

Universidad CENFOTEC

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Diseño del Sistema de Gestión de Seguridad de la Información en el Ministerio de Educación Pública de Costa Rica

Serrano Gamboa Katherine

Campos Pérez María de los Ángeles

Julio 2020

Declaratoria de derechos de autor

Por medio de la presente se prohíbe estrictamente la consulta, reproducción, distribución o retransmisión de manera electrónica o impresa de la tesis “Diseño del Sistema de Gestión de Seguridad de la Información en el Ministerio de Educación Pública de Costa Rica”, efectuada por María de los Ángeles Campos Pérez y Katherine Serrano Gamboa, por un plazo de 5 años según lo acordado entre los estudiantes y la Universidad Cenfotec, debido a que el documento incluye información confidencial del Ministerio de Educación Pública de Costa Rica.

Dedicatoria y agradecimientos

Este proyecto lo dedico a todas las personas que estuvieron apoyándome y motivándome durante estos años, familia, compañeros de trabajo, amigos y principalmente a Dios que es el que me permite levantarme cada día con fuerzas para emprender y ser mejor. Hoy más que nunca puedo decir que rodearse de personas exitosas se convierte en el motor de inspiración para seguir luchando por lograr mejores cosas en la vida.

Gracias a todos los que creyeron en mí, por sus consejos y recomendaciones.

Katherine Serrano Gamboa

Dedico este trabajo principalmente a Dios y a mis padres cuyo apoyo ha sido incondicional durante todos mis años de estudio, ellos son quienes me han impulsado y me han enseñado a no rendirme. También dedico a mis compañeros y amigos que me ayudaron y apoyaron durante todo el proceso universitario.

Un especial agradecimiento al profesor Miguel Pérez Montero por ofrecer su ayuda, guía y consejo durante todo el proceso, aprendimos muchísimo de toda su experiencia y visión.

Maria Campos Pérez

universidad cenfotec_
tecnologías digitales

Universidad Cenfotec
Carrera de Postgrado
Maestría en Ciberseguridad

Acta N° 093

En conformidad con la reglamentación de la Universidad Cenfotec, se inscriben a los estudiantes, ***María de los Ángeles Campos Pérez y Katherine Guiselle Serrano Gamboa,*** número de identificación: ***402140101 y 114880315,*** de la carrera: Maestría en Ciberseguridad, quienes presentaron y defendieron su Proyecto de Investigación Aplicada 2, titulado: ***"Diseño del Sistema de Gestión de Seguridad de la Información en el Ministerio de Educación Pública de Costa Rica".***
Para optar por el grado de: **Maestría en Ciberseguridad.**

Una vez concluida la exposición, el periodo de preguntas y efectuada la deliberación se otorga la calificación de:

[X] Aprobado

[ ] Reprobado. Razones por las que reprobó: _____

_____

		María	Katherine
Documento escrito:	*70%	67.33	67.33
Defensa:	*30%	28.33	28.33
Nota obtenida:		96	96

**Promedio simple de los miembros del tribunal examinador*

Por sus méritos, el Tribunal recomienda la distinción:

[ ] Sin distinción
[X] Cum Laude
[ ] Magna Cum Laude
[ ] Summa Cum Laude

Firmamos conforme, el **03 de julio de 2020**, a las **19:48** horas.

MIGUEL PEREZ MONTERO (FIRMA) Digitally signed by MIGUEL PEREZ MONTERO (FIRMA) Date: 2020.07.06 09:56:07 -06'00'

M. Sc. Miguel Pérez Montero
Tutor

DENNIS ALONSO DURAN CESPEDES (AUTENTICACION) Firmado digitalmente por DENNIS ALONSO DURAN CESPEDES (AUTENTICACION) Razón: Soy el autor de este documento Ubicación: la ubicación de su firma aquí Fecha: 2020-07-06 20:12:30 Foxit Reader Versión: 9.7.0

M. Sc. Dennis Durán Céspedes
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA) Digitally signed by IGNACIO TREJOS ZELAYA (FIRMA) Date: 2020.07.08 12:14:03 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

Tabla de Contenido

ABSTRACT **1**

CAPÍTULO 1. INTRODUCCIÓN **2**

1.1 GENERALIDADES 2

1.2 ANTECEDENTES DEL PROBLEMA 2

1.3 DEFINICIÓN Y DESCRIPCIÓN DEL PROBLEMA 3

1.4 JUSTIFICACIÓN 4

1.5 VIABILIDAD 6

1.6 OBJETIVOS 7

1.6.1 Objetivo General. *7*

1.6.2 Objetivos Específicos. *8*

1.7 ALCANCES Y LIMITACIONES 8

1.7.1 Alcance. *8*

1.7.2 Limitaciones. *10*

1.8 MARCO DE REFERENCIA ORGANIZACIONAL Y SOCIOECONÓMICO 11

1.8.1 Historia. *11*

1.8.2 Tipo de Negocio y Mercado Meta. *13*

1.8.3 Misión, Visión y Valores. *13*

1.8.4 Políticas Institucionales. *15*

1.9 ESTADO DE LA CUESTIÓN 15

1.9.1 Formulación de la pregunta. *15*

1.9.2. Selección de fuentes. *17*

1.9.3. Selección de estudios. *18*

1.9.4. Ejecución de la selección. *18*

1.9.5. Extracción de información. *18*

CAPÍTULO 2. MARCO CONCEPTUAL 19

2.1 ELABORACIÓN DEL MARCO CONCEPTUAL 19

2.2 MARCO CONCEPTUAL 21

CAPÍTULO 3. MARCO METODOLÓGICO 26

3.1. TIPO DE INVESTIGACIÓN 26

3.2. ALCANCE INVESTIGATIVO 27

3.3. ENFOQUE 28

3.4. DISEÑO 28

3.5. SUJETOS Y FUENTES DE INFORMACIÓN 29

3.6. INSTRUMENTOS 30

CAPÍTULO 4. PROPUESTA DE SOLUCIÓN 30

4.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 33

4.2. CONTINUIDAD DE SERVICIOS INFORMÁTICOS 35

CAPÍTULO 5. RESULTADOS 37

CAPÍTULO 6. CONCLUSIONES 40

CAPÍTULO 7. GLOSARIO 43

8. REFERENCIAS 47

9. ANEXOS 52

9.1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 52

9.2. PLAN DE CONTINUIDAD DE SERVICIOS 94

9.3. CRONOGRAMA PARA LA IMPLEMENTACIÓN DEL SGSI 122

9.4. APROBACIÓN DEL MEP DE LOS ENTREGABLES 123

9.5. SELECCIÓN DE ESTUDIOS INICIALES 124

Índice de Figuras

FIGURA 1. CICLO DE VIDA DEL SGSI 11

FIGURA 2. NUBE DE PALABRAS 20

FIGURA 3. MAPA CONCEPTUAL JERÁRQUICO DE CONCEPTOS RELEVANTES 21

FIGURA 4. FAMILIA DE PRODUCTOS COBIT 5 23

FIGURA 5. NIVELES DE DOCUMENTACIÓN 25

FIGURA 6. INVESTIGACIÓN APLICADA 27

FIGURA 7. PRINCIPALES MARCOS TEÓRICOS A PARTIR DE LOS CUALES SE DISEÑA LA INVESTIGACIÓN CUALITATIVA 29

FIGURA 8. EQUIPO DE RECUPERACIÓN 99

FIGURA 9. IMPACTO 103

FIGURA 10. ÁRBOL DE CONTACTOS 105

FIGURA 11. PROCEDIMIENTO DE REANUDACIÓN 107

FIGURA 12. DIAGRAMA DE RED 111

Índice de Tablas

TABLA 1. COSTO DE HORAS CONSULTOR 7

TABLA 2. PALABRAS CLAVE 16

TABLA 3. CONTACTOS 101

TABLA 4. PROCEDIMIENTO DE DIVULGACIÓN 116

TABLA 5. EVALUACIÓN DEL INCIDENTE 117

TABLA 6. LISTA DE CHEQUEO 119

TABLA 7. CRONOGRAMA 122

TABLA 8. ARTÍCULOS RELEVANTES DE SPRINGERLINK 124

TABLA 9. ARTÍCULOS RELEVANTES DE ACM DIGITAL LIBRARY 127

TABLA 10. ARTÍCULOS RELEVANTES DE WEB OF SCIENCE 128

TABLA 11. IEEE XPLORE DIGITAL LIBRARY 128

Abstract

Este proyecto de graduación consiste en diseñar un Sistema de Gestión de la Seguridad de la Información (SGSI) para el Ministerio de Educación Pública (MEP) de Costa Rica, encargado de velar por uno de los principales pilares para el desarrollo nacional, como lo es la educación.

El objetivo del SGSI abarca la creación de políticas de seguridad y un plan de continuidad conforme a estándares de la industria que le ayudarán al MEP a responder a incidentes de manera eficaz y efectiva.

Lo que se propone es entregarle al MEP un diseño de un SGSI que ayude y guíe al MEP a administrar la seguridad informática en toda la organización, puesto que se identificó que el MEP tiene muchas debilidades en esta área.

El proyecto no solo tiene un gran impacto para el departamento administrativo del MEP, sino también para todo el Ministerio en general, ya que estas políticas y plan de continuidad se debe presentar al comité de dirección para ser implementado a nivel general en toda la organización.

Palabras clave: MEP, seguridad, información, políticas, ministerio, educación, pública.

Capítulo 1. Introducción

1.1 Generalidades

Según la Contraloría General de la República (2017), el MEP es el órgano del estado costarricense responsable de la administración de todos los elementos relacionados con la educación en Costa Rica, ya que la educación es una prioridad para el desarrollo del ser humano en búsqueda de romper las barreras de la pobreza y la exclusión social en el país.

El MEP abarca gestiones que cubren la totalidad del territorio del país, con más de cinco mil centros educativos, divididos en veintisiete oficinas regionales, y más de ochenta y cuatro mil funcionarios. Para gestionar una institución de este tamaño, se debe recurrir al eficiente uso de la tecnología, a través de un efectivo Gobierno de las Tecnologías de Información, que garantice de manera razonable el alineamiento con los objetivos estratégicos institucionales y el soporte a los procesos sustantivos y de apoyo administrativo del MEP.

El proyecto se lleva a cabo basado en las buenas prácticas de *International Organization for Standardization* (ISO) 27001 por disposición del MEP. Según el ISO (2020), este estándar 27001 es un estándar para la seguridad de la información que especifica requisitos para implantar un SGSI.

1.2 Antecedentes del Problema

El MEP no ha realizado ninguna acción correctiva para buscar una solución a los problemas de seguridad informática que tiene actualmente, porque no posee políticas, estándares o mejores prácticas a nivel institucional para sus sistemas de

tecnologías de información por lo que cada unidad maneja la seguridad según su criterio.

Además, el MEP no tiene un plan de continuidad de servicios, políticas de seguridad, análisis y manejo de riesgos, control de personal en centros educativos, esto y más, fue visible en una auditoría externa que se realizó por primera vez al departamento administrativo de tecnologías de Información el 30 de noviembre del 2018.

El personal interno tiene poco conocimiento de las debilidades en seguridad informática que presenta esta organización y al existir problemas de comunicación entre las diferentes unidades es mucho más complicado un plan de acción.

1.3 Definición y Descripción del Problema

El MEP cuenta con una infraestructura tecnológica que abarca sus oficinas administrativas y además comprende los centros educativos dispersos por todo el territorio nacional. Cada sistema, computadora, o dispositivo, y además con poca o nula seguridad, representa para la institución un riesgo para su información. Sin bases claras como políticas, estándares o manuales, la seguridad se maneja a discreción de cada unidad o de cada empleado, haciendo la seguridad variable a lo largo de todos los componentes de la institución y no una constante para todas y cada una de las unidades.

El MEP ha identificado varios puntos débiles, inconsistencias y áreas de mejora en sus sistemas e infraestructura tecnológica que debe solventar creando un plan de gestión de la seguridad de la información que ayude a preservar la

confidencialidad, integridad y disponibilidad de la información, mejorando así los problemas de comunicación entre unidades y la poca dirección a la hora de tomar decisiones.

Según la Contraloría General de la República, no se cuenta con un plan para la gestión de la continuidad de servicios que integre los planes de contingencia informática, atención de emergencias, sucesión y recuperación de desastres, entre otros. No cuenta tampoco con un plan de contingencia informática formalmente establecido, actualizado y probado que se involucre e interactúe con todos los procesos de la organización.

Es importante mencionar que en el informe de la Contraloría General de la República se dice que el documento existente titulado “Plan de continuidad del servicio de los procesos críticos de TI”, con que cuenta el MEP constituye más bien una guía para la creación de un plan de continuidad y no corresponde a un plan de gestión de la continuidad de servicios que pueda gestionar situaciones de contingencia o recuperación luego de desastres, pues no especifica ni procedimientos ni responsables.

1.4 Justificación

El MEP abarca cinco mil centros educativos dispersos por todo el territorio nacional, veintisiete oficinas regionales y alrededor de ochenta y cuatro mil funcionarios y docentes.

Al ser el componente medular que administra la educación del país cuenta con una serie de procesos críticos para poder llevar a cabo la tarea de coordinar los

procesos educativos año con año, entre ellos matrículas, planes de estudio, evaluaciones, manejo de planilla, nombramientos, entre otros.

Debido a la relevancia que tiene el MEP para el país se puede justificar la importancia de un proyecto en seguridad informática para salvaguardar su información y asegurar la disponibilidad de sus servicios más críticos.

A lo largo de los años de trabajo del MEP, se han vislumbrado consecuencias por la falta de importancia hacia la seguridad, procesos y políticas claras, además de una cultura organizacional que apoye dicho enfoque. Un grave ejemplo es la noticia publicada en La Nación “funcionario de planillas logró que el MEP pagara 53 millones en salarios a falso profesor” (Cerdas, 2018), donde un funcionario de recursos humanos logró ingresar a una persona al sistema de planilla como profesor interino provocando que se le pagasen 53 millones de colones a un profesor ficticio. Se puede también evidenciar la filtración de las pruebas de bachillerato publicada en el artículo de La Nación “MEP abrirá investigación contra profesor en huelga que compartió examen de bachillerato luego de aplicado” (Gamboa, 2018), el cual relata que un profesor compartió la prueba de Estudios Sociales usando la red social de Facebook.

Todos estos acontecimientos mencionados anteriormente forman parte de una serie de riesgos que atentan contra la seguridad de la información, que debieron ser mitigados o eliminados para evitar su materialización. Es aquí donde un SGSI se centra en conocer, gestionar y minimizar los riesgos utilizando políticas, estándares, controles y métricas.

1.5 Viabilidad

1.5.1 Punto de vista técnico. El conocimiento y comprensión del tema es bastante amplio, ya que se cuenta con las bases académicas para llevarlo a cabo. Además, se hizo una investigación de cómo se han creado e implementado sistemas de gestión de la seguridad de la información en otras empresas, también se tuvo acceso a material sobre los estándares que rigen la industria en seguridad informática y cómo aplicar las buenas prácticas al MEP.

1.5.2 Punto de Vista Operativo. El MEP ha dejado de lado procesos clave que aseguren la continuidad de los servicios de tecnologías de información, la integridad de la información y su confidencialidad, comprometiendo la operación e información clave, tanto para los sistemas actuales que posee como para los sistemas futuros que tiene como objetivo desarrollar e implementar.

Este proyecto ayuda a fortalecer sus puntos débiles y mejorar la operación en lugar de interrumpirla. El personal técnico que tiene el MEP actualmente tiene conocimiento en seguridad informática y se espera que puedan continuar con el cronograma de actividades propuesto, y no sólo asegurarse de que sea puesto en práctica, sino que también opere a todos los niveles de la organización e incluso se dediquen recursos a la seguridad de la información.

1.5.3 Punto de Vista Económico. Desde una perspectiva económica el proyecto no genera gastos de licencias, equipo o recursos tecnológicos, estos insumos podrían requerirse en las fases de implementación del sistema, pero dichas fases quedan fuera del alcance del proyecto.

El único costo son las horas consultor, las cuales asumen las investigadoras dedicadas al proyecto por medio tiempo de lunes a viernes durante 8 meses. La tabla 1 muestra en detalle el costo de dichas horas:

Tabla 1

Costo de horas consultor

Rubro	**Costo teórico anual**
Perfil del asesor*	2 consultores * salario ¢322 000 *8 meses
Total Anual	¢5 152 000

Nota. El salario incluye cargas sociales. Elaboración propia

1.6 Objetivos

La taxonomía cognitiva que se utiliza es la de taxonomía revisada de Bloom, ya que es la más conocida y ampliamente utilizada, especialmente en el ámbito de la enseñanza. La taxonomía clasifica los objetivos de manera jerárquica y los ordena dependiendo de si la actividad requiere un procesamiento más complejo o no. Las seis categorías en la que está compuesta la taxonomía son: recordar, entender, aplicar, analizar, evaluar y crear. Se debe destacar que en Costa Rica se utiliza por el MEP y por universidades públicas como la UCR y la UNED.

1.6.1 Objetivo General. Diseñar el Sistema de Gestión de Seguridad de la Información en el Ministerio de Educación Pública de Costa Rica.

1.6.2 Objetivos Específicos.

- Definir políticas de seguridad que establezcan el compromiso de la dirección y enfoque del MEP en la gestión de la seguridad de la información.
- Analizar la estructura de los sistemas de información con el fin de proponer un plan que guíe al MEP a implantar un sistema de gestión de la seguridad de la información.
- Establecer un plan de continuidad de servicios de información para asegurar la disponibilidad y buen desempeño para uno de los servicios críticos en el MEP.
- Estructurar un cronograma con los hitos y metas que debe seguir el MEP como plan de acción futuro.

1.7 Alcances y Limitaciones

1.7.1 Alcance. Actualmente, el MEP cuenta con una infraestructura tecnológica que se divide en dos grandes áreas: una administrativa y otra educativa, la parte administrativa toma en cuenta las oficinas centrales y regionales; mientras que la parte educativa referencia la infraestructura que se encuentra en centros educativos como escuelas y colegios. Ambas áreas se gestionan de manera independiente y no se siguen estándares o políticas organizacionales para salvaguardar la información del MEP.

Este proyecto pretende generar los cimientos al MEP para implementar un SGSI que a largo plazo permitirá:

- Analizar y organizar la estructura de los sistemas de información.

- Facilitar la definición de procedimientos para mantener la seguridad de la información.
- Disponer de controles que permitan medir la eficacia de las medidas.

El proyecto abarca el diseño del SGSI y un cronograma que indique las fases, etapas y entregables para que el MEP pueda llevar a cabo con el fin de salvaguardar la confidencialidad, disponibilidad e integridad de la información. Queda a discreción del MEP la implementación del sistema de gestión de seguridad de la información una vez que se le entregue.

El diseño del plan de gestión de la seguridad de la información que se realiza se basa en buenas prácticas de la ISO 270001, pero solo se toma en cuenta la infraestructura y procesos que soporten los servicios críticos del MEP, por lo que el plan se desarrolla para el área administrativa.

El proyecto define un plan de continuidad de servicios críticos basado en las buenas prácticas de gobierno de tecnologías de información, cuya implementación puede garantizar razonablemente un servicio continuo de los sistemas más críticos que posee el MEP. El objetivo de un plan de continuidad de servicios es que la organización pueda continuar brindado sus servicios básicos durante el período de contingencia y recuperarse y restaurar los servicios y funciones críticas dentro de un tiempo razonable después de una falla, interrupción o desastre.

Se definen políticas de seguridad para que guíen a la organización a establecer un compromiso con la seguridad de la información a nivel gerencial.

Se le facilitan al MEP varios documentos, entre ellos: las políticas de seguridad, el plan de continuidad de servicios de tecnologías de información con los

pasos a seguir en caso de una interrupción o desastre y un documento con una lista de las cosas que se deben seguir para estar en cumplimiento con lo que se propuso.

Los documentos se entregan en formato .docx, en caso de que a futuro el MEP le quiera hacer algunas modificaciones y mantenerlo actualizado. También se entrega un documento indicando las etapas con las respectivas duraciones para que el MEP pueda continuar con las etapas restantes del proyecto.

Adicional se llevan a cabo reuniones para revisar los documentos y dar continuidad al MEP del por qué es importante seguir trabajando de la mano del sistema de seguridad de la información propuesto.

1.7.2 Limitaciones. El SGSI es bastante amplio ya que abarca muchas áreas de la seguridad informática.

En el proyecto, se planea para cada una de estas áreas, pero solo se trabaja sobre las dos más críticas para el MEP en este momento como lo son las políticas de seguridad y el plan de continuidad de servicios.

Las áreas que quedan pendientes de implementar por el MEP una vez que se les entregue el cronograma con el plan de acción son las siguientes:

- Gestión de activos.
- Gestión de riesgos.
- Seguridad física y perimetral.
- Estrategia de concienciación.

El ciclo del sistema de seguridad de la información se detalla en la Figura 1, el proyecto se enfoca en la etapa de planeamiento para todo lo que enumera y en la

etapa de “hacer” solo para dos de los planes (políticas de seguridad y plan de continuidad de servicios de información).



Figura 1. Ciclo de vida del SGSI (Elaboración propia)

1.8 Marco de Referencia Organizacional y Socioeconómico

En esta sección se incluye la historia, misión, visión y valores del MEP, datos que fueron tomados de su página web https://www.mep.go.cr/.

1.8.1 Historia. En el año 1886, en Costa Rica, se establece y entra en vigencia que la enseñanza primaria es gratuita, obligatoria y costeada por la Nación, se establece que en cada distrito escolar debe haber una Junta de Educación, compuesta por tres propietarios y dos suplentes. Estos organismos tienen el carácter de cuerpo municipal del distrito con las atribuciones que le fija la ley.

En el año 1849, se creó una ley que disponía el establecimiento de colegios por cada provincia y se hizo referencia al primer colegio en Alajuela.

En el año 1879, se inició el primer Colegio Oficial de Varones que ocupó el edificio denominado “Cuartel Viejo”.

Se crean luego sub-administraciones regionales de enseñanza que tenían la responsabilidad de coordinar las funciones técnicas y administrativas de los niveles escolares. Las acciones en el área administrativa, no estaban bajo la coordinación de una instancia provincial o regional, sino del Administrador Provincial o Sub-administrador Regional propiamente, según fuera el caso.

Con el Plan Nacional de Desarrollo Educativo, se hace un esfuerzo por sistematizar una serie de acciones y se creó la llamada Oficina Administrativa, la cual asumió los asuntos de esta índole que afectan a los centros educativos, incluyendo los de educación de adultos.

Como método para garantizar la calidad de la educación, el MEP aplica exámenes al final del último año de secundaria para evaluar los conocimientos en áreas como Matemática, Ciencias (Física, Química, o Biología), Español, Segunda lengua (Inglés, Francés o Italiano), Estudios sociales, y Educación Ciudadana. Estos exámenes son un requisito para obtener el título de bachillerato como también para ingresar a cualquier universidad, tanto pública como privada, en Costa Rica.

Los aspectos que han influenciado en el rendimiento académico en general, están los siguientes: el constante cambio de los directores(as) de las instituciones, al igual que las y los docentes, los grupos de estudiantes numerosos, saturación de algunos centros educativos. También, según el Estado de la Nación, las tasas de

pobreza, que se han mantenido en un 20% de la población, incide en el rendimiento académico de los estudiantes, pues se torna dificultoso el proceso de enseñanza puesto que los docentes no cuentan con los insumos para realizar sus estudios, además es importante agregar el consumo de drogas, la disfunción familiar, los distractores que tienen los estudiantes, como la televisión, los centros de diversión, la pérdida del principio de autoridad de los padres.

La Dirección Regional de Educación de Alajuela, por encontrarse dentro del Gran Área Metropolitana, tiene la misma problemática, la escuela costarricense no se puede sustraer de su entorno, pues de una u otra manera la afecta, no obstante, es través de los proyectos y programas tanto nacionales como regionales, como se puede lograr que cada día aumente en forma positiva la movilidad social de esta Dirección Regional.

1.8.2 Tipo de Negocio y Mercado Meta. El MEP es el órgano del estado costarricense responsable de la administración de todos los elementos relacionados con la educación en Costa Rica.

Abarca gestiones que cubren la totalidad del territorio del país, con más de cinco mil centros educativos, divididos en veintisiete oficinas regionales, y más de ochenta y cuatro mil funcionarios entre administrativos y docentes.

1.8.3 Misión, Visión y Valores.

Misión. 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. Un MEP 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.

Valores.

- Honestidad: para tener comportamientos transparentes honradez, sinceridad, autenticidad, integridad con nuestros semejantes y permitir que la confianza colectiva se transforme en una fuerza de gran valor.
- Justicia: para reconocer y fomentar las buenas acciones y causas, condenar aquellos comportamientos que hacen daño a los individuos y a la sociedad, y velar por la justicia a fin de que no se produzcan actos de corrupción.
- Respeto: empezando por el que nos debemos a nosotros mismos y a nuestros semejantes, al ambiente, a los seres vivos y a la naturaleza, sin olvidar las leyes, normas sociales y la memoria de nuestros antepasados.

- Paz: para fomentar la confianza en nuestras relaciones con los demás, para reaccionar con calma, firmeza y serenidad frente a las agresiones, y para reconocer la dignidad y los derechos de las personas.
- Solidaridad: para que los ciudadanos y ciudadanas colaboren mutuamente frente a problemas o necesidades y se consiga así un fin común, con entusiasmo, firmeza, lealtad, generosidad y fraternidad.
- Responsabilidad: para darnos cuenta de las consecuencias que tiene todo lo que hacemos o dejamos de hacer, sobre nosotros mismos o sobre los demás, y como garantía de los compromisos adquiridos.
- Pluralismo: para fomentar el respeto a la libertad de opinión y de expresión del pensamiento, y para desarrollar libremente personalidad, doctrina e ideología, con respeto al orden jurídico y a los derechos de los demás.

1.8.4 Políticas Institucionales. El MEP actualmente no cuenta con políticas de seguridad institucionales, tampoco cuenta con estándares o procedimientos relacionados a seguridad.

1.9 Estado de la Cuestión

1.9.1 Formulación de la pregunta.

Foco de la pregunta. En esta revisión se busca determinar los estándares más importantes que existen para la seguridad de la información y su enfoque a las diferentes industrias.

Amplitud y calidad de la pregunta.

Definición del problema. Con los ataques informáticos creciendo día a día el mantener la seguridad de la información es una tarea fundamental, especialmente para los gobiernos que se encargan de proveer servicios a un país entero. En este caso el MEP es un ente fundamental que vela por la educación de Costa Rica y la información como pagos a profesores, notas de estudiantes y demás es información crítica para que se cumpla su misión y visión.

Pregunta de Investigación. ¿Qué debe hacer el MEP para gestionar la seguridad de la información con el fin de asegurar su confidencialidad, disponibilidad e integridad?

Palabras claves. La Tabla 2 muestra las palabras clave seleccionadas para la búsqueda en los repositorios, utilizando palabras en el idioma inglés y español.

Tabla 2

Palabras Clave

Palabras Clave	
Sistema de gestión de seguridad de la información.	Vulnerabilidades
Seguridad de la información	Gestión de riesgos
Continuidad del servicio	Gestión de activos
Confidencialidad	Seguridad física y perimetral
Disponibilidad	Cybersecurity
Integridad	Data protection
Amenazas	Plan-Do-Check-Act
Auditoría de seguridad	Contingency plan
ISO 27001	Information security management

Fuente: Elaboración propia.

1.9.2. Selección de fuentes

Definición del criterio de selección de fuentes. El criterio de inclusión es importante para seleccionar las fuentes de los documentos primarios que alimentan la investigación. Se utilizan repositorios de amplio reconocimiento en la comunidad académica informática.

Lenguajes de los estudios. Con el fin de ampliar la literatura para la realización de este proyecto se utilizaron palabras en inglés y en español, para poder consultar los estudios existentes del tema en ambos idiomas.

Identificación de fuentes. Se han identificado las fuentes a utilizar a partir de palabras clave mencionadas anteriormente.

Método de búsqueda en las fuentes. Las fuentes que se toman en cuenta son provenientes de repositorios confiables y también el investigador se asegura que cumplan con los parámetros de calidad académica.

Lista de fuentes. Los repositorios seleccionados han pasado por un proceso previo de moderación para eliminar artículos no científicos. Se toman en cuenta los siguientes:

- ACM Digital Library.
- SpringerLink.
- Web of Science.
- IEEE Xplore Digital Library.

1.9.3. Selección de estudios. Aquí se describe el proceso de selección y evaluación de los estudios primarios, así como los criterios de inclusión y exclusión.

Procedimiento para la selección de estudios. Se siguió un procedimiento basado en la definición y manejo de las palabras clave de búsqueda anteriormente mencionadas.

Definición de criterios de inclusión y exclusión de estudios. Para los criterios de inclusión, se revisa el título y el resumen de cada artículo para asegurar que esté relacionado con el SGSI.

Para evaluar el criterio de exclusión se analiza la información del contenido de la lectura y las conclusiones. Con este criterio, se logra conocer a detalle de qué trata cada documento con el fin de relacionarlo con los objetivos buscados y decidir si es relevante para esta revisión.

1.9.4. Ejecución de la selección.

Selección de estudios iniciales. Se realizó una búsqueda en el título y en el resumen con las palabras clave de búsqueda de la Tabla 2. En la Tabla 3, se muestran los artículos relevantes del repositorio SpringerLink. Se procedió de manera continua con los repositorios ACM Digital Library (Tabla 4), Web of Science (Tabla 5), IEEE Xplore Digital Library (Tablas 6). El total de artículos relevantes encontrados en estos repositorios es de 22 y se pueden observar en el anexo 4.

1.9.5. Extracción de información. En esta sección, se extrae la información que se considera relevante para cada uno de los artículos primarios.

Definición de criterios de inclusión y exclusión de información. Para extraer la información relevante de los estudios primarios seleccionados, en relación con los objetivos de la investigación y el foco de estudio se toma en cuenta lo siguiente:

- Título relacionado con las palabras clave.
- Resumen relacionado al tema de investigación en cuestión.
- Relacionar contenido con los objetivos.

Capítulo 2. Marco Conceptual

2.1 Elaboración del marco conceptual

La elaboración del marco conceptual se realiza utilizando la herramienta nube de palabras, como lo muestra la figura 2, para obtener las palabras más relevantes de los estudios seleccionados en el estado de la cuestión, para ello se utilizó las palabras clave de cada estudio en inglés, es importante destacar que para algunos conceptos se utilizaron reducciones o siglas.



Figura 2. Nube de palabras (Elaboración propia)

Una vez que se generó la nube de palabras se utiliza un mapa conceptual jerárquico comenzando desde los conceptos más genéricos hasta los más específicos, estos establecen el orden en el cual el marco conceptual se redacta y como se unen los conceptos. La figura 3 muestra el mapa conceptual jerárquico vertical con los conceptos más relevantes.

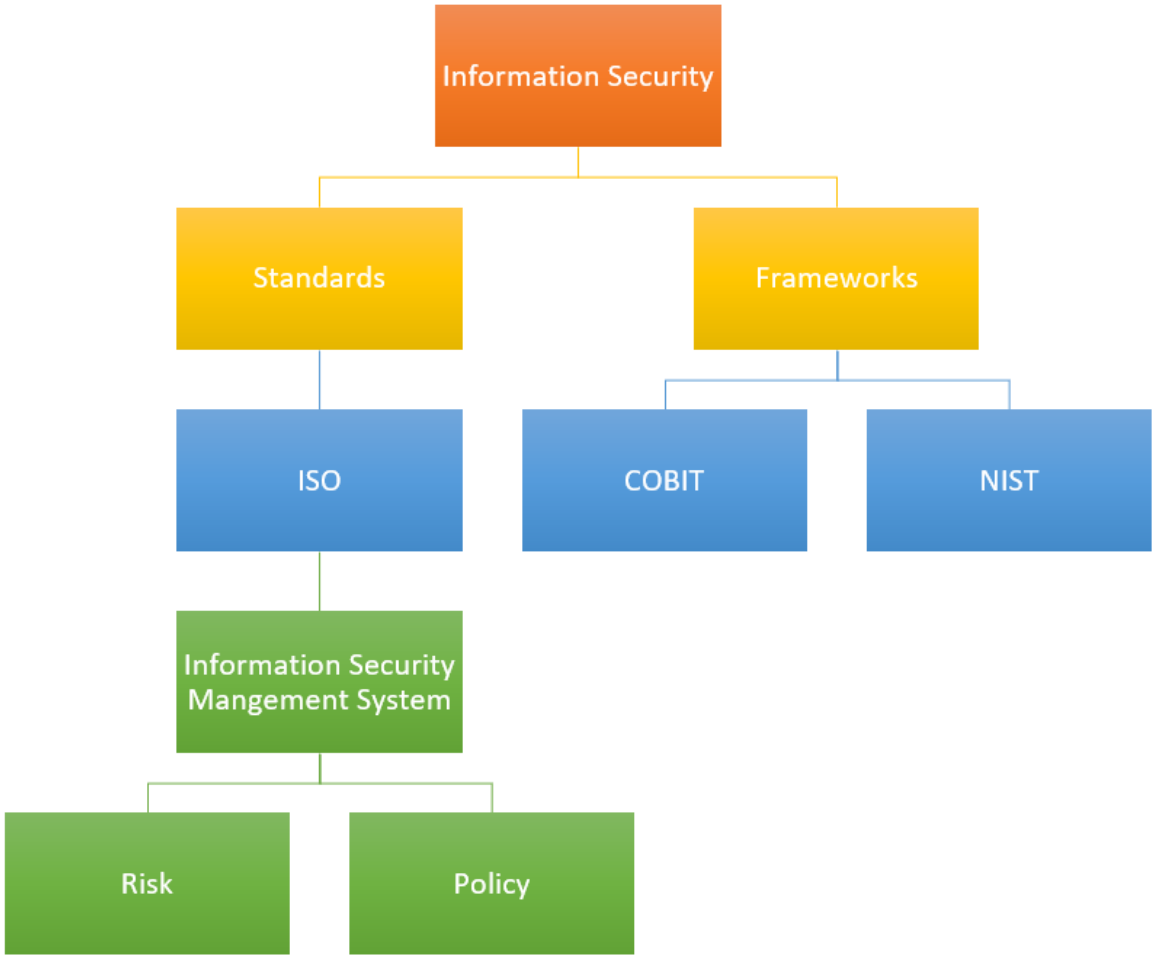


Figura 3. Mapa conceptual jerárquico de conceptos relevantes (Elaboración propia)

2.2 Marco Conceptual

La seguridad informática o seguridad cibernética como explica Humphreys (2011) es considerada como el "conjunto de tecnologías, procesos y prácticas diseñados para proteger las redes informáticas, los sistemas informáticos, el hardware y el software, la información y los datos de ataques, daños o acceso no autorizado". A través de los años, se han creado diferentes marcos de referencia para poder atacar el problema de la seguridad informática que aqueja a todas las

organizaciones y mantener la información, uno de sus activos más importantes, a salvo de riesgos como pérdida de datos, robo de información, modificación no autorizada, disponibilidad y más. Los marcos de referencia y estándares enfocados a la seguridad de la información conforman una serie de procesos documentados que son utilizados para definir políticas y procedimientos para manejar el riesgo.

Marcos de referencia como *Control Objective for Information and Related Technology* (COBIT) ayudan al gobierno y gestión de las tecnologías de la información dentro de una organización, según ISACA (2012) “COBIT permite que las tecnologías de la información y relacionadas se gobiernen y administren de una manera holística a nivel de toda la organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas”. Desde un punto de vista de seguridad de la información, COBIT es un marco de referencia muy amplio cuyo objetivo es la gobernanza de tecnologías de información, que debido a su magnitud usualmente no especifica el cómo realizar las tareas, sino que proporciona más una guía de alto nivel. Como consecuencia se deben tomar en cuenta otros marcos de referencia que se enfoquen más específicamente en la seguridad de la información. La figura 4 muestra la familia de productos COBIT, entre ellos una guía orientada a profesionales de seguridad de la información, si se desea implementar COBIT.

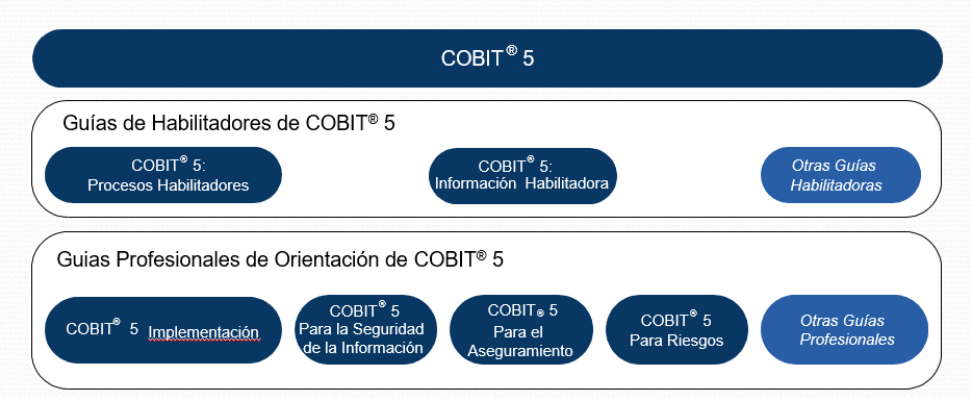


Figura 4. Familia de productos COBIT 5 (COBIT 5 Introducción 2012)

Es importante destacar que existe la posibilidad de combinar marcos de referencia puesto que no son mutuamente excluyentes, pero el enfoque de este trabajo no es crear un gobierno TI sino atacar un problema de seguridad informática.

Otro marco de referencia de ciberseguridad que se puede encontrar a nivel de industria en Estados Unidos, creado por el Instituto Nacional de estándares y Tecnologías (NIST), se diseñó para empresas estadounidenses, pero puede ser aplicado a otras organizaciones. Según NIST (2018) “el marco proporciona un lenguaje común para comprender, gestionar y expresar el riesgo de ciberseguridad para grupos de interés internos y externos. Puede ser utilizado para ayudar a identificar y priorizar acciones para reducir el riesgo de ciberseguridad, además es una herramienta para alinear políticas, negocios y enfoques tecnológicos para la gestión de ese riesgo”. Este marco de referencia puede ser de gran utilidad para el MEP puesto que provee un gran nivel de detalle, además proporciona una guía para establecer requerimientos mínimos de seguridad para proveedores o socios y cuenta con diversos niveles de implementación, pero sus desventajas pueden ser grandes como las expresan Teodoro, Gonçalves & Serrão (2015) puesto que el marco de

referencia del NIST no toma en cuenta factores primordiales de la organización como procesos, recursos humanos y tecnologías ya existentes; no existe una ruta clara de relación entre las actividades y los resultados del marco de referencia, además, faltan las actividades y la estrategia a nivel organizacional.

El último marco de referencia que se discute es la familia de estándares ISO 27000, que según Evans, Tsohou, Tryfonas & Morgan (2010) “proporcionan directrices basadas en un sistema de gestión de la seguridad de la información (SGSI) junto con un enfoque orientado a procesos estructurados en un modelo circular; su propósito es asegurar la selección de controles de seguridad adecuados y proporcionados que protejan los activos de información y a su vez brinden confianza a las partes interesadas, las prácticas y controles aplican para cualquier organización independiente de su tamaño o tipo” (p.4). Las normas ISO, en especial la 27001, ofrecen gran nivel de detalle y buscan proteger incluso la información en papel y no sólo la digital, además son lo suficientemente flexibles para cualquier organización y brindan el enfoque requerido en seguridad.

Para que un marco de referencia sea exitoso debe tomar en cuenta procedimientos y controles de seguridad basados en el riesgo y una medición de la eficacia de los mismos, como también lo mencionan Evans, Tsohou, Tryfonas & Morgan (2010), el SGSI utiliza una metodología para analizar y evaluar el riesgo, así como también ofrece distintas opciones para su tratamiento. Como se describe en la sección de limitantes, el SGSI se implementa utilizando un ciclo continuo de planear, hacer, verificar y actuar, para el actual proyecto el ciclo de planeación es el más

importante, en él se establece el sistema y como se describe a continuación, se compone de elementos críticos:

- Definición de alcance
- Definición de políticas de seguridad
- Definición de metodología para evaluar el riesgo
- Análisis y evaluación de riesgo
- Tratamiento del riesgo
- Entre otros

Un SGSI tiene cuatro niveles de documentación de suma importancia que representan su núcleo y que se van generando en cada una de las etapas de la implementación (planear, hacer, verificar y actuar), la figura 5 muestra los niveles de documentación.



Figura 5. Niveles de documentación (Elaboración propia)

El primer nivel, el manual de seguridad, es el documento que dirige todo el sistema, incluye el alcance, los objetivos, responsabilidades, políticas y directrices principales y más generales. El segundo nivel son procedimientos que realicen la planificación, operación y control de los procesos de seguridad de la información. El

tercer nivel describe documentos de cómo realizar tareas específicas relacionadas con la seguridad. Finalmente, el nivel cuatro son documentos que demuestren el cumplimiento de los requerimientos de SGSI.

Hay dos documentos con especial relevancia para este trabajo, el primero es la política de seguridad que denota el marco general y los objetivos de seguridad de la organización, así como los criterios para evaluar el riesgo, el cual es definido como la combinación de impacto y probabilidad de un evento que puede afectar al negocio (Ataya, 2013). El segundo documento está relacionado a la continuidad del negocio, como explica *British Standard Institution* (citado en Sawalha, Anchor y Meaton, 2015) “es un proceso de gestión integral que identifica las amenazas potenciales para una organización y los impactos en las operaciones comerciales que esas amenazas, si se presentan, pueden causar, y que proporciona un marco para desarrollar la capacidad de recuperación de la organización con la capacidad de una respuesta efectiva que proteja los intereses clave de los grupos de interés, reputación, marca y actividades que generen de valor”.

Capítulo 3. Marco Metodológico

3.1. Tipo de investigación

Debido a la naturaleza de este proyecto el tipo de investigación que se va a implementar es la aplicada, ya que el MEP enfrenta un serio problema con la gestión de la seguridad de la información y se espera resolverlo poniendo en práctica los conocimientos existentes sobre el tema.

Esta investigación no busca producir conocimientos de base, sino utilizar los que ya existen para atender una necesidad particular. Como afirma Bibliotecas Duoc UC (2018) se centra en la resolución de problemas en un contexto determinado, busca la aplicación o utilización de conocimientos con el propósito de implementarlos de forma práctica para satisfacer una necesidad en particular con el fin de proporcionar una solución al problema.

En la figura 6 se muestra el proceso que se lleva a cabo en una investigación aplicada.



Figura 6. Investigación aplicada (Bibliotecas Duoc UC, 2018)

3.2. Alcance Investigativo

El alcance investigativo que se va a utilizar es el descriptivo ya que se pretende recoger información de manera independiente o conjunta sobre los conceptos y categorías de análisis para poder realizar el SGSI (Robles, 2019).

De acuerdo a Fernández, Hernández y Baptista (2006) el investigador debe ser capaz de definir, o al menos visualizar, qué se medirá (qué conceptos, categorías de análisis, componentes, etc.) y sobre qué o quiénes se recolectarán los datos (personas, grupos, comunidades, etc.) (p.92)

La función principal de este alcance descriptivo es profundizar en un tema y poder describir situaciones con el fin de plantear una solución (Pérez, 2016).

3.3. Enfoque

El enfoque que se va a utilizar para la implementación de los cimientos del SGSI es cualitativo.

El enfoque de carácter cualitativo permite el análisis de estudios previos relacionados con el tema en gestión y con esto la generación de pruebas de concepto y recomendaciones sobre su uso (Sanfeliciano, 2018).

Según (Hernández, Fernández y Baptista, 2010, p. 492) “las investigaciones cualitativas no se planean con detalle y están sujetas a las circunstancias de cada ambiente”.

Según Cuenya y Ruetti (2010), “el análisis cualitativo busca comprender los fenómenos dentro de su contexto usual, se basa en las descripciones detalladas de situaciones, eventos, personas, interacciones, comportamientos observados y documentos”.

El método de investigación cualitativa está basado en la recolección de información basada en la observación de comportamientos naturales, discursos, respuestas abiertas para después poder interpretar los significados (Canive, 2019).

3.4. Diseño

Existen varios tipos de diseños cualitativos, y el que se adapta a la elaboración de este proyecto es el diseño de investigación-acción que se detalla en la figura 7.



Figura 7. Principales marcos teóricos a partir de los cuales se diseña la investigación cualitativa. (Elaboración propia a partir de las aportaciones de Hernández, Fernández y Baptista, 2010).

El diseño de investigación-acción tiene como objetivo resolver problemas cotidianos e inmediatos y mejorar prácticas concretas (Alzás, 2017). Más que resolver un problema, se busca que los empleados del MEP sean conscientes del cambio que se necesita para llegar a proteger la información de manera adecuada.

3.5. Sujetos y fuentes de información

Los sujetos y fuentes de información que se analizarán para lograr obtener la información apropiada y que permita calidad en los resultados esperados son los siguientes:

- Revisión de documentación histórica relacionada a la seguridad de la información.

- Revisión de las auditorías realizadas por la Contraloría General de la República de Costa Rica con respecto al tema de gestión de seguridad de la información.
- Revisión de políticas de seguridad de la información (en caso de que se disponga de algunas).
- Reuniones con el personal del departamento administrativo del MEP.
- Reuniones con los encargados de cada uno de los subdepartamentos del MEP.

3.6. Instrumentos

Al ser una investigación con un enfoque cualitativo los instrumentos para la recolección de datos no son estandarizados ni predeterminados.

Se van a utilizar diferentes técnicas como la observación no estructurada (individual y en equipo), entrevistas abiertas, revisión de documentos, discusión en grupo y listas de chequeo.

Capítulo 4. Propuesta de Solución

Como afirma la Organización Internacional para la estandarización (ISO) y la comisión Electrotécnica Internacional (IEC) un SGSI se puede describir primordialmente como “las políticas, procedimientos, directrices y recursos y actividades asociados, administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y

mejorar la seguridad de la información de una organización para lograr los objetivos comerciales" (2018, p.11-12). El SGSI se encuentra plasmado en la familia de estándares ISO/IEC 27000, cuenta con más de 30 normas que establecen los requisitos necesarios para establecer, implantar, mantener y mejorar el SGSI según el conocido "Ciclo de Deming", el cual está conformado por cuatro fases que se describen con mayor detalle según la ISO (2015):

- **Planificar:** establecer los objetivos del sistema y los procesos para entregar los resultados.
- **Hacer:** Implementación y control de lo planeado.
- **Controlar:** monitoreo y procesos de medición y resultados contra políticas, objetivos y requisitos e informes.
- **Actuar:** tomar medidas para mejorar el rendimiento de los procesos (p.2).

La clave de un SGSI exitoso es lograr desarrollar todo el ciclo de Deming sin dejar de lado ninguna fase como a veces usualmente puede pasar con la fase de control o actuar. Por lo cual este conjunto de procesos se debe gestionar eficientemente con el fin alcanzar los tres principios de seguridad: confidencialidad, integridad y disponibilidad.

Actualmente, todas las empresas procesan y guardan una gran cantidad de información, convirtiéndose en uno de los activos más importantes. Debido a esto, la seguridad de la información juega un papel fundamental para el buen funcionamiento de las empresas y la protección dichos activos, por lo que ISO recomienda que sea parte de un sistema que esté regulado, con ciclos de vida periódicos, tareas que

permitan dirigir y controlar los procesos en los diferentes niveles de la organización y que asegure su continuo desarrollo y mejora.

La auditoría realizada por la Contraloría General de la República identificó varias debilidades en los sistemas de información del MEP y sus procesos, como resultado creó una serie de disposiciones que el MEP debe cumplir.

Un SGSI no solo permite cumplir con dichas disposiciones, sino que además permitirá al departamento:

- Adaptarse mejor a los cambios al poseer procesos y procedimientos claros y definidos.
- Aumentar la velocidad de respuesta tanto para incidentes como términos de continuidad de servicios minimizando el impacto de posibles interrupciones.
- Ofrecer una respuesta más rápida a los riesgos y generar controles acordes a una evaluación de riesgos que permita disminuir el impacto de dichos riesgos.
- Establecer un proceso que permita la mejor continuidad basada en métricas.
- Proteger la confidencialidad, integridad y disponibilidad de la información.

Como parte de la propuesta para impulsar al MEP en la implementación de un SGSI se plantea un cronograma con las actividades que el MEP debe realizar y estimados de tiempo para completarlas; permitiendo conocer el progreso de cada

actividad y su estado. El cronograma se dividirá en fases o etapas que se basan en el ciclo de Deming anteriormente expuesto.

4.1. Políticas de seguridad de la información

Las políticas de seguridad de la información proveen no solo una dirección clara, sino que establecen el compromiso de la gerencia hacia la seguridad de la información con el objetivo de proteger la información contra una amplia gama de amenazas, garantizar la continuidad de los servicios y minimizar riesgos empresariales.

Una de las prioridades que se identificó para el MEP es la creación de políticas de seguridad que guíe al departamento de informática de gestión y establezca un estándar de normas de seguridad que mejoren la labor de protección, preservación y resguardo de la información. Actualmente, cada segmento del departamento posee sus propios procedimientos informales e incompletos de seguridad según consideren que aspectos pueden ser relevante para ellos, las políticas que se proponen buscan unificar, formalizar y mejorar la gestión de la seguridad de la información.

El ISO/IEC-27002 define mejores prácticas de gestión de la seguridad de la información por lo que es la base de las políticas de seguridad creadas para el MEP, además se realizaron una serie de entrevistas con los representantes de cada área del departamento para determinar la existencia de procedimientos claros y documentados de seguridad, así como posibles debilidades que ayudarán a mejorar el enfoque de las políticas. Seguidamente se listan las diferentes secciones que componen la política y sus respectivos objetivos:

- Gestión de activos: Proteger y dar hacer uso adecuado a los activos de la organización.
- Control de acceso: Establecer una política que provea expectativas de control de acceso a los diferentes recursos y permita proteger la información de accesos no autorizados.
- Gestión de incidentes: Su principal objetivo es asegurar no solo que los eventos de seguridad sean comunicados y gestionados efectivamente, sino que busca tomar acciones correctivas para evitar su recurrencia.
- Concientización y procedimientos de terminación laboral: Generar en los empleados un buen nivel de concientización sobre la seguridad de la información, mediante educación y capacitaciones constantes. Así como asegurar que los procesos de terminación laboral o cambio de puesto se llevan a cabo de una manera ordenada sin poner en peligro la seguridad de la información.
- Gestión de la continuidad de servicios de tecnologías de información: Proteger los servicios críticos de la organización ante fallos o desastres de seguridad de la información y asegurar su pronta recuperación.
- Seguridad física y ambiental: Prevenir el acceso físico no autorizado y daños a la información y activos de la organización.
- Adquisición, desarrollo y mantenimiento de sistemas de información: Define requerimientos del ciclo de vida de los sistemas y de hardware. Además, provee las bases para un robusto desarrollo, mantenimiento y adquisición de sistemas.

La política de seguridad de la información para el MEP se puede consultar a detalle en la Anexo 1 del presente documento.

4.2. Continuidad de servicios informáticos

La continuidad de servicios es otra de las importantes ramas de la seguridad informática, ya que permite gestionar de manera eficiente la respuesta y recuperación ante eventos imprevistos o desastres que afecten la operación normal del servicio.

El sistema más crítico que para el MEP es INTEGRA2, el cual se encarga de todo lo referente a la planilla de más de 84 mil empleados públicos costarricenses. Este sistema se encuentra hospedado en el Ministerio de Hacienda y los usuarios finales encargados de gestionar todo el proceso de planilla se encuentran en las instalaciones del MEP; debido a esto el plan de continuidad de servicios propuesto está enfocado en el enlace de conexión existente entre ambas instituciones con el fin de mejorar estabilidad y maximizar la disponibilidad tanto a los usuarios finales del sistema, así como a los empleados del MEP.

Este plan de continuidad va a servir de guía para poder desarrollar los demás planes para los restantes sistemas/servicios del MEP. Las áreas que abarca este plan de continuidad son las siguientes:

- Mantenimiento del plan y pruebas: Explica la necesidad dar mantenimiento periódico al plan para mantenerlo actualizado ante cambios en procesos. Así como la realización de diversos tipos de pruebas que permitan evaluar el contenido, los procesos, estructura y ejecución.

- Equipo de recuperación de desastres: Identifica los roles necesarios para ejecutar el plan de continuidad de servicios y cada una de las responsabilidades de cada rol.
- Procedimientos de respuesta a desastres: Se consideran todos los procedimientos para una adecuada respuesta a incidentes.
    - Procedimientos de identificación y evaluación: Indica la necesidad de que el equipo de recuperación dedique tiempo para poder entender el problema y una posible causa. Además, utiliza diferentes criterios a tomar en cuenta para poder evaluar el impacto y la severidad del incidente, para ello se creó además un instrumento que facilita dicha evaluación.
    - Procedimientos de recuperación: El procedimiento de recuperación contiene varios aspectos importantes la notificación a los equipos de recuperación, la inicialización del proceso de recuperación y la comunicación a las partes interesadas.
    - Procedimiento de reanudación: Una vez que se ha mitigado el impacto del evento y se ha podido restablecer las operaciones a un mínimo aceptable el procedimiento de recuperación entra en juego, busca restablecer la conexión al estado anterior al evento. Es importante mencionar que sigue un proceso de retorno a la normalidad, pruebas y comunicación.
    - Procedimiento de revisión: El paso final es esencial para mejora continua se deben revisar las lecciones aprendidas, los resultados,

aspectos positivos y negativos que permitan retroalimentar el plan y establecer cambios.

- Plan de recuperación: Establece los pasos necesarios para recuperar el enlace que conecta el MEP y el Ministerio de Hacienda. Es un plan detallado con pasos técnicos que debe seguir el equipo de recuperación de redes, dicho plan se realizó de la manera más clara y detallada posible.

El plan de continuidad de servicios informáticos para el enlace de conexión entre el MEP y el Ministerio de Hacienda se puede ver en detalle en el Anexo 2 de este documento.

Capítulo 5. Resultados

Uno de los principios fundamentales para la implantación de un SGSI, así como para la implantación de nuevos procesos a nivel de departamento en el MEP es demostrar un compromiso y liderazgo en la dirección por lo que la creación de las políticas de seguridad de la información es una manera eficaz de conseguir dicho objetivo.

Las políticas creadas en este proyecto se adaptan a las necesidades del MEP y buscan fortalecer aquellas debilidades que se identificaron en un proceso de entrevistas y en el informe DFOE-SOC-IF-00019-2018 de la Contraloría General de la República:

- Las secciones de control de acceso y gestión de activos dictan políticas para sentar responsabilidades y dueños de los activos, así como la necesidad de justificar el acceso a los diferentes activos mejorando la “falta de una clara

definición de la propiedad de la información y del necesario acceso a los datos de la planilla salarial pertenecientes a los funcionarios del MEP, que deberían tener los encargados de esta materia en el MEP.” (Contraloría General de la República, 2018).

- Las políticas de gestión de incidentes buscan establecer un procedimiento para la respuesta de incidentes, así como una comunicación transparente mejorando la deficiencia encontrada por la Contraloría General de la República “los servicios relacionados con la planilla salarial del MEP no cuentan con una oportuna respuesta a incidentes” (Contraloría General de la República, 2018).
- Según el informe de la Contraloría General de la República en el 2018 “El equipo de cómputo del MEP… es un equipo obsoleto, sin soporte del fabricante, cuyo sistema operativo se encuentra descontinuado y ya no recibe ningún tipo de actualizaciones de seguridad.” esta es cubierta en la sección de adquisición, mantenimiento y desarrollo de sistemas donde se describe que la importancia de contar solamente con software que todavía sea soportado por el proveedor quien ofrece mejorar, arreglos a problemas o fallas de seguridad.
- “La vulnerabilidad y fragilidad que se presenta, ante el riesgo de accesos no autorizados al ambiente de desarrollo, abre una brecha en la seguridad del sistema, dado que atacantes con acceso al servidor de perfiles de usuario del MEP, podrían facilitar alteraciones o eliminaciones de código computacional del sistema INTEGRA 2.” (Contraloría General de la República, 2018). es

abordada por la política de control de accesos que busca determinar un proceso para la revocación y la adquisición de accesos permitiendo proteger la información de accesos no autorizados.

Dicho documento con políticas abarca siete áreas de la seguridad de la información y es lo suficientemente robusto para que sea escalable a nivel de todo el ministerio. Además, el documento es suficientemente flexible con el fin de que el departamento pueda definir estándares más específicos sin pasar por alto importantes aspectos de la seguridad.

El proceso de entrevistas mencionado anteriormente se utilizó como contribución para el análisis de la estructura de los sistemas de información del MEP con el fin de entender los servicios más críticos de la organización y seleccionar un servicio que serviría para realizar el plan de continuidad de servicios informáticos; el servicio con mayor prioridad fue el enlace que conecta el MEP con el Ministerio Hacienda y permite acceder al sistema INTEGRA2, donde se gestiona la planilla de todos los empleados de esta institución. El documento resultante es utilizado no solo como plan de continuidad, sino como guía para la creación de los demás planes de continuidad, dicho documento se basa en establecer responsabilidades, mantener una comunicación frecuente, evaluar los eventos, recuperarse de los daños y finalmente asegurar la mejora continua.

En el informe DFOE-SOC-IF-00011-2018 la Contraloría General de la República realizó en el 2018 emitió la disposición “Definir y aprobar un plan de gestión de la continuidad de servicio de tecnologías de información. Además, definir y aprobar acciones específicas para probar dicho plan de gestión y mantenerlo

actualizado.” este proyecto ayuda a cumplir dicha disposición para estar en cumplimiento con las regulaciones de seguridad de la información mediante el documento de continuidad de servicios.

Adicionalmente, es importante mencionar que el Sistema de Gestión de Seguridad de la Información, según el ciclo de Deming, abarca varios pasos, los cuales requieren de un gran apoyo por parte de los jerarcas del MEP y además inversión de recursos, como tiempo y humano, para poder administrar e implementar el plan en su totalidad. Debido a esto, se le facilitó al MEP un cronograma el cual detalla los pasos para implementar el SGSI y un estimado del tiempo que este requerirá. Este cronograma se puede ver completo en el Anexo 3.

El cronograma de trabajo creado se validó con el oficial de seguridad encargado en el MEP con el fin de asegurar su implementación en los próximos meses. Las tareas pendientes por implementar requieren de tiempo y recursos, pero con un buen plan de trabajo y buenas bases se puede empezar a darle seguimiento.

Los documentos otorgados como parte de este proyecto van a ayudar mucho a la hora de tomar decisiones o no saber que hacer, ya que especifican de manera detallada cada paso a seguir.

Capítulo 6. Conclusiones

El MEP presenta varias deficiencias en el área de seguridad de la información específicamente en el departamento de gestión informática. Se identifica desde un manejo inadecuado de accesos de usuario, hasta la falta de alineación estratégica con resto de la institución evidenciando el poco apoyo en sus procesos de negocio.

Este proyecto sienta una base y una guía para ayudar al MEP a fortalecer algunas de sus debilidades en el área de seguridad de la información con el fin de incentivar un proceso de mejora continua utilizando un SGSI, el cual va a seguir siendo eficiente durante un largo tiempo, y se adapta efectivamente tanto a los cambios internos de la organización como a los externos. El SGSI también ayudará a mejorar la conexión entre la tecnología y el negocio, tomando en cuenta sus prioridades, la seguridad de la información y siguiendo el proceso de planeación, implementación, medición y mejora haciéndolo robusto.

Desde un punto de vista de las políticas de seguridad de la información se busca evidenciar un compromiso de parte de la alta gerencia y asegurar que cada área del departamento establezca controles de seguridad de acuerdo a un estándar de la industria y no discrecionalmente. A largo plazo se espera que el MEP implemente estas políticas a nivel institucional lo cual llevaría a mejorar la seguridad de sedes regionales e incluso en la infraestructura de escuelas y colegios. Sin duda las políticas son el principio de un cambio positivo en materia de seguridad y requieren mucho trabajo para que sean debidamente implementadas a través de la institución y cumplidas a cabalidad.

Siendo la misión del MEP garantizar el derecho fundamental de la educación a los habitantes de este país se requiere que la institución sea resiliente y pueda afrontar desafíos satisfactoriamente mientras cumple con sus funciones, un paso importante hacia este camino es establecer planes de continuidad para asegurar una prestación de servicios razonables ante la manifestación de un evento; para ello se creó un plan de continuidad para el enlace MEP-Hacienda que funcionará como una

guía para que el MEP siga creando y ejecutando nuevos planes de continuidad. Este aporte también ayuda a cumplir con las disposiciones de seguridad de la información que la Contraloría General de la República le comunicó al MEP en el año 2018 (actualmente el MEP continúa trabajando para cumplir con las disposiciones restantes).

Capítulo 7. Glosario

Activo: “Todo lo que tenga valor para la organización” (ISO, 2008).

Acuerdo de servicio: Acuerdo entre partes donde una accede a proveer un servicio y se determina aspectos como calidad, tiempos de respuesta, disponibilidad, responsabilidades y más.

Amenaza: “Causa potencial de un incidente no deseado, que puede provocar daños a un sistema u organización” (ISO, 2018, p.10).

Autenticación: “Provisión de garantía de que una característica alegada de una entidad es correcta” (ISO, 2018, p.2).

Cliente: Aplicación que consume un servicio remoto.

Código fuente: Conjunto de instrucciones o pasos que debe seguir la computadora/máquina para ejecutar un programa informático.

Confidencialidad: “Propiedad de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados” (ISO, 2018, p.2).

Conflicto de interés: Aplica cuando la toma de decisiones se ve comprometida o influenciada por intereses personales, económicos o familiares.

Control: “Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen el riesgo” (ISO, 2018, p.3).

Disponibilidad: “Propiedad de ser accesible y utilizable a pedido por una entidad autorizada” (ISO, 2018, p.2)

Incidente de Seguridad: “Eventos únicos o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.” (ISO, 2018, p.4)

Identificador de sesión: Identificador único asignado por un servidor a un usuario específico durante un periodo de tiempo para intercambiar mensajes

Información: La información es un activo de la organización y se refiere a un conjunto de datos que poseen un valor para el negocio.

Integridad: “Propiedad de precisión y completitud.” (ISO, 2018, p.5)

Inyección de código: Es una vulnerabilidad que permite procesar datos inválidos y producir resultados inesperados o potencialmente desastrosos.

LDAP: Es un protocolo ligero de acceso a directorios (*Lightweight Directory Access Protocol*), es un protocolo abierto utilizado para gestionar accesos a diferentes recursos en la red.

Macro: Un programa que ejecuta una serie de instrucciones lineales

Mínimo privilegio: Es un principio que busca restringir el acceso de los usuarios al mínimo requerido para poder realizar sus funciones o actividades de trabajo.

Necesidad de saber: Debe proporcionarse acceso a la información únicamente a usuarios que la requieran para ejecutar su trabajo o función.

Necesidad de negocio: Requisitos o metas que el negocio necesita para continuar operando o ser exitoso.

Política de seguridad: “Intenciones y dirección de una organización, tal como lo expresa formalmente su alta dirección” (ISO, 2008)

Seguridad de la información: “Reglas, directivas y prácticas que rigen la forma en que los activos, incluida la información confidencial, se gestionan, protegen y distribuyen dentro de una organización y sus sistemas, particularmente aquellos que impactan los sistemas y elementos asociados.” (ISO, 2008)

Riesgo: “El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.” (ISO, 2008)

Vulnerabilidad: “Debilidad de un activo o control que puede ser explotado por una o más amenazas.” (ISO, 2018, p.11)

Servicio: Conjunto de actividades, procedimientos y procesos que buscan satisfacer una necesidad de un negocio por medio de recursos tecnológicos.

Utilidades: Se refiere al conjunto funciones de software que permiten gestionar los sistemas de información.

Separación de tareas o responsabilidades: Se define como un control cuyo objetivo es evitar el mal uso de un activo y aumentar la posibilidad de detectarlo

Servidor: Aplicación que ofrece un servicio remoto y atiende peticiones del cliente.

Sesión: Es una comunicación temporal entre dos o más dispositivos.

SQL: Lenguaje de consulta estructurado, es utilizado en las bases de datos.

Script: Un programa pequeño normalmente almacenado en archivo de texto.

Sistema crítico: Son sistemas vitales o necesarios para el buen funcionamiento de los procesos y procedimientos de la institución.

Usuario: Persona que utiliza habitualmente ciertos programas, aplicaciones y sistemas en un dispositivo (computadora, tableta o teléfono inteligente).

Valores de registro del sistema operativo: Serie de instrucciones que almacena el sistema operativo relacionadas al núcleo del sistema o aplicaciones.

XML: Lenguaje de marcado extensible (*eXtensible Markup Language*), es utilizado para estructurar datos de forma legible.

XSS: (*Cross-site scripting*) Es una vulnerabilidad que permite a un tercero ejecutar código en la página web o aplicación, usualmente se produce al no realizar validaciones de los datos recibidos.

8. Referencias

Ataya, G. (2013). Information security, risk governance and management frameworks: an overview of COBIT 5. Artículo presentado en 6th International Conference on Security of Information and Networks, *New York*. Recuperado de doi: http://dx.doi.org.una.idm.oclc.org/10.1145/2523514.2523590

Ministerio de Educación Pública (2020). Reseña Histórica. Recuperado de https://www.drea.co.cr/Direccion-Regional-Historia

MEP (2019). Misión y Visión del MEP. Recuperado de https://mepdev.mep.go.cr/transparencia-institucional/informacion/mision-y-vision-del-mep

Alzás, T. (2017). *Diseños generales de la investigación cualitativa: La teoría fundamentada.* Recuperado de https://www.webqda.net/disenos-generales-de-la-investigacion-cualitativa-la-teoria-fundamentada/?lang=es

Canive, T. (2019). *Método de Investigación Cualitativa*. Recuperado de https://www.sinnaps.com/blog-gestion-proyectos/metodologia-cualitativa

Cerdas, D. (octubre de 2018). Funcionario de planillas logró que el MEP pagara 53 millones en salarios a falso profesor. *La Nación*. Recuperado de https://www.nacion.com/el-pais/educacion/funcionario-de-planillas-logro-que-el-mep-pagara/TOZCCYIQPNDSXNETO2ZV5JFQMU/story/

Contraloría General de la República. (2007). Normas Técnicas para la Gestión y el Control de las Tecnologías de Información. Recuperado de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_complet

o.aspx?param1=NRTC&nValor1=1&nValor2=60519&nValor3=68248&strTipM=TCn

Contraloría General de la República de Costa Rica. (2018). Informe de auditoría de carácter especial sobre el alineamiento estratégico de las tecnologías de información y la continuidad de los servicios apoyados en sistemas de información del ministerio de educación pública (MEP) (DFOE-SOC-IF-00011-2018). Recuperado de https://cgrfiles.cgr.go.cr/publico/docs_cgr/2018/SIGYD_D_2018015100.pdf

Contraloría General de la República de Costa Rica. (2018). Informe de auditoría de carácter especial sobre la integración, la gestión de la calidad y la seguridad de los sistemas de información relacionados con los procesos de administración de la planilla salarial del ministerio de educación pública (MEP) (DFOE-SOC-IF-00019-2018). Recuperado de https://cgrfiles.cgr.go.cr/publico/docs_cgr/2018/SIGYD_D_2018020307.pdf

Cuenya, L., & Ruetti, E. (2010). Controversias epistemológicas y metodológicas entre el paradigma cualitativo y cuantitativo en psicología. *Revista Colombiana de Psicología, 19*(2), 271-277. Recuperado de https://revistas.unal.edu.co/index.php/psicologia/article/view/17795/34440

Evans, R., Tsohou, A., Tryfonas, T., & Morgan, T. (2010*).* Engineering secure systems with ISO 26702 and 27001. Articulo presentado en 5th International Conference on System of Systems Engineering*, Loughborough*. Recuperado de doi: 10.1109/SYSOSE.2010.5544065

Gamboa, A. (2018, noviembre 1). MEP abrirá investigación contra profesor en huelga que compartió examen de bachillerato luego de aplicado. *La Nación*. Recuperado de https://www.nacion.com/el-pais/educacion/mep-abrira-investigacion-contra-profesor-en-huelga/GCVBJXOQHZAHBJWBGNYLO47C7Q/story/

Hernández, R., Fernández, C. y Baptista, P. (2006). Metodología de la investigación. Sexta Edición. México: McGraw Hill

Hernández, R., Fernández, C., & Baptista, P. (2010). Metodología de la Investigación. Quinta Edición. México: McGraw Hill

https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Humphreys, E. (2011). Information security management system standards. *Datenschutz und Datensicherheit.* 2011, 35, 7-11. https://doi-org.una.idm.oclc.org/10.1007/s11623-011-0004-3

Instituto Nacional de Ciberseguridad (2018). Guía para la gestión y notificación de brechas de seguridad. Recuperado de https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

International Organization for Standardization. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. Recuperado de https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

International Organization for Standardization. (2015). The process approach in ISO 9001:2015. Recuperado de https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso9001_2015_process_approach.pdf

International Organization for Standardization. (2008). Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model. Recuperado de https://www.iso.org/obp/ui/es/#iso:std:iso-iec:21827:ed-2:v1:en:term:3.4

ISACA. (2012). *COBIT 5 Introducción*. [Diapositivas de Power Point]. Recuperado de http://www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt

Ministerio del Interior Subsecretaria del Interior y Seguridad Pública Intendencia Regional de Atacama. (2012). Política y procedimiento preliminar de control de acceso. Recuperado de http://www.intendenciaatacama.gov.cl/filesapp/Control%20de%20Acceso%20Preliminar.pdf

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Recuperado de https://doi.org/10.6028/NIST.CSWP.04162018

Pérez, K. (2016). *Definición del alcance de la investigación a realizar: Exploratoria, descriptiva, correlacional o explicativa.* Recuperado de https://racionalidadltda.wordpress.com/2016/05/22/definicion-del-alcance-de-la-investigacion-a-realizar-exploratoria-descriptiva-correlacional-o-explicativa/

Ramírez, Y. (2014). Manual de Normas y Políticas de seguridad informática. Recuperado de https://www2.sgc.gov.co/ControlYRendicion/TransparenciasYAccesoAlaInformacion/CircularesManuales/MO-TEC-001-I.pdf

Robles, D. (2019). *Alcances de la investigación científica.* Recuperado de https://investigacioncientifica.org/alcance-la-investigacion-cientifica/

Sanfeliciano, A. (2018). *Diseños de investigación: enfoque cualitativo y cuantitativo*. Recuperado de https://lamenteesmaravillosa.com/disenos-de-investigacion-enfoque-cualitativo-y-cuantitativo/

Sawalha, I.H.S., Anchor, J.R. & Meaton, J. (2015). Continuity Culture: A Key Factor for Building Resilience and Sound Recovery Capabilities*. International Journal of Disaster Risk Science* 2015, *6*, 428–437. https://doi-org.una.idm.oclc.org/10.1007/s13753-015-0070-5

Teodoro, N., Gonçalves, L., & Serrão, C. (2015). *NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements*. Articulo presentado en *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki. Recuperado de doi:10.1109/Trustcom.2015.402

9. Anexos

9.1. Políticas de Seguridad de la Información

Política de seguridad de la información

Ministerio de Educación Pública de Costa Rica

Capítulo 1: Introducción

Las políticas de seguridad ayudan a proteger el activo más crítico de las empresas: la información, contra una amplia gama de amenazas, garantizando la continuidad del negocio y minimizando riesgos empresariales. Se deben procurar mantener los tres pilares de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

1.1 Propósito

Este documento tiene como finalidad dar a conocer las políticas de seguridad que se deben implementar en el Ministerio de Educación Pública para todo el personal y que los funcionarios de la Dirección de Informática de Gestión deben conocer para garantizar su implementación en todos sus alcances. Éstas mismas deben ser respetadas y acatadas por todos los colaboradores, entendiendo que la seguridad de los activos es responsabilidad de todos.

1.2 Objetivo

Establecer los criterios y mecanismos de acatamiento obligatorio para todos los colaboradores del MEP, y en especial para la Dirección de Informática de Gestión que debe velar por el adecuado resguardo y preservación de la información y/o de los sistemas, cumpliendo con los tres principios de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad; acogiendo las mejores prácticas de seguridad de la información, implícitas en el Estándar Internacional ISO/IEC-27002.

1.3 Alcance

Lo enunciado en esta política aplica a todos los funcionarios del MEP, así como para todo aquel colaborador que preste servicios por medio de contrato o que por sus funciones tenga acceso a los equipos de cómputo, infraestructura, equipo de redes, bases de datos, sistemas y aplicaciones institucionales, instalaciones que resguardan el centro de cómputo y en general a todos los recursos del Ministerio de Educación Pública.

1.4 Responsabilidades

La seguridad de la información es responsabilidad de todos los colaboradores del MEP, por lo que se espera que cada uno de los funcionarios mantengan la seguridad dentro de todas las actividades relacionadas con su labor.

El Director de Informática de Gestión es el responsable de velar por la adecuada gestión de la seguridad de la información ministerial.

La Comisión de las Tecnologías de Información debe divulgar y hacer cumplir los mecanismos para la seguridad de la información y elementos conexos.

Cada director o Jefe de Departamento y/o Unidad es responsable de velar que sus colaboradores protejan la información de acuerdo con las normas establecidas.

El Oficial de Seguridad Informática asesora al equipo directivo, brindando apoyo especializado al personal y garantizando que los informes relacionados con la seguridad de la información y elementos conexos estén actualizados y disponibles.

Capítulo 2. Gestión de activos

2.1 Objetivo

Establecer los mecanismos para la protección y uso adecuado de los activos, su divulgación y creación de cultura, en el MEP, dirigidos y controlados por la Dirección de Informática de Gestión.

2.2 Inventario de activos de información y tecnología

La Dirección de Informática de Gestión debe contar con un registro centralizado de todos los activos relacionados con información y tecnología, incluyendo la siguiente información:

- Nombre
- Descripción
- Tipo
- Formato
- Ubicación exacta
- Valor que representa para el negocio
- Licencias
- Estado
- Número de placa o patrimonio
- Responsable

Para el inventario de activos se debe tomar en cuenta, como mínimo, activos de información, aplicaciones, activos físicos, servicios y utilidades. Es vital que el

inventario se actualice constantemente con el fin de contar con información confiable y oportuna. Al realizarse un cambio en la información, se debe generar un nuevo registro en el inventario. Esto en un plazo no mayor de dos semanas. Dicho registro debe contemplar:

- Ingreso y asignación de nuevos activos.
- Reparaciones y traslado de activos.
- Disposición de activos y su causa.

Finalmente, este inventario debe ser almacenado de manera segura y contar con respaldos respectivos.

2.3 Propietario de los activos

Los activos pueden ser asignados/trasladados a un funcionario o dependencia, que tendrá la responsabilidad de su gestión y resguardo. El propietario de los activos debe:

- Asegurar que los activos sean debidamente clasificados y registrados en el inventario.
- Definir y realizar inspecciones periódicas de acceso (Referirse a la política de control de acceso) y clasificación de información.
- Actualizar el inventario de activos constantemente con el fin de contar con información confiable y oportuna.
- Documentar con exactitud los movimientos (ingresos, retiros, préstamos, reparaciones, dados de baja, entre otros). Para ello debe incluir información como descripciones, valores, fecha/hora y firmas.

- Verificar al momento de recepción de activos, que estos correspondan con el activo solicitado/adquirido y la cantidad solicitada.
- Llevar un control de las garantías o licencias de los activos, de igual manera mantenerlo actualizado constantemente.
- Velar por el adecuado uso de los activos, su buen estado físico y la custodia de los activos que tengan asignados.
- Informar a la jefatura superior el faltante, robo o daño detectado en los activos asignados, para lo cual se cuenta con un plazo no mayor a tres días.
- Velar por que los activos asignados cuenten la placa o número de patrimonio (esto cuando sea posible).

2.4 Uso aceptable de los activos

Se debe establecer una serie de reglas sobre el uso adecuado de los activos de información basadas en los principios de:

- Los activos deben manejarse con estándares éticos y técnicos, velando por su adecuado uso, el buen estado y mantenimiento de estos. Además, su adquisición debe reflejar la necesidad de negocio.
- Realizar un proceso de investigación, evaluación y análisis, antes de la toma de decisiones relacionada con la adquisición y uso de los bienes.
- El personal que gestiona y controla los activos debe contar con los conocimientos y experiencia necesarios, de no ser así, deberá buscar capacitación o asesoría de otra persona que maneje el tema.

2.5 Clasificación de la información

La Dirección de Informática de Gestión debe gestionar la clasificación de la información realizada por los propietarios de la misma, se debe definir la clasificación de la información y el significado de cada estrato; tomando para ello en cuenta las necesidades del negocio de compartir y restringir el acceso a la información, su valor, requisitos legales, sensibilidad y criticidad para el negocio. Esto permitirá establecer y aplicar controles de seguridad adecuados según el nivel de clasificación de la información.

El propietario de los activos es quién tiene la responsabilidad de clasificar dicho activo y evaluar su clasificación periódicamente. Una vez clasificados los activos debe definirse una etiqueta (nomenclatura) según el tipo de activo.

Capítulo 3. Control de Accesos

3.1 Objetivo

Establecer políticas que provean el control de acceso a todos los usuarios, que debe administrar la Dirección de Informática de Gestión, a los activos, protegiendo la información de accesos no autorizados; promoviendo la confidencialidad, integridad y disponibilidad de los sistemas y activos de información.

3.2 Lineamientos de control de Acceso

Los permisos que se otorgan a cada usuario o grupo de usuarios pueden ser físicos o lógicos. Estos deben estar claramente documentados, basados en los siguientes principios:

- Necesidad clara del negocio que permita justificar la razón por la cual se debe asignar ese permiso al usuario.
- Asignar los privilegios mínimos.
- Consistencia entre controles de acceso y la clasificación de la información a la cual el usuario tendrá acceso.
- Accesos estandarizados dependiendo de los roles de trabajo más comunes.
- Segregación de labores según las responsabilidades, evitando el conflicto de intereses.
- Todo acceso es denegado, a menos que sea que sea solicitado por los medios establecidos (oficio y/o formulario).
- Prevenir el acceso a usuarios no autorizados.
- Los dueños de los activos de información son los responsables de aprobar/denegar el acceso a dicho activo.

Debe existir una revisión periódica de accesos dependiendo de la clasificación de la información. Esto como mínimo una vez al año, de manera que se asegure que el acceso sea otorgado a las personas que realmente lo requieran. Además, se debe estructurar un proceso de eliminación de accesos, una vez que la necesidad de negocio deja de ser válida debido a:

- Finalización de la relación laboral.
- Cambio de puesto o funciones.
- Traslado a otro departamento/dependencia.
- Inactividad.
- Uso inadecuado de los recursos.

Se deben establecer perfiles y roles definidos por los propietarios de los activos, así como procedimientos para la identificación y autenticación de usuarios y/o recursos de tecnologías de información. La Dirección de Tecnologías de Gestión debe garantizar los mecanismos apropiados para garantizar el establecimiento y uso correcto de estos perfiles y roles.

3.3 Gestión de usuarios

3.3.1 Registro de usuario. Debe existir un proceso de registro asignar/revocar accesos a los usuarios, bajo el principio de necesidad de saber y privilegio mínimo. Según la Contraloría General de la República (2007) “los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones”.

Además, la Contraloría General de la República (2007) indica que es necesario “implementar el uso y control de medios de autenticación e identificación de usuarios (usuario, contraseñas y otros medios) que permitan identificar a quienes utilicen los recursos tecnológicos” del MEP. El uso de cuentas compartidas o

identificadores grupales debe ser limitado, contar con la apropiada documentación y aprobación basada en una necesidad operacional o de negocio.

Crear un registro formal de todas las personas que cuentan con permisos para hacer uso de un servicio o sistema. Generar un proceso para la revocación inmediata de accesos a usuarios que finalizan su relación laboral, cambian de puesto o funciones, se trasladan a otros departamentos/dependencias, por inactividad o por uso inadecuado de los recursos.

3.3.2 Gestión de privilegios. Los sistemas de información deben poseer protección contra accesos no autorizados y deberán seguir un proceso formal de autorización. Basado en los siguientes puntos:

- El control de acceso a la información por medio de una aplicación, será dado por la asignación de roles que administren los privilegios de los usuarios dentro del sistema de información.
- Identificar los privilegios asociados a cada sistema o aplicación.
- Identificar los usuarios que poseen acceso a cada sistema o aplicación.
- Los privilegios serán concedidos basados en una necesidad real de uso; asignándose una vez se haya completado el proceso de autorización.
- Cumplir el principio de privilegio mínimo, es decir, se otorgarán únicamente los accesos necesarios para que la persona puede cumplir con sus labores.
- Seguir el principio de separación de tareas.
- Mantener un historial de los privilegios solicitados, concedidos o aprobados a cada usuario.

- Los privilegios de Administrador deben concederse a un identificador de usuario diferente al que se utiliza para realizar tareas regulares de negocio:
    - Los usuarios con cuentas de administrador no deben utilizarlas para tareas usuales como revisar el correo, navegar en internet u otras tareas. Deben utilizarse únicamente para realizar tareas administrativas debido a que su uso inadecuado puede causar daños o comprometer a los sistemas.
    - Las cuentas de administrador que ya no se requieran deben ser revocadas.
    - Las cuentas de administrador no deben utilizarse para aprobar sus propias solicitudes de acceso.
- El acceso a los sistemas debe ser aprobado por el superior jerárquico de la persona y el propietario de los datos/sistema, los cuales serán responsables de determinar si existe o no una necesidad de negocio.
- Los dueños de los sistemas y de la información deben revisar periódicamente que las personas que tienen acceso a sus sistemas o activos sigan teniendo una necesidad de negocio válida.

3.3.3 Gestión de contraseñas. Según recomienda el Ministerio del Interior Subsecretaria del Interior y Seguridad Pública Intendencia Regional de Atacama (2012) la asignación de contraseñas se deberá controlar a través de un proceso formal de gestión a cargo del área de tecnologías de información. Las recomendaciones para seguir son:

- No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar.
- No habilitar la opción recordar clave en este equipo, que ofrecen los programas
- No enviarla por correo electrónico
- Nunca guardar las contraseñas, en ningún tipo de papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento
- No compartir las contraseñas, con otros usuarios.
- Cambia la contraseña si piensa que alguien más la conoce.
- Seleccionar contraseñas que no sean fáciles de adivinar.
- No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.)
- No utilizar contraseña con números telefónicos, nombre de familia etc.
- Cambiar contraseñas regularmente. (p.8-9)
- Para dar acceso a los usuarios por primera vez o al restablecer una contraseña debe proveerse al usuario de una contraseña temporal, la cual debe forzarse a cambiar al ingresar al sistema.
- Verificar la identidad de los usuarios antes proveer una contraseña temporal.
- Las contraseñas temporales deben ser únicas para cada usuario.

- Cada usuario es responsable de salvaguardar su información de autenticación.
- Cualquier contraseña por defecto que tenga un sistema o equipo debe ser cambiada después del proceso de instalación o configuración.
- No escribir contraseñas en texto claro en archivos de código fuente, configuración, lote, registro, scripts, macros, valores del registro del sistema operativo o cualquier otro formato de archivo son protección.
- Los administradores deben configurar los sistemas, aplicaciones y redes para imponer una autenticación fuerte:
    - No permitir el uso de contraseñas repetidas.
    - Las contraseñas deben expirar después de un periodo de tiempo.
    - Se suspenderán las contraseñas por un periodo después de 10 intentos fallidos de inicio de sesión.
    - Debe haber un mínimo de caracteres definido para cuentas de usuario y otro número de caracteres mayor para las cuentas administrador.
    - Los administradores deberán implementar mecanismos de autenticación que permitan la segura gestión, almacenamiento, uso y transferencia de credenciales.

3.3.4 Responsabilidades de los usuarios.

- Bloquear el equipo, sistema o aplicación al suspender su uso por un periodo corto de tiempo.

- Cerrar sesión en el equipo, sistema o aplicación al finalizar su uso, bloquearlo no es suficiente.
- Los usuarios son responsables de salvaguardar su información de autenticación
- Las contraseñas deben ser confidenciales.
- Cambiar la contraseña de inmediato hay sospecha de que alguien más la conoce.
- Seguir los lineamientos especificados en la sección de gestión de contraseñas.
- Prevenir el acceso a información no autorizada, cualquier información sensible o crítica para el negocio debe ser guardada de manera segura, ya sea electrónica o físicamente.

3.4 Control de acceso a la red

3.4.1 Uso de servicios de red.

- El acceso a los servicios debe restringirse solamente a los cuales fueron específicamente autorizados. Incluyendo acceso a las redes y servicios de red.
- Identificar e implementar procedimientos de autorización para las redes.
- Proteger el acceso a las redes alámbricas o inalámbricas y salvaguardar las redes de intentos de acceso maliciosos.
- Los controles implementados deben basarse en las mejores prácticas de la industria.

- Cualquier puerto de red que no se encuentre en uso debe ser deshabilitado o desconectado.

3.4.2 Autenticación de usuarios para conexiones externas. Identificar y crear un control apropiado de autorización para recibir conexiones externas a la institución, pueden suponer un riesgo de acceso no autorizadas o modificación de información por lo cual:

- Los procedimientos de conexión remotos deben proveer técnicas de autenticación, identificación y cifrado.
- Los dispositivos con conexión directa a internet deberán contar con software de seguridad como firewalls y antivirus.
- Restringir el acceso de terceras partes a navegar por la red de la institución, debe proveerse acceso solamente a los activos necesarios de la organización.
- Gestionar el acceso de terceras partes a la red a través de todo el ciclo de vida, incluyendo la revocación de accesos una vez que no haya necesidad de negocio o se haya incurrido en una falta.

3.4.3 Acceso a puertos de diagnóstico y configuración. Cualquier puerto o servicio instalado en una computadora, dispositivo o facilidad que no sea requerido para una función de negocio debe ser desactivado o removido.

Los puertos específicos para configuración y diagnóstico de dispositivos de red, así como de computadoras deben poseer controles de acceso más restrictivos y deben ser accesibles solamente por ciertos administradores de sistema.

3.4.4 Segmentación de redes. Las redes de la institución deben segmentarse tomando en cuenta los servicios, usuarios y aplicaciones permitiendo aislarlos, prevenir accesos no autorizados y definir perímetros de seguridad. Cada segmento debe determinarse tomando en cuenta lo siguiente:

- Evaluaciones de riesgo
- Requerimientos de seguridad
- Requerimientos de acceso
- Niveles de sensibilidad de la información guardada en el segmento
- Niveles de confianza
- Líneas de negocio

3.4.5 Controles de conexiones de red. El departamento debe implementar controles de enrutamiento que permitan asegurar que las conexiones de las computadoras y la información fluya por la red tomando en cuenta las políticas de control de acceso de este documento. Por lo cual debe existir mecanismos de verificación del origen y destino de los paquetes.

3.5 Control de acceso a los sistemas operativos

3.5.1 Procedimientos de inicio de sesión seguros. Proteger el acceso a los sistemas operativos según recomienda el Ministerio del Interior Subsecretaria del Interior y Seguridad Pública Intendencia Regional de Atacama (2012) mediante un inicio de sesión seguro, que contempla las siguientes condiciones:

- No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
- No suministrar mensajes de ayuda, durante el proceso de autenticación que puedan dar ayudar a un usuario no autorizado.
- Validar los datos de acceso.
- Limitar el número de intentos fallidos de conexión a 10 y auditar los intentos no exitosos.
- No mostrar las contraseñas.
- No transmitir la contraseña en texto claro. (p.8)

3.5.2 Identificación y autenticación de usuarios. Para ingresar a los sistemas y la información del MEP cada usuario debe poseer una cuenta con un identificador único de usuario y una contraseña, para poder asegurar de manera razonable que se identifique a cada usuario y se puedan restringir sus accesos. Ningún usuario debe compartir el mismo identificador con otro usuario dentro del MEP. Cada cuenta debe ser única y debe ser utilizada por el usuario para el cual fue creado, es decir, no se permiten transferencias de usuarios entre el personal.

Las cuentas creadas para usuarios externos o terceras partes deben contener un atributo distintivo que denote que la cuenta es externa.

Las cuentas genéricas, usualmente, son compartidas por más de una persona o sistema, su uso está limitado y solo deben crearse cuando hay una justificación de negocio válida, debe proporcionarse el mínimo acceso basado en dicha necesidad de negocio. Los nombres de cuentas genéricas deben reflejar el propósito para el cual se crearon y deben poseer un dueño primario y secundario. Finalmente, las cuentas genéricas deben ser controladas y revisadas periódicamente para determinar si siguen siendo requeridas o si el acceso que poseen es el adecuado.

Las cuentas de prueba deben ser creadas bajo una justificación de negocio o de un equipo de proyecto y aprobadas por el dueño del sistema, deben darse los privilegios mínimos para cumplir su función y expirar en un plazo no mayor a seis meses.

3.5.3 Sesiones y tiempos de conexión. La sesión debe expirar para usuarios inactivos por un periodo de tiempo, y deberán autenticarse nuevamente. El tiempo de duración de la conexión debe definirse según los siguientes criterios:

- Clasificación de la información
- Evaluaciones de riesgo
- Niveles de confianza
- Niveles de acceso

Los sistemas y aplicaciones deben proveer a los usuarios una opción explícita para terminar su sesión. Las aplicaciones desarrolladas deben asegurar que:

- Identificadores de sesión no sean predecibles.
- No autenticar a los usuarios sin invalidar primero el identificador de sesión existente.
- El identificador de sesión no debe usarse de nuevo una vez se termina la sesión.
- Los identificadores deben protegerse especialmente en tránsito entre el cliente y el servidor.

3.6 Dispositivos móviles y teletrabajo

Según recomienda el Ministerio del Interior Subsecretaria del Interior y Seguridad Pública Intendencia Regional de Atacama (2012) el uso de equipos de cómputo y dispositivos de almacenamiento móviles para labores del MEP está restringido únicamente a los provistos por la institución y deberán contemplar las siguientes directrices:

- Uso de usuario y contraseña para acceso al mismo.
- Cifrado de la información.
- Uso de software antivirus
- Restricción de privilegios administrativos para los usuarios.
- Uso de software licenciado
- Realización de copias de seguridad periódicas.
- Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos.
- Permanecer siempre cerca del dispositivo
- No dejar desatendidos los equipos
- No conectarse a redes WiFi públicas
- Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir. (p.10)
- Establecer mecanismos de protección para los datos guardados en los dispositivos móviles.
- Establecer mecanismos de protección para prevenir el acceso no autorizado.
- Establecer mecanismos de protección contra software malicioso.
- Establecer un procedimiento en caso de robo del dispositivo móvil.

Capítulo 4. Gestión de incidentes

4.1 Lineamientos de gestión de incidentes

Los eventos de seguridad de la información deben ser reportados a través de canales administrativos lo más rápido posible.

Para esto se recomienda que exista un procedimiento establecido, definiendo qué acciones se deben tomar y el punto de contacto que debe comunicar lo sucedido. Es importante que este punto de contacto sea parte de la organización y que esté disponible para trabajar en el evento en el momento que suceda. Ejemplos de eventos de seguridad e incidentes:

- Pérdida de servicio y equipo
- Fallos de sistema o sobrecargas
- Errores humanos
- No cumplir con políticas o lineamientos
- Cambios de sistema descontrolados
- Mal funcionamiento de software y hardware
- Violación de acceso

Según Ramírez Y. (2014) para comunicar un evento de seguridad se deben seguir los siguientes pasos:

- Definir un proceso formal de comunicación de incidentes que incluya:
    - Indicar la acción que se debe seguir.
    - Incluir la detección del incidente.
    - Indicar los recursos necesarios para la investigación y resolución del incidente.
    - Incluir a la persona encargada de realizar el monitoreo.
- Llevar registros de auditoría que incluya: id del usuario, fecha y hora de inicio y terminación de la violación, ubicación.

- Hacer un informe de las amenazas encontradas en los sistemas que incluya el procedimiento de registro y los eventos detectados.
- Registrar, evaluar e identificar aquellos eventos o incidentes que son recurrentes con el fin de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.
- El Departamento de Informática de Gestión debe:
    - Implementar los mecanismos necesarios para tener una buena comunicación y dar a conocer los incidentes/eventos ocurridos, con el fin de minimizar los daños y prevenir que sucedan de nuevo.
    - Definir procedimientos para el manejo de incidentes que garantice una respuesta rápida y eficaz a los incidentes de seguridad informática.
    - Definir la recurrencia de las revisiones o auditorías.
- Este departamento debe garantizar que se definan y ejecuten los procedimientos para identificar, analizar, valorar y solucionar los incidentes, y que también se haga una respectiva evaluación sobre el impacto en el negocio de los incidentes de seguridad identificados.
- Reportar los incidentes de seguridad que se presenten, según lo indique el procedimiento de gestión de incidentes.
- La comunicación del evento o incidente debe incluir:
    - Cantidad de personas afectadas.
    - Fecha y hora en la que se detecta.
    - Fecha y hora en la que se produce el incidente y su duración.

- Circunstancias en que se haya producido el incidente de seguridad (por ejemplo, pérdida, robo, copia, etc.).
- Tipo de los datos personales en cuestión.
- Posibles consecuencias, daños y efectos negativos en los afectados. (p.16-17)

Los objetivos para el manejo de eventos/incidentes de seguridad de la información deben de estar aprobados por la jefatura, y esta se debe de asegurar que los empleados entiendan las prioridades cuando se maneja de incidentes.

Capítulo 5. Seguridad física y ambiental

5.1 Objetivo

Establecer prácticas y controles para salvaguardar física y ambientalmente las personas y los activos propiedad del MEP.

5.2 Asegurar las áreas

Establecer perímetros de seguridad para proteger área que contienen o procesan información es vital y obligatorio. Los perímetros de seguridad deben estar claramente definidos y los controles implementados dependen de los requerimientos y de evaluaciones de riesgo.

El edificio que contiene instalaciones de procesamiento o almacenamiento de información debe poseer las siguientes características:

- Paredes externas sólidas.

- Protección en las puertas.
- Protección en las ventanas.
- Iluminación que no permita zonas oscuras.
- Mecanismos de control de acceso al edificio.
- Sistemas de detección de intrusos, incluyendo cámaras y alarmas.
- No debe haber rótulos indicando donde se encuentran los cuartos seguros.
- Deben tomarse en cuenta medidas de seguridad para:
    - Incendios
    - Terremotos
    - Inundaciones
    - Disturbios
    - Manejo de sustancias peligrosos o inflamables
    - Robos

El acceso a áreas seguras debe documentarse en una bitácora que incluya la fecha y hora de entrada y salida, la cédula de la persona y el motivo de la visita. El acceso también debe restringirse únicamente a las personas autorizadas mediante el uso de controles de seguridad como tarjetas, pines u otros.

Visitantes o terceras partes que entren a las áreas seguras deben ir siempre acompañados por el personal de la organización, y solo se les permitirá acceso bajo una razón de negocio o necesidad operativa. Al igual que los empleados del MEP, deberán hacer uso de la bitácora.

El personal ajeno a las áreas seguras no debe conocer las actividades que se realizan a menos que exista una razón. Además, por seguridad el trabajo que se realice en estas zonas debe ser supervisado por razones de seguridad del personal y para prevenir actividades no autorizadas.

5.3 Seguridad del equipo

Ubicar todo el equipo informático y protegerlo de acceso no autorizado:

- No dejar el equipo de red al fácil alcance.
- Utilizar racks, cuartos seguros, centros de datos, u otros controles para asegurar los equipos.
- Controlar la temperatura de los dispositivos y equipos.
- No comer, beber o fumar cerca de los dispositivos y equipos.
- Proteger el equipo de fallas eléctricas incluyendo fuentes de poder de respaldo o generadores.
- Proteger el equipo de fallas en la ventilación.
- Deben existir apagadores de emergencia cerca de las puertas de emergencias para facilitar un apagado rápido de los equipos en caso de emergencia.
- Debe existir una fuente estable de agua que permita alimentar los sistemas de enfriamiento y también los sistemas contra incendio.
- Los cables deben contar con la protección adecuada y deben estar fuera del alcance cuando sea posible.
- Los cables deben estar correctamente etiquetados para prevenir errores.

- Los cables de red deben ser separados de los cables de electricidad para evitar interferencias. Cuando sea requerido utilizar cables blindados.
- Inspecciones físicas rutinarias para los equipos que ayuden a detectar acceso no autorizado o dispositivos maliciosos conectados.
- Para equipos se encuentre fuera de las instalaciones del MEP.
    - No dejarlos desatendidos
    - Bloquear o apagar los equipos cuando no estén en uso
    - Guardarlos en la cajuela del automóvil
    - Evitar utilizar etiquetar los dispositivos

El mantenimiento de los equipos es necesario para asegurar su correcto funcionamiento, por ello solo personal autorizado debe ejecutar mantenimientos y debe llevarse un registro de todos los mantenimientos realizados.

Para retirar, eliminar o reutilizar equipo, revisar si almacena información sensible o algún tipo de software licenciado y que deberá ser removida, borrada o sobrescrita.

Capítulo 6. Adquisición, desarrollo y mantenimiento de sistemas de información

6.1 Objetivo

La política de adquisición, desarrollo y mantenimiento de sistemas de información define requerimientos del ciclo de vida de los sistemas y de hardware.

Además, provee las bases para un robusto desarrollo, mantenimiento y adquisición de sistemas.

6.2 Requerimientos de seguridad para sistemas de información

Los requerimientos de negocio para nuevas aplicaciones o incluso para mejoras a las aplicaciones ya existentes deben incluir requerimientos de seguridad de la información que reflejen el valor de negocio de la información. Entre estos requerimientos se encuentran:

- Evaluaciones de riesgos.
- Evaluaciones de seguridad.
- Revisión de la arquitectura de la seguridad.
- Definir controles compensatorios si es requerido por las evaluaciones.
- Al desarrollar un sistema, la seguridad de la información debe formar parte del proyecto o metodología desde etapas tempranas.
- Seguir el principio de separación de labores e implementar controles que lo respalden.
- Planificar la capacidad del sistema, permitiendo que las plataformas y la infraestructura puedan satisfacer la demanda en lapsos pico.

6.3 Procesamiento en las aplicaciones

Para prevenir errores, pérdida, modificación o uso incorrecto de la información es necesario establecer controles que ayuden a proteger dicha información.

La validación de los datos de entrada es uno de los controles más básicos e importantes que deben ser aplicados en los sistemas e incluye:

- Revisión de los límites de las entradas de datos o limitar los campos.
- Revisión de las entradas de datos para evitar inyección de código intruso de los siguientes tipos:
    - SQL
    - LDAP
    - Código
    - XML
- Revisión de los datos de entrada para evitar XSS.
- Procedimientos para responder a la validación de errores.
- Definir responsabilidades de las personas involucradas en el proceso de entrada de datos.
- Crear registros de las actividades involucradas en el proceso de entrada de datos.

Es necesario incorporar validaciones que detecten la corrupción de datos mediante:

- Ataques de desbordamiento de búfer, pila y cola.
- Concurrencia de procesos.
- Condiciones de carrera.
- Incorrecto procesamiento de datos debido errores y fallas, por lo que se deben establecer procedimientos de recuperación.

- Incorrecto orden de ejecución de los programas.
- Incorrecta ejecución de tareas o procedimientos después del fallo de una dependencia.

En el caso de los mensajes en las aplicaciones se debe identificar si es necesario validar la integridad de los datos enviados y recibidos. Finalmente, revisar los datos de salida para verificar el procesamiento correcto de los datos mediante pruebas que miden la precisión y que tan completos están dichos datos.

6.4 Controles criptográficos

Identificar la necesidad de crear controles criptográficos que ayuden a mantener la confidencialidad, integridad y autenticidad de los datos. El uso de estos controles, el tipo y fuerza de los algoritmos, debe determinarse mediante evaluaciones de riesgos y requerimientos de seguridad.

Proteger las llaves criptográficas de pérdida, modificación y divulgación mediante estándares y procesos que gestionen la creación, distribución, almacenamiento, revocación, destrucción y recuperación de llaves. Así como la protección de física y de los equipos utilizados para la creación y almacenamiento de las llaves.

6.5 Seguridad de los archivos de sistema

Definir rutinas de mantenimiento para los sistemas de cómputo del MEP que incluyan actualizaciones de software y de las aplicaciones y monitorear los sistemas periódicamente para asegurar que se cumple con las rutinas de mantenimiento.

La implementación de nuevos sistemas o aplicaciones debe hacerse solamente después de haber ejecutado pruebas de usabilidad, seguridad y posible impacto a otras aplicaciones que se encuentren en producción.

Llevar un control de todo el software implementado, su configuración y su documentación. Así como archivar versiones anteriores de los sistemas, incluyendo configuración y parámetros en caso de contingencia.

El software provisto por terceros debe mantenerse en las versiones que todavía soporta el proveedor, quien todavía ofrece mejoras y arreglos a problemas o fallas de seguridad. Si existe software fuera de soporte en la organización debe establecerse un plan para migrar a una nueva versión del software.

En el caso de actualizaciones de software debe medirse los beneficios y la necesidad de negocio antes de realizar los cambios, las actualizaciones de software pueden traer inestabilidad o introducir nuevas fallas. Estos cambios deben probarse en un ambiente aislado o un ambiente de pruebas y pasar un proceso de gestión de cambios (Referirse a la sección gestión de cambios).

Los sistemas y dispositivos que no cumplan con las actualizaciones mínimas de seguridad aprobadas por el departamento de tecnologías de información están sujetas a desconexión o aislamiento hasta que cumpla con los requisitos mínimos de seguridad.

Finalmente, el acceso al código fuente, librerías y documentación de diseño de las aplicaciones desarrolladas por el MEP debe restringirse para prevenir cambios no autorizados.

6.6 Seguridad en el proceso de desarrollo y soporte

Seguir un proceso formal de gestión de cambios para desplegar los nuevos cambios de una aplicación en el ambiente de producción, el proceso debe incluir:

- El impacto de los cambios.
- Análisis de riesgo de dichos cambios.
- Lista de cambios por realizar.
- Sistemas o equipos afectados.
- Los planes o pasos por seguir.
- Documentación de las pruebas que se llevaron a cabo para verificar el correcto funcionamiento de la aplicación.
- Un procedimiento para revertir los cambios en caso de exista un problema.

Dichos cambios deben documentarse y ser aprobados una vez corroborado que cumplen con los requerimientos anteriores. El proceso de gestión de cambios debe seguir el principio de separación de tareas, por lo que la persona que implementa, realiza pruebas y aprueba deben ser diferentes.

Los cambios referentes a sistema operativo deben incluir pruebas de las aplicaciones más críticas del negocio para prevenir impactos adversos en las operaciones del MEP.

Cuando el desarrollo de las aplicaciones subcontratado, el departamento de informática de gestión debe incluir requerimientos de seguridad en el contrato y debe considerarse:

- Revisiones de código

- Evaluaciones de seguridad
- Evaluaciones de calidad
- Controles de seguridad técnicos
- Pruebas antes de la instalación en ambientes de producción
- Arreglos en caso de fallas

6.7 Gestión de vulnerabilidades técnicas

Las vulnerabilidades cambian día con día y es necesario obtener información técnica de las vulnerabilidades en los sistemas de información, evaluarlas y tomar las acciones necesarias en un lapso aceptable. Algunas de las actividades a realizar incluyen:

- Evaluación de vulnerabilidades de los sistemas y de las aplicaciones instaladas.
- Uso de herramientas de detección de vulnerabilidades.
- Trabajar con los dueños de los sistemas o equipos de desarrollo para remediar las vulnerabilidades.
- Definir roles y responsabilidades de las personas involucradas con la gestión de vulnerabilidades:
    - Monitoreo de vulnerabilidades
    - Evaluación de riesgo
    - Pruebas
    - Remediación de las vulnerabilidades

Capítulo 7. Concienciación y procedimientos de terminación laboral

7.1 Objetivos

Generar en los empleados un buen nivel de concienciación sobre la seguridad de la información, mediante educación y capacitaciones constantes.

Asegurar que los procesos de terminación laboral o cambio de puesto se llevan a cabo de una manera ordenada sin poner en peligro la seguridad de la información.

7.2 Conciencia de seguridad de la información, educación y capacitación

- Garantizar que los empleados del departamento de informática de gestión estén conscientes de las amenazas de seguridad de la información, sus respectivas responsabilidades.
- Proveer capacitaciones sobre los procedimientos de seguridad y el uso correcto de la información con el fin de asegurar un adecuado nivel de concienciación y educación.
- Definir un proceso disciplinario para manejar problemas de seguridad de la información.
- Los gerentes del departamento deben:
    - Confirmar previo a otorgar permisos a información sensible a los sistemas de información, que los empleados reciban información adecuada sobre sus roles y responsabilidades informáticas.

    - Motivar a los empleados para cumplir con las políticas de seguridad del departamento.
    - Promover que los empleados alcancen un nivel de conciencia sobre seguridad relevante para sus roles y responsabilidades.
    - Promover la capacitación continua para asegurar que los empleados tengan las habilidades y capacidades apropiadas.
- Los empleados deben recibir una capacitación de concienciación sobre seguridad de la información que incluya la revisión de las políticas y expectativas de seguridad antes de que su primer acceso o privilegio sea otorgado.
- Establecer un plan de capacitación continua en el cual capacite a los empleados en el uso correcto de paquetes de software, equipo, inicio de sesión, proceso disciplinario, entre otros.
- Garantizar que el personal sea consciente de sus respectivas responsabilidades de seguridad informática, de lo contrario estos podrían causar daños considerables a la organización.
- Mantener al personal motivado con el fin de que sean personas más confiables y se mitiguen incidentes de seguridad de la información.

7.3 Terminación laboral o cambio de empleo

- La devolución de todos los activos institucionales previamente asignados incluyendo software, tarjetas de acceso, documentos institucionales,

dispositivos móviles, equipos, tarjetas de crédito, medios electrónicos y otros; deben conformar parte del proceso de terminación laboral.

- Revocar los privilegios de acceso del individuo a los activos asociados con los sistemas y servicios de información al terminar la relación laboral.
- Eliminar todos los privilegios de acceso que no fueron aprobados al cambiar de trabajo o rol. Los privilegios de acceso que deben eliminarse o adaptarse incluyen acceso físico y lógico, claves y tarjetas de identificación.
- Verificar/auditar si las cuentas de un empleado siguen activas después de haber cambiado de puesto o terminado la relación laboral, con el fin de eliminarlas.

Capítulo 8. Gestión de la continuidad de servicios de tecnologías de información

8.1 Seguridad de la información en el proceso de continuidad de servicios informáticos

Un plan de gestión de la continuidad de servicios de TI deberá de ser implementado para minimizar el impacto a la organización y poder recuperarse ante una pérdida de información a un nivel aceptable. Elementos clave para la continuidad de servicios informáticos:

- Identificar los servicios y sistemas críticos, comprender los riesgos que enfrentan en términos de probabilidad e impacto.
- Identificar los activos involucrados en cada servicio.

- Comprender el impacto que tienen las interrupciones causadas por incidentes de seguridad de la información.
- Identificar y considerar la implementación de medidas preventivas para mitigar el impacto definido.

8.2 Continuidad de servicios y evaluación de riesgos

La continuidad de servicios de tecnologías de información para la seguridad de la información debe basarse en la identificación de eventos que puedan causar interrupciones en los servicios críticos, como, por ejemplo: falla en el equipo, errores humanos, robos, incendios, desastres naturales, entre otros.

Seguido de esta identificación, se debe realizar una evaluación de riesgos para determinar la probabilidad, el impacto y medir la magnitud de las consecuencias de dichas interrupciones en términos de tiempo, costos, posibles daños o incluso repercusiones legales. Las evaluaciones de riesgos deben llevarse a cabo con la participación total de los dueños de los servicios o sistemas. La evaluación debe identificar, cuantificar y priorizar los riesgos según objetivos relevantes para la organización.

Basados en los resultados de la evaluación de riesgos, se debe desarrollar una estrategia de continuidad de servicios tecnológicos y la gerencia debe proporcionar el respaldo, crear y aprobar un plan para implementar la estrategia.

8.3 Implementando un plan de continuidad para la seguridad de la información

En el plan continuidad de servicios críticos deberá:

- Identificar y aprobar las responsabilidades y procedimientos de continuidad.
- Identificar la pérdida aceptable de información y servicios.
- Implementar procedimientos que permitan la recuperación y restauración de las operaciones en las escalas de tiempo requeridas.
- Documentar los procedimientos y procesos acordados.
- Educar al personal sobre la gestión de crisis y los procedimientos y procesos acordados.
- Probar y actualizar los planes.

8.4 Marco de planificación para continuidad de servicios de tecnologías de información

Cada plan de continuidad deberá:

- Especificar el plan de escalación y las condiciones para su activación, como también las personas responsables de ejecutar cada sección del plan.
- Tener un propietario asignado.
- Describir el procedimiento de emergencia y acciones a seguir en caso de un incidente.
- Agendar un mantenimiento recurrente que especifique cómo y dónde debería de ser probado y el procedimiento a seguir para darle mantenimiento.
- Garantizar que los procesos sigan siendo efectivos y que las responsabilidades de las personas están claras.
- Especificar los servicios críticos y recursos necesarios para ejecutar el plan de emergencia.

8.5 Mantenimiento, actualización y pruebas del plan de continuidad de servicios de tecnologías de información

Las pruebas del plan de continuidad de servicios de tecnologías de información deben garantizar que las personas encargadas de la recuperación tengan conocimiento de los planes y de sus responsabilidades para cuando se tenga que invocar el plan. Para asegurar que el plan va a funcionar se recomienda:

- Probar varios escenarios.
- Hacer simulaciones.
- Probar la recuperación técnica, garantizando que los sistemas se puedan restablecer de manera efectiva.

Al dar mantenimiento al plan se puede actualizar:

- Personal
- Direcciones o números de teléfono
- Recursos
- Procesos
- Riesgos

Capítulo 9. Gestión de comunicaciones y operaciones

9.1 Objetivo

Mantener la integridad y disponibilidad de la información al detectar actividades no autorizadas, con el fin de que las personas estén al tanto de lo que sucede, resguardando la integridad del software y de la información.

9.2 Gestión de cambios

Se debe considerar:

- Identificar y registrar los cambios significativos.
- Planificar y probar los cambios.
- Evaluar los posibles impactos de los cambios.
- Establecer un procedimiento formal de aprobación para los cambios propuestos.
- Establecer procedimientos alternativos para detener el cambio y recuperarse de cambios fallidos y eventos imprevistos.

9.3 Segregación de labores

La segregación de funciones es una manera de reducir el riesgo con el fin de evitar un mal uso accidental o deliberado de los sistemas facilitando el fraude. Debido a esto se recomienda dividir las transacciones o tareas y tener cuidado de que ninguna persona pueda acceder, modificar o usar activos sin autorización. En caso de ser difícil segregar, se pueden utilizar otros controles, como el monitoreo de actividades y auditorías.

9.4 Monitoreo

Las actividades de monitoreo se efectúan de manera exitosa cuando se cuenta con registros de auditorías en donde se registran actividades de los usuarios y de esta forma se puede identificar qué fue lo que se hizo, quien lo hizo y cuando.

Estos registros sirven a investigaciones futuras, monitoreo y control de acceso. Es recomendable que estos registros incluyen:

- Identificación de usuario.
- Fecha, hora y tipo de evento.
- Ubicación (por ejemplo: una ruta).
- Cambios en la configuración del sistema.
- Uso de privilegios/accesos.
- Las aplicaciones que se han usado.
- Las direcciones de red y protocolos.

Las auditorías se deben llevar a cabo de manera frecuente y con cierta periodicidad y se recomienda:

- Revisar/generar información sobre los incidentes de seguridad encontrados.
- Revisar los registros de auditoría, eventos de seguridad y fallas.

9.5 Planificación y aprobación del sistema

9.5.1 Gestión de capacidad.

- Garantizar el rendimiento de los sistemas mediante el uso de recursos para monitorear, ajustar y hacer proyecciones de los requisitos de capacidad futuros, con el fin también de mejorar la disponibilidad y la eficiencia de los sistemas.
- Identificar los requisitos de capacidad.
- Establecer controles de detección para indicar problemas en el debido tiempo.

9.5.2 Aceptación de sistemas. Definir, acordar, documentar y probar los criterios para la aceptación de nuevos sistemas, actualizaciones y nuevas versiones. Para llevar a cabo esto se debe considerar:

- El rendimiento y capacidad informática.
- Procedimientos de recuperación y planes de contingencia.
- Prueba de procedimientos operativos.
- Identificar controles de seguridad.
- Recolectar evidencias que indiquen que la nueva instalación no va a afectar los sistemas
- Fácil e intuitiva experiencia de usuario ya que de esta manera se evitan errores humanos.

9.6 Protección de código malicioso

Implementar controles de detección, prevención y recuperación para proteger los sistemas contra códigos maliciosos. Se debe:

- Evitar el uso de software no autorizado.
- Proteger contra el acceso no autorizado de archivos y software, ya sea a través de redes externas o en cualquier otro medio.
- Instalar y actualizar periódicamente software de detección y reparación de códigos maliciosos para escanear computadoras.
- Preparar planes de continuidad de servicios de tecnologías de información apropiados para la recuperación de ataques de código malicioso, incluidos todos los detalles necesarios de respaldo y recuperación de datos y software.

9.7 Respaldos

Los respaldos se deberían probar frecuentemente según lo indique la política y se debería:

- Definir el nivel necesario de información a respaldar.
- Generar registros de las copias de seguridad.
- Almacenar las copias de seguridad en una ubicación remota, a una distancia suficiente para escapar de cualquier daño causado por un desastre en el sitio principal.
- Probar regularmente los medios de respaldo para asegurar su confiabilidad.
- Revisar los procedimientos de restauración y probarlos regularmente para asegurar que sean efectivos y que puedan utilizarse para la recuperación.
- Encriptar copias de seguridad en caso de contener datos confidenciales.

9.8 Gestión de la seguridad de la red

- Administrar y controlar las redes adecuadamente, para proteger de las amenazas y mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluida la información en tránsito.
- Definir responsabilidades y procedimientos para la gestión de equipos remotos.
- Aplicar un registro y monitoreo adecuado para permitir el registro de acciones relevantes para la seguridad.

9.2. Plan de continuidad de servicios

Plan de continuidad de servicio de TI para el enlace MEP-Hacienda

Ministerio de Educación Pública de Costa Rica

Control de versiones

Versión	Fecha	Modificaciones	Modificado por:	Aprobado por:
1	Febrero 2020	Creación de documento		

Control de pruebas

Fecha	Tipo de prueba	Realizada por:	Autorizada por:

Capítulo 1. Información general

1.1 Objetivo

Desarrollar y documentar un plan de continuidad de servicio para el enlace de conexión entre el Ministerio de Educación Pública y el Ministerio de Hacienda. La documentación se presenta de forma sencilla, fácil de entender y mediante guías que ayuden a gestionar de manera eficiente la respuesta y recuperación ante eventos imprevistos o desastres que afecten la operación normal del servicio.

1.2 Alcance

El alcance del plan abarca el enlace de conexión administrada por el MEP el cual permite la interacción entre el MEP y el Ministerio de Hacienda para el sistema de planilla llamado *Integra2*. Actualmente Hacienda hospeda el sistema Integra2 en sus instalaciones y el MEP accede a dicho sistema para gestionar la planilla de alrededor de 84 mil funcionarios y más de 80 mil millones de colones mensuales. Por lo tanto, la plataforma tecnológica que une ambas organizaciones es crítica y debe asegurar estabilidad y disponibilidad.

1.3 Supuestos

- El personal requerido o sus respaldos estarán disponibles y contarán con el acceso requerido.
- Tener acceso a una computadora.

- Tener acceso al plan de continuidad de servicio o cualquier documentación relacionada.
- El plan se ha probado y se sigue probando al menos una vez al año.
- El plan se actualiza y se revisa como mínimo una vez al año.
- El personal involucrado conoce el plan de continuidad de servicio.

1.4 Mantenimiento del plan y pruebas

La Dirección de Informática de Gestión (DIG) como encargado de continuidad de servicios tecnológicos, es responsable de actualizar periódicamente el plan de continuidad de servicio, así mismo es responsable de que las partes involucradas conozcan el plan y tengan conocimiento de los procedimientos de recuperación para ello referirse al procedimiento de divulgación en Anexo 1.

Finalmente debe garantizar que el plan de recuperación se pruebe periódicamente, dichas pruebas deben quedar documentadas en la sección de control de pruebas al inicio de este plan.

1.4.1 Pruebas. Para realizar las pruebas del plan es necesario seguir estos pasos:

1. Determinar el objetivo y alcance de la prueba.
2. Estimar el tiempo de duración.
3. Seleccionar el tipo de prueba.
4. Desarrollar un escenario de prueba.
5. Desarrollar un criterio de evaluación.

6. Identificar a los participantes.
7. Identificar los recursos.
8. Realizar la prueba.
9. Evaluar los resultados.
10. Analizar las lecciones aprendidas.
11. Revisar y modificar el plan de acuerdo a las lecciones aprendidas.

Existen dos tipos de pruebas que se recomiendan:

1.4.1.1 Pruebas de escritorio. Tienen el objetivo de revisar la documentación, evaluar su contenido, estructura, procedimientos y procesos. El plan debe leerse completamente y determinar si requiere alguna actualización o cambios, además el procedimiento de recuperación debe leerse y evaluarse paso a paso con el equipo de redes y demás personal involucrado.

Las pruebas de escritorio no deben tomarse como una revisión rápida de la documentación, sino que la persona a cargo de realizar la prueba debe revisar con detalle cada parte del plan. Las pruebas de escritorio deben ejecutarse una vez cada seis meses.

1.4.1.2 Pruebas funcionales. Este tipo de prueba consiste en un simulacro que requiere de la participación de todos los miembros del equipo y busca utilizar un ambiente de pruebas similar al de producción donde se simula un incidente y se ejecutan todos los procedimientos paso a paso. El propósito de la prueba es determinar si todos los procedimientos se ejecutan correctamente, si todas las personas conocen el plan y si todos los pasos a seguir son lo suficientemente claros y detallados. Las pruebas funcionales deben ejecutarse como mínimo una vez al año.

Capítulo 2. Equipo de recuperación de desastres



Figura 8. Equipo de recuperación (Elaboración propia)

2.1 Encargado de la continuidad de servicios

Son las personas responsables de guiar el proceso de continuidad de servicios de TI. Entre las principales responsabilidades se encuentra:

- Comunicar a los líderes de la organización sobre los incidentes mayores, así como proveer la información requerida.
- Coordinar cualquier comunicación durante un evento.
- Coordinar al menos una vez al año la revisión del plan y proveer mejora continua.
- Coordinar al menos una vez al año las pruebas del plan.
- Trabajar con las diferentes áreas del departamento para mantener los procedimientos actualizados.
- Asegurar que los recursos y planes estén disponibles para todos los involucrados.
- En caso de un evento requiera activar el plan de continuidad de servicio, se deben evaluar los resultados y aplicar mejoras al plan.
- Gestionar el equipo de recuperación y tomar decisiones.

2.2 Equipo de Redes

Es el equipo responsable de verificar el daño en la infraestructura de red que enlaza al MEP con el Ministerio de Hacienda. Este equipo debe encargarse de:

- Verificar el impacto y el daño provocado en la infraestructura y recuperarlo en orden de prioridad.

- Comunicar y proveer el progreso de la recuperación.
- Coordinar con terceras partes o proveedores la recuperación del enlace.
- El equipo debe apoyar las pruebas y las revisiones del plan.
- Informar a los encargados de continuidad la necesidad de actualizar el plan.
- Asegurarse de mantener acceso a los procedimientos de recuperación.

2.3 Lista de contactos

Tabla 3

Contactos

Nombre	Email	Número de teléfono	Respaldo
GBM	support@gbm.net	2284-3911	No aplica
Hacienda	notificamesadtic@hacienda.go.cr	2539- 4774	No aplica
Ronny Rojas Vargas	ronny.rojas.vargas@mep.go.cr	2256-7011 ext:2570	Valerie Castro Espinoza
Berny Salazar Rojas	berny.salazar.rojas@mep.go.cr	2256-8132 ext:1590	Ronny Rojas
Valerie Castro Espinoza	valerie.castro.espinoza@mep.go.cr	2256-8132 ext:1597	Kenneth Gamboa Vargas
Kenneth Gamboa Vargas	kenneth.gamboa.vargas@mep.go.cr	2221-9107 ext:4658	Valerie Castro

ICE	No aplica	800-SOPORTE (7676783) Línea: 1730-3360	No aplica
RACSA	No aplica	22870333 22870404 Línea: C2041-013	No aplica

Fuente: Elaboración propia.

Capítulo 3. Procedimientos de respuesta a desastres

3.1 Procedimientos de identificación y evaluación

3.1.1 Evaluación de severidad. Es necesario recolectar toda la información posible y se deben evaluar los siguientes puntos para determinar la severidad del evento:

- Información o notificación inicial del evento.
- Existencia de daños a la infraestructura.
- Cantidad de usuarios afectados.
- Determinar la gravedad de la interrupción a las operaciones.
- Existencia de pérdida financiera.
- Existencia de incumplimiento contractual o legal.
- Urgencia.

Una vez recolectada la información debe evaluarse el impacto del evento.

3.1.2 Evaluación de impacto. El impacto a la organización ayudará a determinar si el plan de recuperación debe activarse o no. Estos son algunos criterios de evaluación del impacto:

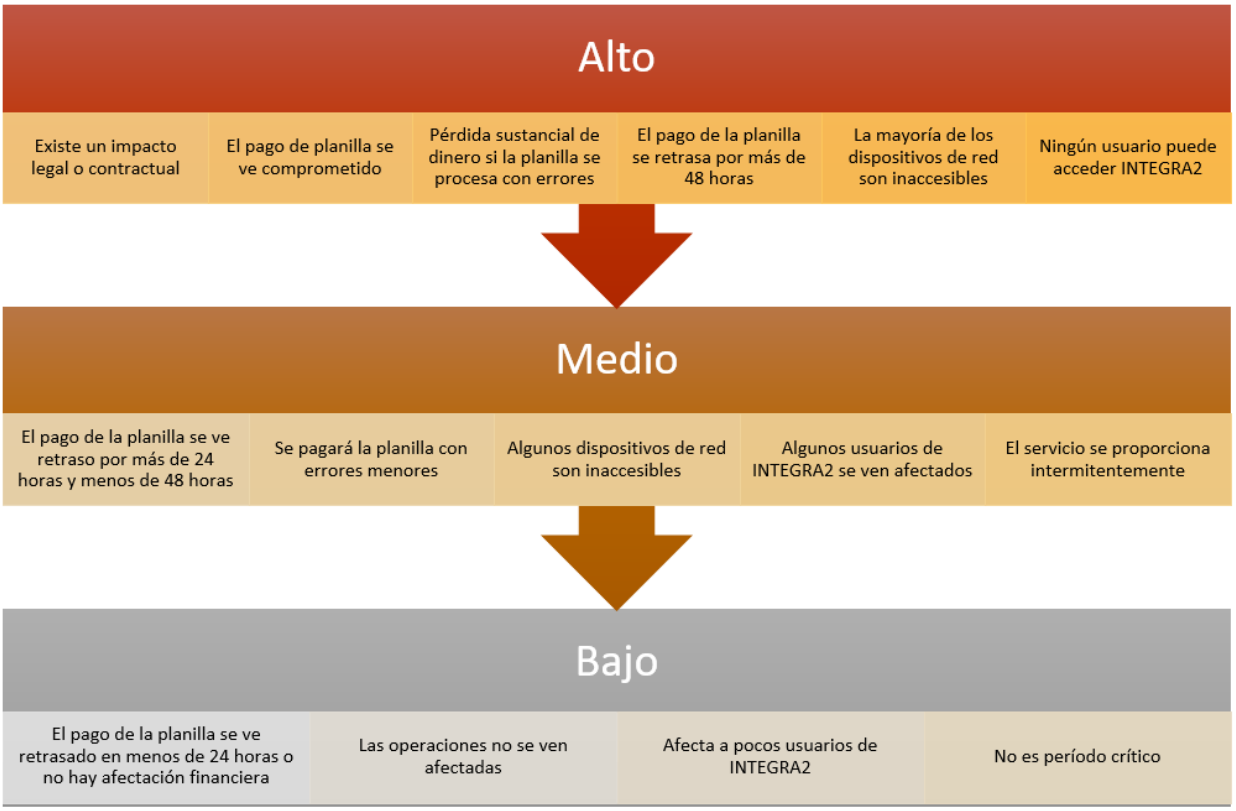


Figura 9. Impacto (Elaboración propia)

Se recomienda utilizar el anexo dos como instrumento para realizar la evaluación.

3.1.3 Declaración de desastre. Una vez se ha materializado el evento/incidente, el encargado de continuidad de servicios debe hacer una evaluación final y determinar si el plan de recuperación debe activarse.

Se recomienda que para incidentes o eventos con bajo impacto, no se active el plan y solo se monitoree la situación. En el caso de eventos de impacto medio o alto, el encargado debe evaluar toda la información pertinente y tomar la decisión de declarar un desastre y comunicar a todas las partes interesadas.

3.2 Procedimientos de recuperación

3.2.1 Notificación de los equipos. Una vez se tome la decisión de activar el plan de recuperación el encargado de continuidad debe notificar a los equipos de recuperación y responsables de actividades de recuperación para iniciar con el plan, como principal canal de comunicación se utilizará el teléfono y/o correo.

Es también necesario que se notifique al director de la Dirección de Informática de Gestión (DIG) y al director de Recursos Humanos. La descripción del evento, el posible impacto, un estado y tiempo estimado de recuperación son imprescindibles.

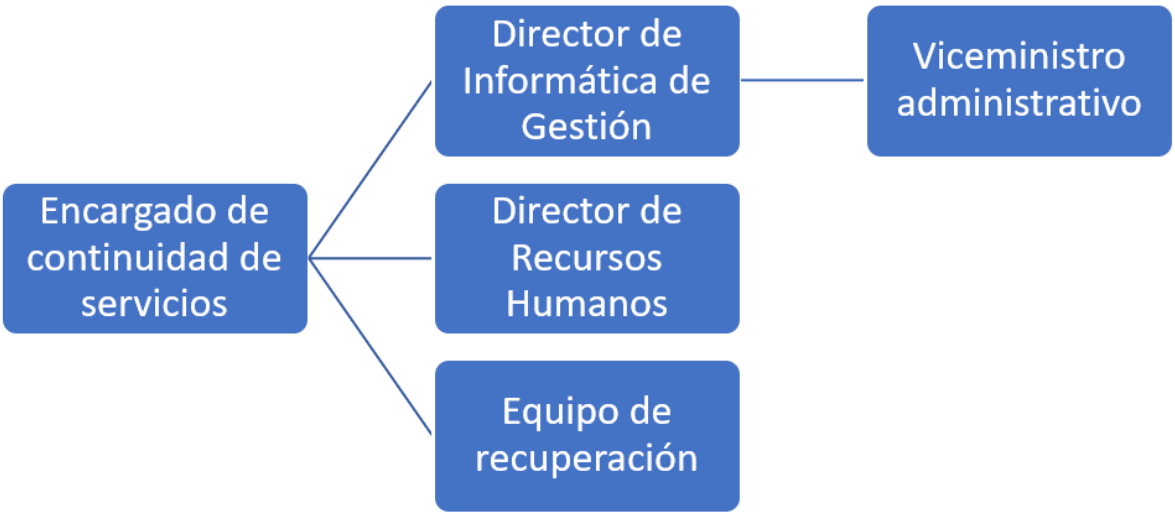


Figura 10. Árbol de contactos (Elaboración propia)

3.2.2 Inicialización de la recuperación. Los equipos de recuperación se encargan de realizar un diagnóstico para determinar posibles causas del evento, así como su alcance. Se recomienda utilizar herramientas de diagnósticos, historiales, revisiones de cambios o incluso inspecciones físicas que ayuden a determinar la condición/estado de los equipos.

Los procedimientos de diagnóstico pueden variar según el incidente y se recomienda evaluar la cantidad de tiempo a invertir en determinar la causa, es importante que el equipo se concentre en la recuperación del enlace MEP-Hacienda.

A la hora de iniciar los procesos de recuperación se deben determinar las prioridades de recuperación en este caso sería el enlace Rofas como medio alternativo de comunicación entre el MEP y Hacienda, esto incluye recuperación del Switch core y del Router del edificio principal.

3.2.3 Comunicación del progreso. Se recomienda comunicar el progreso de los procedimientos de recuperación en intervalos de tiempo que sean definidos según el impacto del incidente, es decir mientras más grave sea el incidente recomienda una comunicación más constante siempre dando tiempo al equipo de recuperación para realizar tareas. Para incidentes graves se recomienda comunicaciones cada dos horas y para incidentes con impacto medio se recomienda cada tres horas, es importante que el encargado de continuidad de servicios determine el intervalo adecuado.

Los mensajes a comunicar por parte del encargado de continuidad de servicios deben ser claros y concisos, es importante que describan el evento, expliquen el progreso y los pasos a seguir; se utilizará el correo electrónico como principal canal de comunicación.

3.2.4 Soporte al equipo de recuperación. Es posible que los equipos de recuperación trabajen largas horas para poder reestablecer el enlace MEP-Hacienda, por ello es importante tomar en cuenta los siguientes puntos:

- ¿El personal del equipo recibió comida y agua para mantenerse efectivos?
- ¿Existe alguna necesidad personal de los empleados que requiera atención?
- ¿El equipo cuenta con los recursos adecuado?
- ¿Existe la necesidad de viajar a otras instalaciones?

3.3 Procedimiento de reanudación

Una vez se ha logrado contener y mitigar el impacto del evento se inicia el camino hasta el retorno a la normalidad de las operaciones, es decir las condiciones en las que estaba el enlace antes del evento/incidente. Para ello se utilizan tres pasos:



Figura 11. Procedimiento de reanudación (Elaboración propia)

Primero se evalúa el enlace de manera lógica, física, así como la necesidad existente de cualquier recurso que permitan retomar las operaciones con normalidad.

Después el equipo de redes debe realizar una serie de pruebas que para validar el funcionamiento correcto y normal del enlace entre el MEP y Hacienda. Pueden utilizarse herramientas como ping, tracert, analizadores de protocolo y paquetes, analizadores de velocidad de conexión, monitores, entre otros.

Finalmente se debe realizar una última comunicación una vez que se haya recuperado exitosamente la conexión entre el MEP y el Ministerio de Hacienda, explicando el retorno a la normalidad.

La comunicación debe ser creada por el encargado de continuidad de negocio y debe enviarse a:

- Director de Dirección de Informática de Gestión (DIG).
- Director de Recursos Humanos.
- Usuarios afectados.

3.4 Procedimiento de revisión

El procedimiento de revisión es muy importante para poder cumplir con el ciclo de Deming: planear, hacer, verificar y actuar, que es parte fundamental de la norma ISO 27001.

Durante esta etapa el encargado de continuidad hará una revisión de las lecciones aprendidas y resultados del plan y de todos los procedimientos seguidos. Por lo que es necesario recolectar esta información con el equipo de recuperación, jefes de área y cualquier otro personal involucrado; se recomienda enfocarse en tres puntos:

- Aspectos positivos.
- Aspectos negativos.
- Oportunidades de mejora al proceso.

Los resultados obtenidos de este proceso se derivarán en una serie de acciones entre las cuales pueden estar:

- Actualizar el plan y los procedimientos.

- Capacitación del personal.
- Actualizar las pruebas.
- Nuevos tipos de monitoreo.
- Mejoras en el enlace.

El encargado de continuidad de servicios velará por la ejecución de las mejoras y las acciones derivadas de la revisión, por ello es importante que se determinen fechas límite y responsables.

Capítulo 4. Planes de recuperación de Redes

4.1 Responsables

- Ronny Rojas Vargas
- Valerie Castro Espinoza

4.2 Respaldos

Estrategia de respaldo: Se realiza un respaldo de la configuración de los dispositivos cada vez que hay un cambio en la configuración, esto se efectúa mediante el software OPManager de la empresa Manage Engine.

4.3 Estrategia de recuperación

La estrategia de recuperación se basa en dos enlaces alternos. El primero se encuentra en el edificio de la antigua embajada, este enlace comparte cierta infraestructura de red con el enlace principal, este enlace alimenta las oficinas

centrales y las regionales. El segundo enlace alterno se encuentra ubicado en el edificio Rofas el cual se puede configurar para poder alimentar las oficinas centrales y regionales si el enlace de la Antigua Embajada queda inoperativo debido a fallos en el equipo de Router.

4.4 Supuestos

- El edificio Rofas y el edificio de la Antigua Embajada cuentan con electricidad.
- Las líneas de comunicación de red se encuentran funcionales.
- Se tiene acceso físico al Centro de Datos.

4.5 Diagrama de red

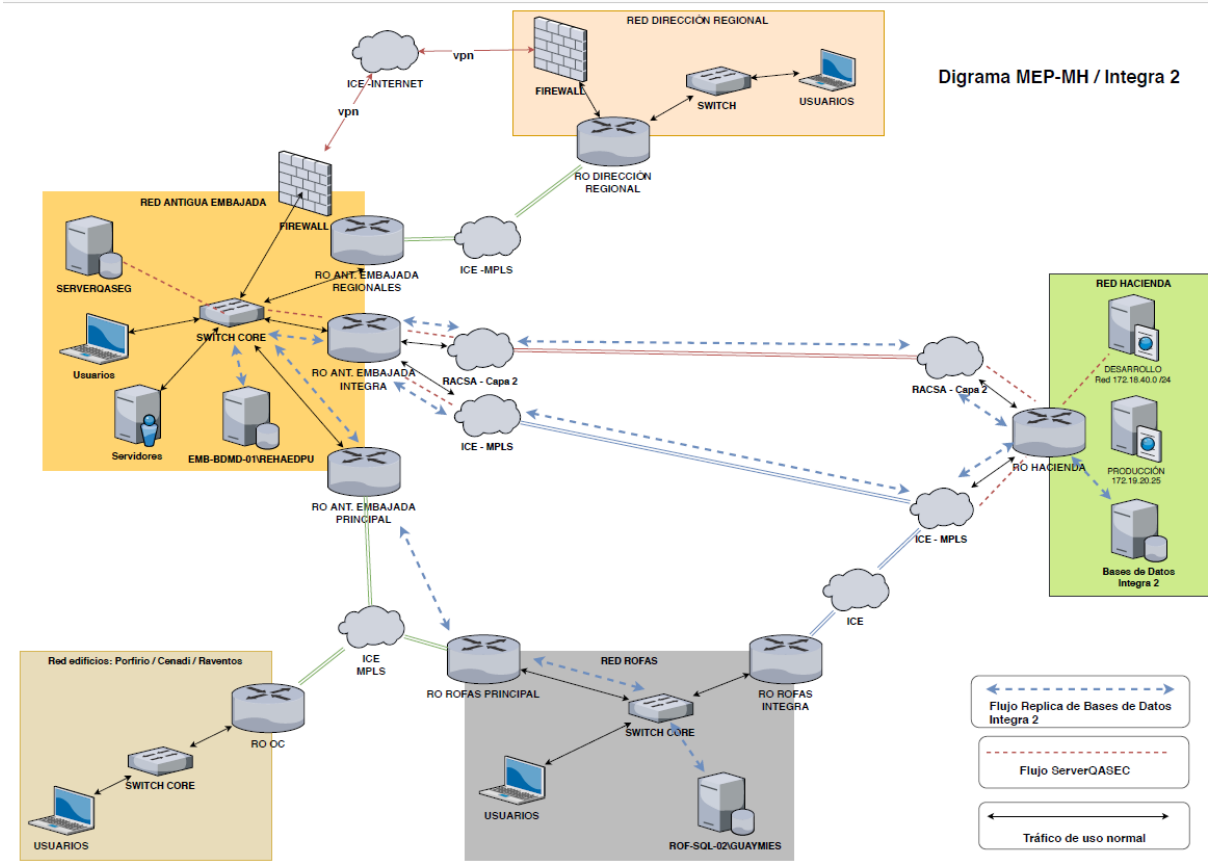


Figura 12. Diagrama de red (Ministerio de Educación Pública de Costa Rica)

4.6 Procedimiento de recuperación

Resumen de los pasos a seguir:

1. Transferir el enlace MEP-Hacienda al edificio Rofas.
2. Verificar con los proveedores de servicio ICE y RACSA el estado de las conexiones en el edificio antigua embajada.
3. Contactar con GBM para la recuperación física enrutador del Centro de Datos.
4. Contactar con el equipo que administra OPmanager para extraer del OPmanager la configuración del enrutador
5. Restaurar el servicio para la Antigua Embajada.

Detalle del procedimiento

1. Transferir el enlace MEP-Hacienda al edificio Rofas.
    a. Inicias sesión en SW-Core-01 del centro de datos de la antigua embajada.
        i. Usar el usuario y contraseña se encuentran guardados por el jefe del Departamento de Redes y Telecomunicaciones, Berny Salazar Rojas.
    b. Identificar las rutas estáticas que van a integra2.
        i. Ejecutar el comando “display current-configuration | include 10.10.1.104” de esta manera mostrará toda la configuración que incluye la IP 10.10.1.104.

ii. Se debe excluir cualquier configuración que no contemple 10.10.1.104.

iii. Copiar el resultado en archivo y guardarlo en un lugar apropiado con el nombre “Switch-Core” (Este archivo será necesario más adelante).

c. Realizar la configuración de enrutamiento de integra2 hacia la nueva ruta en el switch core.

i. Ejecutar el siguiente comando undo para eliminar cada ruta estática, a modo de ejemplo: “undo ip route-static 172.18.51.38 32 10.10.1.104” Este comando se debe ejecutar una vez por cada ruta estática obtenida en el punto b.

ii. Agregar las rutas estáticas con la nueva dirección IP (10.10.1.105) y a modo de ejemplo: “ip route-static 172.18.51.38 32 10.10.1.105”. Este comando se debe ejecutar una vez por cada ruta estática obtenida en el punto b.

d. Iniciar sesión en Router_Embajada_A del edificio Antigua embajada para extraer la configuración de enrutamiento de Integra2 hacia la nueva ruta.

i. Usar el usuario y contraseña se encuentran guardados por el jefe del Departamento de Redes y Telecomunicaciones, Berny Salazar Rojas.

e. Identificar las rutas estáticas del Router de antigua embajada.

i. Ejecutar el comando “show running-config | include 10.10.1.104” de esta manera mostrará toda la configuración que incluye la IP 10.10.1.104.

ii. Copiar el resultado en archivo y guardarlo con el nombre “Router” en un lugar apropiado (Este archivo será necesario más adelante).

f. Realizar la configuración de enrutamiento de integra2 hacia la nueva ruta en el enrutador Router_Embajada_A.

i. Ejecutar el siguiente comando “no” para eliminar cada ruta estática, a modo de ejemplo: “No ip route 172.16.51.38 255.255.255.255 10.10.1.104”.

ii. Agrega las rutas estáticas con la nueva dirección IP, a modo de ejemplo: “ip route 172.18.51.38 255.255.255.255 tunnel10”.

2. Contactar con los proveedores RACSA e ICE para determinar el estado del servicio en el edificio de la Antigua Embajada.
3. Contactar con GBM para la recuperación física del enrutador del Centro de Datos, modelo cisco 3900 con el nombre MEP-MH-01.
4. Contactar con el equipo que administra OPmanager para extraer del OPmanager la configuración del enrutador MEP-MH-01.
    a. Contactar con los administradores de OPmanager Valerie Castro Espinoza y Kenneth Gamboa Vargas.
    b. Solicitar un archivo de texto con la configuración más reciente del enrutador.

c. Proveer el archivo a GBM para la recuperación.

5. Restaurar el servicio para la Antigua Embajada.
    a. Iniciar sesión en el SW-Core-01 del Centro de Datos de la Antigua Embajada.
        i. Usar el usuario y contraseña se encuentran guardados por el jefe del Departamento de Redes y Telecomunicaciones, Berny Salazar Rojas.
    b. Realizar la configuración de enrutamiento de integra2 hacia la nueva ruta en el switch core.
        i. Utilizar el archivo con el nombre “Switch-Core” que contiene las rutas estáticas.
        ii. Ejecutar el siguiente comando undo para eliminar cada ruta estática, a modo de ejemplo: “undo ip route-static 172.18.51.38 32 10.10.1.105”. Este comando se debe ejecutar una vez por cada ruta estática dentro del archivo “Switch-Core”.
        iii. Agregar las rutas estáticas con la nueva dirección IP (10.10.1.104) y a modo de ejemplo: “ip route-static 172.18.51.38 32 10.10.1.104”. Este comando se debe ejecutar una vez por cada ruta estática obtenida dentro del archivo “Switch-Core”.
    c. Iniciar sesión en el enrutador Router_Embajada_A para realizar la configuración de enrutamiento de Integra2 hacia la nueva ruta.

i. Usar el usuario y contraseña se encuentran guardados por el jefe del Departamento de Redes y Telecomunicaciones, Berny Salazar Rojas.

d. Realizar la configuración de enrutamiento de integra2 hacia la nueva ruta en el enrutador Router_Embajada_A.
   i. Usar el archivo con el nombre router.
   ii. Ejecutar el siguiente comando “no” para eliminar cada ruta estática, a modo de ejemplo: “No ip route 172.18.51.38 255.255.255.255 tunnel10”.
   iii. Agrega las rutas estáticas con la nueva dirección IP, a modo de ejemplo: “ip route-static 172.16.51.38 255.255.255.255 10.10.1.104”.

Capítulo 5. Anexos

5.1 Procedimiento de divulgación

En caso de que suceda un evento/incidente, es importante que todos los involucrados y sus respaldos conozcan el plan que se desarrolló y los procedimientos a seguir.

El encargado de continuidad de negocio tendrá la tarea de comunicar el plan y asegurarse de que todos los involucrados lo entiendan. Para esto se pueden tomar en cuenta los siguientes puntos:

- Los involucrados y sus jefes deben tener acceso al plan ya sea físicamente o mediante software.
- El equipo de recuperación de redes debe comprender los pasos de recuperación.
- En caso de no tener los conocimientos para ejecutar el plan de recuperación debe realizarse una capacitación entre los miembros del equipo.

Tabla 4

Procedimiento de divulgación

Persona	Acceso al plan	Conoce el plan	Requiere capacitación	Fecha	Firma

Fuente: Elaboración propia.

5.2 Evaluación del incidente

Esta es una de las preguntas que el encargado de continuidad de negocio debe realizar para poder evaluar el impacto y severidad del incidente.

La primera columna corresponde a la pregunta que se debe realizar, la segunda el criterio que se evalúa para esa pregunta y por último la respuesta final en donde se elige el número según el criterio, siendo 1 el de menor impacto y 3 el de mayor impacto. Al finalizar se suman todas las respuestas y se obtiene un total, el cual ayuda a identificar si se tiene o no que activar el plan de continuidad.

El resultado total se debe utilizar para evaluar el impacto según lo siguiente:

Alto (21-27)	Medio (16-20)	Bajo (9-15)

Se aconseja que se active el plan de recuperación si la afectación es alta. Si la afectación es media se recomienda tomar una decisión tomando en cuenta si es un periodo crítico para el negocio, si habrá pérdidas financieras o repercusiones legales. Si es baja se recomienda no activar el plan y seguir el procedimiento normal de atención a incidentes.

Tabla 5

Evaluación del incidente

Pregunta	**Criterio**	**Respuesta**		
		1	2	3
¿Hay daños a la infraestructura?	No aplica			

Cantidad de usuarios afectados	**Bajo**:<15 o 15 **Medio**:>15 y <50 **Alto**: 50 o >50			
Posibilidad de incumplimiento contractual	No aplica			
Posibilidad de incumplimiento legal	No aplica			
¿Es periodo de pago?	No aplica			
Pérdida financiera si se procesa la planilla con errores	**Bajo**: No hay pérdida **Medio**: Pérdida menor **Alto**: Pérdida sustancial de dinero			
Retraso en el pago de planilla	**Bajo**:<24 horas **Medio**:>25 horas y <48 **Alto**: >48 horas			
Funcionamiento del enlace	**Bajo**: Intermitente con cortos periodos de desconexión **Medio**: Intermitente con largos periodos de desconexión **Alto**: No hay conexión			
Afectación a las operaciones diarias	**Bajo**: Algunas operaciones básicas se ven afectadas **Medio**: Varias operaciones afectadas **Alto**: Las operaciones diarias se ven afectadas			
Total				

Fuente: Elaboración propia.

Fecha	**Encargado de continuidad**	**Firma**

5.3 Lista de chequeo procedimiento de recuperación y reanudación

Se recomienda seguir esta lista de chequeo en el momento que se activa el plan de recuperación. Marcar con una “X” la casilla respectiva en caso de estar completo.

Tabla 6

Lista de chequeo

Actividad	Completo
Sección 1: Identificación y evaluación del incidente.	
Realizar la evaluación de impacto y severidad (Utilizar anexo 2).	
Realizar la declaración formal.	
Sección 2: Notificación de los equipos.	
Informar a los involucrados para activar el plan.	
Notificación inicial del evento a las partes interesadas. Incluye descripción inicial del evento.	
Sección 3: Inicialización de la recuperación.	
Determinar la cantidad de tiempo a dedicar para el diagnóstico inicial.	

Realizar un diagnóstico inicial que ayude a determinar la condición o estado de los equipos.	
Repasar las prioridades de recuperación con el equipo de recuperación.	
Sección 4: Comunicación del proceso.	
Definir intervalos de comunicación.	
Comunicar el progreso periódicamente incluir una descripción, proceso y pasos a seguir.	
Notificar al director de la Dirección Informática de Gestión (DIG)	
Notificar al Director de Recursos Humanos.	
Notificar a usuarios afectados.	
Sección 5: Soporte al equipo de recuperación.	
Verificar que el equipo reciba comida y agua para mantenerse efectivo.	
Verificar si existe alguna necesidad personal que requiera atención.	
Revisar si el equipo cuenta con los recursos adecuados.	
Revisar si existe la necesidad de viajar a otras instalaciones.	
Sección 6: Plan de recuperación de redes.	
Comprobar que las personas adecuadas del equipo de red están presentes.	

Verificar que poseen los contactos adecuados.	
Comprobar que el equipo cuenta con los accesos requeridos para realizar la tarea.	
Verificar el respaldo adecuado de la configuración de los dispositivos.	
Revisar que el equipo de redes cuenta con los recursos tecnológicos requeridos.	
Verificar que se está utiliza y sigue el procedimiento de recuperación paso a paso.	
Verificar la mitigación del incidente, es decir comprobar que exista un servicio mínimo aceptable.	
Notificar el progreso una vez se ha conseguido el servicio mínimo aceptable.	
Sección 7: Procedimiento de reanudación.	
Completar los procedimientos de reanudación.	
Evaluar el correcto funcionamiento del enlace.	
Notificar al director de la Dirección de Informática de Gestión del retorno a la normalidad.	
Notificar al Director de Recursos Humanos del retorno a la normalidad.	
Notificar a usuarios afectados del retorno a la normalidad.	

Fuente: Elaboración propia.

9.3. Cronograma para la implementación del SGSI

Tabla 7

Cronograma

Nombre	Duración	Estado
Fase 1: Anális	**3 meses**	
Levantamiento de información	3 meses	Completado
Fase 2: Creación de documentos base	**6 meses**	
Política de seguridad de la información	3 meses	Completado
Plan de continuidad de servicios informáticos	3 meses	En progreso
Fase 3: Implementación del Ciclo de Deming	**4 años**	
Gestión de activos	**9 meses**	
Crear inventario de activos	6 meses	Pendiente
Clasificación de la información	2 meses	Pendiente
Revisión	1 mes	Pendiente
Gestión de riesgos	**13 meses**	
Identificación de riesgos	3 meses	Pendiente
Crear el registro de riesgos	1 mes	Pendiente
Evaluación de riesgos	3 meses	Pendiente
Medidas correctoras y plan de contingencias	4 meses	Pendiente
Seguimiento y control de riesgos	2 meses	Pendiente
Control de accesos	**8 meses**	
Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio.	5 meses	Pendiente
Establecer procedimientos para la identificación y autenticación del acceso a la información	3 meses	Pendiente
Gestión de Incidentes de seguridad	**5 meses**	
Establecer un procedimiento formal para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes	2 meses	Pendiente
Establecer un procedimiento formal de comunicación y de respuesta a incidentes	3 meses	Pendiente
Continuidad de servicios criticos	**15 meses**	
Identificar los procesos críticos del negocio	2 meses	Completado
Identificar los activos involucrados en cada procesos críticos del negocio.	2 meses	En progreso
Comprender el impacto que tienen las interrupciones	3 meses	En progreso
Implementar procedimientos para permitir la recuperación y restauración	5 meses	En progreso
Probar y actualizar los planes.	3 meses	Pendiente

Fuente: Elaboración propia.

Nota aclaratoria: La fase 3 menciona que se duran 4 años, pero es importante mencionar que varias de estas actividades se pueden realizar en paralelo, lo que aceleraría el proceso.

9.4. Aprobación del MEP de los entregables

Politicas de seguridad

Marlon Vasquez Vasquez <marlon.vasquez.vasquez@mep.go.cr> 17 de abril de 2020, 17:05
Para: MARIA DE LOS ANGELES CAMPOS PEREZ <mcamposp@ucenfotec.ac.cr>
Cc: Ivan Rojas Alvarez <ivan.rojas.alvarez@mep.go.cr>, Jose Sandi Zuniga <jose.sandi.zuniga@mep.go.cr>

Buenas tardes María de los Angeles

Por este medio hago de su conocimiento, que el documento adjunto no fue revisado por todos los departamentos que conforman la Dirección de Informática de Gestión, dado las circunstancias de emergencia nacional que actualmente estamos viviendo.-

Sin embargo, mi persona y los departamentos que logramos revisar el documento, realizamos recomendaciones de redacción de forma y fondo.

El documento como tal le servirá a la institución, como un punto de partida para formular los lineamientos de seguridad de la información, los cuales van a reforzar y ayudar a alcanzar los objetivos estratégicos del MEP.-

No omito indicarle que dicho documento será sometido a futuro a un análisis más exhaustivo, por parte de la Dirección de Informática de Gestión, con el fin de dilucidar los ajustes y modificaciones que correspondan, tomando en consideración la documentación de procesos, procedimientos, lineamientos, directrices, otros, que tiene actualmente la institución-

Expuesto lo anterior y esperando la compresión del caso, hago de su conocimiento que se brinda el visto bueno del documento denominado "Propuesta de políticas de seguridad de la información" , como parte de las labores de investigación que ustedes realizaron en el MEP, en su trabajo de Maestría.-

Muchos éxitos en sus estudios y carrera profesional.-

Saludos cordiales,

Marlon Vásquez Vásquez
Dirección de Informática de Gestión
Ministerio de Educación Pública

9.5. Selección de estudios Iniciales

Tabla 8

Artículos relevantes de SpringerLink

Artículo
Título: Contingency Planning. Autor: Kenneth B. Ackerman. Cita: Ackerman K.B. (1997) Contingency Planning. In: Practical Handbook of Warehousing. Springer, Boston, MA. Link: https://link-springer-com.una.idm.oclc.org/chapter/10.1007/978-1-4615-6013-5_17
Título: Sistema de Gestión de Información para la Investigación y Postgrado. Autor: Z. NodaI. MoreraM. OjedaM. LópezS. Fernández. Cita: Noda Z., Morera I., Ojeda M., López M., Fernández S. (2013) Sistema de Gestión de Información para la Investigación y Postgrado. In: Folgueras Méndez J. et al. (eds) V Latin American Congress on Biomedical Engineering CLAIB 2011 May 16-21, 2011, Habana, Cuba. IFMBE Proceedings, vol 33. Springer, Berlín, Heidelberg Link: https://link-springer-com.una.idm.oclc.org/chapter/10.1007/978-3-642-21198-0_99
Título: A pattern-based method for establishing a cloud-specific information security management system. Autor: Kristian Beckers, Isabelle CôtéStephan FaßbenderMaritta HeiselStefan Hofbauer. Cita: Beckers, K., Côté, I., Faßbender, S. et al. Requirements Eng (2013).

Link: https://link-springer-com.una.idm.oclc.org/article/10.1007/s00766-013-0174-7
Título: Information security management system standards. Autor: Edward Humphreys. Cita: Humphreys, E. DuD (2011) 35: 7. https://doi-org.una.idm.oclc.org/10.1007/s11623-011-0004-3. Link: https://link-springer-com.una.idm.oclc.org/article/10.1007/s11623-011-0004-3
Título: Standardization in information security management. Autor: A. M. Fal. Cita: Fal', A.M. Cybern Syst Anal (2010) 46: 512. https://doi-org.una.idm.oclc.org/10.1007/s10559-010-9227-9. Link: https://link-springer-com.una.idm.oclc.org/article/10.1007/s10559-010-9227-9
Título: Survey results on adults and cybersecurity education. Autor: Joseph Ricci, Frank Breitinger, Ibrahim Baggili. Cita: Ricci, J., Breitinger, F. & Baggili, I. Educ Inf Technol (2019) 24: 231. https://doi-org.una.idm.oclc.org/10.1007/s10639-018-9765-8 Link: https://link-springer-com.una.idm.oclc.org/article/10.1007/s10639-018-9765-8
Título: Leveraging information security and computational trust for cybersecurity. Autor: Robson de Oliveira Albuquerque, Luis Javier García Villalba, Ana Lucila Sandoval Orozco Rafael Timóteo de Sousa Júnior. Cita: de Oliveira Albuquerque, R., García Villalba, L.J., Sandoval Orozco, A.L. et al. J Supercomput (2016) 72: 3729. https://doi-org.una.idm.oclc.org/10.1007/s11227-015-1543-4 Link: https://link-springer-com.una.idm.oclc.org/article/10.1007/s11227-015-1543-4

Título: Assessment of IT Governance of COBIT Framework. Autor: Woong Chul ChoiDaeHun Yoo. Cita: Choi W., Yoo D. (2009) Assessment of IT Governance of COBIT Framework. In: Ślęzak D. et al. (eds) U- and E-Service, Science and Technology. UNESST 2009. Communications in Computer and Information Science, vol 62. Springer, Berlín, Heidelberg Link: https://link-springer-com.una.idm.oclc.org/chapter/10.1007/978-3-642-10580-7_13
Título: Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001. Autor: Diogo Proença, José Borbinha. Cita: Proença D., Borbinha J. (2018) Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001. In: Abramowicz W., Paschke A. (eds) Business Information Systems. BIS 2018. Lecture Notes in Business Information Processing, vol 320. Springer, Cham. Link: https://link-springer-com.una.idm.oclc.org/chapter/10.1007/978-3-319-93931-5_8
Título: Interactive Selection of ISO 27001 Controls under Multiple Objectives. Autor: Thomas Neubauer Andreas Ekelhart Stefan Fenz. Cita: Neubauer T., Ekelhart A., Fenz S. (2008) Interactive Selection of ISO 27001 Controls under Multiple Objectives. In: Jajodia S., Samarati P., Cimato S. (eds) Proceedings of The Ifip Tc 11 23rd International Information Security Conference.

SEC 2008. IFIP – The International Federation for Information Processing, vol 278. Springer, Boston, MA. Link: https://link-springer-com.una.idm.oclc.org/chapter/10.1007/978-0-387-09699-5_31

Fuente: Elaboración propia.

Tabla 9

Artículos relevantes de ACM Digital Library

Artículo
Título: Information security, risk governance and management frameworks: an overview of COBIT 5. Autor: Georges Ataya. Link: https://dl-acm-org.una.idm.oclc.org/citation.cfm?id=2523590
Título: "Shadow security" as a tool for the learning organization. Autor: Iacovos Kirlappos, Simon Parkin, M. Angela Sasse. Link: https://dl-acm-org.una.idm.oclc.org/citation.cfm?id=2738216
Título: A New Perspective to Information Security: Total Quality Information Security. Management. Autor: Mehrdad Sepehri Sharbaf. Link: https://dl-acm-org.una.idm.oclc.org/citation.cfm?id=2659666
Título: Lightweight modeling and analysis of security concepts. Autor: Jörn Eichler. Link: https://dl-acm-org.una.idm.oclc.org/citation.cfm?id=1946355
Título: Information security culture: a behaviour compliance conceptual framework.

Autor: Salahuddin Alfawaz, Karen Nelson, Kavoos Mohannak. Link: https://dl-acm-org.una.idm.oclc.org/citation.cfm?id=1862275
Título: Information security management: protecting the business with policies. Autor: Gregory H. Harris. Link: https://dl-acm-org.una.idm.oclc.org/citation.cfm?id=1941006

Fuente: Elaboración propia.

Tabla 10

Artículos relevantes de Web of Science

Artículo
No encontrados.

Fuente: Elaboración propia.

Tabla 11

IEEE Xplore Digital Library

Artículo
Título: NIST CyberSecurity Framework Compliance: A Generic Model for Dynamic Assessment and Predictive Requirements. Autor: Nuno Teodoro; Luís Gonçalves; Carlos Serrão Link: https://ieeexplore-ieee-org.una.idm.oclc.org/document/7345310
Título: Cybersecurity Standards: Managing Risk and Creating Resilience Autor: Zachary A. Collier; Daniel DiMase; Steve Walters; Mark Mohammad Tehranipoor; James H. Lambert. Link: https://ieeexplore-ieee-org.una.idm.oclc.org/document/6701301
Título: Quantified Model of COBIT for Corporate IT Governance Autor: S.J. Hussain; M.S. Siddiqui.

Link: https://ieeexplore-ieee-org.una.idm.oclc.org/document/1598575
Título: Engineering secure systems with ISO 26702 and 2700. Autor: Rhys Evans; Aggeliki Tsohou; Theo Tryfonas; Thea Morgan. Link: https://ieeexplore-ieee-org.una.idm.oclc.org/document/5544065
Título: ISO/IEC 27001 implementation in public organizations: A case study. Autor: Bayona Sussy; Chauca Wilber; Lopez Milagros; Maldonado Carlos. Link: https://ieeexplore-ieee-org.una.idm.oclc.org/document/7170355
Título: Swiss army knife of software processes generic framework of ISO 27001 and its mapping on resource management. Autor: Lala Rukh, Ali Afzal Malik. Link: https://ieeexplore-ieee-org.una.idm.oclc.org/document/8065742

Fuente: Elaboración propia.