UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADOS

PROPUESTA DE UNA GUÍA DE AUDITORÍA PARA EVALUAR EL CUMPLIMIENTO DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL MINISTERIO DE EDUCACIÓN PÚBLICA, DE CONFORMIDAD CON LAS NORMAS TÉCNICAS PARA LA GESTIÓN Y EL CONTROL DE LAS TECNOLOGÍAS DE INFORMACIÓN (N-2-2007-CO-DFOE)

Trabajo Final de Investigación Aplicada sometido a la consideración de la Comisión del Programa de Estudios de Posgrados en Administración y Dirección de Empresas para optar al grado y título de Maestría Profesional en Auditoría en Tecnologías de Información

ROSIBEL RUÍZ HERNÁNDEZ

Ciudad Universitaria Rodrigo Facio, San José, Costa Rica
Junio 2013

Agradecimientos

A mis profesores, el Dr. Sergio Espinoza Guido y el MATI Andrés Casas Cruz, por su colaboración durante el desarrollo de esta práctica profesional.

Además, quiero agradecer al Auditor Interno del MEP, Lic. Harry Maynard, por darme la oportunidad de realizar la práctica profesional en la Dirección de Auditoría Interna a su cargo.

Agradezco en especial a la MATI Edna Mora Quirós, Jefa del Departamento de Auditoría de Sistemas, por su incondicional colaboración y apoyo como lectora en el desarrollo de esta práctica profesional.

El presente trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar por el grado y título de Maestría Profesional en Auditoría en Tecnologías de Información.

_____	_____
Dr. Aníbal Barquero Chacón Director Programa de Posgrado en Administración y Dirección de Empresas	**Dr. Sergio Espinoza Guido** Profesor Tutor
_____	_____
MATI Andrés Casas Cruz Lector	**MATI Edna Mora Quirós** Lectora

_____

Rosibel Ruiz Hernández
Sustentante

Tabla de contenido

Índice de tablas

Índice de fíguras

Resumen

Esta práctica profesional se desarrolló en la Dirección de Auditoría Interna del Ministerio de Educación Pública y tiene como finalidad proponer una guía de auditoría para evaluar la gestión de la seguridad de la información de conformidad con las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE).

El Capítulo I desarrolla y establece el alcance, las limitaciones, los objetivos, la operacionalidad de las variables y la metodología utilizada en este estudio.

El Capítulo II plasma el detalle de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información. Se discute algunos lineamientos generales en torno a la seguridad y se describe el entorno organizacional del Ministerio de Educación Pública y su Dirección de Auditoría Interna.

La propuesta de guía de auditoría se presenta en el Capítulo III, en el cual se diseña un Plan General de Auditoría para evaluar la implementación de la norma 1.4 Gestión de la Seguridad de la Información, además se proponen 10 instrumentos que guían al auditor en el desarrollo de su trabajo.

El Capítulo IV plantea las conclusiones de haber desarrollado la práctica profesional, en particular el hecho de que este estudio constituye un aporte a la mejora continua de la Dirección de Auditoría Interna.

Índice de abreviaturas

AI	Adquirir e Implementar.
CGR	Contraloría General de la República.
COBIT	*Control Objective for Information and Related Technologies.*
DAI	Dirección de Auditoría Interna.
DAS	Departamento de Auditoría de Sistemas.
DE	Decreto ejecutivo.
DFOE	División de Fiscalización Operativa y Evaluativa.
DS	Entregar y dar Soporte.
INFOSEC	*National Information Systems Security (INFOSEC) Glosary.*
ISO/IEC	*International Organization for Standardization* e *International Electrotechnical Commission.*
ME	Monitorear y Evaluar.
MEP	Ministerio de Educación Pública.
NT	Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE).
OECD	*Organization for Economic Co-operation and Development.*
PDCA	*Plan–Do–Check–Act*.
PMBOK	*Project Management Body of Knowledge.*
PO	Planear y Organizar.
PROMECE	Programa Mejoramiento la Calidad Educativa.
SEVRI	Sistema Específico de Valoración de Riesgo Institucional.
SGSI	Sistema de Gestión de Seguridad de Información.
TI	Tecnologías de información, conjunto de tecnologías dedicadas al manejo de la información organizacional. Término genérico que incluye los recursos de: información, *software*, infraestructura y personas relacionadas.
TIC	Tecnología de Información y comunicación.
TICS	Tecnologías de Información y comunicaciones.

CAPÍTULO I: TEMA DE LA PRÁCTICA PROFESIONAL

El presente capítulo tiene como objetivo introducir el tema de este estudio, los alcances, las limitaciones, los objetivos, la operacionalidad de las variables y la metodología utilizada.

1.1 Título

El tema de este trabajo final de graduación es:

> *Propuesta de una Guía de Auditoría para Evaluar el Cumplimiento de la Gestión de la Seguridad de la Información en el Ministerio de Educación Pública, de Conformidad con las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE).*

1.2 Introducción

Actualmente, cada vez más organizaciones han incorporado las tecnologías de información en su gestión, por las múltiples ventajas que pueden obtener. Es claro, que el uso de las tecnologías conlleva a la aparición de nuevas amenazas, por lo que hay que implementar mecanismos y procedimientos para salvaguardar la integridad y seguridad de los sistemas y de la información.

De igual manera, el uso de las tecnologías de información en el Sector Público costarricense se ha convertido en un instrumento esencial en la prestación de los servicios estatales, representando inversiones importantes en el presupuesto del Estado, así como la exposición a posibles amenazas.

Ante este panorama, la Contraloría General de la República (CGR) emitió el Manual sobre Normas Técnicas de Control Interno relativas a los Sistemas de Información Computadorizados en el año 1996, en La Gaceta N° 24 del 2/02/96. Posteriormente, este manual fue derogado con la promulgación de las Normas Técnicas para la

Gestión y el Control de las Tecnologías de Información (NT), publicado en La Gaceta N°119 del 21/06/07.

La gestión y el control de las tecnologías de información en el Sector Público son sujetos de fiscalización, por lo que se solicitó la colaboración a la Dirección de Auditoría Interna (DAI) del Ministerio de Educación Pública (MEP) para realizar la práctica profesional de la Maestría en Auditoría en Tecnologías de Información, obteniendo su aprobación para analizar las normas referentes a la gestión de la seguridad de la información.

La información se ha convertido en uno de los activos más importantes, tanto para el MEP como para las organizaciones, por lo que es necesario velar por su seguridad.

Cabe indicar que la DAI fue creada mediante Decreto Ejecutivo N° 19994 del 26/10/90 pero fue hasta 1999 cuando se le asignaron las plazas, entre ellas las de Auditor Interno y Subauditor Interno y se estableció como actividad presupuestaria. Actualmente su organización está regulada por el Decreto Ejecutivo N°34427 que establece la siguiente estructura:

> *a) La jefatura de la Auditoría Interna, integrada por el Auditor Interno y el Subauditor Interno,*
> *b) El Departamento de Auditoría Administrativa,*
> *c) El Departamento de Auditoría de Programas,*
> *d) El Departamento de Auditoría de Sistemas,*
> *e) El Departamento de Auditorías Regionales,*
> *f) El Departamento Legal, y*
> *g) La Unidad de Documentación Interna y Legalización de Libros.*

Según la estructura cada departamento está a cargo de un Jefe de Departamento y la unidad de documentación y legalización a cargo de la jefatura de la Auditoría Interna, no obstante la DAI está a la espera de la publicación del decreto ejecutivo donde se crean los Departamento de Seguimiento y Control y el Departamento de Denuncias, los cuales a mayo del 2013 se encuentran en funcionamiento.

1.3 Alcances y limitaciones

La propuesta de guía de auditoría ha sido desarrollada entre setiembre de 2012 y mayo de 2013, de conformidad con la norma 1.4 del Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE).

Para el diseño del guía de auditoría se va a utilizar el Manual de Normas Generales de Auditoría para el Sector Público (M-2-2006-CO-DFOE), que establece una base normativa común y actualizada para el ejercicio en nuestro país de la auditoría en el sector público y el Manual de Normas y Políticas de la Auditoría Interna de la DAI, vigente al 31 de octubre del 2012.

También, se va a considerar la reglamentación interna emitida por el MEP, referente al proceso de implementación de dichas normas y algunas buenas prácticas como las Normas Internacionales de Auditoría, COBIT, ISO/IEC 27001 y ISO/IEC 27002, entre otras.

La guía de auditoría que se proponga no va a ser aplicada, para no exponer al MEP a ningún riesgo, ya que existe la posibilidad de que terceros utilicen los posibles hallazgos en su perjuicio, por lo que debe ser una autoridad competente como la DAI la que evalué el cumplimiento de dicha normativa.

Entonces, de las etapas del proceso de la auditoría solo se va a desarrollar la fase de planificación para el desarrollo de la guía.

1.4 Objetivos del trabajo

1.4.1 Objetivo general

Proponer una guía de auditoría para evaluar el cumplimiento de las normas de la gestión de la seguridad de la información, mediante la revisión y análisis de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información y la reglamentación interna del MEP, con el fin facilitar la labor de fiscalización de la DAI.

1.4.2 Objetivos específicos

1) Proponer la planificación de la auditoría de gestión de la seguridad de la información, considerando la Normas Técnicas para la Gestión y el Control de las Tecnologías de Información y la reglamentación interna del MEP.
2) Proponer una guía con instrumentos de auditoría para evaluar las normas de gestión de la seguridad de la información, establecidas en el numeral 1.4 de la Normas Técnicas para la Gestión y el Control de las Tecnologías de Información.
3) Incluir en los instrumentos los elementos básicos de seguridad que se deben observar, con base en la normativa aplicable.
4) Establecer las conclusiones de haber realizado la guía de auditoría.

1.5 Operacionalidad de las variables

La operacionalidad de las variables se constituye como uno de los aspectos más importantes en esta fase de la investigación ya que por medio de esta se comprende mejor los conceptos y otros elementos que intervienen en el problema por investigar.

Uno de los conceptos fundamentales es el de las NT (2007), el cual establece las directrices de control que deben ser observadas como parte de la gestión institucional que se apoya en las Tecnologías de Información. Dicha norma establece, en cuanto a la Gestión de la Seguridad, que *"La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales."*[1]

El plan de trabajo que se va a utilizar corresponde a la fase de planeación de la auditoría, establecida en el Manual de Normas Generales de Auditoría para el Sector Público (M-2-2006-CO-DFOE), que indica que toda auditoría debe ser planificada de manera que sus objetivos sean alcanzados; que el plan general debe indicar los objetivos, la naturaleza, alcance, oportunidad, plazo de los procedimientos; los elementos de coordinación, dirección, supervisión, revisión requeridos; los recursos para el desarrollo del trabajo, además debe considerar los siguientes aspectos:

> *a) Comprensión de las actividades de la entidad.*
> *b) Comprensión del sistema de control interno de la entidad y los resultados de la autoevaluación de ese sistema.*
> *c) Los resultados de la valoración del riesgo institucional.*
> *d) Los objetivos planteados en el estudio de auditoría por realizar.*[2]

Otra variable por estudiar es la seguridad de la información, la cual según la *International Organization for Standardization* se define como "*Preservación de confidencialidad, integración y disponibilidad de la información; además también*

---

[1] CGR. (N-2-2007-CO-DFOE). *Normas Técnicas para la Gestión y el Control de las Tecnologías de Información*. (Norma 1.4).
[2] CGR. (M-2-2006-CO-DFOE). *Manual de Normas Generales de Auditoría para el Sector Público* (Norma 203, 05).

puede involucrar otra propiedades como autenticidad, responsabilidad, no-repudiación y confiabilidad."[3] Asimismo, se va a citar el punto de vista de otros autores sobre los diferentes conceptos entorno a la seguridad de la información.

También, para efecto del desarrollo de la guía de auditoría se considera las NT (2007), evaluando el marco de seguridad de la información, la seguridad física y ambiental, la seguridad en las operaciones y comunicaciones, la seguridad en el control de accesos, seguridad en la implementación y mantenimiento de *software* e infraestructura de tecnológica y la seguridad en la continuidad de los servicios de TI.

1.6 Metodología

La metodología que se emplea en esta práctica profesional está sujeta a la investigación documental, la que se apoya en fuentes de carácter documental, tales como leyes, reglamentos, libros y tesis. Esta etapa implica la recolección, síntesis, organización y comprensión de la información, correspondientes fundamentalmente a la normativa emitida en relación con la gestión de la seguridad de la información, tales como manuales, directrices, reglamentos, circulares y estándares internaciones; los cuales van a ser analizados para establecer los criterios de la guía de auditoría.

La guía de auditoría que se va a proponer utiliza la metodología establecida en el Manual de Normas Generales de Auditoría para el Sector Público (M-2-2006-CO-DFOE), aprobado mediante Resolución del Despacho de la Contraloría General de la República, N° R-CO-94-2006 del 17/11/06 y publicada en La Gaceta N° 236 del 8/12/06. Dicha normativa establece estándares mínimos para el ejercicio del proceso de auditoría en el sector público, de manera uniforme, competente, íntegra, objetiva e independiente, la cual tiene el propósito de promover un mejoramiento continuo y asegurar razonablemente la calidad y productos de dichas auditorías.

---

[3] ISO/IEC 27002:2005. *Information technology - Security techniques - Code of practice for information security management*. USA.

Para diseñar la guía de auditoría es necesario tener un entendimiento de la organización y los procesos que realiza, por lo que se va utilizar la entrevista como instrumento para recolectar información, dado que es una forma específica de interacción social que permite que el auditor recoja más información y más estructurada que la proporcionada por otros medios.

Con la aplicación de la entrevista, se esperar obtener un conocimiento general del MEP, así como los procedimientos en torno a la gestión de la seguridad de la información, por lo que algunas preguntas por considerar son las que se detallan a continuación:

1) ¿Cuál es estructura orgánica del MEP?
2) ¿Cuáles son los resultados de la última evaluación del SEVRI?
3) ¿Existen políticas y procedimientos formalmente establecidos en relación con la gestión de la seguridad de la información?
4) ¿Cuál es el porcentaje de implementación de las NT (2007)?
5) ¿Cuál es la normativa interna que ha emitido el MEP en relación con las NT (2007)?
6) ¿Cuál ha sido el proceso de capacitación de los funcionarios sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI?
7) ¿Existen controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas?
8) ¿Existen políticas, reglas y procedimientos relacionados con el acceso a la información, al *software* de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación?

La información que se recopile en las entrevistas, va a ser analizada y a servir de base para desarrollar la guía con los instrumentos de auditoría.

CAPÍTULO II: UBICACIÓN DEL TEMA EN EL CONTEXTO

El este capítulo se describen los conceptos relacionados con las NT (2007), así como algunos lineamientos generales de seguridad, información, estándares internacionales y finalmente describe la organización del MEP, su entorno y como la TIC se han integrado en sus procesos cotidianos.

2.1 Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)

Las NT (2007) es el marco normativo establecido para la CGR, el cual establece:

> *(…) los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios públicos, representando inversiones importantes en el presupuesto del Estado.*
> *(…) de acatamiento obligatorio para la Contraloría General de la República y las instituciones y órganos sujetos a su fiscalización, excluyendo a las instituciones de menor tamaño, (…)*
> *(…) que la Administración contará con dos años a partir de su entrada en vigencia para cumplir con lo regulado en esta normativa, lapso en el cual, dentro de los primeros seis meses, deberá planificar las actividades necesarias para lograr una implementación efectiva y controlada de lo establecido en dicha normativa*[4]*.*

Tales normas pretenden establecer un marco de control y procuran una mejor gestión de las TI, están estructuradas por capítulos: el Capítulo I hace referencia a las *"Normas de aplicación general"*, el Capítulo II corresponde a la *"Planificación y organización"*, el Capítulo III se enfoca en la *"Implementación de tecnologías de información"*, el Capítulo IV corresponde a las normas de "*Prestación de servicios y mantenimiento"* y finalmente el Capítulo IV se refiere al *"Seguimiento"*.

Cabe señalar que estos criterios de control referentes a las TI han sido incorporados en las Normas de Control Interno para el Sector Público de la siguiente forma:

---

[4] CGR. (N-2-2007-CO-DFOE). *Normas Técnicas para la Gestión y el Control de las Tecnologías de Información.* (Art. 1 al 7).

> *5.9 Tecnologías de Información. El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. Para ello deben observar la normativa relacionada con las tecnologías de información, emitida por la CGR.*[5]

Además, de conformidad con lo establecido en la Ley de Control Interno, N°8292 (2005) el jerarca y los titulares subordinados como responsables de esa gestión, deben establecer, mantener, evaluar y perfeccionar ese marco de control interno, así las cosas, en todas las instituciones del Estado deben existir políticas, reglamentos y manuales relativos a la administración de las TI.

2.1.1 Normas de gestión de la seguridad de la información

Las NT (2007), en el numeral 1.4, establecen que la gestión de la seguridad de la información es parte del conjunto de normas de aplicación general y en lo que nos interesa señala que *"La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales."*[6]

La norma se refiere a que la Administración debe enfocar sus esfuerzos en documentar e implementar una política de seguridad de la información y los procedimientos correspondientes con los recursos necesarios para tal fin. Además, señala que la Administración debe establecer medidas de seguridad como las siguientes:

> *- El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.*
> *- El manejo de la documentación.*
> *- La terminación normal de contratos, su rescisión o resolución.*
> *- La salud y seguridad del personal.*[7]

---

[5] CGR. (N-2-2009-CO-2009). *Normas de Control Interno para el Sector Público*. (Norma N° 5.9).
[6] CGR. (2007). Op. cit. (Norma 1.4).
[7] Ídem.

No obstante, debe mantener una proporción razonable entre su costo y los riesgos asociados.

La gestión de la seguridad está comprendida en siete normas que a continuación se enlistan y se hace una breve descripción.

a) Implementación de un marco de seguridad de la información

Norma establecida en el numeral 1.4.1 de la NT (2007), la cual señala que la organización debe implementar un marco de seguridad de la información, respaldado en un marco metodológico, con una clasificación de los recursos de TI, el nivel de riesgo, su identificación y su evaluación, así como la implementación de un plan para determinar las medidas de seguridad, su impacto y la capacitación al personal.

b) Compromiso del personal con la seguridad de la información

Norma establecida en el numeral 1.4.2 de las NT (2007), la cual busca reducir el riesgo humano, robo, fraude o uso inadecuado de los recursos de TI, así que se requiere que el personal de la organización conozca y esté comprometido con las normas de seguridad y confidencialidad.

Para el cumplimiento de esta norma se ha encomendado al jerarca las siguientes acciones tendientes a apoyar el compromiso del personal con la seguridad de la información:

> *a) Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.*
> *b) Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.*
> *c) Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos.*[8]

[8] CGR. (2007). Op. cit. (Norma 1.4.2).

c) Seguridad física y ambiental

Norma establecida en el numeral 1.4.3 de las NT (2007), la cual dice que le corresponde a la organización la protección de los recursos de TI, mediante el establecimiento de políticas de seguridad y un adecuado análisis de riesgos para establecer un ambiente físico seguro y controlado. Dicha norma enlista las siguientes consideraciones que debe tomar la organización para lograr la protección de los recursos de TI:

> *a) Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.*
> *b) La ubicación física segura de los recursos de TI.*
> *c) El ingreso y salida de equipos de la organización.*
> *d) El debido control de los servicios de mantenimiento.*
> *e) Los controles para el desecho y reutilización de recursos de TI.*
> *f) La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas.*
> *g) El acceso de terceros.*
> *h) Los riesgos asociados con el ambiente.*[9]

d) Seguridad en las operaciones y comunicaciones

Norma establecida en el numeral 1.4.4 de las NT (2007), la cual tiene el objetivo de que la organización implemente las medidas de seguridad relacionadas con las operaciones de los recursos de TI y las comunicaciones, que ayuden a minimizar los riesgos de fallas, así como proteger la integridad del *software* y de la información.

Señala la citada norma, que para su cumplimiento la organización debe concentrar sus esfuerzos en los siguientes aspectos:

> *a) Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.*
> *b) Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.*

---

[9] CGR. (2007). Op. cit. (Norma 1.4.3).

c) Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus.[10]

e) Control de acceso

Norma establecida en el numeral 1.4.5 de las NT (2007), la cual señala que la organización es la responsable de proteger la información de los accesos no autorizados, además, establece las siguientes acciones que debe implementar la organización para controlar el acceso de la información:

a) Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.
b) Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.
c) Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.
Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.
d) Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.
e) Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.
f) Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.
i) Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.
k) Manejar de manera restringida y controlada la información sobre la seguridad de las TI.[11]

f) Seguridad en la implementación y mantenimiento de *software* e infraestructura tecnológica

Norma establecida en el numeral 1.4.6 de las NT (2007), la cual centra en los procesos de implementación y mantenimiento de *software* e infraestructura, además,

[10] CGR. (2007). Op. cit. (Norma 1.4.4).
[11] CGR. (2007). Op. cit. (Norma 1.4.5).

señala que a la organización le corresponde velar su integridad, evitando el acceso no autorizado así como la pérdida de información. Para el cumplimiento de dicha norma la Administración debe cumplir las siguientes acciones:

> *a) Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.*
> *b) Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.*
> *c) Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.*
> *d) Controlar el acceso a los programas fuente y a los datos de prueba.*[12]

h) Continuidad de los servicios de TI

Norma establecida en el numeral 1.4.7 de las NT (2007), la cual se refiere a la continuidad de los procesos de TI, por lo que la organización debe velar porque sus usuarios no se vean afectados significativamente por la interrupción. Además, señala la norma citada que la organización debe realizar acciones preventivas y correctivas, a mediano y largo plazo para asegurar la continuidad de los servicios de TI, así como realizar una evaluación de los recursos de TI, para determinar su nivel de riesgo, impacto y probabilidad de ocurrencia.

2.2 Lineamientos generales de la seguridad

El siguiente apartado hace revisión sucinta de algunas definiciones de seguridad, de COBIT 4.1, *Control Objetive for Information and Related Technologies,* el cual es un marco aceptado internacionalmente como una buena práctica para el control de la información, para el control de la TI y los riesgos que conllevan y la serie de normas ISO/IEC 27000 creadas por la *International Organization for Standardization* y por la *International Electrotechnical Commission (ISO/IEC).*

[12] CGR. (2007). Op. cit. (Norma 1.4.6).

2.2.1 Definiciones

Respecto a la seguridad de las tecnologías de información, hay una gran variedad de definiciones, desde seguridad informática, de sistemas de información, seguridad física y lógica, seguridad de redes, seguridad base de datos, entre otras, por lo que a continuación se hace un pequeño extracto de algunas definiciones propuestas por algunos autores.

El estándar internacional ISO/IEC 27002:2005, define la seguridad de la información como "*Preservación de confidencialidad, integración y disponibilidad de la información; además también puede involucrar otra propiedades como autenticidad, responsabilidad, no-repudiación y confiabilidad.*"[13]

Tupia (2010) define la información como *"el conjunto de ideas que aportan el significado de hechos o conceptos y que pueden manifestarse a través del lenguaje hablado o escrito o por medio del empleo de símbolos y códigos."*[14] También, señala que existen algunas características de la información relacionadas con la seguridad, tales como la integridad, confidencialidad, disponibilidad, autenticidad y no repudio, adaptabilidad, las cuales las define como:

> *1.3.1.1 Integridad*
> *La información debe estar protegida contra modificaciones no autorizadas. La integridad es la garantía de que los datos sean correctos y de la completitud de la información.*
> *1.3.1.2 Confidencialidad*
> *Cosiste en que la información sea apreciada, manipulada o difundida por aquellas personas que tengan derecho a conocerla. Es garantía de que la información llegue a las personas autorizadas.*
> *1.3.1.3 Disponibilidad*
> *Esta característica se refiere a que la información se puede utilizar cuando se la necesite. Garantía de que los servicios ofrecidos por el negocio, puedan operar y ser usados cuando sea preciso. Actualmente se está considerando como parte de la disponibilidad, la rapidez con que se pueden ofrecer servicios o realizar transacciones, dado que el costo de oportunidad es fundamental en la teoría de negocios moderna.*
> *1.3.1.4 Autenticidad y no repudio*

---

[13] *International Organization for Standardization*. ISO/IEC 27002:2005. *Information technology - Security techniques - Code of practice for information security management.* USA (Apartado 2.5).
[14] Tupía, M. (2010). *Administración de la Seguridad de Información*. Lima: GRAFICAR. (Pág. 19).

> *Está referido a las operaciones de negocio y los intercambio de información entre distintas ubicaciones. Se entiende como la garantía de que, quien se hace responsable por una información, transacción o presentación de servicios ante una contraparte, sea quien dice ser. El concepto de no repudio por su parte, es la aceptación de la transacción realizada.*
> *1.3.15 Auditabilidad*
> *Garantía de que en todo momento es posible identificar el origen (autor) de la transacción/operación, la fecha de realización y los medios empleados para la misma.*[15]

Igualmente, Tupia (2010) define el concepto de de seguridad como "*la ausencia de riesgos en determinados entornos, sean éstos humanos o empresariales" y* seguridad de la información como *"el conjunto de procesos y actividades que permiten mantener libre de peligros y daños por accidentes o ataque a los activos de información que forman parte de una organización"*[16]*.*

Otros autores, como Gómez y Suárez (2009), definen la seguridad informática como:

> *(…) cualquier medida que implica la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipo o bloquear el acceso de usuarios autorizados al sistema.*[17]

Además, cita la definición propuesta por INFOSEC *Glossary* 2000: "*Seguridad informática son las medidas y controles que aseguran la confidencialidad, integridad y la disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican."*[18]

La seguridad de los sistemas de información, para Piattini (2001), es *"la doctrina que trata de los riesgos informáticos o creados por la informática, entonces la auditoría es*

---

[15] Tupía M. (2010). Op. cit. (Pág. 20).
[16] Tupía M. (2010). Op. cit. (Pág. 21).
[17] Gómez A. y Suárez C. (2009). *Sistemas de Información: Herramienta práctica para la gestión.* 3 Edición. México D.F. Alfaomega Grupo Editor. (Pág. 228).
[18] Ídem.

una de las figuras involucradas en este proceso de protección y preservación de la información y de sus medios de procesos."[19]

Finalmente, Muñoz (2002) define los siguientes conceptos relacionados con la seguridad que es importante conocer:

> ***Seguridad física***
> *Es todo lo relacionado con la seguridad y salvaguarda de los bienes tangibles de los sistemas computacionales de la empresas, tales como el hardware, periféricos y equipos asociados, las instalaciones eléctricas, las instalaciones de comunicación y de datos, las construcciones, el mobiliario y equipo de oficina, así como la protección a los accesos al centro de sistematización. En sí, es todo lo relacionado con la seguridad, la prevención de riesgo y protección de los recursos físicos informáticos de la empresa.*
> ***Seguridad lógica***
> *Es todo lo relacionado con la seguridad de los bienes intangibles de los centros informático, tales como software (aplicaciones, sistemas operativos y lenguajes), así como lo relacionado con los métodos y procedimientos de operación, los niveles de acceso a los sistemas y programas institucionales, el uso de contraseñas, los privilegios y restricciones de los usuarios, la protección de los archivos e información de la empresa y las medidas y programas para prevenir y erradicar cualquier virus informático. En sí, todo lo relacionado con las medida de seguridad, protección y forma de accesos a los archivo e información del sistema.*
> ***Seguridad de las bases de datos***
> *Es la protección específica de la información que se maneja en las áreas de sistemas de la empresas, ya sea a través de las medidas de seguridad y control que limiten el acceso y uso de esa información, o mediante sus respaldos periódicos con el fin de mantener su confidencialidad y provenir las alteraciones, descuido, robos y otros actos delictivos que afecten su manejo.*
> ***Seguridad en la operación***
> *Se refiere a la seguridad en la operación de los sistemas computacionales en cuanto a su acceso y aprovechamiento por parte del personal informático y de los usuarios, al acceso a la información y los programas institucionales, a la forma de proteger la operación de los equipos, los archivos y programas, así como las instalaciones, mobiliario, etcétera.*
> ***Seguridad del personal de informática***
> *Se refiere a las seguridad y protección de los operadores, analistas, programadores y demás personal que está en contacto directo con el sistema, así como a la seguridad de los beneficiaros de la información.*
> ***Seguridad de las telecomunicaciones***
> *Es todo lo relacionado con la seguridad y protección de los niveles de acceso, privilegios, recepción y envío de información por medio del sistema de cómputo, protocolos, software, equipos e instalaciones que permiten la comunicación y transmisión de la información en la empresa, etcétera.*
> ***Seguridad en las redes***

[19] Piattini, M. y Navarro, E. (2001). *Auditoria Informática, un enfoque práctico*. 2 Edición Ampliada y Revisada. México D.F. Alfaomega Grupo Editor. (Pág. 46).

Es todo lo relacionado con la seguridad y control de contingencias para la protección adecuada de los sistemas de redes de cómputo, en cuanto a las salvaguarda de información y datos de las redes la seguridad en el acceso a los sistemas computacionales, a la información y a los programas del sistema, así como la protección de accesos físicos, del mobiliario, del equipo y de los usuarios de los sistemas. Incluyendo el respaldo de la información y los privilegios de accesos a sistemas, información y programas.[20]

2.2.2 COBIT 4.1, DS5 Garantizar la seguridad de los sistemas

Como parte de las buenas prácticas en el marco del Gobierno de las TI, se encuentra la última versión liberada de COBIT 4.1[21], la cual tiene una alineación entre sus procesos y las disposiciones emitidas por la CGR en las NT (2007). En la siguiente tabla se muestra tal alineación para la norma de la 1.4 Gestión de la Seguridad de la Información.

Tabla 1: Asociación lineamiento de las normas técnicas de la CGR con procesos del marco de referencia COBIT

Norma 1.4 Gestión de la seguridad de la información	Procesos asociado de COBIT
1.4.1 Implementación de un marco de seguridad de la información.	DS 5 Garantizar la seguridad de los sistemas.
1.4.2 Compromiso del personal con la seguridad de la información.	DS 5 Garantizar la seguridad de los sistemas.
1.4.3 Seguridad física y ambiental.	DS 12 Administrar el ambiente físico.
1.4.4 Seguridad en las operaciones y comunicaciones.	DS 5 Garantizar la seguridad de los sistemas.
1.4.5 Control de acceso.	DS 5 Garantizar la seguridad de los sistemas.
1.4.6. Seguridad en la implementación y mantenimiento de *software* e infraestructura tecnológica.	AI 2, Adquirir y mantener el *software* aplicativo. AI 3 Adquirir y mantener la infraestructura tecnológica.
1.4.7. Continuidad de los servicios de TI.	DS 4 Garantizar la continuidad del servicio.

Fuente: Elaboración propia basado en las NT (2007) y COBIT 4.1

[20] Muñoz, C. (2002). *Auditoría en Sistemas Computacionales.* México D.F. Pearson Prentice Hall. (Pág. 164 y 165).
[21] IT Governance Institute, ITGI. (COBIT 4.1, 2007). *Control Objective for Information and Related Technologies*. EE.UU.

Además, el marco de control COBIT 4.1 ha desarrollado una serie de guías de implementación, las cuales son una muy buena fuente para determinar cómo se pueden auditar los lineamientos establecidos por la CGR en la NT (2007).

El marco de control COBIT tiene como misión:

> *Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.*[22]

COBIT 4.1 (2007) subdivide en 34 procesos las actividades de TI en las organizaciones, de acuerdo con 5 dominios, Planear y Organizar (PO), Adquirir e Implementar (AI), Entregar y dar Soporte (DS), Monitorear y Evaluar (ME), de los cuales el DS es el dominio más importante y más relacionado con el tema de la seguridad de la información, específicamente el DS 5 Garantizar la Seguridad de los Sistemas señala:

> *La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, política, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.*[23]

Dicho dominio establece los siguientes once objetivos de control, tal como se transcribe a continuación:

> ***DS5.1 Administración de la Seguridad de TI***
> *Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de la seguridad estén en línea con los requerimientos del negocio.*
> ***DS5.2 Plan de Seguridad de TI***
> *Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan está implementado en las políticas*

[22] Ídem.
[23] ITGI. (2007). Op. cit. (DS 5, Pág.117).

procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

DS5.3 Administración de Identidad

Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienen actualizados para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

DS5.4 Administración de Cuentas del Usuario

Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.

DS5.5 Pruebas, Vigilancia y Monitoreo

Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (login) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.

DS5.6 Definición de Incidente de Seguridad

Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas.

DS5.7 Protección de la Tecnología de Seguridad

Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.

DS5.8 Administración de Llaves Criptográficas

Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantados, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas

DS5.9 Prevención, Detección y Corrección de Software Malicioso

Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura).

DS5.10 Seguridad de la Red
Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.
DS5.11 Intercambio de Datos Sensitivos
Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen. [24]

2.2.3 Normas ISO/IEC

Respecto a la seguridad de la información hay toda una familia de estándares creados por la *ISO/IEC,* correspondientes a la serie de normas ISO 27000, tal como se detalla a continuación:

ISO/IEC 27001:2005
Information technology -- Security techniques -- Information security management systems – Requirements.
ISO/IEC 27002:2005
Information technology -- Security techniques -- Code of practice for information security management.
ISO/IEC 27003:2010
Information technology -- Security techniques -- Information security management system implementation guidance.
ISO/IEC 27004:2009
Information technology -- Security techniques -- Information security management – Measurement.
ISO/IEC 27005:2011
Information technology -- Security techniques -- Information security risk management.
ISO/IEC 27006:2011
Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.
ISO/IEC 27007:2011
Information technology -- Security techniques -- Guidelines for information security management systems auditing.
ISO/IEC TR 27008:2011
Information technology -- Security techniques -- Guidelines for auditors on information security controls.
ISO/IEC 27010:2012
Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications.
ISO/IEC 27013:2012
Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1. [25]

---

[24] ITGI. (2007). Op. cit. (DS 5, Pág.118).

A continuación, se hace un pequeño detalle de los estándares ISO/IEC 27001:2005 e ISO/IEC 27002:2005 para mayor conocimiento.

ISO/IEC 27001:2005

Destaca la ISO/IEC 27001:2005 como un estándar que permite la certificación de la Implementación de un Sistema de Gestión de Seguridad de Información, norma que fue aprobada y publicada en octubre de 2005 y tiene como fin "*proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de Gestión de Seguridad de la Información (SGSI)"*[26]*.* Además, adopta un modelo de proceso de "Planear-Hacer-Chequear-Actuar" (PDCA) por sus siglas en ingles de *Plan–Do–Check–Act*, el cual se puede aplicar a todos los procesos de SGSI, tal como se detalla en la siguiente tabla.

Tabla 2 Acciones para desarrollar cada etapa de ciclo PDCA

Etapa	Acciones
Planear (establecer el SGSI)	Establece política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI.
Chequear (Monitorear y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
Actuar (mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Fuente: ISO/IEC 27001:2005.

[25] ISO Org. Búsqueda avanzada. en el sitio *we*b http://www.iso.org recuperado el 30 de abril de 2013.
[26] International Organization for Standardization. (2005) *ISO/IEC* 27001:2005*. Information technology-Security techniques-Information security management systems–Requirements. USA* (Apartado 01 General).

La norma puede ser implementada en todo tipo de organización, el SGSI especifica todos los requerimientos, por lo que asegura la selección adecuada y proporciona controles de seguridad que protegen los activos de información.

La norma está estructurada de la siguiente forma:

0 Prefacio.
1 Alcance de la norma.
2 Referencias normativas.
3 Términos y definiciones.
4 El sistema de gestión de la seguridad de información en sí.
5 Responsabilidad de la Gerencia.
6 Auditoría Interna al SGSI.
7 Revisión gerencial del SGSI.
8 Mejoramiento continúo del SGSI.
Anexo A: Objetivo de control y controles
Anexos B: Guía de los principios OECD para administración de riesgos y su correspondencia con el ciclo de Derming PDCA.
Anexo C: Correspondencia de esta norma con los estándares ISO 9001:2000 e ISO 140001:2004.[27]

ISO/IEC 27002:2005

La norma ISO/IEC 27002:2005, Tecnologías de la Información-Técnicas de Seguridad-Código para la Práctica de la Gestión de la Seguridad de la Información, es el nuevo nombre que se le dio al estándar ISO/IEC 17799:2000, como parte del esquema de numeración utilizado por la serie ISO/IEC 27000.

Dicha norma es un código de prácticas para la seguridad de la información, en cada apartado, se especifican los objetivos de los distintos controles para la seguridad de la información y una guía para su implantación, además, la norma no es certificable y está estructurada de la siguiente forma:

0. *Introducción.*
1. *Alcance.*
2. *Términos y definiciones.*
3. *Estructura del estándar*
4. *Evaluación y tratamiento del riesgo.*

[27] ISO/IEC. (27001:2005). Op. cit. (Índice).

5. *Política de Seguridad de la Información.*
6. *Organización de la Seguridad de la Información.*
7. *Gestión de Activos de Información.*
8. *Seguridad de los Recursos Humanos.*
9. *Seguridad Física y Ambiental.*
10. *Gestión de las Comunicaciones y Operaciones.*
11. *Control de Accesos.*
12. *Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.*
13. *Gestión de Incidentes en la Seguridad de la Información.*
14. *Gestión de Continuidad del Negocio.*
15. *Cumplimiento.*[28]

2.3 Entorno organizacional

A continuación se hace una reseña del MEP y la DAI para enmarcar el entorno en donde se aplicaría la práctica profesional.

2.3.1 Ministerio de Educación Pública

De conformidad con la Ley Orgánica del Ministerio de Educación Pública, Ley Nº 3481, el artículo 1 establece que dicho Ministerio es:

> *(…) el órgano del Poder Ejecutivo en el ramo de la Educación y de la Cultura, a cuyo cargo está la función de administrar todos los elementos que integran aquel ramo, para la ejecución de las disposiciones pertinentes del título sétimo de la Constitución Política, de la Ley Fundamental de Educación, de las leyes conexas y de los respectivos reglamentos.*
> *(NOTA: Lo relativo a "Cultura" compete actualmente al Ministerio de Cultura, Juventud y Deportes, según su Ley de Creación No.4788 del 5 de julio de 1971).*

Actualmente la educación costarricense está regulada en la Ley Fundamental de Educación, Ley N°2160, promulgada por el Presidente de la República, José Figueres Ferrer y el Ministro de Educación, Uladislao Gómez Solano el 25 de setiembre de 1957, la cual establece en el artículo 2, que los fines de la educación costarricense son:

---

[28] *International Organization for Standardization.* (2005) ISO/IEC 27002:2005. *Information technology-Security techniques-Information security management systems–Requirements.* EE.UU. (Índice).

> *a) La formación de ciudadanos amantes de su Patria, conscientes de sus deberes, de sus derechos y de sus libertades fundamentales, con profundo sentido de responsabilidad y de respeto a la dignidad humana;*
> *b) Contribuir al desenvolvimiento pleno de la personalidad humana;*
> *c) Formar ciudadanos para una democracia en que se concilien los intereses del individuo con los de la comunidad;*
> *d) Estimular el desarrollo de la solidaridad y de la comprensión humanas; y*
> *e) Conservar y ampliar la herencia cultural, impartiendo conocimientos sobre la historia del hombre, las grandes obras de la literatura y los conceptos filosóficos fundamentales.*

Además, es importante conocer la misión, visión y objetivos institucionales que ha establecido el MEP, los cuales se encuentran publicados en su página web y a continuación se transcriben.

> ***Misión institucional***
> *Como ente rector de todo el Sistema Educativo, al Ministerio de Educación Pública le corresponde promover el desarrollo y consolidación de un sistema educativo de excelencia que permita el acceso de toda la población a una educación de calidad, centrada en el desarrollo integral de las personas y en la promoción de una sociedad costarricense integrada por las oportunidades y la equidad social.*
> ***Visión Institucional***
> *Un Ministerio de Educación Pública renovado y moderno al servicio de los estudiantes y sus familias, de los docentes, de los directores de centros educativos y, en general de las comunidades. Un Ministerio caracterizado por una gestión administrativa eficiente, oportuna y transparente, que promueve el desarrollo integral del ser humano y las capacidades humanas necesarias para vivir e integrarnos en una sociedad global, con base en el ingenio, el conocimiento y las destrezas. Un Ministerio que contribuya a descubrirnos, entendernos, expresarnos y reconstruirnos como ciudadanos del mundo, capaces de guiarse en la búsqueda permanente y crítica de lo que es justo.*
> ***Objetivos Institucionales***
> *El título VII de la Constitución Político (sic) establece las definiciones y mandatos esenciales para la Educación y la Cultura Costarricenses en el marco del Estado Social de Derecho, y por tanto, las definiciones y mandatos esenciales para el Ministerio de Educación Pública.* [29]

Organización administrativa MEP

La organización administrativa de las oficinas centrales está establecida en el Decreto Ejecutivo N°36451-MP (2011), el cual consig na que está a cargo de un Ministro como máximo jerarca de la institución, que tiene a cargo 3 áreas de especialización para el desarrollo de sus competencias y atribuciones, bajo la

[29] MEP. *Misión & Visión.* Recuperado del sitio web http://www.mep.go.cr el 10 de abril 2013.

responsabilidad de un Viceministerio de Planificación Institucional y Coordinación Regional, un Viceministerio Académico y un Viceministerio Administrativo.

El marco normativo citado anteriormente establece la clasificación de las dependencias del MEP en cuatro niveles de responsabilidades: nivel político, asesor, director y ejecutor, tal como se detalla a continuación:

> *Artículo 4º—Al Nivel Político le corresponde la dirección superior del Ministerio de Educación Pública, la ejecución de las disposiciones emanadas del Consejo Superior de Educación (CSE), la conducción de la política educativa, así como el cumplimiento de las competencias, funciones y atribuciones técnico-administrativas que le son propias, de conformidad con el ordenamiento jurídico.*
> *Artículo 5º—Al Nivel Asesor le corresponde brindar asesoría especializada al Nivel Político en áreas estratégicas para su funcionamiento. Asimismo, brindar asesoría a las dependencias que conforman el Nivel Director y el Nivel Ejecutor, de acuerdo con lo establecido en el presente decreto y los lineamientos que dicte el Ministro de Educación Pública para tales efectos.*
> *Artículo 6º—Al Nivel Director le corresponde planificar, desarrollar, coordinar, dirigir, dar seguimiento y evaluar los procesos estratégicos, de mediano y largo plazo, necesarios para la ejecución de la política educativa y para la prestación del servicio de educación pública en todos los ciclos y ofertas educativas.*
> *Artículo 7º—Al Nivel Ejecutor le corresponde implementar las políticas, planes, programas y proyectos establecidos para la prestación del servicio de educación pública en todos los ciclos y ofertas educativas, así como la realización de los trámites relacionados, de conformidad con los manuales de procedimientos establecidos por el Nivel Director, según corresponda.*

Ver Anexo 1, Organigrama del MEP para mayor detalle.

Política Nacional en aplicación de las Tecnologías de la Información y la Comunicación a la Educación

El MEP, en cumplimento de los lineamientos estipulados por la CGR para la implementación de las NT (2007), ha creado un marco normativo de las TICS, por lo que en el año 2009 emitió la “Política Nacional en Aplicación de las Tecnologías de la Información y la Comunicación a la Educción” la cual:

> *(…) es una herramienta estratégica para darle orientación, visión y pertinencia a la integración de estas al quehacer educativo, considerándolas como un recurso que complementa y que puede transformar el entorno educativo, pero que para ello debe ir*

> *vinculado con los contextos y el uso de quienes deberán determinar y propiciar el efecto, el fin último de todo esfuerzo: estudiantes, personal docente y administrativo y comunidad.*[30]

La política que tiene como objetivo:

> *Promover la transformación del sistema educativo costarricense, de forma que se desarrolle la utilización de las tecnologías digitales al servicio de la educación nacional, como estrategia para propiciar el desarrollo y el enriquecimiento de la enseñanza, el aprendizaje y la gestión educativa.*[31]

Además, tiene los siguientes propósitos específicos:

> *1. Preparar a la comunidad educativa para ser usuaria eficiente, autónoma y creativa de las TIC, mediante procesos de sensibilización y de capacitación en su uso.*
> *2. Aprovechar las potencialidades de las TIC para mantener una oferta permanente de programas y de proyectos educativos que sean flexibles, ricos en vivencias con ambientes activos e interactivos centrados en el aprendizaje.*
> *3. Promover el diseño y el desarrollo de prácticas pedagógicas basadas en las tecnologías de la información y la comunicación con el fin de integrar conocimientos de las distintas áreas.*
> *4. Desarrollar el equipamiento informático, los proyectos de redes en los centros educativos y la capacitación de docentes en informática para usos educativos, integrando todos los niveles.*
> *5. Fomentar la producción, la difusión y la localización de los recursos multimedia por parte de docentes, de estudiantes y de grupos de investigación y desarrollo.*
> *6. Poner en práctica estrategias y líneas de acción para garantizar la infraestructura tecnológica necesaria para las acciones educativas, que incluyan la selección, instalación, mantenimiento, soporte técnico y actualización de los equipos.*
> *7. Establecer los mecanismos necesarios que garanticen el acceso equitativo a las TIC en educación en áreas rurales y para poblaciones en riesgo.*
> *8. Promover la investigación y desarrollo de nuevas formas de organización escolar, curricular, elaboración de contenidos y evaluación de aprendizajes.*
> *9. Garantizar la existencia de programas de formación, capacitación y actualización permanente para el profesorado de los diferentes niveles y el personal administrativo del sistema educativo.*
> *10. Generar la definición y aseguramiento de los recursos financieros necesarios de inversión inicial y para la instrumentación a corto, mediano y largo plazo.*
> *11. Establecer las estrategias para la certificación y evaluación mediante la construcción de indicadores que valoren los resultados y la pertinencia de las acciones propuestas, así como la inclusión de reformas y modificaciones necesarias en el desarrollo y al final de cada etapa de los proyectos.*[32]

---

[30] MEP (2009). *Política Nacional en Aplicación de las Tecnologías de la Información y la Comunicación a la Educación.* Recuperado del sitio web http://www.mep.go.cr el 5 de abril de 2013.
[31] Ídem.
[32] Ídem.

Dicha política establece que para su seguimiento y evaluación la creación de un Comité Gerencial en TIC *"cuyo principal propósito es la elaboración y seguimiento del Plan Estratégico que se derive de la Política Nacional de TIC y Educación"*, Comité que está integrado por las siguientes dependencias: Dirección de Planificación Institucional, Dirección de Informática de Gestión, Dirección de Desarrollo Curricular, Dirección de Educación Técnica y Capacidades Emprendedoras, Dirección de Recursos Tecnológicos en Educación, Dirección de Gestión y Evaluación de la Calidad, Dirección del Instituto de Desarrollo Profesional Uladislao Gámez Solano, Dirección del Programa Mejoramiento de la Calidad Educativa (PROMECE), así como un representante del Ministro de Educación y un representante de la Fundación Omar Dengo.

También, propicia su desarrollo mediante cuatro ejes que enmarcan el norte de la aplicación de la Tecnología de la Informática y la Comunicación al Sistema Educativo Costarricense, las cuales se detalla a continuación.

> *a) Programa de Informática Educativa*
> *Objetivo: Promover el desarrollo en el estudiantado de competencias cognitivas, éticas y sociales basadas en la apropiación de las tecnologías digitales.*
> *b) Informática como herramienta didáctica*
> *Objetivo: Promover la utilización y apropiación de las tecnologías informáticas en el quehacer pedagógico, tanto por parte del profesorado como del estudiantado.*
> *c) Certificación de competencias en el manejo de la herramienta informática*
> *Objetivo: Desarrollar, en el personal docente y administrativo y en el estudiantado, capacidades en el manejo y la aplicación de las tecnologías de la información y la comunicación.*
> *d) Utilización de la informática en la gestión administrativa de las tareas educativas*
> *Objetivo: Promover el empleo de diversas herramientas informáticas para la búsqueda de la eficiencia y la eficacia en el manejo de los asuntos administrativos de los centros escolares, circuitos educativos, direcciones regionales y el sistema central del Ministerio de Educación Pública.*[33]

Normativa emitida en relación con las TICS

El MEP ha emitido una serie de normas como manuales, procedimientos, planes, debidamente aprobados y de aplicación obligatoria para sus funcionarios en

[33] Ídem.

cumplimiento de la NT (2007), por lo que a continuación se citan algunas de ellas y se hace una pequeña descripción.

a) Manual de Estándares Informáticos (2012)

El Manual de Estándares Informáticos[34] es una metodología de procesos unificada que regula los procesos de adquisición de tecnología informática en la Institución, donde se establecen los estándares informáticos de las especificaciones técnicas y procedimentales del desarrollo del *software*, la adquisición de tecnología y la administración de la plataforma tecnológica.

b) Manual Modelo de la Arquitectura de Información (2012)

El MEP desarrolló el Manual Modelo de la Arquitectura de Información, en el cual plasmó un modelo de arquitectura de información que tiene como objetivo *"Crear un modelo de arquitectura de información basada en los estándares informáticos, de tal forma que pueda ser cambiado según la incorporación de nueva infraestructura tecnológica".*[35]

c) Manual Estándar para el Desarrollo de un Proyecto en TI (2010)

El Manual Estándar para el Desarrollo de un Proyecto en TI[36], establece los lineamientos generales para el adecuado y eficiente desarrollo de proyectos en TI, utiliza como marco de referencia la Guía de los Fundamentos para la Dirección de Proyectos (Guía del *PMBOK*) que describe normas métodos y prácticas establecidas en la dirección de proyectos.

---

[34] Padilla. F. (Versión 1, 2012). *Manual de Estándares Informáticos*. Recuperado del sitio web http://www.mep.go.cr el 19 de enero de 2013.
[35] MEP (Versión 1, 23 febrero 2012). *Manual Modelo de la Arquitectura de Información*. Recuperado del sitio web http://www.mep.go.cr el 19 de enero de 2013.
[36] Morera I. (Versión 1, del 11 de febrero 2010). *Manual Estándar para el Desarrollo de un Proyecto en TI*. Recuperado del sitio web http://www.mep.go.cr el 19 de enero de 2013.

d) Manual de Configuraciones de Redes y Telecomunicaciones (2012)

El objetivo del Manual de Configuraciones de Redes y Telecomunicaciones es:

> *Brindar un conocimiento básico de la estructura de las redes existentes y operar como una guía para la implementación de soluciones en corto tiempo, con la garantía de que éstas serán compatibles y funcionales con los procesos y aplicaciones que se ejecutan en el Ministerio.*[37]

Dicho manual establece un estándar en la configuración de los diferentes equipos de comunicación que tiene el Ministerio.

e) Plan de Aseguramiento para la Continuidad del Servicio en los Procesos Críticos de TI (2012)

El MEP dispone de un Plan de Aseguramiento de la Continuidad del Servicio de los Procesos Críticos de TI[38], con el cual se pretende que las dependencias protejan su información con el fin de asegurar la continuidad de los procesos.

f) Procedimiento para la presupuestación y elaboración del plan de adquisiciones de TI

El Comité de TICS fue el encargado de emitir el procedimiento para la adquisición de tecnologías de información, cual tiene por objetivo *"Brindar una guía clara a los diferentes actores de cómo se elabora el presupuesto y plan de adquisiciones de Tecnologías de Información"*[39]*.* El alcance de dicho procedimiento corresponde desde la solicitud de requerimientos de presupuesto por parte de la Dirección de Informática de Gestión, hasta el proceso de adquisición de los bienes y servicios de tecnologías de información por parte de la Dirección de la Proveeduría Institucional.

---

[37] Morera C. (Versión 4, del 8 de abril 2012). *Manual de Configuraciones de Redes y Telecomunicaciones.* Recuperado del sitio web http://www.mep.go.cr el 19 de enero de 2013.
[38] MEP. (Versión1, 23 Febrero del 2012). *Plan de Aseguramiento para la Continuidad del Servicio en los Procesos Críticos de TI.* Recuperado del sitio web http://www.mep.go.cr el 19 de enero de 2013.
[39] Sánchez R. (s.f.). *Procedimiento para la Presupuestación y Elaboración del Plan de Adquisiciones de Equipo de Cómputo para Oficinas Centrales y Direcciones Regionales*. Recuperado del sitio web http://www.mep.go.cr el 19 de enero de 2013.

g) Procedimiento Contratación de Servicios Prestados por Terceros

La Dirección de Informática de Gestión estableció el Procedimiento para la Contratación de Servicios Prestados por Terceros, el cual tiene como objetivo "*Establecer el proceso para la adquisición tecnológica de todos los programas presupuestarios del MEP"* [40], cabe indicar que no incluye el proceso interno realizado por la Dirección de Proveeduría Institucional. Así las cosas, toda adquisición de recursos o servicios de TI, independientemente de quién la ejecute, se tramita de forma unificada en el Plan de Adquisiciones de Tecnologías de Información.

h) Estándares para el Proceso Institucional de Desarrollo y Mantenimiento de Software

El MEP estableció un Manual de Estándar para el Proceso Institucional de Desarrollo y Mantenimiento del *Software*, con el siguiente objetivo *"Establecer los estándares que permitan describir detalladamente los procesos de captura, diseño, validación, selección, manipulación, procesamiento, conservación y aseguramiento de la información con el fin de mejorar el proceso de toma de decisiones de los analistas".* [41]

Además, estableció que el Departamento de Innovación Tecnológica y Control Informático sea el responsable por el cumplimiento de dicho manual.

i) Manual de Lineamientos del Uso de los Recursos Informáticos Institucionales

EL MEP emitió el Manual de Lineamientos del Uso de los Recursos Informáticos Institucionales, con el detalle de las políticas y lineamientos generales del uso de los recursos informáticos para todo el personal.

El Manual tiene como objetivos específicos los siguientes:

---

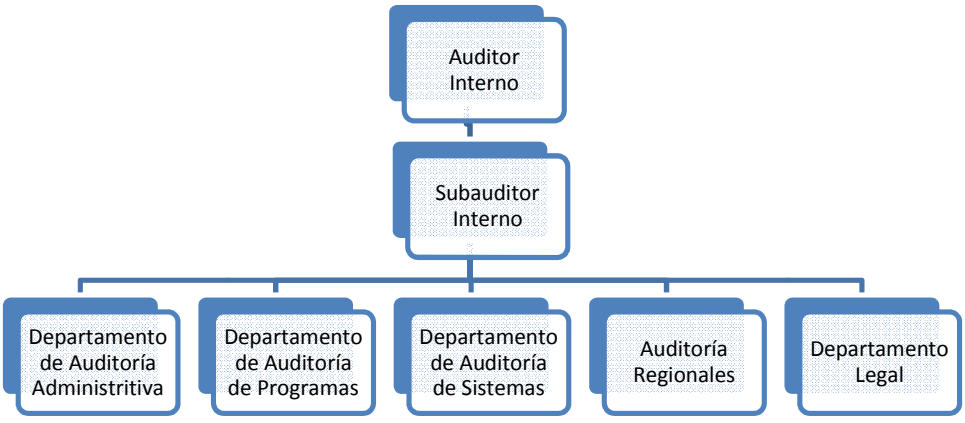
[40] Dirección de Informática de Gestión. (s.f.) *Procedimiento Contratación de Servicios Prestados por Terceros*. Recuperado del sitio web http://www.mep.go.cr el 19 de enero de 2013.
[41] MEP. (Versión 3, del 15 de febrero de 2012). *Estándares para el Proceso Institucional de Desarrollo y Mantenimiento de Software.* Recuperado del sitio web http://www.mep.go.cr el 19 de enero de 2013.

- Uniformar criterios sobre los lineamientos técnicos para el adecuado e idóneo uso de los bienes informáticos del Ministerio y asegurar el cumplimiento de las rutinas de uso conveniente y apropiado de éstos.
- Aumentar la eficiencia general en las labores cotidianas de esta institución en las que se requiera el uso de estos instrumentos de trabajo.
- Facilitar la evaluación del control interno que se debe ejercer en cada dependencia y centro educativo del Ministerio sobre dichos bienes y/o servicios informáticos.
- Promover medidas de seguridad para el hardware y software en todas las dependencias de la Institución.
- Analizar periódicamente las políticas y lineamientos que se den en pro de la optimización del uso de los recursos informáticos.
- Fiscalizar la administración de la plataforma informática y telemática del ministerio, a nivel de hardware y software, en lo relacionado con aplicaciones, bases de datos y los servicios en red, como también los recursos informáticos asignados individualmente a los funcionarios de la institución, para garantizar su máximo aprovechamiento y la mayor eficiencia permisible. [42]

2.3.2 Dirección de Auditoría Interna

La DAI tiene sus orígenes en Decreto Ejecutivo N°19994 y actualmente está organizada según el DE N°34427, con la siguiente estructura organizacional, no obstante está en proceso de modificación.

Figura 1: Organigrama de la DAI



Fuente: Elaboración propia basada en el Decreto Ejecutivo N°34427 .

[42]MEP (Versión 3, del 14 de febrero de 2012). *Manual de Lineamientos del Uso de los Recursos Informáticos Institucionales*. Recuperado del sitio web http://www.mep.go.cr el 19 de enero de 2013.

Aunado a lo anterior, es importante conocer algunos aspectos de la DAI, tales como la misión, la visión y objetivos institucionales, los cuales se encuentra publicados en la página oficial del MEP y a continuación se transcriben.

> ***Visión***
> *Ser un órgano con impacto real en el desarrollo estratégico del Ministerio y las instituciones sujetas a su competencia.*
> ***Misión***
> *Somos un órgano fiscalizador y asesor que proporciona un servicio oportuno, integral y con una actitud proactiva en materia de control gerencial y operativo, mediante investigaciones y evaluaciones de carácter interdisciplinario, para generar valor agregado en el cumplimiento de los objetivos institucionales.*
> ***Objetivo Estratégico***
> *Valorar el sistema de control interno a nivel institucional para procurar su mejora continua.*
> ***Objetivos Específicos***
> *-Generar informes que impacten*
> *-Mejorar cobertura*
> *-Mejorar atención al usuario*
> *-Tener un adecuado ambiente de control interno*
> *-Tener personal capacitado*[43]

Cabe indicar que el uso de las TI y la automatización de muchos procesos, así como los nuevos requerimientos normativos en el MEP, implicó para la DAI un cambio en su estructura organizacional, así que en el año 2008 se crea formalmente el Departamento de Auditoría de Sistemas, según el artículo 18 del Decreto Ejecutivo N°34427, el cual dice que:

> ***El Departamento de Auditoría de Sistemas.*** *El Departamento de Auditoría de Sistemas estará encargado de efectuar estudios especiales sobre todos los sistemas informáticos del Ministerio, dar asesoría y apoyo especializado a los otros departamentos y brindar el soporte necesario a los equipos y programas de la Auditoría Interna.*[44]

Actualmente dicho departamento cuenta con una jefatura y cuatro funcionarios a su cargo, no obstante, estos recursos son insuficientes para las labores de fiscalización, dada la capacidad operativa del MEP.

---

[43] DAI. Recuperado del sitio web http://www.mep.go.cr el 11 de enero de 2013.
[44] El Presidente de la República y el Ministro de Educación Pública. (2008). *Decreto Ejecutivo N°34427-MEP 2008* . (Art 18).

CAPÍTULO III: PROPUESTA GUIA DE AUDITORÍA

El presente capítulo corresponde a la propuesta de la guía de auditoría, para evaluar en el MEP el cumplimiento de la implementación de las normas de gestión de la seguridad de la información de las NT (2007), la cual está compuesta de un Plan General de Auditoría y se desarrollan 10 instrumentos con los procedimientos de auditoría que pueden ser aplicados.

Introducción

La propuesta de la guía de auditoría sigue la estructura establecida por la CGR en el manual de Normas Generales de Auditoría para el Sector Público (M-2-2006-CO-DFOE), la cual es una base normativa común para el ejercicio de la auditoría en el sector público costarricense y es de acatamiento obligatorio para la:

> *"Contraloría General de la República, las auditorías internas del sector público, los entes y órganos de control, los sujetos componentes de la Hacienda Pública y los profesionales autorizados —de forma unipersonal u organizados por medio de despachos o firmas de auditoría— cuando actúan en labores de auditoría en el sector público, por lo que este Manual deberá prevalecer sobre cualquier disposición que en contrario emitan las auditorías internas y la Administración activa, pudiendo su incumplimiento injustificado dar lugar a lo dispuesto en el Capítulo V de la Ley General de Control Interno, Nro. 8292.*[45]

La Norma 2.2 del citado manual establece las etapas del proceso de auditoría correspondientes a "*las etapas de planificación, examen, comunicación de resultados y seguimiento de disposiciones o recomendaciones"* [46], así que para efecto de la propuesta solo se va a considerar la etapa de planificación.

Aunado a lo anterior la Norma 203 Planificación de la Auditoría, en lo que nos interesa sobre la elaboración de Plan General de Auditoría, señala que deben considerarse al menos los siguientes aspectos:

---

[45] CGR. (2006). *Manual de Normas Generales de Auditoría para el Sector Público (M-2-2006-CO-DFOE)*. Recuperado del sitio web http://documentos.cgr.go.cr el 5 de mayo de 2013.
[46] CGR. (2006). Op. cit. (Norma 202.01).

a) Comprensión de las actividades de la entidad.
b) Comprensión del sistema de control interno de la entidad y los resultados de la autoevaluación de ese sistema.
c) Los resultados de la valoración del riesgo institucional.
d) Los objetivos planteados en el estudio de auditoría por realizar.[47]

Además, la misma norma, en el numeral 06, señala que el plan general de la auditoría en el sector público debe indicar, al menos, los siguientes asuntos:

a) Objetivos de la auditoría.
b) Naturaleza, alcance, oportunidad y plazo de los procedimientos.
c) Elementos de coordinación, dirección, supervisión y revisión requeridos.
d) Recursos para el desarrollo del trabajo.[48]

Entonces, tales consideraciones se plasman a continuación.

[47] CGR. (2006). Op. cit. Norma 203.05.
[48] CGR. (2006). Op. cit. Norma 203.06.

3.1 Consideraciones para la elaboración del plan general de auditoría

3.1.1 Comprensión de las actividades de la entidad

Antes de desarrollar el Plan General de Auditoría es necesario tener un conocimiento general de la entidad o unidad que se esté auditando, por lo que a continuación se propone una guía de auditoría para obtener dicha información.

GUÍA DE AUDITORÍA **Comprensión de las actividades de la entidad**				**G-1**
Objetivo:	Obtenga una mayor comprensión de las actividades de la entidad auditada.			
Procedimiento:	Aplique los siguientes procedimientos.			
No.	**Procedimientos**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Realice un estudio preliminar de la dependencia por auditar, mediante el análisis de la cantidad suficiente de antecedentes e información que pueda recabarse, considerando como mínimo lo siguiente:			
	– Resultados de auditorías anteriores u otros estudios relacionados con los objetivos de la auditoría por realizar, identificando las acciones correctivas que se tomaron para atender los hallazgos significativos y las recomendaciones.			
	– Estructura orgánica.			
	– Manuales de puestos.			
	– Manuales de procedimientos			
	– Funciones y responsabilidades asignadas.			
	– Misión, visión, objetivos institucionales.			
	– Marco jurídico aplicable.			
	– Plan Operativo Anual.			
	– Presupuesto autorizado.			
	– Estándares o indicadores de gestión que utiliza.			
	– Movimientos de personal.			
	– Cambios en los sistemas.			
Elaborado por:		Revisado por:		
Fecha:		Fecha:		

3.1.2 Comprensión del sistema de control interno de la entidad y los resultados de la autoevaluación de ese sistema

El auditor necesita comprender el sistema de control interno, para ello se propone la siguiente guía de auditoría para evaluar el control interno organizacional y cuestionario de control interno para ser aplicado a una muestra de funcionarios, con el fin conocer su perspectiva sobre la gestión de la seguridad de la información.

GUÍA DE AUDITORÍA **Evaluación de control interno organizacional**				**G-2**
Objetivo:	Evaluar el control interno organizacional.			
Procedimiento:	Aplique los siguientes procedimientos.			
No.	**Procedimientos**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Confeccione un papel de trabajo con el fundamento jurídico del Sistema Específico de Valoración del Riesgo Institucional, considerando las directrices, manuales y procedimientos emitidos.			
2.	Indague sobre resultados de auditorías anteriores u otros estudios que se hayan realizado sobre el SEVRI.			
3.	Solicite y analice el instructivo o manual del Sistema Específico de Valoración del Riesgo Institucional-MEP.			
4.	Determine si para la ejecución de SEVRI se cuenta con todos los recursos financieros, humanos, técnicos, materiales y demás necesarios para su establecimiento, operación, perfeccionamiento y evaluación necesarios.			
5.	Solicite y revise el cuestionario de la última autoevaluación de control interno y la matriz de identificación y análisis de riesgos.			
6.	Solicite y analice las acciones realizadas por la Administración de acuerdo con los resultados de la autoevaluación de control interno y verifique su cumplimiento.			
7.	Solicite y analice los informes de seguimiento de la autoevaluación.			
8.	Aplique el Modelo de Madurez del Sistema de Control Interno Institucional, emitido por la CGR.			
Elaborado por:		Supervisado por:		
Fecha:		Fecha:		

GUÍA DE AUDITORÍA **Cuestionario de evaluación de la gestión de la seguridad de la información**				**G-3**
Objetivo:	Evaluar desde la perspectiva de los funcionarios el nivel de cumplimiento de la gestión de la seguridad por parte de la Administración.			
Procedimiento:	Tabule los resultados obtenidos y prepare un análisis estadístico.			
N°	Pregunta	SÍ	NO	No sabe
1.	¿Cuántos años tiene de laborar para el Ministerio?_____			
2.	¿Se siente satisfecho de laborar para el MEP?			
3.	¿Conoce la misión, visión, objetivos institucionales?			
4.	¿Se le ha informado por parte de la Administración sobre la política de seguridad de la institución?			
5.	¿Ha recibido alguna capacitación en seguridad de la información? ¿Cuándo? – Un mes. – Seis meses. – Un año. – Tres años o más.			
6.	¿Se le ha informado cuáles son sus responsabilidades y los riesgos asociados a las tecnologías de información?			
7.	¿Tiene claro cuáles son sus responsabilidades respecto a su función?			
8.	¿Conoce las implicaciones penales por robo y fraude de la información?			
9.	¿Tiene conocimiento de qué es un acuerdo de confidencialidad?			
10.	¿Ha firmado algún acuerdo de confidencialidad?			
11.	¿Conoce funcionarios que hayan firmado algún acuerdo de confidencialidad?			
12.	¿La entidad ha establecido y difundido una política de puertas abiertas?			
13.	¿Existen mecanismos para que los niveles inferiores puedan presentar propuestas o sugerencias?			
14.	¿Perciben que las propuestas o sugerencias son analizadas en los niveles correspondientes?			
15.	¿Las instalaciones donde labora tienen una protección adecuada contra siniestros?			
16.	¿Considera que la ubicación física de los equipos de			

	cómputo es la más adecuada?			
17.	¿Considera que existen procedimientos para asegurar la confidencialidad de la información crítica o calificada de la entidad?			
18.	¿Sabe donde están los extintores de fuego?			
19.	¿Tiene conocimiento de cómo utilizar un extintor?			
20.	¿Ha recibido alguna capacitación para utilizar un extintor?			
21.	¿Conoce dónde están las salidas de emergencia?			
22.	En caso afirmativo en la pregunta anterior, ¿las ha utilizado?			
23.	¿En alguna ocasión se ha generado algún corto circuito dentro de las instalaciones?			
24.	¿Conoce las responsabilidades y funciones ante la pruebas de continuidad de los servicios de TI?			
25.	¿En alguna ocasión se ha extraviado alguna *laptop* o equipo propiedad del MEP o de algún funcionario?			
26.	¿En alguna ocasión se ha extraviado algún periférico (bocinas, audífonos, teclado, mouse, teclado numérico, etc.) de una computadora?			
27.	¿Cada componente de su computadora y periféricos tiene placa inventariada del Ministerio?			
28.	¿Considera usted que hay demasiada humedad o excesivo calor, lo cual pueda deteriorar los equipos informáticos?			
29.	¿Conoce los peligros que provocan los virus, caballos, troyanos?			
30.	¿Cambia regularmente sus claves confidenciales?			
31.	¿Cierra las sesiones activas cuando tiene que dejar el equipo desatendido?			
Elaborado por:		Supervisado por:		
Fecha:		Fecha		

3.1.3 Los resultados de la valoración del riesgo institucional

Para la elaboración de Plan General de Auditoría es prioritario considerar los resultados del SEVRI y las acciones tomadas por la Administración para controlar los riesgos a los que está expuesto el Ministerio y así determinar qué tan confiable es el sistema de control interno. Este punto es evaluado en la Guía 2, ya que es parte del control interno.

3.2 Diseño del plan general de la auditoría

A continuación se detalla algunas consideraciones que debe tener el Plan General de Auditoría y los instrumentos de auditoría para evaluar cada uno de los enunciados de la norma 1.4 Gestión de la seguridad de la información.

3.2.1 Objetivos de la auditoría

Como objetivo general para el desarrollo de una auditoría de la gestión de la seguridad de la información se propone el siguiente:

> Objetivo: Evaluar el cumplimiento de la Norma 1.4 Gestión de la seguridad de la información, por medio de la revisión y análisis de los lineamientos del Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2207-CO-DFOE) y la normativa interna, con el fin de promover una mejora continua de la TIC en el Ministerio de Educación Pública.

3.2.2 Naturaleza, alcance, oportunidad y plazo de los procedimientos

El plan general debe definir cuál es la naturaleza del estudio, el alcance, la oportunidad de fiscalización y establecer un estimado del plazo que ejecución de los procedimientos, tal como se detalla a continuación.

Naturaleza

La naturaleza del estudio debe estar contemplada dentro de los lineamientos del plan de trabajo de la Dirección de Auditoría Interna, para el año (en el cual se ejecute el estudio), lo anterior en cumplimiento de la NT (2007).

Alcance

El alcance de la auditoría debe especificar las actividades concretas que van a ser auditadas, así como la normativa aplicable, el periodo de estudio y la extensión de la ejecución de la auditoría, así como las limitaciones que se determinen en el estudio.

Oportunidad

La DAI no ha realizado estudios sobre el cumplimiento de las NT (2007) y el MEP ha realizado un proceso tendiente a la implementación de dichas normas, por lo que es una oportunidad para el DAS de poder fiscalizar el proceso realizado y ayudar a mejorar la gestión de las TIC.

Plazos de los procedimientos

De acuerdo con la experiencia, la DAI debe darse a la tarea de estimar un plazo razonable y determinar cuándo es el mejor momento para iniciar la ejecución de la auditoría y el tiempo estimado que requiere para llevarla a cabo.

3.2.3 Elementos de coordinación, dirección, supervisión y revisión requeridos

Para el desarrollo de la auditoría es recomendable que queden documentadas las responsabilidades de dirección y supervisión requeridas, así como la coordinación de la disponibilidad del equipo de auditores.

3.2.4 Recursos para el desarrollo del trabajo

Para el desarrollo de la auditoría es necesario considerar la disponibilidad del equipo de auditores, materiales como el equipo de cómputo entre ellos portátiles, escáner, impresora, cámara fotográfica o de video, así como otros suministros de oficina.

También es necesario considerar la disponibilidad de los vehículos, en caso de realizar una gira y reservar los fondos para cubrir los viáticos de los auditores.

3.2.5 Plan General de Auditoría

A continuación se presenta la propuesta de Plan General de Auditoría.

Plan General de Auditoría				P-1
Objetivo:	Evaluar el cumplimiento de la Norma 1.4 Gestión de la seguridad de la información, por medio de la revisión y análisis de los lineamientos del Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2207-CO-DFOE) y la normativa interna, con el fin de promover una mejora continua de la TIC en el Ministerio de Educación Pública.			
Naturaleza:	La naturaleza del estudio está contemplada dentro de los lineamientos del plan de trabajo de la Dirección de Auditoría Interna, para el año (**incluir**). Lo anterior en cumplimiento del Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2207-CO-DFOE), emitido por la Contraloría General de la República.			
Alcance:	**(Incluir).**			
Plazo:	**(Incluir)**			

No.	**Procedimientos**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Obtenga o actualice el cocimiento de la organización.	G-1		
2.	Realice una evaluación de control interno y comprenda el Sistema de Control Interno de la Entidad.	G-2		
3.	Aplique un cuestionario a los funcionarios para evaluar el cumplimiento de la gestión de la seguridad de la información.	G-3		
4.	Elabore una serie de procedimientos por cada una de las siguientes normas de la gestión de la seguridad de la información, en función del objetivo general y de la información obtenida en las actividades anteriores.			
	– Norma 1.4.1 Implementación de un marco de seguridad de la información.	G-4		
	– Norma 1.4.2 Compromiso del personal con la seguridad de la información.	G-5		
	– Norma 1.4.3 Seguridad física y ambiental.	G-6		
	– Norma 1.4.4 Seguridad en las operaciones y comunicaciones.	G-7		
	– Norma 1.4.5 Control de accesos.	G-8		
	– Norma 1.4.6 Seguridad en la implementación y mantenimiento de *software* e infraestructura tecnológica.	G-9		
	– Norma 1.4.7 Continuidad de los servicios de TI	G-10		
5.	Elabore un papel de trabajo con las deficiencias encontradas y realice una presentación al equipo auditor.			
6.	Elabore el informe de auditoría, sométalo a revisión y discusión de los auditados.			

Elaborado por:		Supervisado por:	
Fecha:		Fecha:	

3.2.5.1 Diseño guía de auditoría

Parar cada uno de los enunciados de la norma 1.4 Gestión de la Seguridad de la Información se ha desarrollado un instrumento de auditoría que busca evaluar el grado de cumplimiento de la Administración, tal como se detalla a continuación.

GUÍA DE AUDITORÍA **Evaluación de la Implementación de un Marco de Seguridad de la Información**				**G-4**
Objetivo:	Evaluar la implementación de un marco de seguridad de la información en MEP.			
Criterio:	Norma 1.4.1 Implementación de un marco de seguridad de la información. La organización debe implementar un marco de seguridad de la información, para lo cual debe: a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal. b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización. c. Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.			
No.	**Procedimientos**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Determine si la Administración elaboró el marco de seguridad de la información para toda la institución y si se encuentra aprobado y divulgado.			
2.	Solicite y revise la política de seguridad de la información y determine si esta fue debidamente; – Aprobada. – Publicada. – Comunicada a todos los funcionarios y las partes externa relevantes.			
3.	Determine si la política de seguridad considera: – Una definición de la seguridad de la información. – Objetivos de seguridad. – El alcance de la política. – Principios de la seguridad de la información.			

	– Estructura para la evaluación de riesgos. – Políticas, principios y requerimientos. – Referencias a otros documentos.			
4.	Determine si la política de seguridad de la información está alineada con las normas y procedimiento existente.			
5.	Determine cuál es la estructura organizacional de la seguridad de la información. – Integrantes, nombre de los funcionarios y puesto. – Funciones y responsabilidades.			
6.	Determine si las funciones y responsabilidades de los funcionarios están en concordancia con la política de seguridad.			
7.	Indague cómo se aprueban los controles de seguridad de la información, si estos se consideran idóneos y cómo se coordina su implementación.			
8.	Determine cuál es la metodología usada para la valoración de riesgo institucional.			
9.	Verifique si las actividades de seguridad ejecutadas concuerdan con la política de seguridad de información.			
10.	Indague como el Ministerio ha promovido la educación, capacitación y conocimiento de la política de seguridad de la información a sus funcionarios.			
11.	Verifique la existencia de un programa formal de concienciación sobre seguridad para todos los empleados.			
12.	Verifique que el programa de concienciación sobre seguridad proporcione diversos métodos para informar y educar a los funcionarios, por ejemplo, carteles, cartas, notas, capacitación basada en la web, reuniones y promociones.			
13.	Verifique cuáles funcionarios han participado de la capacitación sobre concienciación de la seguridad de la información.			
14.	Verifique que el programa de concienciación sobre seguridad exija a los empleados que reconozcan, por escrito o de forma electrónica, al menos una vez al año, haber leído y entendido la política de seguridad de la información de la empresa.			
15.	Indague si han ocurrido cambios significativos, que ameriten la actualización de la política de seguridad para asegurar su continuidad, eficiencia y eficacia; considere los siguientes aspectos:			

	– Si ha habido alguna *retroalimentación*. – Alguna evaluación de la política de seguridad o revisión interna. – Acciones preventiva y correctiva implementadas por el Ministerio. – Cambio en el ambiente laboral, disponibilidad de los recursos, condiciones contractuales, regulaciones internas y legales o cambio en el ambiente técnico.			
16.	Prepare un cuestionario para determinar si el personal tiene conocimiento del marco de seguridad de la información.			

Elaborado por:		Supervisado por:	
Fecha:		Fecha	

GUÍA DE AUDITORÍA Evaluación del Compromiso del Personal con la Seguridad de la Información	G-5
Objetivo:	Evaluar el compromiso del personal de la unidad auditada con la seguridad de la información.
Criterio:	Norma 1.4.2 Compromiso del personal con la seguridad de la información El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI. Para ello, el jerarca, debe: a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI. b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades. c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos.

No.	Procedimientos	Ref. P/T	Hecho por	Fecha
1.	Solicite al jerarca o funcionario enlace: – Los oficios o circulares donde se informa al personal sobre las regulaciones en seguridad y confidencialidad de la información. – El detalle de las capacitaciones impartidas sobre la seguridad de la información y la documentación brindada al personal. – Mecanismos para vigilar el cumplimiento de las responsabilidades de los funcionarios.			
2.	Verifique con la Dirección de Planificación Institucional y el Instituto de Desarrollo Profesional Uladislao Gámez Solano el detalle de las capacitaciones brindadas al personal, sobre la seguridad de la información, en los últimos 3 años.			
3.	Indague en el Departamento de Asuntos Disciplinarios, sobre procedimientos disciplinarios contra funcionarios por asuntos relacionados con violaciones a la seguridad de la información. Prepare una hoja de trabajo con el detalle de la situación encontrada para cada caso, el estado del proceso, causa que se investiga.			
4.	Obtenga y revise el procedimiento para subscribir acuerdos de confidencialidad con el personal.			
5.	Indague sobre los tipos de acuerdos de			

	confidencialidad, considerando lo siguiente: – La persona responsable de custodiar los acuerdos de confidencialidad. – Establezca una lista de los tipos de acuerdos de confidencialidad. – Solicite copia del formato de los acuerdos de confidencialidad que se subscriben. – Determine quiénes son las personas autorizadas para firmar los acuerdos de confidencialidad por parte del MEP. – Solicite la lista del personal que, por sus funciones, deben firmar acuerdos de confidencialidad y verifique que existe el acuerdo de confidencialidad debidamente firmado, el estado del funcionario y la dependencia en que labora.			
6.	Analice los acuerdos de confidencialidad existentes y determine si los requerimientos de confidencialidad reflejan las necesidades de la organización para proteger la información. Tome en consideración: – El establecimiento o identificación de la información que debe protegerse. – Duración del acuerdo, inclusive la confidencialidad indefinidamente. – Procedimiento cuando se vencen los acuerdos. – Responsabilidades y funciones de los funcionarios. – Propiedad de la información, secretos comerciales y propiedad intelectual. – Uso permitido de la información confidencial. – Proceso ante un incumplimiento del acuerdo de confidencialidad. – Cumplimiento del ordenamiento jurídico.			
7.	Indague sobre el mecanismo de control que tiene la Administración para determinar el cumplimiento de los acuerdos de confidencialidad.			
8.	Prepare un cuestionario para evaluar el conocimiento del personal sobre la seguridad de la información, considerando aspectos como: responsabilidades, regulaciones en seguridad de la información, riesgos, capacitación, robo, fraude, errores humanos y acuerdos de confidencialidad.			

Elaborado por:		Supervisado por:	
Fecha:		Fecha	

GUÍA DE AUDITORÍA Evaluación de la Seguridad Física y Ambiental				G-6
Objetivo:	Verificar la gestión de la seguridad física y ambiental.			
Criterio:	Norma 1.4.3 Seguridad física y ambiental La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos. Como parte de esa protección debe considerar: a. Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas. b. La ubicación física segura de los recursos de TI. c. El ingreso y salida de equipos de la organización. d. El debido control de los servicios de mantenimiento. e. Los controles para el desecho y reutilización de recursos de TI. f. La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas. g. El acceso de terceros. h. Los riesgos asociados con el ambiente.			
No.	**Procedimientos**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Indague con la administración y analice cuáles son los perímetros de seguridad físicos de las instalaciones.			
2.	Solicite y analice la política y procedimientos para el control de ingreso físico a las instalaciones y las áreas donde se procesa o almacena información sensible.			
3.	Determine si existen políticas relacionas con el ingreso y salida del *software* que aseguren que este sea: – Revisado (contenido, cantidad, destino). – Esté registrado formalmente en la empresa. – Justificado. – Aprobado por un responsable autorizado. – Registrado (quién y a qué hora salió). – Devuelto (comparar con fecha estimada de devolución). – Devuelto en las mismas condiciones en que salió.			
4.	Determine si existen políticas relacionadas con el ingreso y salida del *hardware* que aseguren que este sea:			

	– Revisado (contenido, cantidad, destino). – Justificado (comprado, pruebas reemplazo, devolución, dado de baja, otros). – Aprobado por un responsable autorizado. – Registrado (responsable, hora, motivo, etcétera). – Devuelto (comparar con la fecha estimada de salida). – Devuelto en las mismas condiciones de entrada.			
5.	Determine si se cuenta con controles y procedimientos para : – Clasificación y justificación del personal con acceso a los centros de cómputo y las oficinas del personal de informática. – Definición y difusión de las horas de acceso al centro de cómputo. – Definición de hora de entrada de los visitantes. – Manejo de bitácoras especiales para los visitantes a los centros de cómputo. – Control de identificación visible, tanto para funcionarios como visitantes, el cual también identifique áreas de acceso. – Ingreso físico para el personal de servicios prestados por terceros.			
6.	Determine si existen cámaras de vigilancia u otros mecanismos de control de acceso y si están funcionando correctamente para supervisar los puntos de entrada/salida de áreas confidenciales. En caso afirmativo: – Verifique que estén protegidos contra alteraciones y desactivaciones. – Verifique sean supervisados y los datos de dichas cámaras o mecanismos se almacenen durante al menos tres meses.			
7.	Determine si el lugar donde se encuentran los equipos de cómputo están a salvo de: – Inundaciones. – Terremoto. – Fuego. – Sabotaje.			
8.	Observe la salida de los visitantes de las instalaciones para verificar que se cumple con los procedimientos establecidos para el ingreso de			

	terceros.			
9.	Determine si existe personal de seguridad encargado de salvaguardar los equipos de cómputo de la institución, si está capacitado o ha sido asignado a las diferentes áreas.			
10.	Investigue cómo se asignan los derechos de ingreso físico, si se requiere alguna autorización, si existe algún registro o lista, cómo se revocan ingresos y cómo se comunica a los funcionarios de control de accesos.			
11.	Determine si los directorios y teléfonos internos que identifican los medios de procesamiento no son accesibles al público.			
12.	Determine si se restringe el acceso de equipo fotográfico, de video, audio, almacenamiento y otro equipo de grabación a las áreas aseguradas.			
13.	Determine si existen lineamientos sobre comer o beber en las proximidades de los equipos de cómputo.			
14.	Verifique que el sistema de alarmas contra incendio y extintores ha tenido el adecuado mantenimiento.			
15.	Determine si existe una alarma para detectar fugas de agua.			
16.	Verifique si existen pólizas de seguro y determine qué equipo está asegurado.			
17.	Determine si existe un plan de mantenimiento de las instalaciones eléctricas.			
18.	Verifique que los cables de energía están separados de los cables de comunicaciones para evitar interferencias.			
19.	Verifique que se utilizan marcadores de cables y equipo identificables.			
20.	Verifique si existe una lista de empalmes documentados.			
21.	Realice una inspección y determine si: – Existe un área de recepción para controlar el acceso a los locales y edificios. – Existe alguna barrera física para prevenir el acceso físico no autorizado. – Las puertas de salidas de emergencia cuentan con alarma. – Las puertas de emergencia cumplen con los estándares internacionales contra incendios. – Hay alarmas contra intrusos en todas las puertas externas y ventanas accesibles y en otros aposentos críticos.			

	– Los materiales peligrosos o combustibles son almacenados en un área segura, custodiados y de acceso restringido con un responsable. – Los suministros a granel, como papelería, no deben estar en el área asegurada. – Existe una distancia adecuada entre el equipo de reemplazo y los medios de respaldos para evitar daños de un desastre que afecte el local principal. – Existen extintores, si están ubicados adecuadamente y si funcionan de manera correcta. – Existen alarmas contra incendio y detectores de humo. – Existen mecanismos de control de rayos en todas líneas de ingreso de energía y comunicaciones. – Las paredes externas son sólidas y si las ventanas tienen verjas. – Las áreas donde se procesa información sensible son discretas, sin rótulos llamativos que identifiquen la presencia de actividades de procesamiento de la información. – Existen áreas aseguradas vacías, si están bajo llaves e indague si son revisadas periódicamente. – Existen controles de humedad y temperatura en las áreas donde está instalado el equipo de cómputo (deshumidificadores y aires acondicionados). – Los equipos están conectados a un dispositivo de suministro de energía ininterrumpido (UPS). – Existe un generador de emergencia y determine a qué equipos provee energía. – Existen luces de emergencia y verifique su adecuado funcionamiento. – Existen carteles para recordar las prohibiciones de fumar, tomar alimentos y refresco en las áreas donde están instalados los equipos de cómputo.			

Elaborado por:		Supervisado por:	
Fecha:		Fecha	

GUÍA DE AUDITORÍA Evaluación de la Seguridad en las Operaciones y Comunicaciones		G-7
Objetivo:	Evaluar la seguridad en las operaciones y comunicaciones.	
Criterio:	Norma 1.4.4 Seguridad en las operaciones y comunicaciones La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del *software* y de la información. Para ello debe: a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información. b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios. c. Establecer medidas preventivas, detectivas y correctivas con respecto a *software* "malicioso" o virus.	

No.	Procedimientos	Ref. P/T	Hecho por	Fecha
1.	Solicite y revise la política de seguridad en las operaciones y comunicaciones.			
2.	Indague sobre los controles que ha implementado la Administración para asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.			
3.	Determine cuáles son los procedimientos que ha establecido la Administración para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.			
4.	Determine cuáles son las medidas preventivas, detectivas y correctivas que ha establecido la Administración respecto a *software* "malicioso" o virus.			
5.	Obtener y revisar el diagrama completo de red, incluyendo una copia del diagrama de configuración del *hardware*, con todas las conexiones de la topología de red servidores, equipo de comunicaciones, estaciones, puentes y repetidores; además, determine que el diagrama de la red externa indica cómo acceder a partes de la red y de los			

	servicios.			
6.	Verifique que las normas de configuración del *firewall* y del *router* incluyan la descripción de grupos, roles y responsabilidades para una administración lógica de los componentes de la red.			
7.	Identifique servicios, protocolos y puertos no seguros.			
8.	Verifique la existencia de *firewalls* de perímetro instalados entre las redes inalámbricas y los sistemas que almacenan datos y que estos *firewalls* niegan y controlan todo el tráfico.			
9.	Verifique que todos los mecanismos antivirus sean actuales y que estén en funcionamiento.			
10.	Indague si la Administración hace revisiones regulares para detectar el uso de *software* no autorizado.			
11.	Determine si existe un inventario de las aplicaciones accesibles desde el exterior y servicios.			
12.	Determine si existe un terminal específico diseñado para monitorizar la actividad dentro del sistema *online.*			
13.	Determine cuáles son los controles de los medios de desarrollo, prueba y operación.			
14.	Determine si los servicios prestados por terceros son monitoreados y revisados regularmente considerando: – Niveles de desempeño del servicio. – Reportes de servicios. – Incidentes de seguridad de la información. – Rastros de auditoría. – Eventos de seguridad. – Problemas operacionales. – Fallas de monitoreo e interrupciones del servicio entregado.			
15.	Determine cuáles son los controles implementados para la instalación y actualización del *software*.			

Elaborado por:		Supervisado por:	
Fecha:		Fecha	

GUÍA DE AUDITORÍA Evaluación del Control de Accesos	G-8
Objetivo:	Evaluar el control de accesos.
Criterio:	Norma 1.4.5 Control de acceso. La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe: a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al *software* de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación. b. Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad. c. Definir la propiedad, custodia y responsabilidad sobre los recursos de TI. d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI. e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones. f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.[49] i. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios. j. Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI. k. Manejar de manera restringida y controlada la información sobre la seguridad de las

No.	Procedimientos	Ref. P/T	Hecho por	Fecha
1.	Obtenga y revise las políticas, reglas y procedimientos relacionados con el acceso a la información, al *software* de base y de aplicación, a las bases de datos			

[49] En el original no existe el punto g y h.

	y a las terminales y otros recursos de comunicación.			
2.	Indague sobre la clasificación de los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.			
3.	Verifique que la responsabilidad de supervisar y controlar todos los accesos a los datos esté formalmente asignada.			
4.	Determine cuáles son los controles para definir la propiedad, custodia y responsabilidad sobre los recursos de TI.			
5.	Obtenga y revise los manuales de procedimientos donde se definen los perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.			
6.	Determine si hay un proceso para revisión de los derechos de los usuarios, dado un cambio en el puesto y las funcione o salida de un funcionario, así como los derechos de privilegios para asegurarse que no se hayan obtenido accesos o privilegios no autorizados.			
7.	Verifique que todos los usuarios (muestra) tengan asignada una ID (identificador único) para tener acceso a componentes del sistema.			
8.	Verifique mediante una muestra que los derechos asignados a los usuarios corresponden a los establecidos en las políticas estabilidad por el MEP.			
9.	Verifique que todos los medios se hayan clasificado de manera que la sensibilidad de los datos se pueda determinar.			
10.	Determine cuáles son los controles para la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.			
11.	Verifique que se cumplen los procedimientos para el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI.			
12.	Determine cuáles son los controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.			
13.	Identifique cuáles son los mecanismos que permiten establecer las pistas de auditoría, para el adecuado y			

	periódico seguimiento al acceso a las TI.			
14.	Determine si un existe sistema de monitoreo que considere: usuario, fecha y hora de los eventos claves, tipos de eventos, archivos a los cuáles se tuvo acceso a programas/utilidades utilizados, intentos no autorizados, detección de intrusos, alerta o falla del sistema entre otros.			
15.	Indague cuál es el procedimiento para registrar las fallas y las acciones que ha tomado la Administración.			
16.	Determine cuáles son los procedimientos para identificar la identidad de una persona antes de proporcionar una clave nueva, sustituta o temporal.			
17.	Determine cuáles son los lineamientos para la selección y uso de las claves confidenciales para el uso de los sistemas.			
18.	Seleccione una muestra de empleados cesantes en los últimos seis meses y revise las listas de acceso de usuario actuales para verificar que sus ID se hayan desactivado o eliminado.			
19.	Verifique que el acceso físico a los puntos de acceso inalámbricos, *gateways*, dispositivos manuales, *hardware* de redes/comunicaciones y líneas de telecomunicaciones haya sido correctamente limitado.			
20.	Mediante observación y entrevista al administrador del sistema, verifique que las pistas de auditoría estén habilitadas y activas para los componentes del sistema.			
21.	Verifique que solo las personas que lo necesiten por motivos relacionados con el trabajo, puedan visualizar los archivos de las pistas de auditoría			
22.	Verifique que los archivos actuales de las pistas de auditoría estén protegidos contra modificaciones no autorizadas a través de los mecanismos de control de acceso, segregación física o segregación de redes.			
23.	Verifique que se haya realizado copia de seguridad de los archivos actuales de las pistas de auditoría inmediatamente en un servidor de registros central o en los medios que resulten difíciles de modificar.			
24.	Verifique que los registros de auditoría se encuentren disponibles durante al menos un año y que se implementen los procesos para restaurar al menos los registros de los últimos tres meses para el análisis inmediato.			

Elaborado por:		Supervisado por:	
Fecha:		Fecha	

GUÍA DE AUDITORÍA **Evaluación de la Seguridad en la Implementación y Mantenimiento de *Software* e Infraestructura Tecnológica**	**G-9**
Objetivo:	Evaluar la seguridad en la implementación y mantenimiento de *software* e infraestructura tecnológica.
Criterio:	1.4.6 Seguridad en la implementación y mantenimiento de *software* e Infraestructura tecnológica. La organización debe mantener la integridad de los procesos de implementación y mantenimiento de *software* e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información. Para ello debe: a. Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de *software* e infraestructura. b. Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del *software* e infraestructura. c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción. d. Controlar el acceso a los programas fuente y a los datos de prueba.

No.	**Procedimientos**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Determine cuáles han sido los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de *software* e infraestructura.			
2.	Determine cuáles son los procedimientos establecidos para el mantenimiento y puesta en producción del *software* e infraestructura.			
3.	Determine cuáles son los controles para mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.			
4.	Determine cuáles son los controles establecidos para controlar el acceso a los programas fuentes y a los datos de prueba.			
5.	Examine que se incluya la seguridad de la información en todos los procesos de desarrollo de *software* escritos.			
6.	Revise la aplicación, adquisición, implementación y planes de pruebas para confirmar que se han abordado la seguridad de las aplicaciones y la disponibilidad en el entorno integrado.			

Elaborado por:		Supervisado por:	
Fecha:		Fecha	

GUÍA DE AUDITORÍA Evaluación de la Continuidad del los Servicios de TI				G-10
Objetivo:	Evaluar la gestión de la continuidad de los servicios de TI.			
Criterio:	Norma 1.4.7 Continuidad de los servicios de TI. La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.			
No.	**Procedimientos**	**Ref. P/T**	**Hecho por**	**Fecha**
1.	Indague sobre la existencia un plan de continuidad de servicio de TI o recuperación de desastres para todas las funciones de negocio claves y procesos.			
2.	Determine si los diferentes actores tienen establecidos su rol, responsabilidades y los procedimientos para la efectiva ejecución del plan de continuidad de los servicios de TI y si están documentados y actualizados.			
3.	Verifique si el Plan de Continuidad de los servicios de TI está: a) Actualizado. b) Aprobado. c) Comunicado a los funcionarios. d) Es de conocimiento de los funcionarios.			
4.	Determine que hay un control de cambios para asegurar el plan de continuidad de los servicios de TI. Si existe, verifique que se mantiene actualizado y responde a los requerimientos actuales del negocio, considerando: – La adquisición de nuevo equipo. – Actualización de los sistemas – Y cambios en: a) Personal. b) Direcciones o número de teléfono. c) Estrategia comercial. d) Local, medios y recursos. e) Legislación. f) Contratista, proveedores y clientes clave. g) Proceso, los nuevos o los eliminados. h) Riesgo (operacional y funcional).			

5.	Determine si el plan Continuidad de los Servicios de TI considera: a) Guía sobre cómo utilizar el plan de continuidad de los servicios de TI. b) Procedimientos de respuesta definidos para retornar al estado que estaba antes del incidente o desastre. c) Procedimientos de recuperación en un eventual desastre. d) Procedimientos para salvaguarda y reconstrucción de las instalaciones de procedimientos normales. e) Procedimientos de coordinación con autoridades públicas. f) Procedimientos de comunicación con los funcionarios, dependencias externas, proveedores críticos, directores y el Ministro. g) El almacenamiento externo de copias de respaldo, documentación y otros recursos de TI, catalogados como críticos. h) Análisis del impacto por la falta de continuidad de los servicios de TI.			
6.	Verifique que se ha identificado los eventos a los que está expuesto el Ministerio, que pueden causar interrupciones a los procesos, junto con la probabilidad e impacto, así como las consecuencias que puede tener sobre la seguridad de la información.			
7.	Determine si el Plan de Continuidad de los Servicios de TI establece los responsables de la ejecución.			
8.	Determine, luego de verificar la evaluación de riesgo, si se ha establecido una estrategia de continuidad de los servicios de TI.			
9.	Dado que en el plan de continuidad de los servicios de TI hay información confidencial, solicite: – La estrategia de distribución de los planes de continuidad de TI. – Lista de personal con acceso al Plan. – Ubicación de los lugares donde están almacenados las copias de los planes de continuidad de los servicios de TI. – Solicite al personal con acceso a los planes el Plan de Continuidad de TI. Asegúrese de que los planes se distribuyen de forma apropiada y segura y que están disponibles entre las partes involucradas y autorizadas cuando			

	se requiera.			
10.	Solicite los reportes o informes con los resultados de las pruebas realizadas al plan de continuidad de los servicios de TI y determine si el programa de pruebas considera: – Pruebas flexibles de simulación con varios escenarios. – Simulaciones. – Pruebas de recuperación técnica, asegurado que los sistemas puedan restaurarse de manera efectiva. – Pruebas de recuperación local alternativas, corriendo los procesos en paralelo a las operaciones. – Pruebas de los medios y servicios del proveedor. – Ensayos completos, con toda la organización y el personal. Además, analice los resultados obtenidos en las pruebas y las acciones tomadas.			
11.	En el caso de una reanudación de las funciones de TI, determine cuáles han sido las acciones de la Administración para valorar el adecuado plan y si se requiere alguna actualización. Además, determine si existen procedimientos para tal fin.			
12.	Determine si existen procedimientos alternativos de procesamiento, que puedan ser utilizados mientras la función de TI sea capaz de restaurar completamente los servicios después de un evento o desastre.			
13.	Solicite el inventario actualizado de los equipos informáticos, su ubicación y nivel de uso institucional para los procesos críticos.			
14.	En el caso de que los equipos sean arrendados, solicite y analice los acuerdos del contrato. Además, solicite copia de las pólizas de seguro que cubren los equipos informáticos y determine qué equipos están cubiertos y cuál es el tipo de cobertura y el monto asegurado.			
15.	Determine si existe un procedimiento para efectuar el proceso de evaluación y selección y contratación de los seguros.			
16.	Determine si hay datos y operaciones críticas debidamente identificadas, documentadas, priorizadas y aprobadas por los dueños de la información, en razón de una política institucional y			

	mediante un manual de procedimientos.			
17.	Determine si existe un procedimiento para el almacenamiento de los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI.			
18.	Determine si la Administración ha realizado alguna evaluación de los centros de almacenamiento externos, respecto al contenido, la protección ambiental y la seguridad.			
19.	Determine el impacto que pueden tener las interrupciones causadas por incidentes en la seguridad de la información.			

Elaborado por:		Supervisado por:	
Fecha:		Fecha	

3.2.5.2 Diseño de la hoja de hallazgos

En razón de que la DAI tiene establecidas sus políticas y procedimiento, para la hoja de hallazgo no se va a proponer ningún diseño, no obstante, en el Manual de Políticas y Procedimientos de Auditoría de la DAI se establecen los lineamientos que se deben observar en la elaboración de los estudios, específicamente en el numeral 4.11, que señala que los atributos del hallazgo son:

> *a) Condición: constituye la situación encontrada por el auditor con respecto a una operación, actividad o transacción. La condición refleja el grado en que los criterios están siendo logrados o aplicados.*
> *b) Criterio: Es la norma o parámetro con la cual el auditor mide la condición. Son las metas que la entidad u órgano auditado está tratando de lograr o las normas relacionadas con su logro. Constituyen las unidades de medida que permiten la evaluación de la condición.*
> *c) Causas: Es la razón o razones fundamentales por las cuales se presentó la condición, o es el motivo por el que no se cumplió el criterio o la norma. Las recomendaciones que se formulen como resultado del estudio, deben estar directamente relacionadas con las causas que se hayan identificado.*
> *d) Efecto: Es el resultado o consecuencia real o potencial que resulta de la comparación entre la condición y el criterio que debió ser aplicado. Sean estos reales o potenciales, deben definirse en lo posible en términos cuantitativos, como moneda, tiempo, unidades de producción o números de transacciones. El establecimiento de efectos ayuda a demostrar la necesidad de acción correctiva y provee la evidencia sobre la importancia del hallazgo. Algunas veces no es posible la cuantificación del*

efecto, sin embargo esto no es una razón válida para no informar sobre observaciones importantes.[50]

Además, debe tener los siguientes requisitos básicos:

a) Importancia relativa que amerite su desarrollo y comunicación formal.
b) Basado en hechos y evidencia precisos que figuren en los papeles de trabajo.
c) Objetivo, al fundamentarse en hechos reales.
d) Basado en una labor de auditoría suficiente para respaldar las conclusiones resultantes.
e) Convincente para una persona que no ha participado en la ejecución de la auditoría.[51]

Y adicionalmente es importante considerar los siguientes elementos:

a) Identificar las líneas de autoridad y de responsabilidad en la entidad u órgano con respecto a la condición encontrada.
b) Determinar si la deficiencia es aislada o muy difundida, o sea la frecuencia de la deficiencia para evaluar si se trata de un caso aislado o representa una debilidad sistemática general.
c) Obtener opiniones de los funcionarios y entidades directamente relacionadas.
d) Determinar las conclusiones de auditoría con base en la evidencia acumulada.
e) Definir las acciones correctivas (recomendaciones).[52]

3.2.5.3 Elaboración del informe

No se va a proponer ningún esquema de elaboración del informe, ya que la DAI ha dispuesto, en su Manual de Políticas y Procedimientos de Auditoría, que los capítulos del texto de un informe son *"la Introducción, los Comentarios, las Conclusiones, las Recomendaciones y los Anexos. El informe deberá llevar un índice al inicio y el resumen ejecutivo que se solicita en el punto 7.18".*[53]

Además, ha establecido una serie de normas en cuanto a la presentación del informe y sobre el fondo, las cuales son de acatamiento obligatorio.

---

[50] DAI. (2012). Manual de Políticas y Procedimientos de auditoría. (numeral 4.11).
[51] DAI. (2012). Op. Cit. (Numeral 4.12).
[52] DAI. (2012). Op. Cit. (Numeral 4.12).
[53] DAI. (2012). Op. Cit. (Numeral 7).

CAPÍTULO IV: CONCLUSIONES

En este capítulo se plasman las conclusiones de haber planteado la propuesta de la guía de auditoría de TI desarrollada en los capítulos anteriores.

En relación con los objetivos planteados y la guía de auditoría realizada en el desarrollo de esta práctica profesional, merecen destacarse las siguientes conclusiones.

La dependencia de la TI se ha acrecentado en una herramienta para la prestación de los servicios públicos, representando importantes inversiones en el presupuesto del MEP en particular y del Estado en general.

Existen varios marcos de control aceptados internacionalmente, como la serie de estándares ISO 27000, entre ellas destaca la ISO 27001 e ISO 27002 para la gestión de la seguridad de la información, así como COBIT 4.1 para el control de la información.

A nivel personal se identificó dos beneficios. Primero, se logró un mayor conocimiento del estándar ISO 27002 con el desarrollo de esta guía de auditoría, la cual es un marco de referencia que provee un norte para iniciar el proceso de gestión de la seguridad de la información. Cualquier organización puede implementar las buenas prácticas de este estándar de la forma que más se adecue a la naturaleza de sus operaciones. Cabe indicar que Sistema de Gestión de la Seguridad es certificable mediante la ISO 27001, por lo que aquella organización que siga estos estándares puede solicitar una auditoría a una entidad certificadora acreditada para obtener la respectiva acreditación.

Segundo, se adquirió mayor conocimiento en los procesos de control de Cobit 4.1, el cual es una guía de mejores prácticas en la gestión de las TI, en especial en los controles relacionados con la seguridad de la información.

A nivel institucional, en cuanto a los aspectos de seguridad de la NT (2007) se puede concluir los siete aspectos siguientes.

El marco de seguridad de la información en toda institución es un tema que debe ser desarrollado a lo interno de la organización y para ser implementado se requiere el compromiso desde la más alta jerarquía para una buena gestión de la seguridad de la información.

La seguridad física y ambiental logra prevenir el acceso físico no autorizado, daños a la información y las instalaciones.

La seguridad en las operaciones y comunicaciones proporciona la correcta y segura operación de las áreas de procesamiento.

El control de acceso físico y lógico a los activos de información establece parámetros para controlar el acceso de los usuarios no autorizados que pretendan afectar la disponibilidad, la integridad y la confidencialidad de la información.

La seguridad en la implementación y mantenimiento de *software* e infraestructura tecnológica establece la inclusión de controles de seguridad en los sistemas de información.

Con la gestión de la continuidad de los servicios de TI se minimiza el impacto sobre la organización de aquellos procesos críticos consecuencia de los efectos de fallas o desastres en los sistemas de información y facilita recuperarse de las pérdidas de activos de información a un nivel aceptable, para que objetivos organizacionales no se vean afectados.

El MEP ha realizado un esfuerzo importante en la implementación de las NT (2007), con el fin de cumplir con el ordenamiento aplicable, por lo que es necesario evaluar la gestión de la seguridad de la información pues la falta de fiscalización podría convertirse en un riesgo, ya que la gestión podría estarse dando de forma no controlada, de manera que afecte el cumplimiento de los objetivos organizacionales y la seguridad de la información.

REFERENCIAS

Libros

Arens, A. y Loebbecke, J. (1996). *Auditoría un Enfoque Integral.* 6° edición, México D.F.: Pearson Prentice Hall.

Azofeifa, I. (1979). Guía para la investigación y desarrollo de un tema. San José: Editorial UCR.

Cano, J. (2009). *Computación Forense*. México D.F.: Alfaomega Grupo Editor.

Delgado, X. (1997). *Auditoría Informática*. San José: Editorial Universidad Estatal a Distancia.

Echenique, J. (2001). *Auditoría en Informática*. México D.F.: McGraw-Hill.

Gómez A. y Suárez C. (2009). *Sistemas de Información: Herramienta práctica para la gestión.* 3° edición. México D.F.: Alfaomega Grupo Editor.

Hernández, E. (2000). *Auditoría en Informática*. 2° edición. México D.F.: CECSA.

Muñoz, C. (2002). *Auditoría en Sistemas Computacionales.* México D.F.: Pearson Prentice Hall.

Piattini, M. y Navarro, E. (2001). *Auditoria Informática, un enfoque práctico*. 2° edición ampliada y revisada. México D.F.: Alfaomega Grupo Editor.

Tupia, M. (2010). *Administración de la Seguridad de Información.* Lima: GRAFICAR.

Otros documentos

CGR (N-2-2009- CO-2009). *Normas de Control Interno para el Sector Público.*

DAI (2012). *Manual de Políticas y Procedimiento de la Auditoría*.

El Presidente de la República y el Ministro de Educación Pública. (2008). *Decreto Ejecutivo N°34427-MEP* .

International Organization for Standardization. ISO/IEC 27002:2005. *Information technology - Security techniques - Code of practice for information security management.* EE.UU.

*International Organization for Standardizatio*n. (2005) ISO/IEC 27001:2005. *Information technology-Security techniques-Information security management systems–Requirements*. EE.UU.

International Organization for Standardization. (2005) ISO/IEC 27002:2005. *Information technology-Security techniques-Information security management systems–Requirements*. EE.UU.

IT Governance Institute, ITGI. (COBIT 4.1, 2007). *Control Objective for Information and Related Technologies.* EE.UU.CGR. (N-2-2009- CO-2009). Normas de Control Interno para el Sector Público.

Documentos electrónicos

CGR. (2009). *Normas Técnicas en Tecnologías de Información y Comunicaciones.* Recuperado de http://documentos.cgr.go.cr el 21 de setiembre de 2012.

CGR. (2006). *Manual de Normas Generales de Auditoría para el Sector Público (M-2-2006-CO-DFOE)*. Recuperado del sitio *web* http://documentos.cgr.go.cr el 5 de mayo de 2013.

Dirección de Informática de Gestión. (s.f.) *Procedimiento Contratación de Servicios Prestados por Terceros*. Recuperado del sitio *web* http://www.mep.go.cr el 19 de enero de 2013.

MEP. (2009). *Política Nacional en Aplicación de las Tecnologías de la Información y la Comunicación a la Educación.* Recuperado del sitio *web* http://www.mep.go.cr el 5 de abril de 2013.

MEP. (Versión 1, 23 febrero 2012). *Manual Modelo de la Arquitectura de Información*. Recuperado del sitio *web* http://www.mep.go.cr el 19 de enero de 2013.

MEP. (Versión 3, del 14 de febrero de 2012). *Manual de Lineamientos del Uso de los Recursos Informáticos Institucionales*. Recuperado del sitio *web* http://www.mep.go.cr el 19 de enero de 2013.

MEP. (Versión 3, del 15 de febrero de 2012). *Estándares para el Proceso Institucional de Desarrollo y Mantenimiento de Software.* Recuperado del sitio *web* http://www.mep.go.cr el 19 de enero de 2013.

MEP. (Versión 1, 23 Febrero del 2012). *Plan de Aseguramiento para la Continuidad del Servicio en los Procesos Críticos de TI.* Recuperado del sitio *web* http://www.mep.go.cr el 19 de enero de 2013.

MEP. *Misión & Visión.* Recuperado del sitio *web* http://www.mep.go.cr el 10 de abril 2013.

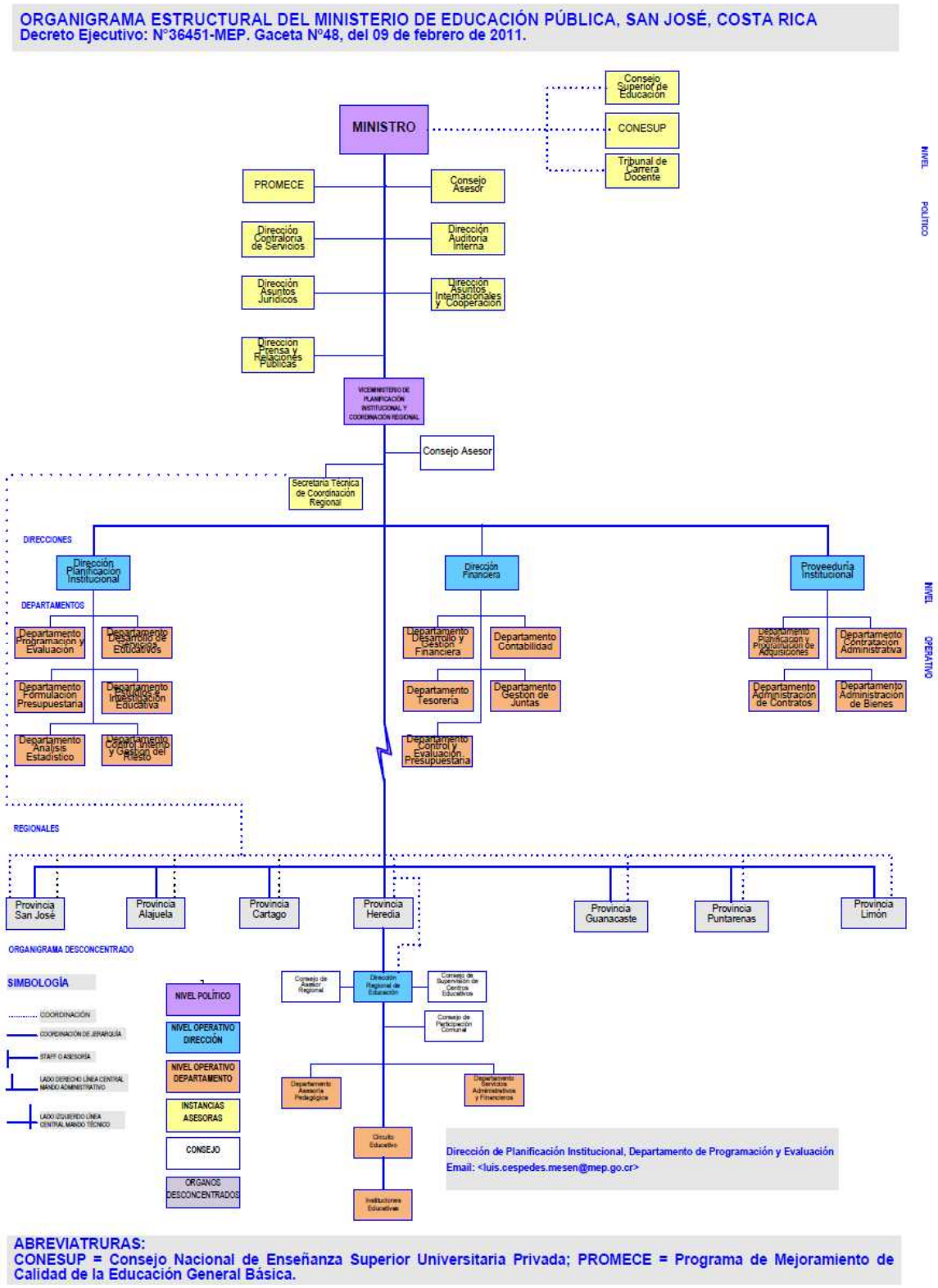
Morera C. (Versión 4, del 8 de abril 2012). *Manual de Configuraciones de Redes y Telecomunicaciones.* Recuperado del sitio *web* http://www.mep.go.cr el 19 de enero de 2013.

Morera I. (Versión 1, del 11 de febrero 2010). *Manual Estándar para el Desarrollo de un Proyecto en TI*. Recuperado del sitio *web* http://www.mep.go.cr el 19 de enero de 2013.

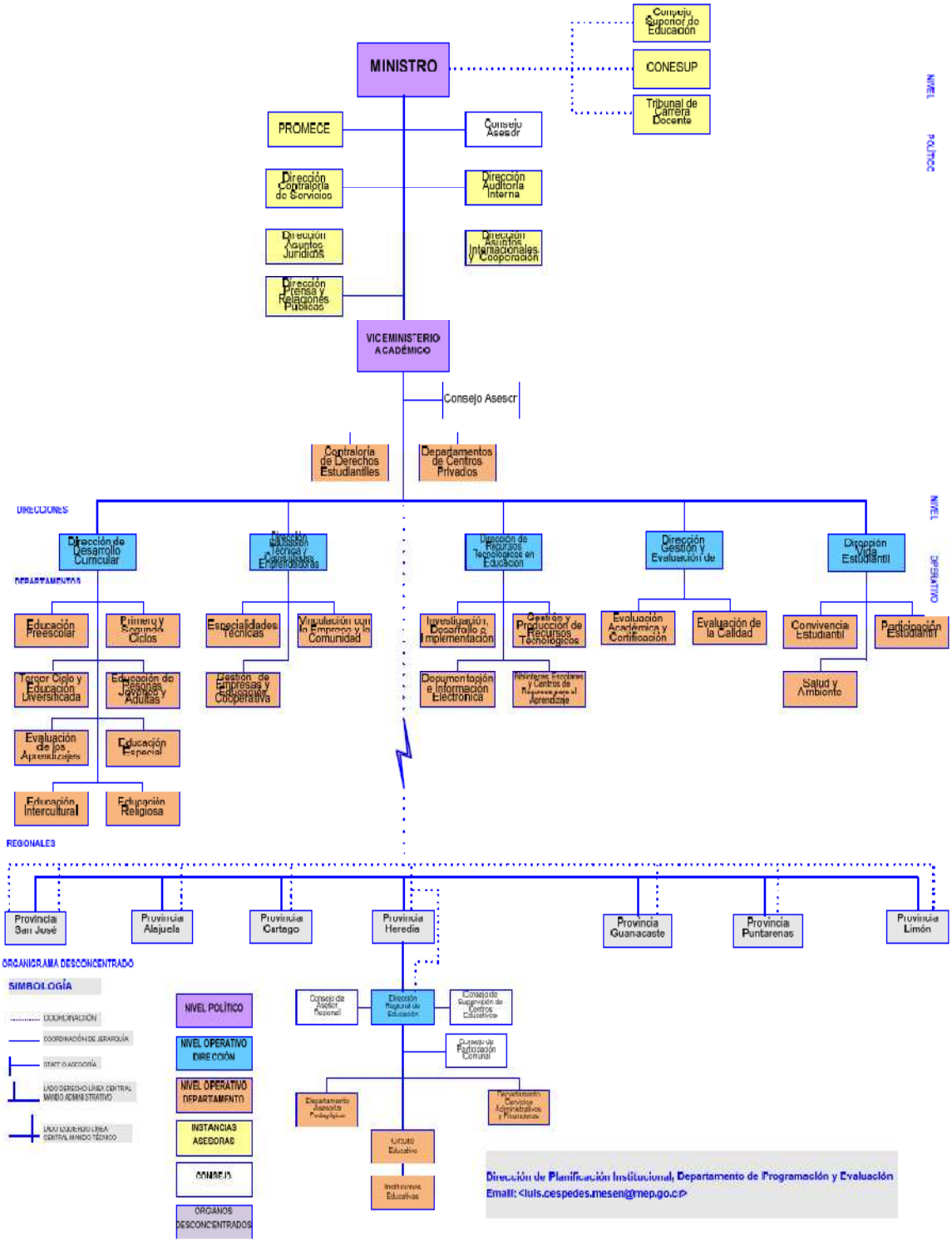
Padilla. F. (Versión 1, 2012). *Manual de estándares informáticos*. Recuperado del sitio *web* http://www.mep.go.cr el 19 de enero de 2013.

Sánchez R. (s.f.). *Procedimiento para la Presupuestación y Elaboración del Plan de Adquisiciones de Equipo de Cómputo para Oficinas Centrales y Direcciones Regionales.* Recuperado del sitio web http://www.mep.go.cr el 19 de enero de 2013.

ANEXO: Organigrama MEP

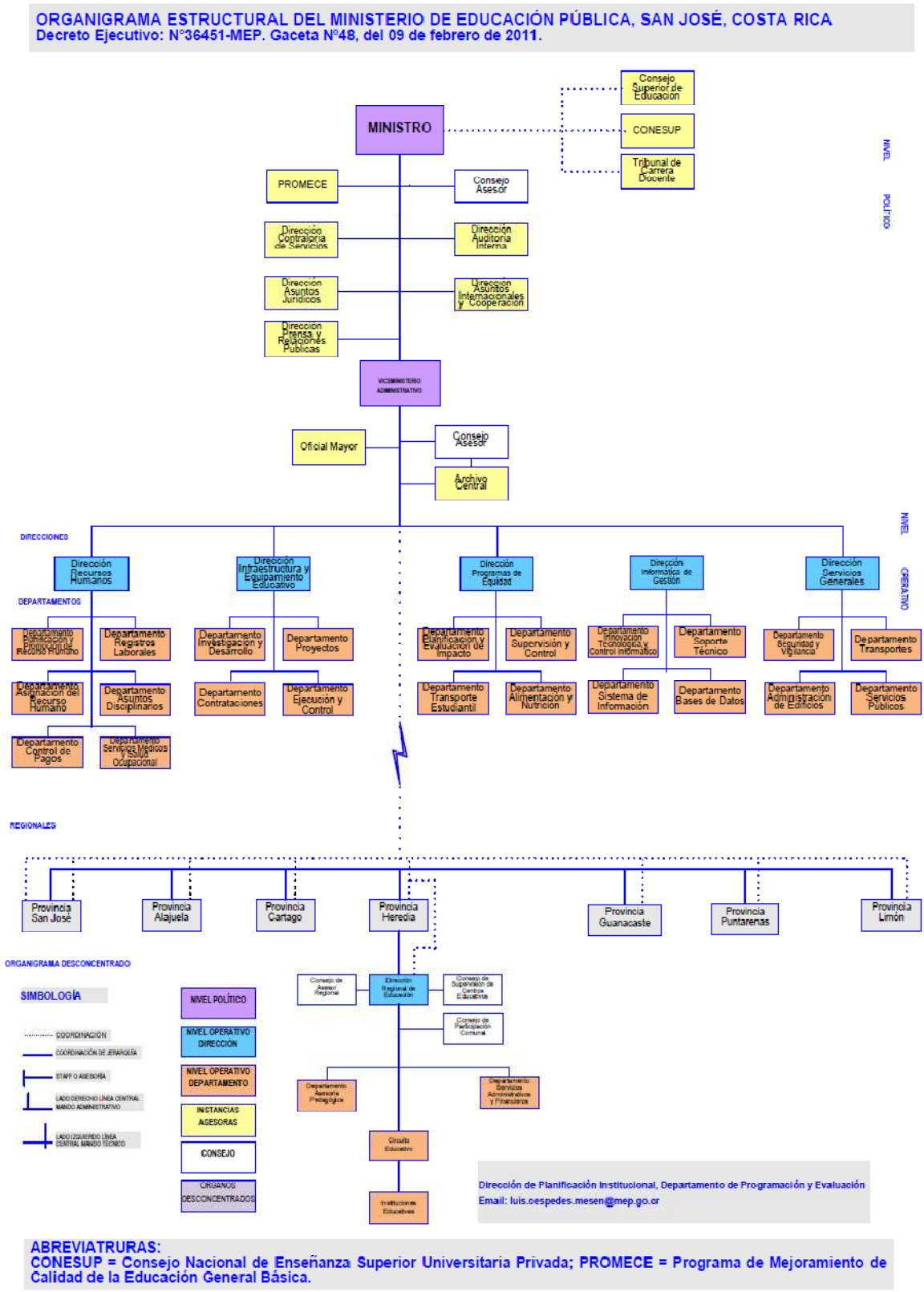


ORGANIGRAMA ESTRUCTURAL DEL MINISTERIO DE EDUCACIÓN PÚBLICA, SAN JOSÉ, COSTA RICA
Decreto Ejecutivo: N°36451-MEP. Gaceta Nº48, del 09 de febrero de 2011.



Dirección de Planificación Institucional, Departamento de Programación y Evaluación
Email: <luis.cespedes.mesen@mep.go.cr>

ABREVIATRURAS:
CONESUP = Consejo Nacional de Enseñanza Superior Universitaria Privada; PROMECE = Programa de Mejoramiento de Calidad de la Educación General Básica.



Fuente: MEP recuperado de http://www.mep.go.cr/acercadelmep/organizacion.aspx el 10 de enero de 2013.