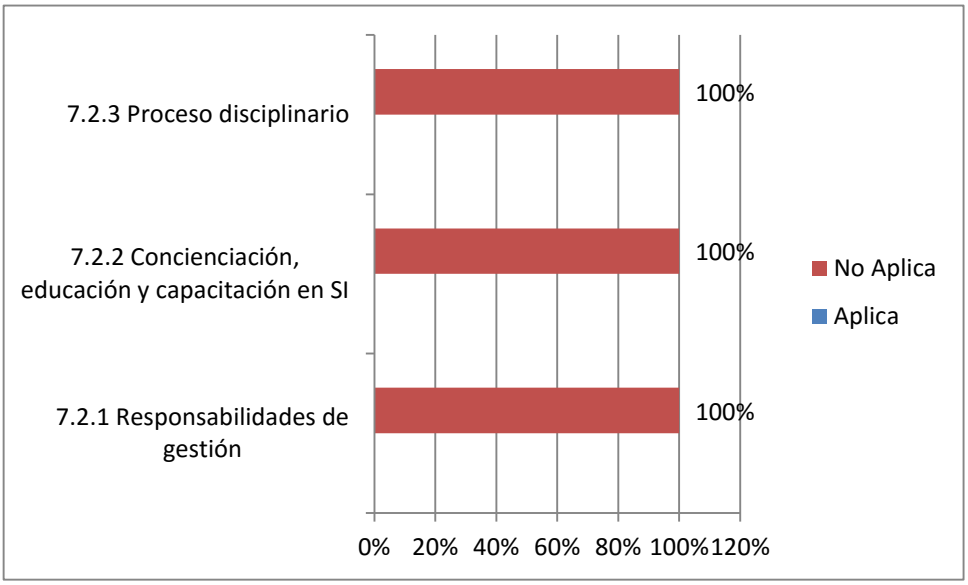



Fuente: la presente investigación – Año 2015

En el tema de las acciones emprendidas antes de la contratación del personal para garantizar la seguridad en la información, se pudo encontrar que en lo referente a la investigación de antecedentes el área de talento humano de la SED realiza adecuadamente las revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

En contraposición a lo anterior el 100% de la muestra consultada cree que muchas veces no existe claridad en los términos y condiciones de contratación frente al manejo de los sistemas de información que maneja la SED.

**Gráfico 5. Durante la contratación**

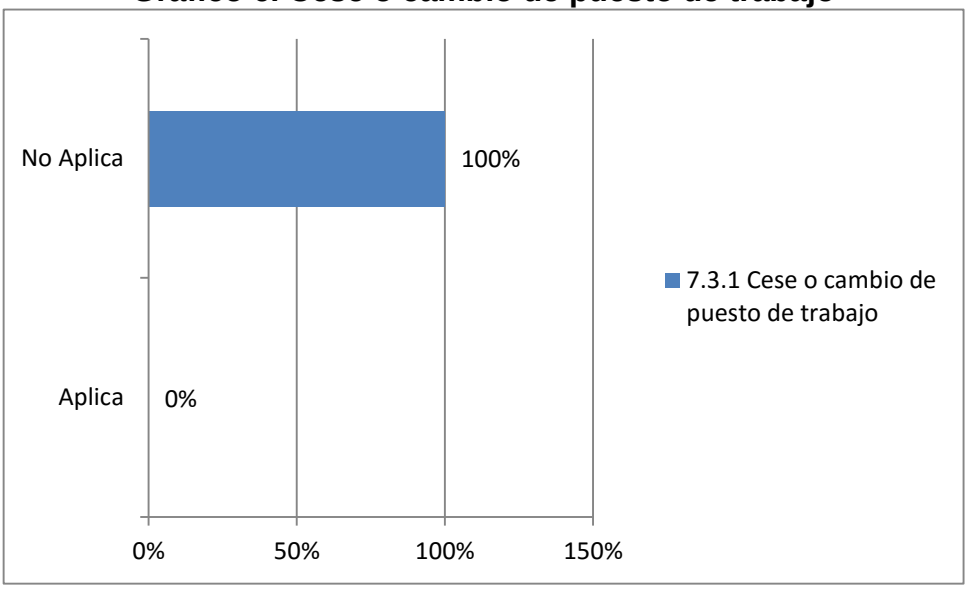



Fuente: la presente investigación – Año 2015

En cuanto a las acciones emprendidas durante la contratación del personal para garantizar la seguridad en la información del área financiera de la SED, se encontró que el 100% de la muestra encuestada considera que se deben mejorar la totalidad de los procedimientos que se efectúan en este sentido.

Lo anterior sustentado en parte en las deficiencias para aplicar la seguridad en concordancia con las políticas y los procedimientos, la falta de entrenamiento apropiado y actualizaciones regulares en políticas y procedimientos organizacionales y la inexistencia de un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.

**Gráfico 6. Cese o cambio de puesto de trabajo**

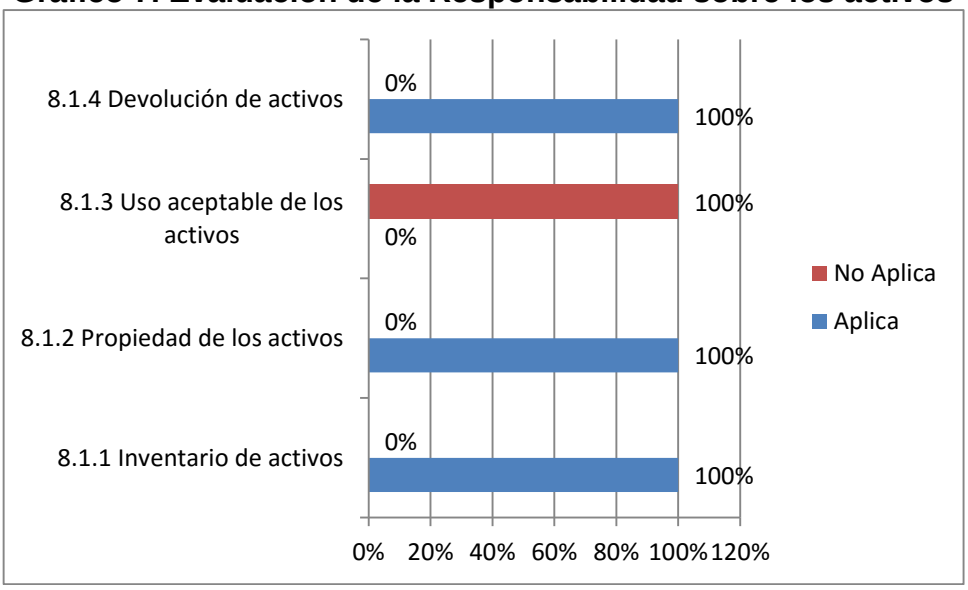



Fuente: la presente investigación – Año 2015

En el tema de cese o cambio de puesto de trabajo en un 100% de los casos, la muestra consultada denota dificultad en la asignación de las responsabilidades para ejecutar la finalización de un empleo al interior de la SED, pues dichos procedimientos no se encuentra claramente definidos y comunicados y eventualmente pueden suscitar fugas, infiltraciones y pérdidas de información relevante, confidencial o privilegiada.

- **Capítulo 8. Gestión de Activos**

**Gráfico 7. Evaluación de la Responsabilidad sobre los activos**

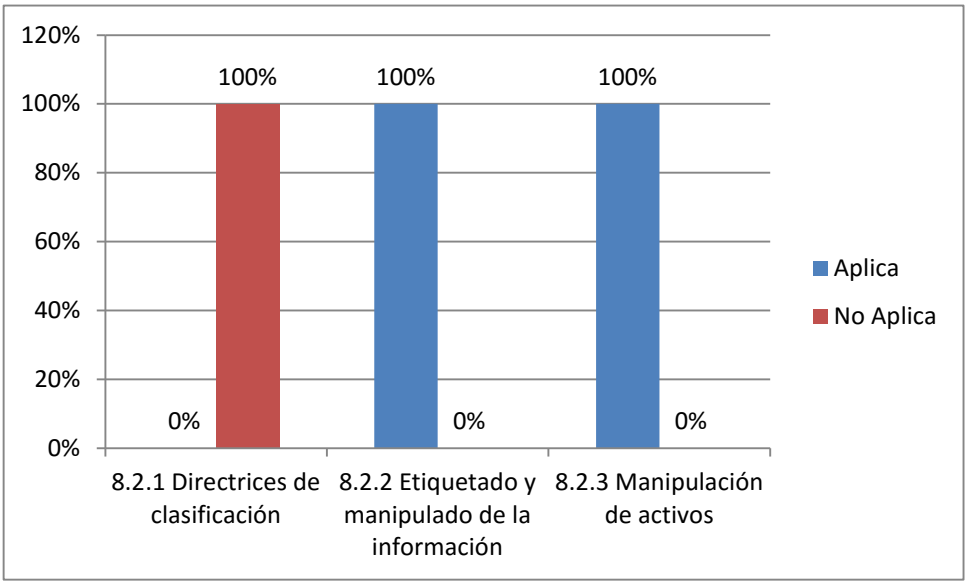



Fuente: la presente investigación – Año 2015

En lo referente a la gestión de activos y la responsabilidad en el manejo de los mismos para soportar los sistemas de información, se pudo encontrar que se realiza un adecuado inventario de activos, se designan dichos activos de forma pertinente y se hace seguimiento a la devolución de activos cuando se finaliza un período contractual.

Sin embargo la muestra consultada considera que existen falencias en cuanto a la identificación, documentación e implantación de regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

**Gráfico 8. Evaluación de la Clasificación de la información**

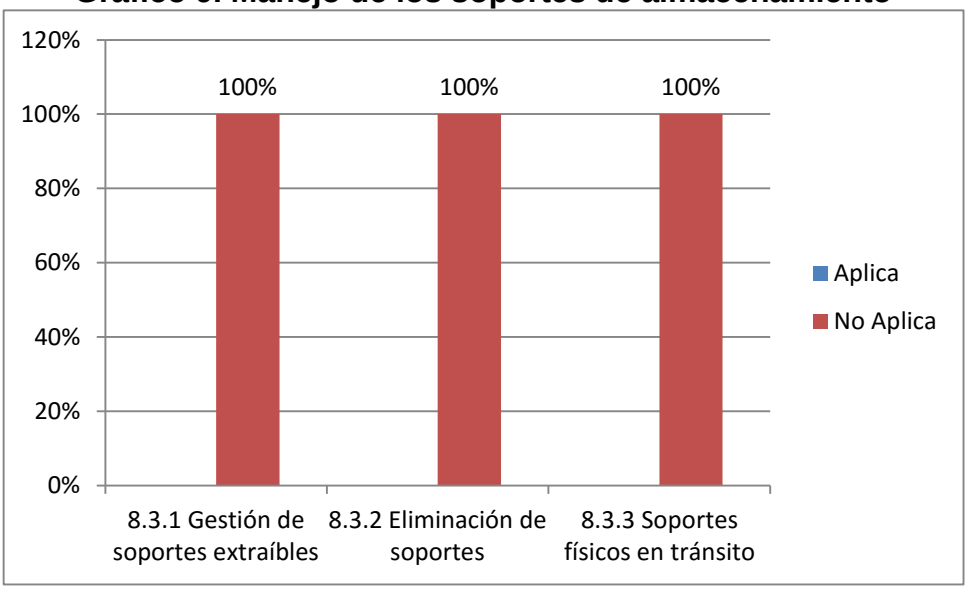



Fuente: la presente investigación – Año 2015

En el tema de clasificación de la información de activos, un 100% de la muestra encuestada considera que se hace una adecuada gestión en el tema de etiquetado y manipulación de la información y de los activos frente a un 100% que considera que existen falencias en el tema de formulación en las directrices de clasificación.

Teniendo en cuenta esta información se debe mejorar la manera en el que el área clasifica la información en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización.

**Gráfico 9. Manejo de los soportes de almacenamiento**



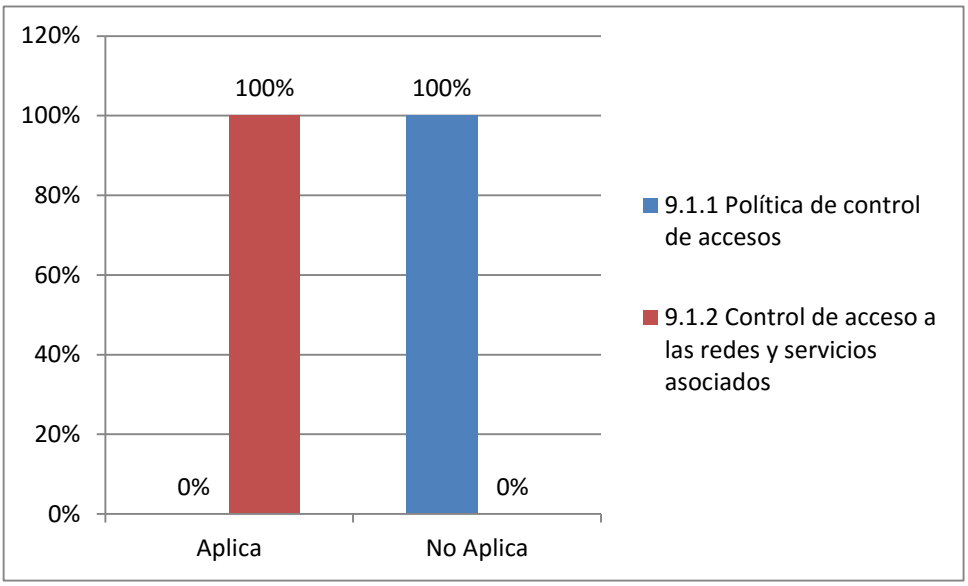

Fuente: la presente investigación – Año 2015

En el tema de manejo de los soportes de almacenamiento el 100% de la muestra consultada opina que debe mejorarse ostensiblemente en aspectos como la gestión de soportes extraíbles, la eliminación de soportes y los soportes físicos en tránsito.

Con base en lo anterior se concluye que existen deficiencias en cuanto al establecimiento de procedimientos para la gestión de los medios informáticos removibles, no se eliminan los medios de forma segura y sin riesgo cuando ya no sean requeridos y no se protege adecuadamente los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización.

- **Capítulo 9. Control de accesos**

**Gráfico 10. Evaluación de los requisitos del negocio para el control de accesos**

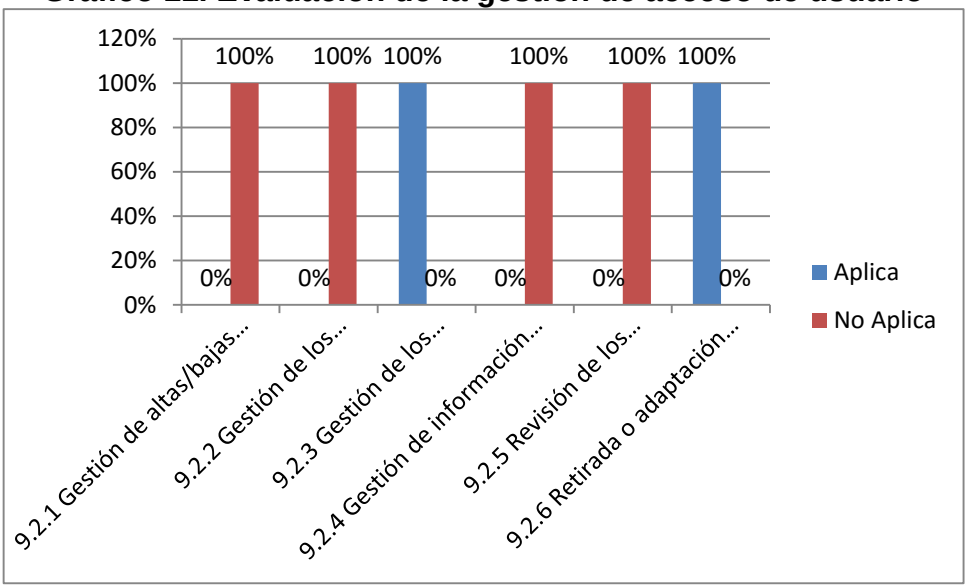



Fuente: la presente investigación – Año 2015

En cuanto al control de accesos se valúo los requisitos del negocio para el control de accesos obteniendo opiniones divididas entre la muestra consultada en donde un 100% considera que la gestión en cuanto a control de accesos a las redes y servicios asociados es pertinente en contraposición por con la políticas generales en el control de accesos.

Lo anterior permite inferir que existen deficiencias por mejorar en temas como establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización.

**Gráfico 11. Evaluación de la gestión de acceso de usuario**



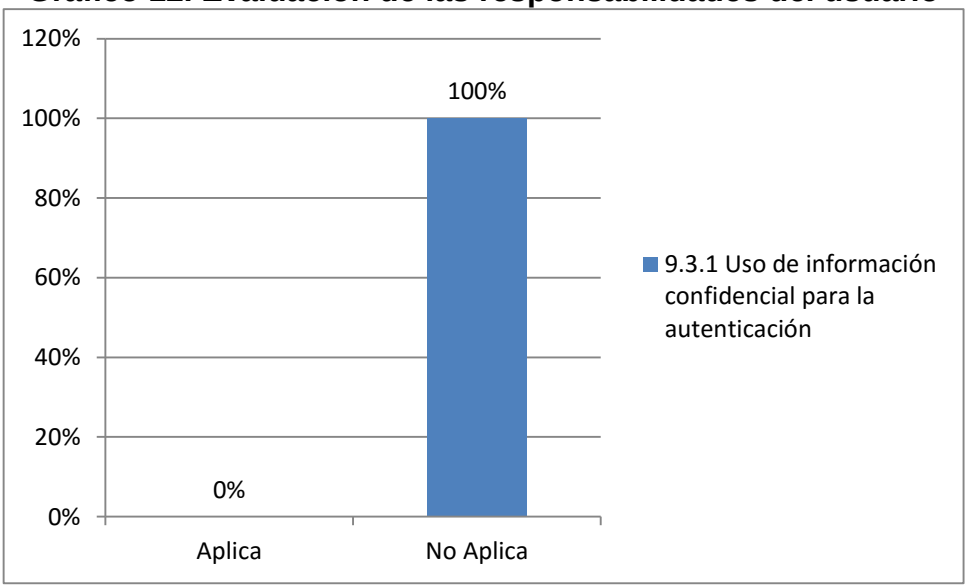

Fuente: la presente investigación – Año 2015

En cuanto a la gestión de acceso de usuario se pudo encontrar que un 100% de la muestra consultada resalta un adecuado direccionamiento en temas como la gestión de los derechos de acceso con privilegios especiales y la adaptación de los derechos de acceso.

Frente a lo anterior el 100% de la muestra opina que se deben mejorar aspectos como la gestión de altas/bajas en el registro de usuarios, la gestión de los derechos de acceso asignados a usuario, la gestión de información confidencial de autenticación de usuarios y la revisión de los derechos de acceso de los usuarios.

Teniendo en cuenta estos resultados se debe implementar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios.

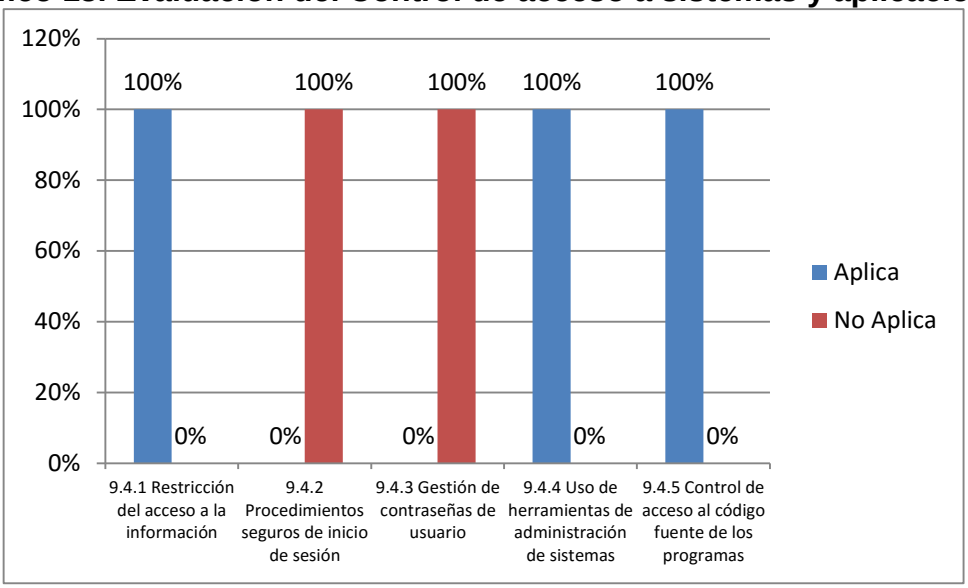
**Gráfico 12. Evaluación de las responsabilidades del usuario**




Fuente: la presente investigación – Año 2015

En referencia a la evaluación de las de las responsabilidades del usuario se pudo encontrar que el 100% de la muestra indagada cree que se debe mejorar en la exigencia a los usuarios en el uso de las buenas prácticas de seguridad de la organización y sobretodo en el uso de información confidencial para la autenticación.

**Gráfico 13. Evaluación del Control de acceso a sistemas y aplicaciones**



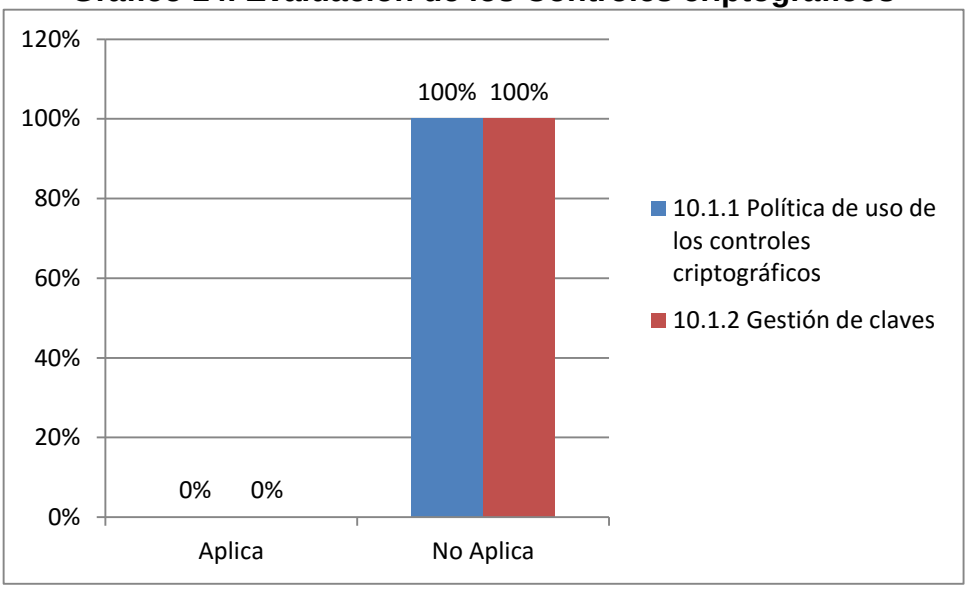

Fuente: la presente investigación – Año 2015

En el tema de control de acceso a sistemas y aplicaciones un 100% de la muestra consultada considera que existe una adecuada gestión en cuanto a la restricción del acceso a la información, el uso de herramientas de administración de sistemas y el control de acceso al código fuente de los programas.

Pese a esto, el 100% de la muestra consultada coincide en afirmar que existen falencias en temas como los procedimientos seguros de inicio de sesión y gestión de contraseñas de usuario, situación que induce a pensar en procesos de mejora en cuanto a la política de control de accesos y aplicaciones mediante un procedimiento seguro de log-on y sistemas de gestión de contraseñas más interactivos y que aseguren contraseñas de calidad.

- **Capítulo 10. Cifrado**

**Gráfico 14. Evaluación de los Controles criptográficos**

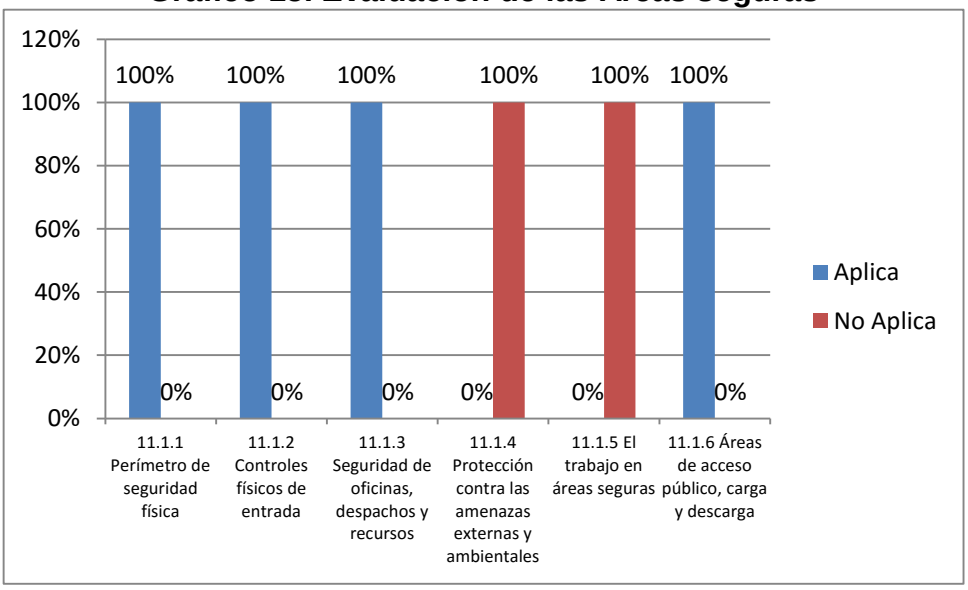



Fuente: la presente investigación – Año 2015

Para la evaluación del capítulo de cifrado se tuvo en cuenta el ítem controles criptográficos encontrando que según la opinión del 100% de la muestra consultada, el área financiera de la SED no desarrolla e implementa una política que regule el uso de controles criptográficos para la protección de la información y tampoco se implementa una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.

- **Capítulo 11. Seguridad física y Ambiental**

**Gráfico 15. Evaluación de las Áreas seguras**




Fuente: la presente investigación – Año 2015

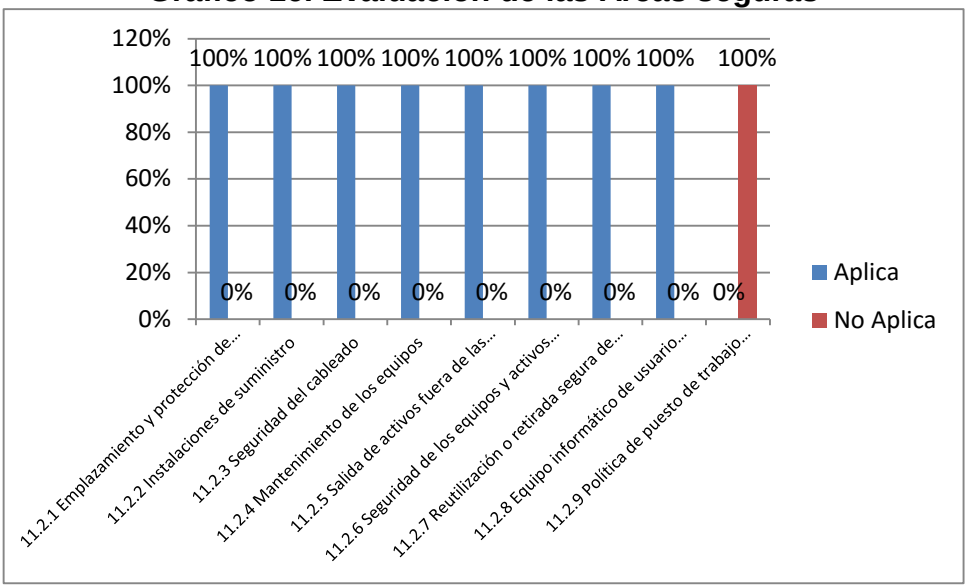
Para el análisis del capítulo 11 de seguridad física y ambiental se tuvieron en cuenta la evaluación de las áreas seguras y la seguridad de los equipos.

En cuanto a la evaluación de las áreas seguras se obtuvo que el 100% de la muestra consultada considera que se hace una gestión pertinente en temas como el perímetro de seguridad física, los controles físicos de entrada, la seguridad de oficinas, despachos y recursos y las áreas de acceso público, carga y descarga.

En contraste con lo anterior el 100% de la muestra encuentra falencias en tópicos importantes como la protección contra las amenazas externas y ambientales y el trabajo en áreas seguras.

De lo anterior se concluye que es necesario diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes, así como también procedimientos para el desarrollo de trabajos y actividades en áreas seguras.

**Gráfico 16. Evaluación de las Áreas seguras**



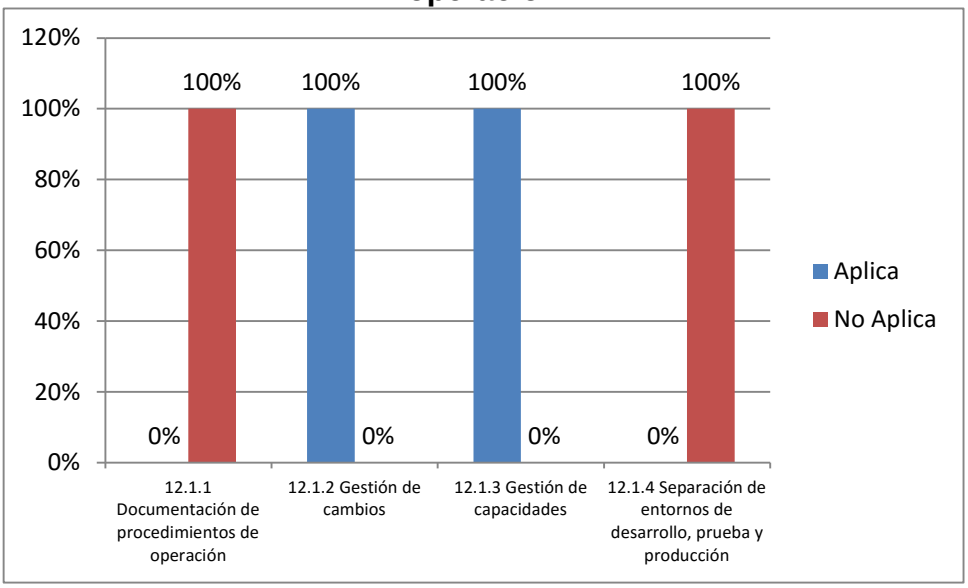

Fuente: la presente investigación – Año 2015

En referencia a la evaluación de la seguridad en los equipos se obtuvo que el 100% de la muestra consultada considera como fortaleza la gestión en aspectos como el emplazamiento y protección de equipos, las instalaciones de suministro, la seguridad del cableado, el mantenimiento de los equipos, la salida de activos fuera de las dependencias de la empresa, la seguridad de los equipos y activos fuera de las instalaciones, la reutilización o retirada segura de dispositivos de almacenamiento y el seguimiento hecho al equipo informático de usuario desatendido.

Frente a lo anterior, el 100% de la muestra coincide en encontrar debilidades en el tema de políticas de puesto de trabajo despejado y bloqueo de pantalla, por lo cual es necesario adoptar una política que permita la documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.

- **Capítulo 12. Seguridad en la Operación**

**Gráfico 17. Evaluación de las Responsabilidades y procedimientos de operación**




Fuente: la presente investigación – Año 2015

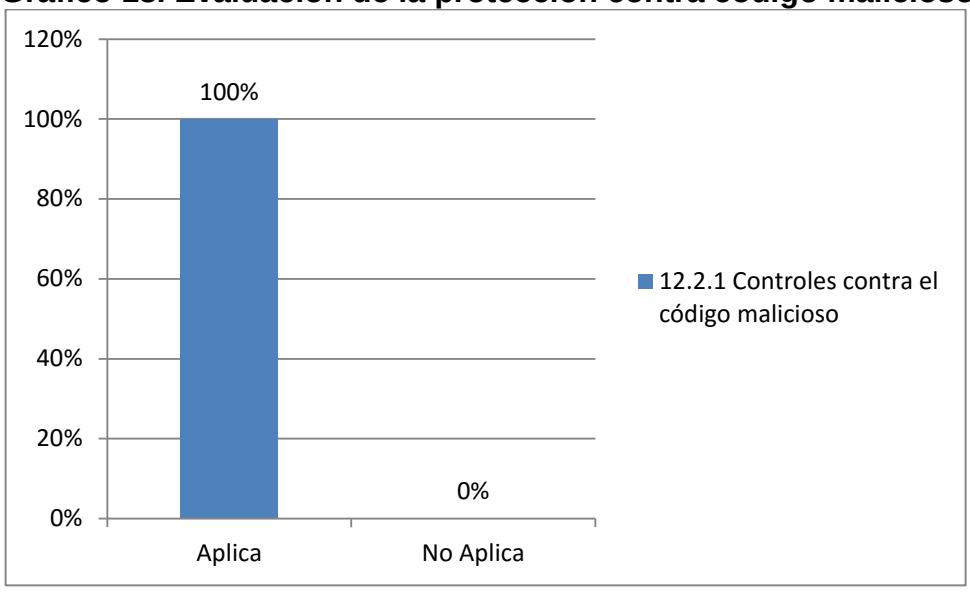
Para el análisis del capítulo 12 de seguridad en la parte operativa se tuvieron en cuenta los tópicos: responsabilidades y procedimientos de operación, protección contra código malicioso, copias de seguridad, registro de actividad y supervisión, control del software en explotación, gestión de la vulnerabilidad técnica y consideraciones de las auditorías de los sistemas de información.

En cuanto a la evaluación de las responsabilidades y procedimientos de operación se obtuvo que el 100% de la muestra consultada considera que existe una adecuada gestión en temas como la documentación de procedimientos de operación y la separación de entornos de desarrollo, prueba y producción.

Frente a lo anterior el 100% de la muestra coincide en señalar como debilidades los procesos asociados a gestión del cambio y gestión de capacidades, lo que da pie a inferir que se debe mejorar en aspectos como el control de los cambios que afectan a la seguridad de la información en la organización y procesos de negocio,

las instalaciones y sistemas de procesamiento de información y el monitoreo y ajuste en el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.

**Gráfico 18. Evaluación de la protección contra código malicioso**

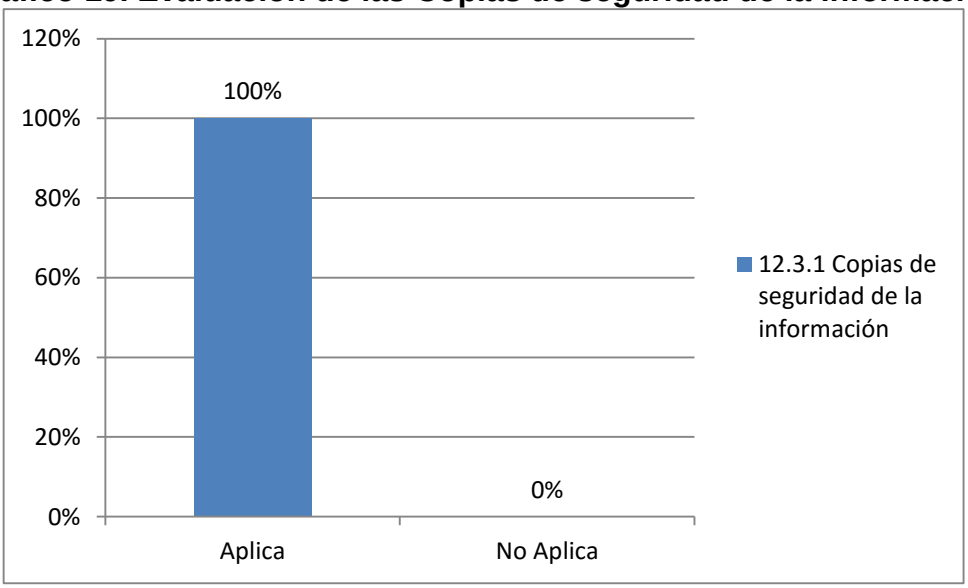



Fuente: la presente investigación – Año 2015

El 100% de la muestra consultada sostiene que el área financiera de la SED implementa controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.

Lo anterior muestra amplia fortaleza en cuanto a la continua actualización frente a virus informáticos en el área financiera de la SED.

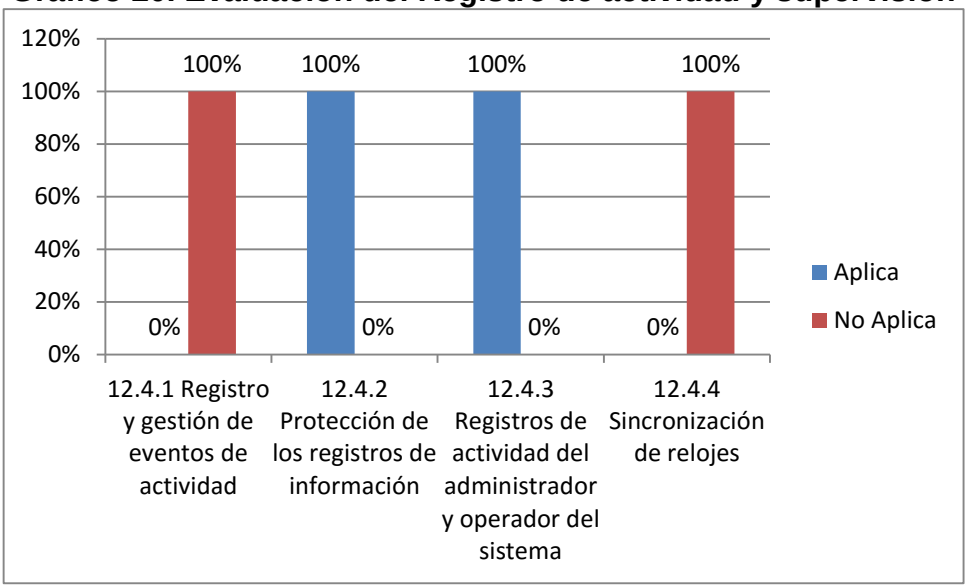
**Gráfico 19. Evaluación de las Copias de seguridad de la información**




Fuente: la presente investigación – Año 2015

El 100% de la muestra consultada sostiene que el área financiera de la SED implementa procedimientos para realizar copias de seguridad de la información, lo que demuestra que al interior del área se realizan pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.

**Gráfico 20. Evaluación del Registro de actividad y supervisión**

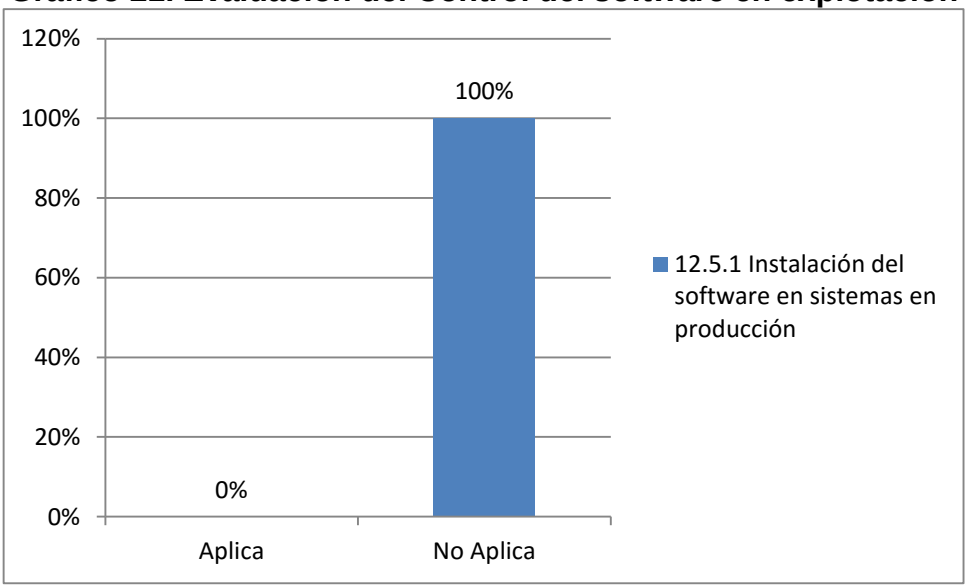



Fuente: la presente investigación – Año 2015

En cuanto a la evaluación del registro de actividad y supervisión se obtuvo que el 100% de la muestra consultada considera que existe una adecuada en cuanto a la protección de los registros de información y los registros de actividad.

En contraste con lo anterior, el 100% de la muestra coincide en señalar como debilidades los procesos asociados al registro y gestión de eventos de actividad y la sincronización de relojes, situación que supone el mejoramiento en aspectos como la producción, mantenimiento y evaluación periódica de los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información, así como también la sincronización de los relojes de todos los sistemas de procesamiento de información pertinentes procurando una fuente de sincronización única de referencia.

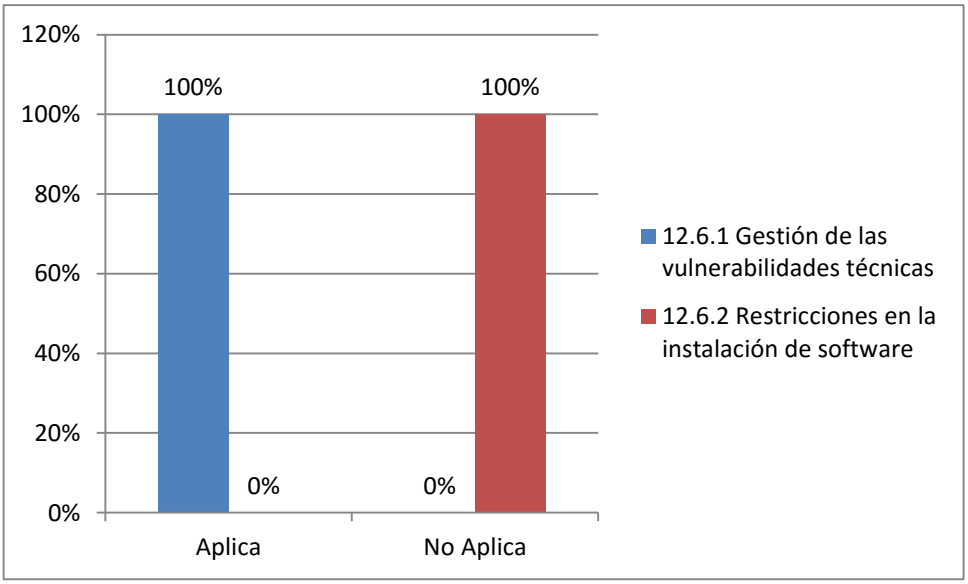
**Gráfico 21. Evaluación del Control del software en explotación**




Fuente: la presente investigación – Año 2015

El 100% de la muestra consultada sostiene que el área financiera de la SED tiene deficiencias en cuanto a la implementación de procedimientos para controlar la instalación de software en sistemas operacionales, situación que supone un enorme riesgo de afectación en la infección del sistema por malware o virus informáticos provenientes de internet.

**Gráfico 22. Evaluación de la Gestión de la vulnerabilidad técnica**

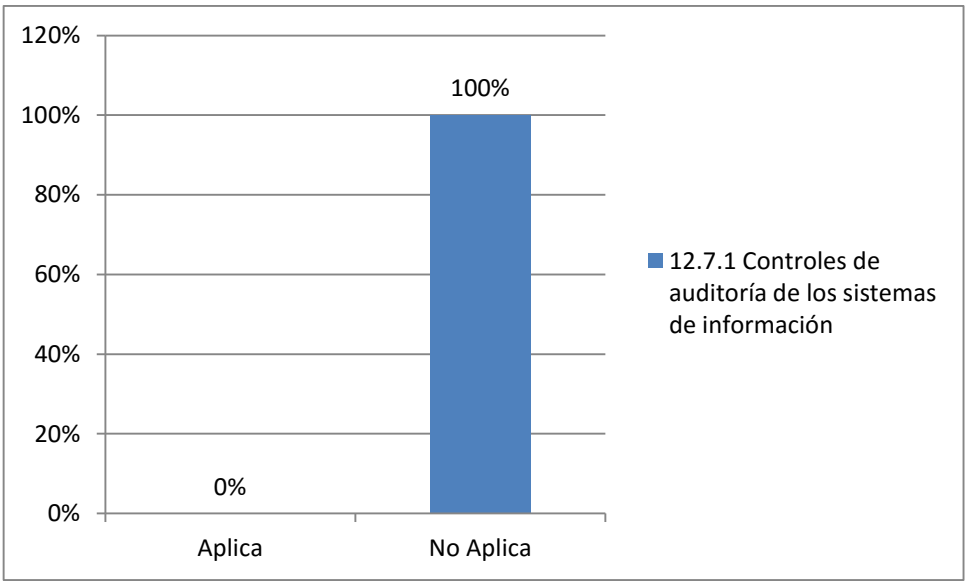



Fuente: la presente investigación – Año 2015

En cuanto a la evaluación de la gestión de la vulnerabilidad técnica se encontraron opiniones divididas entre la muestra consultada, pues un 100% opina que es pertinente la gestión en el tema de vulnerabilidades técnicas mientras al tiempo que coincide en encontrar falencias en las restricciones en la instalación de software.

Teniendo en cuenta estos resultados se puede inferir que es necesario establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios con el ánimo de proteger la información de los ordenadores del área financiera de la SED.

**Gráfico 23. Evaluación de las Consideraciones de las auditorías de los sistemas de información**



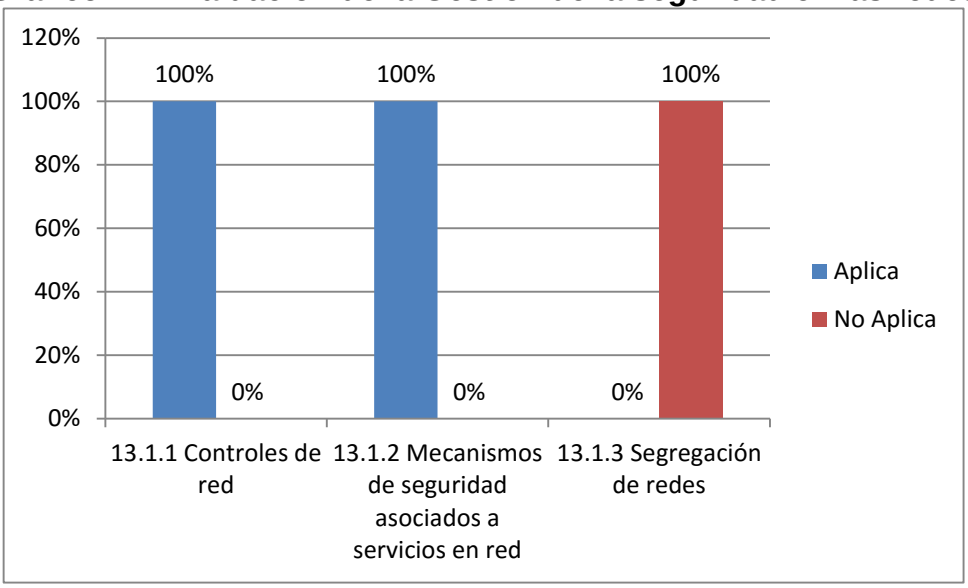

Fuente: la presente investigación – Año 2015

El 100% de la muestra consultada sostiene que el área financiera de la SED tiene deficiencias en cuanto a la planificación de los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.

Por lo que es necesario implantar políticas de auditoría de sistemas claramente definidas y contextualizadas a las necesidades del área.

- **Capítulo 13. Seguridad en las Telecomunicaciones**

**Gráfico 24. Evaluación de la Gestión de la seguridad en las redes**



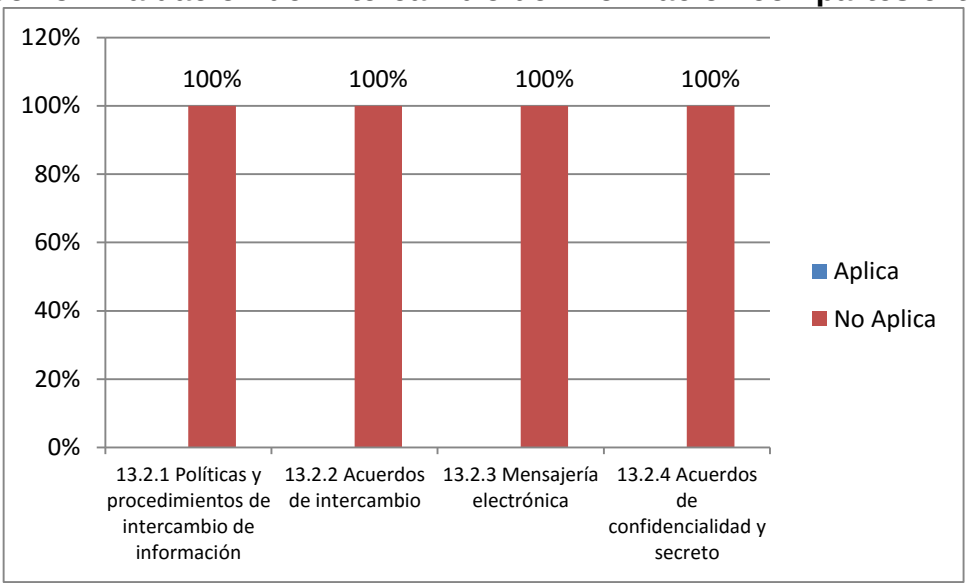

Fuente: la presente investigación – Año 2015

Para el análisis del capítulo 13 de seguridad en las telecomunicaciones se tuvieron en cuenta los tópicos: gestión de la seguridad en las redes e intercambio de información con partes externas.

En cuanto al tema de gestión de la seguridad en las redes el 100% de la muestra reconoce una adecuada gestión en ítems como los controles de red y los mecanismos de seguridad asociados a servicios de red.

En contraposición a lo anterior la muestra consultada en un 100% opina que existen falencias en la segregación de las redes lo que quiere decir que se debe mejorar en una mejor distribución de las redes en función de los grupos de servicios, usuarios y sistemas de información.

**Gráfico 25. Evaluación del Intercambio de información con partes externas**



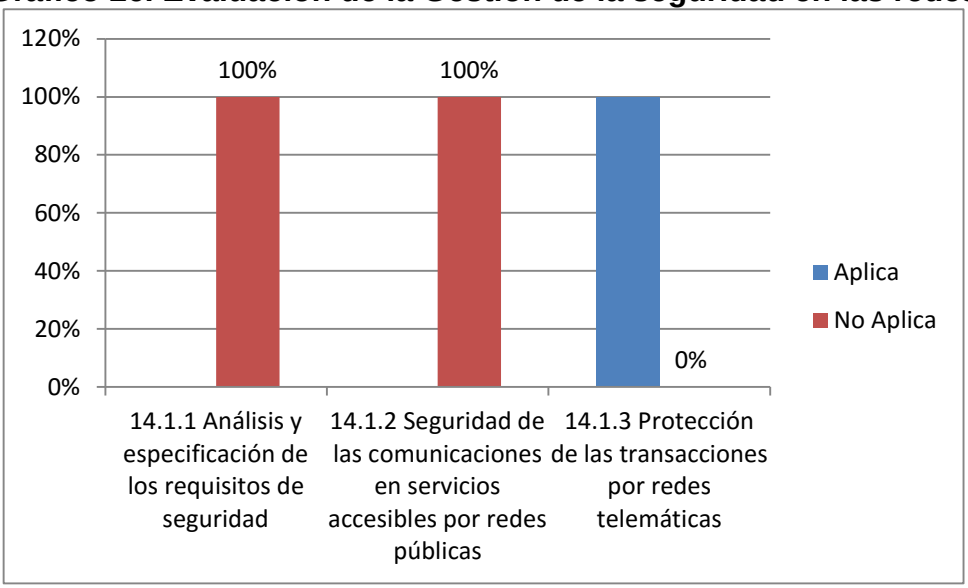

Fuente: la presente investigación – Año 2015

En cuanto al tema de intercambio de información con partes externas el 100% de la muestra consultada considera que existen falencias las políticas y procedimientos de intercambio de información, los acuerdos de intercambio, la mensajería electrónica y los acuerdos de confidencialidad y secreto.

Situaciones que se evidencien en la inexistencia de políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.

- **Capítulo 14. Adquisición, desarrollo y Mantenimiento de los sistemas de información**

**Gráfico 26. Evaluación de la Gestión de la seguridad en las redes**




Fuente: la presente investigación – Año 2015

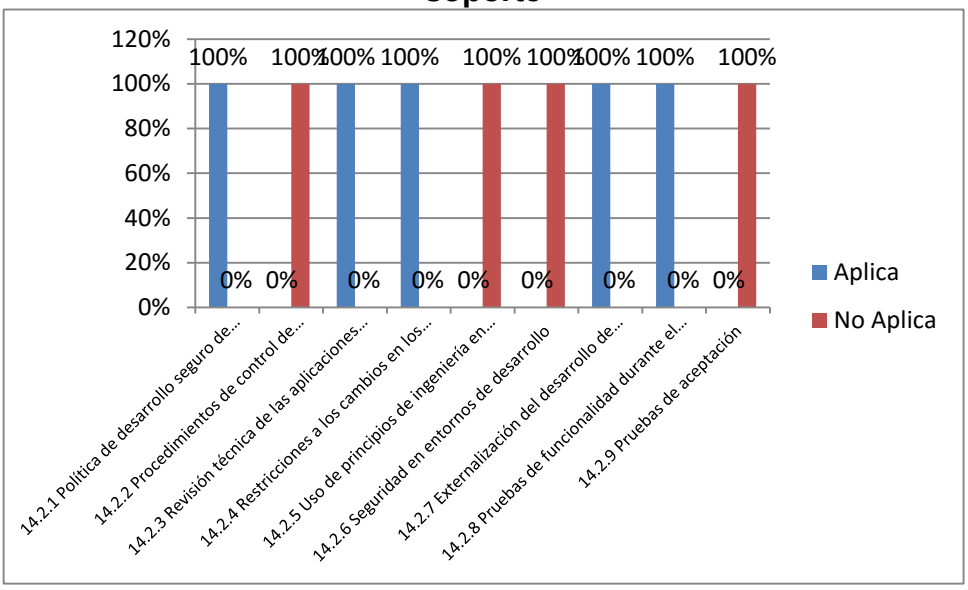
Para el análisis del capítulo 14 sobre adquisición, desarrollo y mantenimiento de los sistemas de información se tuvieron en cuenta los tópicos: requisitos de seguridad de los sistemas de información, seguridad en los procesos de desarrollo y soporte y datos de prueba

En cuanto al tema de requisitos de seguridad de los sistemas de información el 100% de la muestra reconoce fortaleza en la gestión de la protección de las transacciones por redes telemáticas.

Frente a lo anterior se identifican debilidades en torno al análisis y especificación de los requisitos de seguridad y la seguridad de las comunicaciones en servicios accesibles por redes públicas, lo cual induce a pensar que se debe mejorar en aspectos como la inclusión de los requisitos relacionados con la seguridad de la

información para los nuevos sistemas y la protección contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.

**Gráfico 27. Evaluación de la Seguridad en los procesos de desarrollo y soporte**

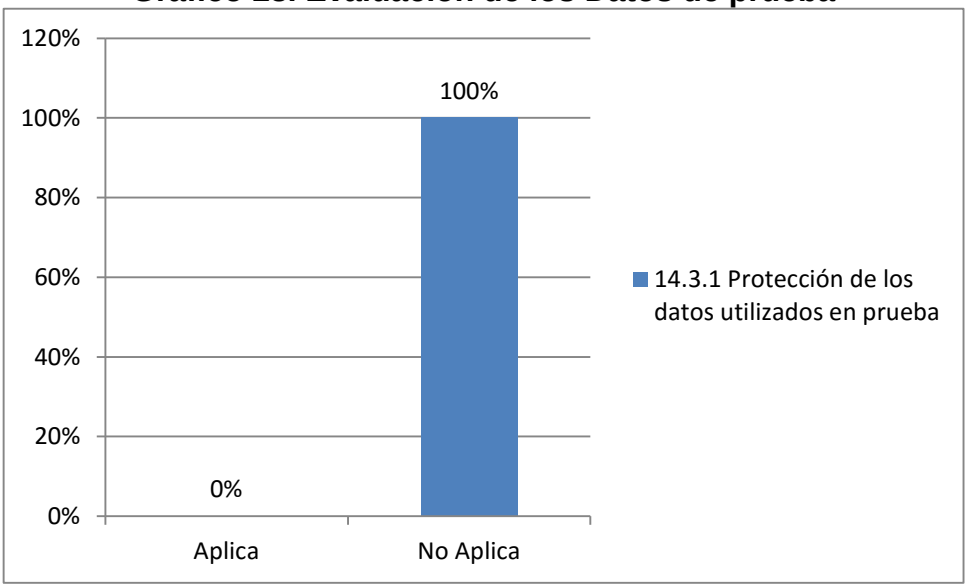



Fuente: la presente investigación – Año 2015

Con respecto al tema de seguridad en los procesos de desarrollo y soporte el 100% de la muestra consultada encuentra amplias fortalezas en temas como: la política de desarrollo seguro de software, la revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo, las restricciones a los cambios en los paquetes de software, la externalización del desarrollo de software y las pruebas de funcionalidad durante el desarrollo de los sistemas.

Frente a lo anterior la muestra consultada señala debilidades en aspectos como: los procedimientos de control de cambios en los sistemas, el uso de principios de ingeniería en protección de sistemas, la seguridad en entornos de desarrollo y las pruebas de aceptación

**Gráfico 28. Evaluación de los Datos de prueba**



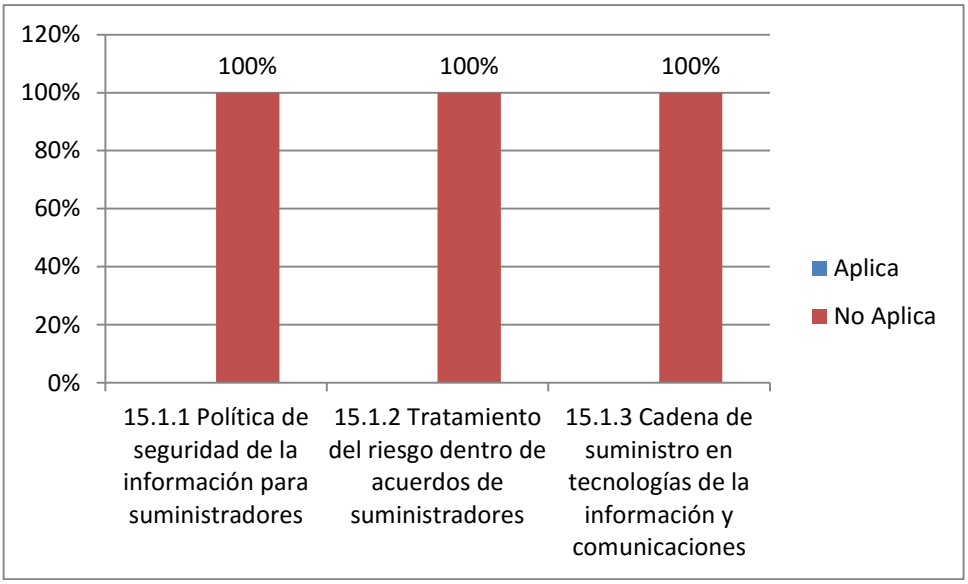

Fuente: la presente investigación – Año 2015

El 100% de la muestra consultada considera que a nivel interno el área financiera de la SED no gestión adecuadamente la protección de los datos utilizados en prueba.

Lo anterior supone que existen deficiencias en cuanto a la selección cuidadosa y la protección y control de los datos utilizados para la realización de pruebas con información del área.

- **Capítulo 15. Relaciones con Suministradores**

**Gráfico 29. Evaluación de la Seguridad de la información en las relaciones con suministradores**



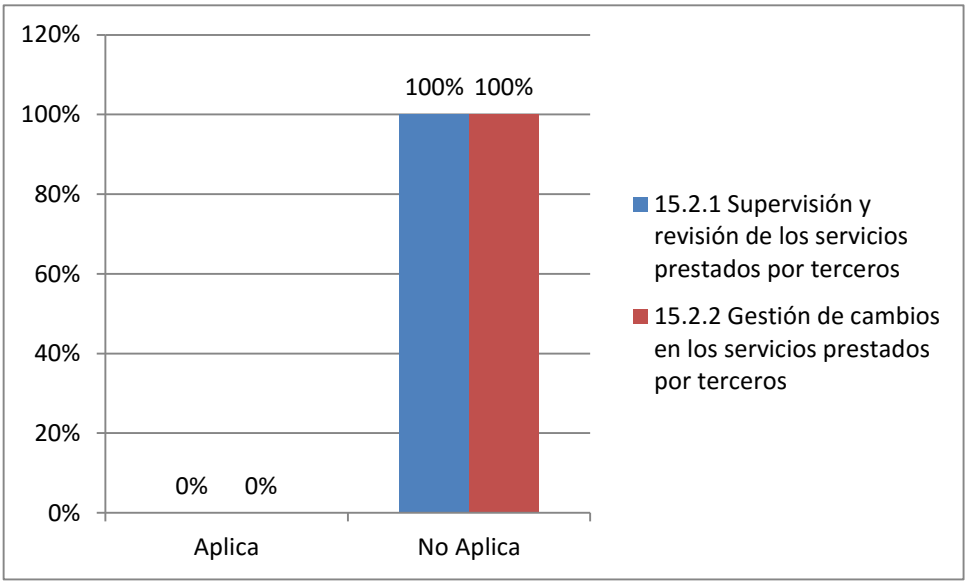

Fuente: la presente investigación – Año 2015

Para el análisis del capítulo 15 sobre seguridad de la información en las relaciones con suministradores se tuvieron en cuenta los tópicos: seguridad de la información en las relaciones con suministradores y gestión de la prestación del servicio por suministradores.

En cuanto al tema de seguridad de la información en las relaciones con suministradores se pudo denotar según la opinión del 100% de la muestra consultada que existen falencias en los ítems: política de seguridad de la información para suministradores, tratamiento del riesgo dentro de acuerdos de suministradores y cadena de suministro en tecnologías de la información y comunicaciones.

Lo anterior se evidencia en la ausencia de un plan para mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas al SI, la falta de requisitos de seguridad de la información para que cada proveedor pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización y la ausencia de acuerdos con los proveedores que incluyan los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro.

**Gráfico 30. Evaluación de la gestión de la prestación del servicio por suministradores**



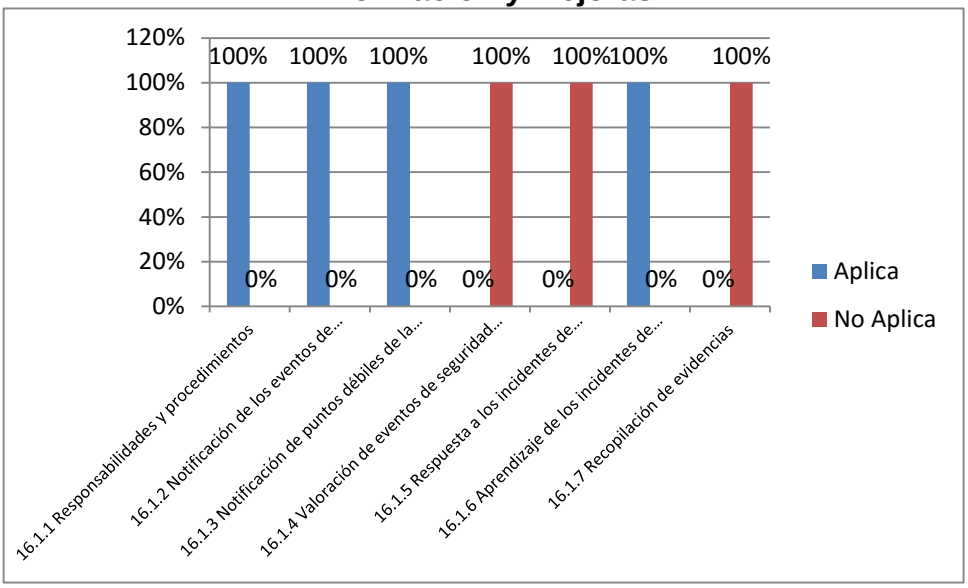

Fuente: la presente investigación – Año 2015

El 100% de la muestra encuestada considera que la gestión de la prestación del servicio por suministradores en la organización es deficiente por cuanto no se monitorean, revisan y auditan la presentación de servicios del proveedor regularmente, ni tampoco se administran adecuadamente los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos.

En tal sentido se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos.

- **Capítulo 16. Gestión de Incidentes**

**Gráfico 31. Evaluación de la gestión de incidentes de seguridad de la información y mejoras**




Fuente: la presente investigación – Año 2015

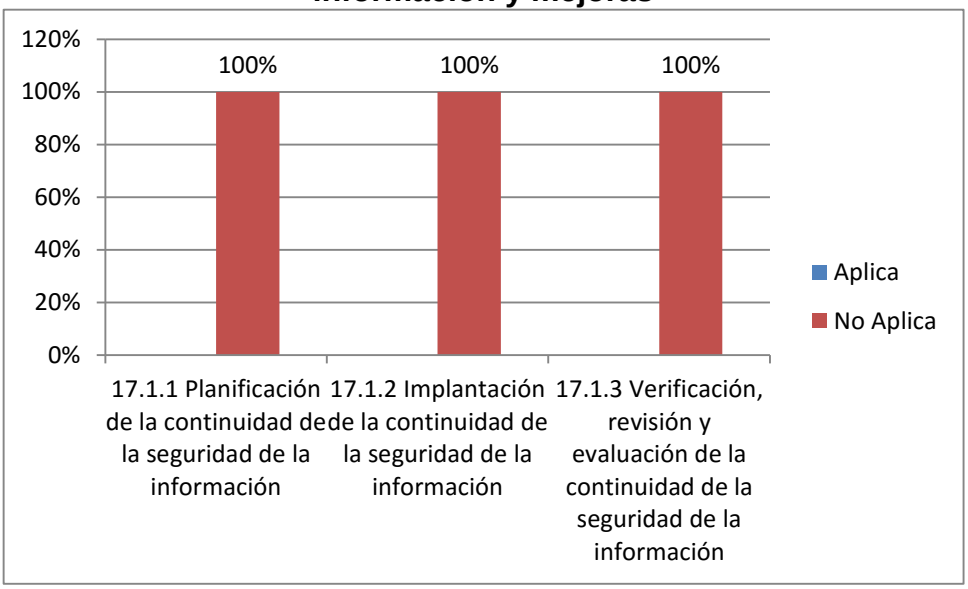
Para el análisis del capítulo 16 sobre gestión de incidentes se tuvo en cuenta el tópico: gestión de incidentes de seguridad de la información y mejoras, obteniendo que según la opinión del 100% de la muestra encuestada existen fortalezas en la gestión de aspectos como las responsabilidades y procedimientos, la notificación de los eventos de seguridad de la información, la notificación de puntos débiles de la seguridad, la respuesta a los incidentes de seguridad y el aprendizaje de los incidentes de seguridad de la información.

Frente a lo anterior se encontraron falencias en temas como la valoración de eventos de seguridad de la información y toma de decisiones y la recopilación de evidencias, situaciones que sugieren el mejoramiento de elementos como la

decisión frente a la clasificación de incidentes y la definición y aplicación de los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia de estos incidentes.

- **Capítulo 17. Aspectos de los SI en la Gestión de la Continuidad de Negocio**

**Gráfico 32. Evaluación de la gestión de incidentes de seguridad de la información y mejoras**



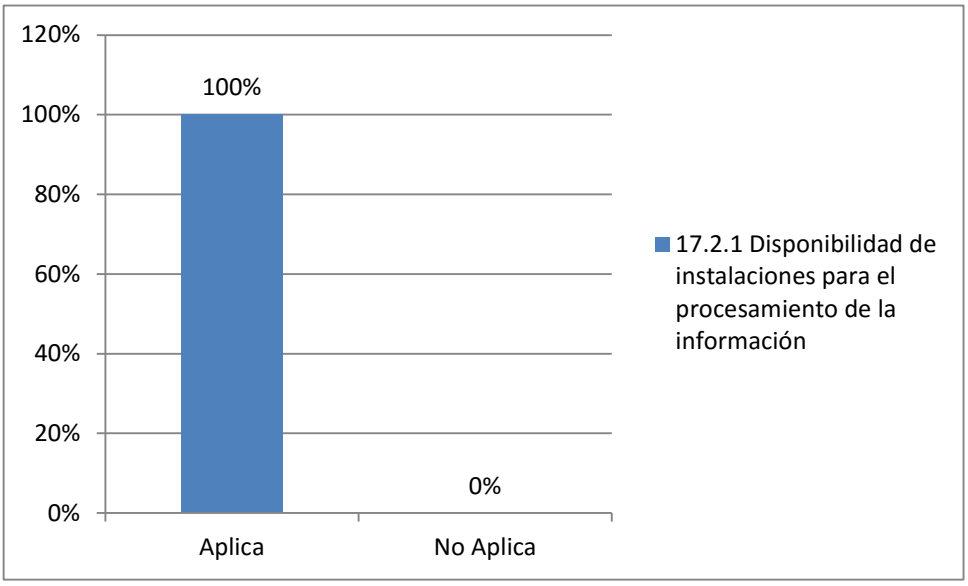

Fuente: la presente investigación – Año 2015

Para el análisis del capítulo 16 sobre Aspectos de los SI en la Gestión de la Continuidad de Negocio se tuvieron en cuenta los tópicos: Continuidad de la seguridad de la información y Redundancias.

Frente al tema de Continuidad de la seguridad de la información el 100% de la muestra consultada opinó que se deben mejorar integralmente aspectos como la planificación de la continuidad de la seguridad de la información, la implantación de la continuidad de la seguridad de la información y la verificación, revisión y evaluación de la continuidad de la seguridad de la información, pues se tienen deficiencias en cuanto a la determinación de los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre, documentación, implementación y mantenimiento de los procesos,

procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información y verificación regular de los controles de continuidad de seguridad de la información.

**Gráfico 33. Evaluación de las redundancias**

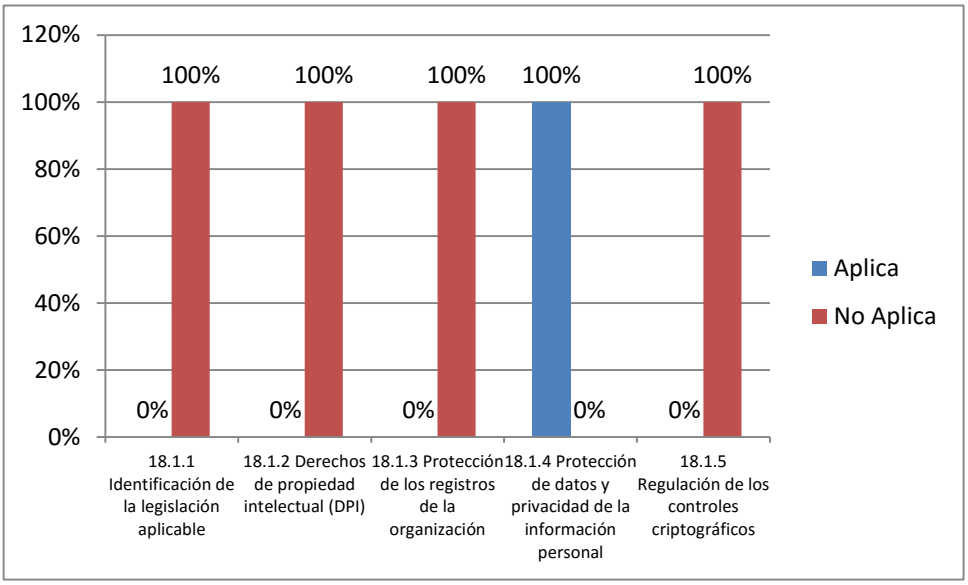



Fuente: la presente investigación – Año 2015

EL 100% de la muestra consultada consideró que existe disponibilidad de instalaciones para el procesamiento de la información lo que significa que se implementa la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad a nivel del área financiera de la SED.

- **Capítulo 18. Cumplimiento**

**Gráfico 34. Evaluación del cumplimiento de los requisitos legales y contractuales**




Fuente: la presente investigación –Año 2015

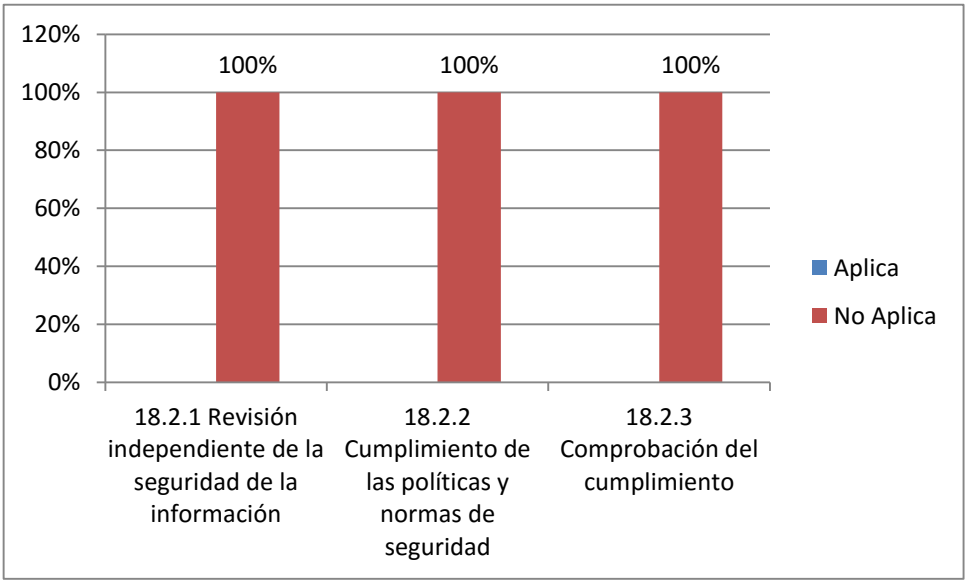
Para el análisis del capítulo 18 referido al cumplimiento se tuvieron en cuenta los tópicos: cumplimiento de los requisitos legales y contractuales y revisiones de la seguridad de la información.

En lo que tiene que ver con el cumplimiento de los requisitos legales y contractuales, el 100% de la muestra consultada resalta la gestión en cuanto a la protección de datos y privacidad de la información personal, mientras que permanece crítica frente a temas como la identificación de la legislación aplicable, los derechos de propiedad intelectual (DPI), la protección de los registros de la organización y la regulación de los controles criptográficos.

Por lo tanto es necesario mejorar en aspectos como documentar y mantiene al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos, respetar la propiedad intelectual y utilizar productos software originales, proteger los registros

del área financiera contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados y utilizar controles de cifrado de la información.

**Gráfico 35. Evaluación de las revisiones de la seguridad de la información**




Fuente: la presente investigación – Año 2015

Finalmente en el tema de revisiones de la seguridad de la información, el 100% de la muestra consultada considera que existen falencias en la revisión independiente de la seguridad de la información, el cumplimiento de las políticas y normas de seguridad y la comprobación del cumplimiento.

Situaciones que se evidencian en el confuso enfoque de la organización para la implementación y gestión de la seguridad de la información con base a revisiones independientes e intervalos planificados, el escaso seguimiento al cumplimiento del procesamiento y los procedimientos de información dentro del área y la deficiente revisión para verificar cumplimiento de los SI con las políticas y normas de seguridad.

## 4.5 PLAN DE IMPLEMENTACIÓN

Teniendo en cuenta los resultados obtenidos a través de la implementación de la lista de chequeo propuesta en el plan de auditoría, se proponen las siguientes estrategias como elementos fundamentales para una gestión de calidad en el área financiera de la SED en atención a los parámetros de la norma ISO/IEC 27002:

## Tabla 13. Plan de implementación

| Capítulo de la norma ISO/IEC 27002:2005 | Numeral de la norma ISO/IEC 27002:2005 | Estrategia | Peso (%) | Actividades | Peso (%) | Peso Ponderado (%) | Nombre del Indicador | Indicador y/o Evidencia | Responsable | Recursos | Aplicación o revisión (Tiempo) | Meta |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5. POLÍTICAS DE SEGURIDAD | 5.1 Directrices de la Dirección en seguridad de la información | Establecer las políticas que garanticen la seguridad de la información en la SED | **10** | Realizar un diagnóstico de seguridad en la información en la SED | **25** | **2,5** | Diagnóstico de seguridad en la información | Documento que contenga el Diagnóstico de seguridad en la información | Consultor Externo, Secretario de Educación, jefe de Planeación, jefe de Control Interno, Jefe de Tesorería, Jefe de Sistemas | $ 10.000.000,00 | Anual | Conocer el estado actual de seguridad en la información en la SED |
| | | | | Establecer puntos críticos de control para la seguridad de la información | **25** | **2,5** | Mapa de riesgos de seguridad en la información | Levantamiento del mapa de riesgos de seguridad en la información de la SED | | $ 10.000.000,00 | Una sola vez (con actualización anual) | Disminuir a <10% los procesos con puntos críticos de control |
| | | | | Diseñar las políticas que garanticen la seguridad de la información en la SED | **25** | **2,5** | Políticas de seguridad de la información en la SED | Documenta que contenga las políticas de seguridad de la información en la SED | | $ 10.000.000,00 | Una sola vez (con actualización anual) | Contar con unas políticas claras de seguridad de la información en la SED |
| | | | | Divulgar las políticas que garanticen la seguridad de la información en la SED | **25** | **2,5** | Eventos de divulgación | (# de socializaciones efectuadas / # de socializaciones programadas) | | $ 0,00 | Anual | 100% de ejecución en las socializaciones programadas |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 6. ASPECTOS ORGANIZATIVOS SI | 6.1 Organización interna | Establecer una estructura formal para la organización interna de los SI | **3** | Definir los roles y responsabilidades | **50** | **1,5** | Manual de funciones en el SI | Documento que contenga el manual de funciones en el SI | Jefe de sistemas, Jefe de Planeación | $ 0,00 | Una sola vez | Contar con un Manual de funciones en el SI |
| | | | | Efectuar retroalimentación con los responsables de los procesos relacionados con los SI | **50** | **1,5** | Reuniones realizadas | (# de reuniones de retroalimentación efectuadas / # de reuniones de retroalimentación efectuadas ) | Jefe de sistemas, Jefe de Planeación | $ 0,00 | Trimestral | > 90% de cumplimiento en las reuniones de retroalimentación programadas |
| | 6.2 Dispositivos para movilidad y teletrabajo | Gestionar la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones | **7** | Definir las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones. | **100** | **7** | Manual de Protocolos de seguridad contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones. | Documento que contenga el Manual de Protocolos de seguridad contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones | Consultor externo, Jefe de sistemas, Jefe de Planeación | $ 5.000.000,00 | Una sola vez | Contar con un Manual de Protocolos de seguridad contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones |
| da a los an te la co nt | | Foment | **5** | Capacitar a | **100** | **5** | Colaboradore | (# de | Consulto | $ | Anual | 100% de |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ar educación y capacitación en SI | | la totalidad de los colaboradores del área financiera de la SED en el tema de seguridad en los SI | | | s capacitados | colaboradores capacitados / Total colaboradores Del área) * 100 | r externo, Jefe de Talento humano, Jefe de Tesorería | 10.000.000,00 | | colaboradores capacitados en el tema de seguridad en los SI |
| 8. Gestión Activos | 8.1 Responsabilidad sobre los activos | Establecer protocolos para que regulen el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información | **3** | Realizar un manual que permita regular el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información | **100** | **3** | Manual de uso de activos y tratamiento de la información | Documento que contenga un Manual de uso de activos y tratamiento de la información | Jefe de Control Interno | $ 0,00 | Una sola vez | Contar con un Manual de uso de activos y tratamiento de la información |
| | 8.2 Clasificación de la informaci | Clasificar la información en | **3** | Conformar bancos de datos (Data WareHouse | **100** | **3** | Clasificación de la información | Banco de datos de información legal | Empresas proveedora de | $ 25.000.000,00 | Una sola vez | Salvaguardar la información legal, |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización | | ) para el manejo de la información legal, confidencial y crítica del área financiera de la SED | | | | Banco de datos de información con carácter confidencial<br><br>Banco de datos de información crítica para la organización (financiera) | SaaS, Jefe de Planeación, jefe de Control Interno, Jefe de Tesorería, Jefe de Sistemas | | | confidencial y crítica del área financiera de la SED mediante estrategias de Data WareHouse |
| | 8.3 Manejo de los soportes de almacenamiento | Establecer protocolos para el uso de medios extraíbles | **4** | Documentar los procedimientos para la gestión de los medios informáticos removibles (CD, USB) | **100** | **4** | Manual para el uso de medios extraíbles | Documento que contenga el manual de procedimientos para la gestión de los medios informáticos removibles (CD, USB) | Jefe de sistemas, Jefe de Tesorería | $ 0,00 | Una sola vez | Contar con un manual de procedimientos para la gestión de los medios informáticos removibles (CD, USB) |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 9. Control de Accesos | 9.2 Gestión de acceso de usuario | Gestionar adecuadamente el control de acceso para los usuarios que asigna el SI | **5** | Gestionar las altas/bajas en el registro de usuarios | **100** | **5** | altas/bajas en el registro de usuarios | (# de usuarios nuevos año actual / # usuarios nuevos año anterior ) - 1) * 100<br><br>(# de usuarios dados de baja en el SI año actual / # usuarios dados de baja en el SI año anterior ) - 1) * 100 | Jefe de sistemas , Jefe de Tesorería | $ 0,00 | Anual | Monitorear constantemente la variación anual de altas/bajas en el registro de usuarios |
| | 9.3 Responsabilidades del usuario | Gestionar el uso de información confidencial para la autenticación de los usuarios del SI | **5** | Disminuir la reasignación de usuarios por clave olvidada | **100** | **5** | Usuarios reasignados | (# de usuarios reasignados año actual / # usuarios reasignados año anterior ) - 1) * 100 | Jefe de sistemas | $ 0,00 | Mensual | Disminuir a <20% los usuarios reasignados en el SI por clave olvidada |
| 10. Cifrado | 10.1 Controles criptográficos | Implementar una política | **2,5** | Encriptar las claves de acceso a los SI | **100** | **2,5** | Claves encriptadas | # de claves de token asignadas para el | Jefe de sistemas , Jefe de Tesorerí | $ 5.000.000 ,00 | Anual | Hacer seguimiento sobre al acceso de |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | que regule el uso de controles criptográficos para la protección de la información confidencial y crítica del Área de Tesorería de la SED | | bancaria mediante el uso de tokens de la SED y tokens bancarios | | | | acceso al SI del área de Tesorería de la SED | a | | | los colaboradores del área de Tesorería de la SED frente a los SI y los portales bancarios que maneja la SED |
| 11. Seguridad física y Ambiental | 11.1 Áreas seguras | Gestionar la compra de herramientas para la protección física contra ataques maliciosos | **2,5** | Implementar herramientas de software anti-phishing para el acceso a portales bancarios | **100** | **2,5** | Uso de herramientas de software anti-phishing | (# de computadores del área de Tesorería con software anti-phishing implementado / total computadores del área) * 100 | Jefe de sistemas, Jefe de Tesorería | $ 20.000.000,00 | Anual | 100% de computadores del área de Tesorería de la SED con software anti-phishing vigente y actualizado |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12. Seguridad en la Operativa | 12.1 Responsabilidades y procedimientos de operación | Divulgar los manuales de procesos y procedimientos del área de Tesorería de la SED | **2,5** | Programar eventos para la divulgación de los manuales de procesos y procedimientos del área de Tesorería de la SED | **100** | **2,5** | Eventos de divulgación | (# de socializaciones efectuadas / # de socializaciones programadas ) | Jefe de Talento humano, Jefe de Tesorería | $ 0,00 | Anual | Conocimiento de los manuales de procesos y procedimientos por parte de los colaboradores del área de Tesorería de la SED superior al 90% |
| | 12.4 Registro de actividad y supervisión | Gestionar los eventos de actividad en los sistemas de información | **2,5** | Monitorear eventos de caída del sistemas y dificultades para su acceso | **100** | **2,5** | Caídas del sistema | (# de caídas del sistema año actual / # de caídas del sistema año anterior ) - 1) * 100 | Jefe de sistemas , Jefe de Tesorería | $ 0,00 | Anual | Disminuir hasta en un 30% adicional, las caídas del sistema con respecto al año anterior |
| | 12.6 Gestión de la vulnerabilidad técnica | Administrar adecuadamente las vulnerabilidades técnicas del SI | **2,5** | Establecer restricciones en la instalación de software y acceso a páginas web | **100** | **2,5** | Soporte técnico adicional | Índice de soporte técnico adicional para la instalación de nuevo software<br><br>Índice de intentos de acceso a páginas web | Jefe de sistemas | $ 5.000.000 ,00 | Anual | Disminuir la vulnerabilidad del sistema de información |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | restringidas | | | | |
| | 12.7 Consideraciones de las auditorías de los sistemas de información | Establecer controles periódicos de auditoría de los sistemas de información | **2,5** | Realizar periódicamente controles de auditoría a los SI | **100** | **2,5** | Controles de auditorías | (# de controles de auditoría efectuados / # de controles de auditoría programados) | Jefe de sistemas, Jefe de Control Interno | $ 0,00 | Anual | 100% de ejecución en los controles de auditoría realizados |
| 13. Seguridad en las Telecomunicaciones | 13.2 Intercambio de información con partes externas | Proteger el intercambio de información con partes externas | **5** | Promover un uso adecuado de la información enviada vía mail | **50** | **2,5** | aviso de notificación legal | Incorporar un aviso de notificación legal a la mensajería que sale de los servidores de la SED | Jefe de sistemas | $ 0,00 | Una sola vez | Procurar un buen uso de la información contenida en la mensajería de correo electrónico de la SED |
| | | | | Encriptar los correos electrónicos del área de Tesorería que contengan información confidencial o crítica para sus destinatarios | **50** | **2,5** | correos encriptados | (# de correos encriptados / total mails enviados) | Jefe de sistemas, Jefe de Tesorería | $ 0,00 | Mensual | Medir la frecuencia en el uso de correos con información confidencial o crítica |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14. Adquisición, desarrollo y Mantenimiento de los sistemas de información | 14.2 Seguridad en los procesos de desarrollo y soporte | Reafirmar la utilización de los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información | **5** | Programar jornadas no laborales para la actualización de los SI | **100** | **5** | Jornadas de actualización mensual | (# de jornadas de actualización del SI / 12) * 100 | Jefe de sistemas | $ 0,00 | Mensual | Contar con al menos 1 jornada de actualización mensual de los SI |
| 15. Relaciones con Suministradores | 15.1 Seguridad de la información en las relaciones con suministradores | Establecer políticas para el tratamiento conjunto de riesgos en los SI compartidos con | **2,5** | Establecer parámetros de seguridad para la información compartida que es recepcionada de los suministradores | **100** | **2,5** | Manual de seguridad para la información compartida | Documento que contenga el manual de seguridad para la información compartida | Jefe de sistemas | $ 0,00 | Una sola vez | Contar con un manual de seguridad para la información compartida |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | suministradores de información | | | | | | | | | | |
| | 15.2 Gestión de la prestación del servicio por suministradores | Monitorear la ejecución y el buen funcionamiento de los software en modalidad de SaaS que se encuentran en uso | **2,5** | Hacer seguimiento oportuno a la respuesta a inconsistencias y nuevos desarrollos sugeridos en los software contratados por SaaS y que se utilizan en el área | **100** | **2,5** | Deficiencias Detectadas<br><br>Nuevos Desarrollos | # de soluciones efectuadas a las deficiencias detectadas / total deficiencias<br><br># nuevos desarrollos efectuados / total desarrollos propuestos | Jefe de sistemas, Jefe de Tesorería | $ 0,00 | Anual | Verificar el cumplimiento de los suministradores de software por SaaS frente a la solución a inconsistencias y nuevos desarrollos |
| 16. Gestión de Incidentes | 16.1 Gestión de incidentes de seguridad de la información y mejoras | Evaluar los eventos de seguridad de la información y decidir su clasificación como incident | **5** | Mitigar los incidentes ocurridos en el SI mediante la toma de acciones correctivas | **100** | **5** | Acciones correctivas efectuadas en el SI | (# de acciones correctivas año actual / # de acciones correctivas a año anterior ) - 1) * 100 | Jefe de sistemas, Jefe de Tesorería, Responsable de Calidad | $ 0,00 | Anual | Disminuir en un 50% anual la toma de acciones correctivas efectuadas en el SI |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | es | | | | | | | | | | |
| | | Hacer un seguimiento regular a los incidentes ocurridos en el SI | **5** | Documentar periódicamente los incidentes ocurridos en el SI | **100** | **5** | Incidentes documentados | (# de incidentes ocurridos documentados año actual / total incidentes ocurridos año actual) | Jefe de sistemas, Jefe de Tesorería, Responsable de Calidad | $ 0,00 | Anual | Llevar registro y seguimiento a los incidentes ocurridos por año en el SI |
| 17. Aspectos de la SI en la Gestión de la Continuidad de Negocio | 17.1 Continuidad de la seguridad de la información | Planificar los eventos de crisis provocados por los SI | **5** | Diseñar un plan de crisis | **100** | **5** | Plan de crisis | Documento que contenga un plan de crisis frente a los eventos provocados por los SI | Secretario de Educación, jefe de Planeación, jefe de Control Interno, Jefe de Tesorería, Jefe de Sistemas | $ 0,00 | Una sola vez (con actualización anual) | Contar con un plan de crisis que permita afrontar los eventos provocados por los SI |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 18. Cumplimiento | 18.2 Revisiones de la seguridad de la información | Gestionar el manejo de los SI de acuerdo con los procedimientos establecidos en el área de Tesorería y la SED para tal fin | **10** | Realizar una auditoría interna acerca del manejo de los SI en términos de uso adecuado de hardware y software | **100** | **10** | Auditoría Interna sobre SI | Índice de hardware en estado de obsolescencia<br><br>Índice de software en estado de obsolescencia | Jefe de sistemas, Jefe de Tesorería | $ 0,00 | Anual | Hacer seguimiento sobre al manejo del hardware y software del área manejo de acuerdo con los procedimientos establecidos |
| **TOTAL** | | | **100** | | **100** | | | | | **$ 100.000.000** | | |

Fuente: la presente investigación – Año 2015

# 5. CONCLUSIONES

Teniendo en cuenta los resultados del plan de auditoría de sistemas planteado como elemento fundamental en la fase de recolección de información y en general la observación in situ frente al problema de investigación planteado, se llegó a las siguientes conclusiones las cuales parten del análisis de la norma ISO/IEC 27002:2005 capítulo por capítulo así:

**Capítulo 5. Políticas de Seguridad.** No se cuenta con políticas para la seguridad de la información, aprobadas por la dirección, publicadas y comunicadas a los empleados y a todas las partes externas relevantes. Lo anterior sugiere la necesidad de formular la política de seguridad del área financiera de la SED, entendiendo la importancia de la información que se maneja y el riesgo que supone no contar con claras directrices en este sentido.

**Capítulo 6. Aspectos Organizativos de los Sistemas de Información.** Con respecto a los aspectos organizativos no existe una gestión eficiente. Lo anterior se soporta en la carencia en la asignación de las responsabilidades para la seguridad de la información, deficientes políticas de segregación de tareas y escaso relacionamiento con grupos o foros de seguridad especializados entre otros aspectos.

Por su parte las políticas de organización de los sistemas de información en el área financiera de la SED en el tema de los dispositivos para movilidad y teletrabajo se encuentran en una fase temprana de estructuración y aplicación.

**Capítulo 7. Seguridad Ligada a los recursos humanos.** no existe claridad en los términos y condiciones de contratación frente al manejo de los sistemas de información que maneja la SED.

Además, se deben mejorar la totalidad de los procedimientos que se efectúan en cuanto a las acciones emprendidas durante la contratación del personal para garantizar la seguridad en la información. lo anterior teniendo en cuenta las deficiencias para aplicar la seguridad en concordancia con las políticas y los procedimientos, la falta de entrenamiento apropiado y actualizaciones regulares en políticas y procedimientos organizacionales y la inexistencia de un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad.

**Capítulo 8. Gestión de Activos.** Existen falencias en cuanto a la identificación, documentación e implantación de regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información. También se debe mejorar la manera en el que el área clasifica la información en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización y fortalecer el manejo de los soportes de almacenamiento.

**Capítulo 9. Control de accesos.** Existen deficiencias por mejorar en temas como establecer, documentar y revisar una política de control de accesos con base a las necesidades de seguridad de la Organización. Además se debe implementar un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios y fortalecer la política de control de accesos y aplicaciones mediante un procedimiento seguro de log-on y sistemas de gestión de contraseñas más interactivos y que aseguren contraseñas de calidad.

**Capítulo 10. Cifrado.** El área financiera de la SED no desarrolla e implementa una política que regule el uso de controles criptográficos para la protección de la información y tampoco se implementa una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.

**Capítulo 11. Seguridad física y Ambiental.** Es necesario diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes, así como también procedimientos para el desarrollo de trabajos y actividades en áreas seguras.

**Capítulo 12. Seguridad en la Operación.** Se encontraron debilidades en los procesos asociados a gestión del cambio y gestión de capacidades, lo que da pie a inferir que se debe mejorar en aspectos como el control de los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información y el monitoreo y ajuste en el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.

Se implementa controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios y se realizan pruebas regulares de las copias de la información, del

software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.

Sin embargo, es necesario establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios con el ánimo de proteger la información de los ordenadores del área financiera de la SED así como también implantar políticas de auditoría de sistemas claramente definidas y contextualizadas a las necesidades del área.

**Capítulo 13. Seguridad en las Telecomunicaciones.** Existen falencias en la segregación de las redes lo que quiere decir que se debe mejorar en una mejor distribución de las redes en función de los grupos de servicios, usuarios y sistemas de información así como también hay inexistencia de políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.

**Capítulo 14. Adquisición, desarrollo y Mantenimiento de los sistemas de información.** Se identifican debilidades en torno al análisis y especificación de los requisitos de seguridad y la seguridad de las comunicaciones en servicios accesibles por redes públicas, lo cual induce a pensar que se debe mejorar en aspectos como la inclusión de los requisitos relacionados con la seguridad de la información para los nuevos sistemas y la protección contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada así como también en los procedimientos de control de cambios en los sistemas, el uso de principios de ingeniería en protección de sistemas, la seguridad en entornos de desarrollo y las pruebas de aceptación.

**Capítulo 15. Relaciones con Suministradores.** Se encontraron aspectos por mejorar en cuanto a la ausencia de un plan para mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas al SI, la falta de requisitos de seguridad de la información para que cada proveedor pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización y la ausencia de acuerdos con los proveedores que incluyan los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro.

Frente a esto también se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos.

**Capítulo 16. Gestión de Incidentes.** Se encontraron falencias en temas como la valoración de eventos de seguridad de la información y toma de decisiones y la recopilación de evidencias, situaciones que sugieren el mejoramiento de elementos como la decisión frente a la clasificación de incidentes y la definición y aplicación de los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia de estos incidentes.

**Capítulo 17. Aspectos de los SI en la Gestión de la Continuidad de Negocio.** se deben mejorar integralmente aspectos como la planificación de la continuidad de la seguridad de la información, la implantación de la continuidad de la seguridad de la información y la verificación, revisión y evaluación de la continuidad de la seguridad de la información, pues se tienen deficiencias en cuanto a la determinación de los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre, documentación, implementación y mantenimiento de los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información y verificación regular de los controles de continuidad de seguridad de la información.

Frente a lo anterior existe fortaleza en cuanto a la disponibilidad de instalaciones para el procesamiento de la información lo que significa que se implementa la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad a nivel del área financiera de la SED.

**Capítulo 18. Cumplimiento.** Es necesario mejorar en aspectos como documentar y mantiene al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos, respetar la propiedad intelectual y utilizar productos software originales, proteger los registros del área financiera contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados y utilizar controles de cifrado de la información.

Además se debe fortalecer el enfoque de la organización para la implementación y gestión de la seguridad de la información con base a revisiones independientes e intervalos planificados, el escaso seguimiento al cumplimiento del procesamiento y los procedimientos de información dentro del área y la deficiente revisión para verificar cumplimiento de los SI con las políticas y normas de seguridad.

# 6. RECOMENDACIONES

Teniendo en cuenta las estrategias de acción planteadas frente a cada capítulo y numeral de la norma ISO/IEC 27002:2005, el equipo gestor del proyecto, recomienda lo siguiente:

En el tema de **políticas de seguridad**, se hace necesario establecer las políticas que garanticen la seguridad de la información en la SED, esto se logra a través de acciones como: realizar un diagnóstico de seguridad en la información en la SED, establecer puntos críticos de control para la seguridad de la información, diseñar las políticas que garanticen la seguridad de la información en la SED y divulgar las políticas que garanticen la seguridad de la información.

Por su parte, en lo que tiene que ver con los **aspectos organizativos de los sistemas de información**, se recomienda establecer una estructura formal para la organización interna de los SI, mediante actividades como definir los roles y responsabilidades y efectuar retroalimentación con los responsables de los procesos relacionados con los SI; también es necesario gestionar la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones mediante la definición de las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de este tipo de elementos.

Frente al tópico de **seguridad ligada a los recursos humanos** se hace pertinente fomentar la educación y capacitación en SI lo cual supone capacitar a la totalidad de los colaboradores del área financiera de la SED en el tema de seguridad en los SI.

En lo que tiene que ver con la **gestión de activos** se recomienda establecer protocolos para que regulen el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información, clasificar la información en relación a su valor, requisitos legales, sensibilidad y criticidad para la organización y establecer protocolos para el uso de medios extraíbles.

Con respecto al tema de **control de accesos**, se evidencia como necesario gestionar las altas/bajas en el registro de usuarios y administrar el uso de

información confidencial para la autenticación de los usuarios del SI mediante la disminución en la reasignación de usuarios por clave olvidada.
En el tema de **cifrado** se debe implementar una política que regule el uso de controles criptográficos para la protección de la información confidencial y crítica del Área de Tesorería de la SED.

Por su parte, en lo referente a **seguridad física y ambiental,** es necesario tener en cuenta la gestión en la compra de herramientas para la protección física contra ataques maliciosos en donde resulta oportuno implementar herramientas de software anti-phishing para el acceso a portales bancarios.

Frente al tema de **seguridad en la parte operativa**, se recomienda divulgar los manuales de procesos y procedimientos del área de Tesorería de la SED, gestionar los eventos de actividad en los sistemas de información, administrar adecuadamente las vulnerabilidades técnicas del SI y establecer controles periódicos de auditoría de los sistemas de información.

En el ítem de **seguridad en las telecomunicaciones**, se hace preciso proteger el intercambio de información con partes externas a través de actividades como promover un uso adecuado de la información enviada vía mail y encriptar los correos electrónicos del área de Tesorería que contengan información confidencial o crítica para sus destinatarios.

En cuanto a **adquisición, desarrollo y mantenimiento de los sistemas de información**, se recomienda reafirmar la utilización de los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.

En el tópico de **relaciones con suministradores**, es necesario establecer políticas para el tratamiento conjunto de riesgos en los SI compartidos con suministradores de información y monitorear la ejecución y el buen funcionamiento del software en modalidad de SaaS que se encuentran en uso.

En lo que tiene que ver con la **gestión de incidentes**, se recomienda evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes y hacer un seguimiento regular a los incidentes ocurridos en el SI mediante su respectiva documentación.

En los **aspectos de la SI en la gestión de la continuidad de negocio**, se deben planificar los eventos de crisis provocados por los SI mediante el diseño de un plan de crisis.

En cuanto al tópico **cumplimiento** se debe gestionar el manejo de los SI de acuerdo con los procedimientos establecidos en el área de Tesorería y la SED para tal fin, situación que se logra mediante la realización de una auditoría interna acerca del manejo de los SI en términos de uso adecuado de hardware y software.

## BIBLIOGRAFÍA


BENAVIDES RUANO, M. C. SOLARTE SOLARTE, F. N. J. MÓDULO GUÍA: RIESGOS Y CONTROL INFORMÁTICO. Pasto: Universidad Nacional Abierta y a Distancia, 2013. 98p.

ERAZO ARCINIEGAS, Andrea, MORAN BRAVO Carmen, Políticas de seguridad para el área de sistemas del instituto Colombiano de bienestar familiar regional Nariño. Pasto: I. U CESMAG. 101p.

ICONTEC. COMPENDIO: Sistema de gestión de la seguridad de la información (SGSI), Colombia, 2006. 97p.

LLERENA RIASCOS Rafael Esteban y GUERRA ERASO José Daniel. Diagnóstico del estado de los sistemas de gestión de seguridad de la información (SGSI), con la aplicación de un software, en las instituciones de educación superior de San Juan de Pasto. Pasto: I. U CESMAG, 2009. 119p.

PATIÑO ALPALA Luis Olmedo, Propuesta De Actualización, Apropiación y Aplicación de Políticas de Seguridad Informática en una Empresa Corporativa, Propolsinecor. Pasto: UNAD. 98p.

## NETGRAFÍA


ACADEMY. ¿Qué es norma ISO 27001? [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.iso27001standard.com/es/que-es-iso-27001/.

ALCALDÍA DE BOGOTÁ D.C. Ley 715 del 21 de diciembre de 2001. . [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.alcaldiabogota.gov.co.

ALCALDÍA DE BOGOTA. LEY 1213 DE 2009. . [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

ALCALDÍA DE BOGOTA. LEY 1581 DE 2012. . [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981.

ALCALDÍA DE BOGOTA. LEY 527 DE 1999. [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276.

ALTAGRACIA, Arelys. DISEÑO DE UN PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. CASO: DIRECCIÓN DE INFORMÁTICA DE LA ALCALDÍA DEL MUNICIPIO JIMÉNEZ DEL ESTADO LARA. [en línea]. [consultado el 06 de mayo de 2015]. Disponible en: http://bibcyt.ucla.edu.ve/Edocs_Bciucla/Repositorio/TGMQA76.9.A25L662011.pdf.

Real Academia Española. Diccionario de la Lengua Española. 22.a ed. [en línea]. (2001). [consultado el 02 de mayo de 2015]. Disponible en http://www.rae.es/rae.html

BLAZQUEZ, Florentino. Sociedad de la información y la educación. [en línea]. [consultado el 09 de mayo de 2015]. Disponible en http://es.calameo.com/books/0009207604661982da885.

BUITRAGO ESTRADA, Johanna Carolina; BONILLA PINEDA, Diego Hernando y MURILLO VARON, Carol Estefanie. DISEÑO DE UNA METODOLOGIA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI, EN EL SECTOR DE LABORATORIOS DE ANALISIS MICROBIOLOGICOS, BASADO EN ISO 27001. [en línea]. [consultado el 05 de mayo de 2015]. Disponible en http://repository.ean.edu.co/bitstream/handle/10882/2692/MurilloCarol2012.pdf?sequence=1.

CALAMEO. Manual de procesos y procedimientos. [en línea]. [consultado el 09 de mayo de 2015]. Disponible en: http://es.calameo.com/books/0009207604661982da885.

CONISEC. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. LINA, Andrea. Norma ISO 27000. [en línea]. [consultado el 07 de mayo de 2015]. Disponible en http://www.conisec.com/file3.html.

DNP. LINEAMIENTOS PARA LA ADMINISTRACION DE RIESGOS EN LOS PROCESOS DEL DNP. [en línea]. [consultado el 06 de mayo de 2015]. Disponible en https://colaboracion.dnp.gov.co/CDT/DNP/AR-L02%20Lineamientos%20Administracion%20Riesgos.Pu.pdf.

GERENCIE.COM Auditoría de Sistemas. [en línea]. [consultado el 06 de mayo de 2015]. Disponible en http://www.gerencie.com/tipos-de-riesgos-de-auditoria.html.

GESTION – CALIDAD.COM. La Serie ISO 27000. [en línea]. [consultado el 05 de mayo de 2015]. Disponible en http://www.gestion-calidad.com/iso-27000.html.

HERNANDEZ, Adriana. Análisis de Riesgo. [en línea]. [consultado el 09 de mayo de 2015]. Disponible en http://adrianajhdez.blogspot.com/2013/05/analisis-e-l-analisis-del-riesgo-es-un.html.

ICONTEC. COMPENDIO: Sistema de gestión de la seguridad de la información. LINA, Andrea. Norma ISO 27000. [en línea]. [consultado el 03 de mayo de 2015]. Disponible en http://www.Icontec.org.co.

INSOR. PLAN DE SEGURIDAD. [en línea]. [consultado el 08 de mayo de 2015]. Disponible en: http://www.insor.gov.co/descargar/plan_de_seguridad.pdf.

ISO 27000. El portal de ISO 27001 en Español. [en línea]. [consultado el 05 de mayo de 2015]. Disponible en http://www.iso27000.es/iso27000.html.

LINA, Andrea. Norma ISO 27000. [en línea]. [consultado el 05 de mayo de 2015]. Disponible en http://linaandrea2-mantenimientodepc.blogspot.com/2010/09/norma-iso-27000.html.

MARCOTRIGIANO, Laura. Discusión del concepto de “activo” dentro del Marco Conceptual de las Normas Internacionales de Información Financiera. [en línea]. [consultado el 09 de mayo de 2015]. Disponible en: http://www.saber.ula.ve/bitstream/123456789/34234/3/articulo5.pdf.

MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA. Ley 115 del 8 de febrero de 1994. . [en línea]. [consultado el 10 de mayo de 2015]. Disponible en: http://www.mineducacion.gov.co.

MINISTERIO DE EDUCACIÓN NACIONAL DE COLOMBIA. Proyecto de Modernización de Secretarías de Educación: Estructura. [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.modernizacionsecretarias.gov.co.

MINISTERIO DE *TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1151 del 14 de Abril de 2008. [en línea]. [consultado el 10 de mayo de 2015]. Disponible* en http://programa.gobiernoenlinea.gov.co/

REAL ACADEMIA ESPAÑOLA. Auditoría Informática. [en línea]. [consultado el 02 de mayo de 2015]. Disponible en http://www.rae.es/rae.html.

ROMERO, Luis Alfonso. Seguridad Informática Conceptos Generales. [en línea]. [consultado el 09 de mayo de 2015]. Disponible en: http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf.

SENADO DE LA REPÚBLICA. LEY 962 DE 2005. . [en línea]. [consultado el 10 de mayo de 2015]. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_0962_2005.html.

SIRE. METODOLOGÍAS DE ANÁLISIS DE RIESGO. [en línea]. [consultado el 09 de mayo de 2015]. Disponible en http://www.sire.gov.co/documents/13276/69801/A.3.4+Metodologias+AR.pdf/288b65be-c4d8-4d3f-a5f6-51942324e699

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS. Subsistema de Seguridad de la Información (SGSI). [en línea]. [consultado el 09 de mayo de 2015]. Disponible en http://comunidad.udistrital.edu.co/sigud/subsistema-de-seguridad-de-la-informacion-sgsi/

WIKIPEDIA. Auditoría de seguridad de sistemas de información. [en línea]. [consultado el 22 de mayo de 2015]. Disponible en http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3

# ANEXOS

**A**

**P sto**

| ÍTEM | | DESCRIPCIÓN | VALOR EN PESOS (CO) POR ACTIVIDAD DEL PROYECTO | | | | TOTAL |
|---|---|---|---|---|---|---|---|
| | | | Recolección de información | Visita preliminar del área de estudio | COBIT | Documentación final | |
| MATERIAL TEXTUAL | **Libros** | Documentos especificados en la bibliografía que no se encuentran disponibles de forma gratuita. | **70.000** | | | | **70.000** |
| | **Soportes físicos** | Guías, manuales, normatividad, etc. de la SED entre otros requeridos. | **20.000** | **10.000** | **10.000** | **10.000** | **50.000** |
| | **Impresiones y fotocopias** | Documentos que se requieren en formato físico para revisión o entrega. | **20000** | **5000** | **15000** | **30000** | **70.000** |
| **VIÁTICOS** | **Transporte personal y de equipos.** | Movilidad entre el lugar de estudio y el lugar de trabajo además del transporte de insumos necesarios en el proceso de auditoría. | **20.000** | **5.000** | **10.000** | **10.000** | **45.000** |
| **SERVICIOS** | **Internet** | Consumo normal de servicio de internet según el cobro del proveedor del servicio o ISP | **40.000** | **10.000** | **30.000** | **10.000** | **90.000** |
| HARDWARE | **Computadores portátiles y de escritorio** | Equipos personales de los ejecutores del proyecto. | | | | | **0** |
| | **Impresoras** | Obtención de algunos documentos en formato físico. | **100.000** | | | | **100.000** |
| | **Almacenamiento masivo (USB, DVD, Discos duros, etc.)** | Tecnologías para almacenar información como copia de | **50.000** | | | **10.000** | **60.000** |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | seguridad o transporte | | | | | |
| | **Modem** | Para conexión a internet y verificación de algunos controles de la norma ISO 27001 | **70.000** | | | | **70.000** |
| **SOFTWARE** | **Software Ofimática** | Se hará uso preferencial de software de tipo *freeware* y aplicativos web. | | | | | **0** |
| | **Gantt Project** | | | | | | **0** |
| **PERSONAL** | **Honorarios de los ejecutores del proyecto** | Al ser un proyecto académico se ofreció como tal ante la SED y no se solicitaron honorarios. | | | | | **0** |
| | **Asesoramiento externo** | Asesoramiento en momentos específicos del proyecto. | **100.000** | | **100.000** | | **200.000** |
| **IMPREVISTOS** | | 3% del total para imprevistos y gastos ocasionales. | | | | | **0** |

*Los valores de la tabla obedecen a valores aproximados máximos y son asumidos en su totalidad por los ejecutores del proyecto.
*Las asesorías consecuentes a los resultados del proyecto o aplicación de las propuestas no están incluidos en esta tabla.

| | | | | | |
|---|---|---|---|---|---|
| **TOTAL DE RUBROS Y/O ACTIVIDADES DEL PROYECTO** | **490.000** | **30.000** | **165.000** | **70.000** | **$ 755.000,00** |

**Cronograma**

| Actividad | 2015 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Abril | | | | Mayo | | | | Junio | | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Recolectar, clasificar y analizar información sobre las normas y estándares de seguridad | | | | | | | | | | | | |
| Reconocer el funcionamiento del área financiera | | | | | | | | | | | | |
| Elaborar el plan de auditoría | | | | | | | | | | | | |
| Ejecutar el plan de trabajo | | | | | | | | | | | | |
| Elaborar el informe final de los resultados obtenidos en la auditoria | | | | | | | | | | | | |
| Entregar documento guía para la implementación de un SGSI acorde a las necesidades de la SED Nariño | | | | | | | | | | | | |

**A**

## Evidencias de los resu le la lista de chequeo

| Capítulo de la norma ISO/IEC 27002:2005 | Numeral de la norma ISO/IEC 27002:2005 | Actividades a Auditar | Verificación | Calificación de Verificación | | |
|---|---|---|---|---|---|---|
| | | | | Aplica | No Aplica | En proceso |
| 5. POLÍTICAS DE SEGURIDAD | 5.1 Directrices de la Dirección en seguridad de la información | 5.1.1 Políticas para la seguridad de la información | La entidad cuenta con conjunto de políticas para la seguridad de la información, aprobado por la dirección, publicado y comunicado a los empleados así como a todas las partes externas relevantes. | | x | |
| | | 5.1.2 Revisión de las políticas para la seguridad de la información | Las políticas para la seguridad de la información se planifican y revisan con regularidad; si ocurren cambios significativos se adecuan para garantizar su idoneidad y efectividad. | | X | |
| 6. ASPECTOS ORGANIZATIVOS SI | 6.1 Organización interna | 6.1.1 Asignación de responsabilidades para la SI | Se definen y asignan claramente todas las responsabilidades para la seguridad de la información. | | X | |
| | | 6.1.2 Segregación de tareas | Se segregan tareas y áreas de responsabilidad ante posibles conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización. | | X | |
| | | 6.1.3 Contacto con las autoridades | Se mantienen los contactos apropiados con las autoridades pertinentes. | | X | |
| | | 6.1.4 Contacto con grupos de interés especial | Se mantiene el contacto con grupos o foros de seguridad especializados y asociaciones profesionales. | | X | |
| | | 6.1.5 Seguridad de la información en la gestión de proyectos | Se contempla la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización. | | X | |
| | 6.2 Dispositivos para movilidad y teletrabajo | 6.2.1 Política de uso de dispositivos para movilidad | Se establece una política formal y se adopta las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones. | | X | |
| | | 6.2.2 Teletrabajo | Se desarrolla e implanta una política y medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo. | x | | |
| 7. Seguridad Ligada a los recursos humanos | 7.1 Antes de la contratación | 7.1.1 Investigación de antecedentes | Se realizan revisiones de verificación de antecedentes de los candidatos al empleo en concordancia con las regulaciones, ética y leyes relevantes y proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. | x | | |
| | | 7.1.2 Términos y condiciones de contratación | Como parte de su obligación contractual, empleados, contratistas y terceros, se aceptan y firman los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la | | X | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | seguridad de información. | | | |
| | 7.2 Durante la contratación | 7.2.1 Responsabilidades de gestión | La Dirección requiere a empleados, contratistas y usuarios de terceras partes para aplicar la seguridad en concordancia con las políticas y los procedimientos. | | X | |
| | | 7.2.2 Concienciación, educación y capacitación en SI | Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros reciben entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo. | | X | |
| | | 7.2.3 Proceso disciplinario | Existe un proceso formal disciplinario comunicado a empleados que produzcan brechas en la seguridad. | | X | |
| | 7.3 Cese o cambio de puesto de trabajo | 7.3.1 Cese o cambio de puesto de trabajo | Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste están claramente definidas, comunicadas a empleado o contratista y asignadas efectivamente. | | X | |
| 8. Gestión Activos | 8.1 Responsabilidad sobre los activos | 8.1.1 Inventario de activos | Todos los activos están claramente identificados, confeccionando y manteniendo un inventario con los más importantes. | x | | |
| | | 8.1.2 Propiedad de los activos | Toda la información y activos del inventario asociados a los recursos para el tratamiento de la información pertenecen a una parte designada de la Organización. | x | | |
| | | 8.1.3 Uso aceptable de los activos | Se identifican, documentan e implantan regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información. | | X | |
| | | 8.1.4 Devolución de activos | Todos los empleados y usuarios de terceras partes devuelven todos los activos de la organización que estén en su posesión/responsabilidad una vez finalizado el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo. | x | | |
| | 8.2 Clasificación de la información | 8.2.1 Directrices de clasificación | La información se clasifica en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización. | | X | |
| | | 8.2.2 Etiquetado y manipulado de la información | Se desarrolla e implanta un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la organización. | x | | |
| | | 8.2.3 Manipulación de activos | Se desarrolla e implanta procedimientos para la manipulación de los activos acordes con el esquema de clasificación de la información adoptado por la organización. | x | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 8.3 Manejo de los soportes de almacenamiento | 8.3.1 Gestión de soportes extraíbles | Se establecen procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la organización. | | X | |
| | | 8.3.2 Eliminación de soportes | Se eliminan los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales. | | X | |
| | | 8.3.3 Soportes físicos en tránsito | Se protegen los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización. | | X | |
| 9. Control de Accesos | 9.1 Requisitos de negocio para el control de accesos | 9.1.1 Política de control de accesos | Se establece, documenta y revisa una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización. | | X | |
| | | 9.1.2 Control de acceso a las redes y servicios asociados | Se provee a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar. | x | | |
| | 9.2 Gestión de acceso de usuario | 9.2.1 Gestión de altas/bajas en el registro de usuarios | Existe un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso. | | X | |
| | | 9.2.2 Gestión de los derechos de acceso asignados a usuario | Se implementa un proceso formal de aprovisionamiento de accesos a los usuarios para asignar o revocar derechos de acceso a todos los tipos de usuarios y para todos los sistemas y servicios. | | X | |
| | | 9.2.3 Gestión de los derechos de acceso con privilegios especiales | La asignación y uso de derechos de acceso con privilegios especiales es restringida y controlada. | x | | |
| | | 9.2.4 Gestión de información confidencial de autenticación de usuarios | La asignación de información confidencial para la autenticación es controlada mediante un proceso de gestión controlado. | | X | |
| | | 9.2.5 Revisión de los derechos de acceso de los usuarios | Los propietarios de los activos revisan con regularidad los derechos de acceso de los usuarios. | | X | |
| | | 9.2.6 Retirada o adaptación de los derechos de acceso | Se retiran los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o son revisados en caso de cambio. | x | | |
| | 9.3 Responsabilidades del usuario | 9.3.1 Uso de información confidencial para la autenticación | Se exige a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación. | | X | |
| | 9.4 Control de acceso a sistemas y aplicaciones | 9.4.1 Restricción del acceso a la información | Se restringe el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida. | x | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 9.4.2 Procedimientos seguros de inicio de sesión | Cuando sea requerido por la política de control de accesos se controla el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on | | X | |
| | | 9.4.3 Gestión de contraseñas de usuario | Los sistemas de gestión de contraseñas son interactivos y aseguran contraseñas de calidad. | | X | |
| | | 9.4.4 Uso de herramientas de administración de sistemas | El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas está restringido y estrechamente controlado. | x | | |
| | | 9.4.5 Control de acceso al código fuente de los programas | Se restringe el acceso al código fuente de las aplicaciones software. | x | | |
| 10. Cifrado | 10.1 Controles criptográficos | 10.1.1 Política de uso de los controles criptográficos | Se desarrolla e implementa una política que regule el uso de controles criptográficos para la protección de la información. | | X | |
| | | 10.1.2 Gestión de claves | Se desarrolla e implementa una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida. | | X | |
| 11. Seguridad física y Ambiental | 11.1 Áreas seguras | 11.1.1 Perímetro de seguridad física | Se definen y utilizan perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica. | x | | |
| | | 11.1.2 Controles físicos de entrada | Las áreas seguras están protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso. | x | | |
| | | 11.1.3 Seguridad de oficinas, despachos y recursos | Se diseña y aplica un sistema de seguridad física a las oficinas, salas e instalaciones de la organización. | x | | |
| | | 11.1.4 Protección contra las amenazas externas y ambientales | Se diseña y aplica una protección física contra desastres naturales, ataques maliciosos o accidentes. | | X | |
| | | 11.1.5 El trabajo en áreas seguras | Se diseña y aplica procedimientos para el desarrollo de trabajos y actividades en áreas seguras. | | X | |
| | | 11.1.6 Áreas de acceso público, carga y descarga | Se controlan puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información. | x | | |
| | 11.2 Seguridad de los equipos | 11.2.1 Emplazamiento y protección de equipos | Los equipos son emplazados y protegidos para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado. | x | | |
| | | 11.2.2 Instalaciones de suministro | Los equipos son protegidos contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos de apoyo. | x | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 11.2.3 Seguridad del cableado | Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se protegen contra la intercepción, interferencia o posibles daños. | x | | |
| | | 11.2.4 Mantenimiento de los equipos | Los equipos se mantienen adecuadamente con el objeto de garantizar su disponibilidad e integridad continuas. | x | | |
| | | 11.2.5 Salida de activos fuera de las dependencias de la empresa | Los equipos, la información o el software no se retiran del sitio sin previa autorización. | x | | |
| | | 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones | Se aplica la seguridad a los activos requeridos para actividades fuera de las dependencias de la organización y en consideración de los distintos riesgos | x | | |
| | | 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento | Se verifican todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización. | x | | |
| | | 11.2.8 Equipo informático de usuario desatendido | Los usuarios aseguran de que los equipos no supervisados cuentan con la protección adecuada. | x | | |
| | | 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla | Se adopta una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información. | | X | |
| 12. Seguridad en la Operativa | 12.1 Responsabilidades y procedimientos de operación | 12.1.1 Documentación de procedimientos de operación | Se documentan los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten. | | X | |
| | | 12.1.2 Gestión de cambios | Se controlan los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información. | x | | |
| | | 12.1.3 Gestión de capacidades | Se monitorea y ajusta el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas. | x | | |
| | | 12.1.4 Separación de entornos de desarrollo, prueba y producción | Los entornos de desarrollo, pruebas y operacionales permanecen separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional. | | X | |
| | 12.2 Protección contra código malicioso | 12.2.1 Controles contra el código malicioso | Se implementan controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios. | x | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 12.3 Copias de seguridad | 12.3.1 Copias de seguridad de la información | Se realizan pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida. | x | | |
| | 12.4 Registro de actividad y supervisión | 12.4.1 Registro y gestión de eventos de actividad | Se producen, mantienen y revisan periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información. | | X | |
| | | 12.4.2 Protección de los registros de información | Se protegen contra posibles alteraciones y accesos no autorizados la información de los registros. | x | | |
| | | 12.4.3 Registros de actividad del administrador y operador del sistema | Se registran las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular. | x | | |
| | | 12.4.4 Sincronización de relojes | Se sincronizan los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad y en relación a una fuente de sincronización única de referencia. | | X | |
| | 12.5 Control del software en explotación | 12.5.1 Instalación del software en sistemas en producción | Se implementan procedimientos para controlar la instalación de software en sistemas operacionales. | | X | |
| | 12.6 Gestión de la vulnerabilidad técnica | 12.6.1 Gestión de las vulnerabilidades técnicas | Se obtiene información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados. | x | | |
| | | 12.6.2 Restricciones en la instalación de software | Se establece e implementa las reglas que rigen la instalación de software por parte de los usuarios. | | X | |
| | 12.7 Consideraciones de las auditorías de los sistemas de información | 12.7.1 Controles de auditoría de los sistemas de información | Se planifican los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio. | | X | |
| 13. Seguridad en las Telecomunicaciones | 13.1 Gestión de la seguridad en las redes | 13.1.1 Controles de red | Se administra y controla las redes para proteger la información en sistemas y aplicaciones. | x | | |
| | | 13.1.2 Mecanismos de seguridad asociados a servicios en red | Se identifica e incluye en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados. | x | | |
| | | 13.1.3 Segregación de redes | Se segregan las redes en función de los grupos de servicios, usuarios y sistemas de información. | | X | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 13.2 Intercambio de información con partes externas | 13.2.1 Políticas y procedimientos de intercambio de información | Existen políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación. | | X | |
| | | 13.2.2 Acuerdos de intercambio | Los acuerdos abordan la transferencia segura de información comercial entre la organización y las partes externas. | | X | |
| | | 13.2.3 Mensajería electrónica | Se protege adecuadamente la información referida en la mensajería electrónica. | | X | |
| | | 13.2.4 Acuerdos de confidencialidad y secreto | Se identifica, revisa y documenta de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información. | | X | |
| 14. Aquisición, desarrollo y Mantenimiento de los sistemas de información | 14.1 Requisitos de seguridad de los sistemas de información | 14.1.1 Análisis y especificación de los requisitos de seguridad | Los requisitos relacionados con la seguridad de la información se incluyen en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes. | | X | |
| | | 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas | La información de los servicios de aplicación que pasan a través de redes públicas se protege contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada. | | X | |
| | | 14.1.3 Protección de las transacciones por redes telemáticas | La información en transacciones de servicios de aplicación se protege para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción. | x | | |
| | 14.2 Seguridad en los procesos de desarrollo y soporte | 14.2.1 Política de desarrollo seguro de software | Se establecen y aplican reglas para el desarrollo de software y sistemas dentro de la organización. | x | | |
| | | 14.2.2 Procedimientos de control de cambios en los sistemas | En el ciclo de vida de desarrollo se hace uso de procedimientos formales de control de cambios. | | X | |
| | | 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo | Las aplicaciones críticas para el negocio se deben revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la organización. | x | | |
| | | 14.2.4 Restricciones a los cambios en los paquetes de software | Se evitan modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente. | x | | |
| | | 14.2.5 Uso de principios de ingeniería en protección de sistemas | Se establecen, documentan, mantienen y aplican los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información. | | X | |
| | | 14.2.6 Seguridad en entornos de desarrollo | La organización establece y protege adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema. | | X | |
| | | 14.2.7 Externalización del desarrollo de software | La organización supervisa y monitorea las actividades de desarrollo del sistema que se hayan externalizado. | x | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas | Se realizan pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo. | x | | |
| | | 14.2.9 Pruebas de aceptación | Se establecen programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones. | | X | |
| | 14.3 Datos de prueba | 14.3.1 Protección de los datos utilizados en prueba | Los datos de pruebas se seleccionan cuidadosamente y se deberían proteger y controlar. | | X | |
| 15. Relaciones con Suministradores | 15.1 Seguridad de la información en las relaciones con suministradores | 15.1.1 Política de seguridad de la información para suministradores | Se documentan adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas. | | X | |
| | | 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores | Se establecen todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la organización. | | X | |
| | | 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones | Los acuerdos con los proveedores incluyen los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones. | | X | |
| | 15.2 Gestión de la prestación del servicio por suministradores | 15.2.1 Supervisión y revisión de los servicios prestados por terceros | Las organizaciones monitorean, revisan y auditan la presentación de servicios del proveedor regularmente. | | X | |
| | | 15.2.2 Gestión de cambios en los servicios prestados por terceros | Se administran los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos. Se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos. | | X | |
| 16. Gestión de Incidentes | 16.1 Gestión de incidentes de seguridad de la información y mejoras | 16.1.1 Responsabilidades y procedimientos | Se establecen las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. | x | | |
| | | 16.1.2 Notificación de los eventos de seguridad de la información | Los eventos de seguridad de la información se informan lo antes posible utilizando los canales de administración adecuados. | x | | |
| | | 16.1.3 Notificación de puntos débiles de la seguridad | Se anota e informa sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la organización. | x | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones | Se evalúan los eventos de seguridad de la información y decidir su clasificación como incidentes. | | X | |
| | | 16.1.5 Respuesta a los incidentes de seguridad | Se responde ante los incidentes de seguridad de la información en atención a los procedimientos documentados. | | X | |
| | | 16.1.6 Aprendizaje de los incidentes de seguridad de la información | Se el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro. | x | | |
| | | 16.1.7 Recopilación de evidencias | Se define y aplica los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia. | | X | |
| 17. Aspectos de la SI en la Gestión de la Continuidad de Negocio | 17.1 Continuidad de la seguridad de la información | 17.1.1 Planificación de la continuidad de la seguridad de la información | La organización determina los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre. | | X | |
| | | 17.1.2 Implantación de la continuidad de la seguridad de la información | La organización establece, documenta, implementa y mantiene los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas. | | X | |
| | | 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información | La organización verifica regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas. | | X | |
| | 17.2 Redundancias | 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información | Se implementa la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad. | x | | |
| 18. Cumplimiento | 18.1 Cumplimiento de los requisitos legales y contractuales | 18.1.1 Identificación de la legislación aplicable | Se identifica, documentar y mantiene al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos. | | X | |
| | | 18.1.2 Derechos de propiedad intelectual (DPI) | Se implementa procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software originales. | | X | |
| | | 18.1.3 Protección de los registros de la organización | Los registros se protegen contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales. | | X | |
| | | 18.1.4 Protección de datos y privacidad de la información personal | Se garantiza la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan. | x | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 18.1.5 Regulación de los controles criptográficos | Se utilizan controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes. | | X | |
| | 18.2 Revisiones de la seguridad de la información | 18.2.1 Revisión independiente de la seguridad de la información | Se revisa el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la organización. | | X | |
| | | 18.2.2 Cumplimiento de las políticas y normas de seguridad | Los gerentes revisan regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente. | | X | |
| | | 18.2.3 Comprobación del cumplimiento | Los sistemas de información se revisan regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización. | | X | |
| **TOTAL** | | | | | **0** | **0** |

Fuente: la presente investigación – Año 2015