UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACUTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE INF/TI

EXAMEN DE CARÁCTER COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

"MANUAL DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION BASADO EN LOS ESTANDARES ITIL V3 PARA LA UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA"

AUTOR

HENRY SLEINER MARIN HERNANDEZ

LA LIBERTAD – ECUADOR
2020

APROBACIÒN DEL TUTOR

En mi calidad de tutor del trabajo de componente práctico del examen de carácter complexivo: “MANUAL DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION BASADO EN LOS ESTANDARES ITIL V3 PARA LA UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA”, elaborado por el Sr. Marin Hernández Henry Sleiner, de la carrera de Tecnologías de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

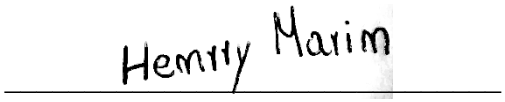
La libertad, 1 de Septiembre del 2020.

_____

Ing. Jimmy Rivera Ramírez, Mgt.

DECLARACIÓN

El contenido del presente componente práctico del examen de carácter complexivo es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



Henry Marin Hernández

AGRADECIMIENTO

En primer lugar, quiero agradecer a mis difuntos padres: Flor Hernández y Otto Marin por darme su apoyo en todo momento hasta el último día de sus vidas, sin ellos no podría haber alcanzado este logro tan importante en la vida. Estoy seguro de que estarían tan orgullosos como lo estoy yo. Donde quiera que estén, gracias, madre y padre.

A mis hermanas Tatiana Marin y Amanda Marin que me apoyaron a terminar mis estudios en uno de los momentos más difíciles de la vida.

A todos los docentes de la Carrera de Tecnologías de la Información que me brindaron su apoyo y conocimiento que ayudaron a formarme como profesional.

Henry Marin

DEDICATORIA

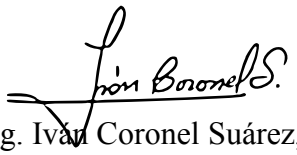
Dedico este logro a quienes me inspiraron, a quienes me ayudaron a llegar donde he llegado, a mis padres, a mis héroes.

Henry Marin

TRIBUNAL DE GRADO

Ing. Samuel Bustos Gaibor, Mgt.

DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

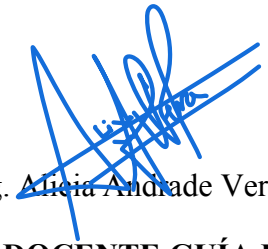


Ing. Iván Coronel Suárez, Mgt.

DOCENTE ESPECIALISTA

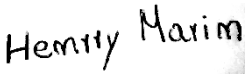
Ing. Jimmy Rivera Ramírez, Mgt.

DOCENTE TUTOR



Ing. Alicia Andrade Vera, Mgt.

DOCENTE GUÍA UIC



Henry Marin Hernández

Estudiante

RESUMEN

La Universidad Estatal Península de Santa Elena, se encuentra constantemente en la búsqueda de optimizar sus procesos académicos, administrativos y demás, esto con el fin de mantener la acreditación de la misma cumpliendo los requerimientos establecidos por los entes encargado de evaluar las Universidades, estos entes demandan a las universidades una apuesta por la innovación para la gestión de procesos, y en este caso nos vamos a enfocar en lo que es el departamento de tecnologías de la información y en los procesos que este sigue al momento en el que se presenten incidentes relacionados con la seguridad de la información

Estos incidentes deben ser gestionados en base a procesos que se hayan sido analizados y desarrollados en base a estándares y normas de buenas prácticas, que en la practica el departamento de TI posee normas de buenas practicas relacionadas a la gestión de servicios.

Por ende, con la implementación de este proyecto, se buscará adaptar las normas existentes en el departamento de TI a la gestión de incidentes de seguridad de la información basándonos en las normas de buenas practicas ITIL V3 para así de esta forma optimizar el tiempo de respuesta del departamento de TI ante un incidente que se pueda presentar en las instalaciones de la Universidad.

ABSTRACT

The “Universidad Estatal Peninsula de Santa Elena”, is constantly in the search to optimize its academic, administrative and other processes, this in order to maintain its accreditation, complying with the requirements established by the entities in charge of evaluating the Universities, these entities demand from universities a commitment to innovation for process management, and in this case we are going to focus on what the information technology department is and on the processes that it follows at the time when related incidents occur with information security

These incidents must be managed based on processes that have been analyzed and developed based on standards and good practices norms, which in practice the IT department has good practice norms related to service management.

Therefore, with the implementation of this project, it will be sought to adapt the existing standards in the IT department to the management of information security incidents based on the ITIL V3 good practice standards in order to optimize the response time of the IT department in the event of an incident that may occur at the University facilities.

Índice

Índice de ilustraciones

Índice de tablas

Capítulo 1

1. FUNDAMENTACIÓN

1.1 ANTECEDENTES

Desde que nació la industria informática, lo aparatos tecnológicos nacidos de esta han generado cambios trascendentales en el mundo, más que nada debido a su incesante desarrollo y a su impacto a todo modelo de negocio, educativo o industrial generando en estos una marcada dependencia que incorpora grandes cantidades de información digitalizada y los sistemas de información que la proveen [1].

Por ende, la seguridad a la información es de suma importancia, ya que es considerada como el activo más significativo de la entidad en este caso educativa, siendo necesario el inmediato accionar ante cualquier situación que pueda causar la perdida de la información. Debido a la importancia de esta es que organizaciones internacionales de estandarización han creado normas que permiten la gestión para poder realizar el resguardo y buen uso de la información [2].

La Universidad Estatal Península de Santa Elena ubicada en el cantón La Libertad de la Provincia de Santa Elena cuenta con un departamento encargado de proveer servicios a la comunidad en ámbitos tecnológicos, asesoría técnica y desarrollo de soluciones informáticas, para fortalecer la matriz productiva local y contribuir con el conocimiento como valor insustituible y principal de la comunidad.

El departamento de Tics es el encargado de velar por los servicios que ofrece a la comunidad universitaria, así como por la seguridad de la información de la misma, actualmente la universidad cuenta con tres servidores dedicados cada uno respectivamente a: base de datos, aplicaciones informáticos y páginas web

Al no existir un manual de procedimientos que permita un inmediato accionar, al momento de que se presente un ataque de seguridad de la información dentro de la universidad, surge la necesidad del desarrollo de un manual de Gestión de incidentes de seguridad de la información para el departamento de Tics dentro de la Universidad Estatal Península de Santa Elena.

Para la propuesta antes mencionada se realizó un levantamiento de información mediante entrevistas (ver anexo1) al director del departamento de Tics el cual es el encargado de los incidentes de seguridad de la información dentro de la universidad. Con el levantamiento de información realizado al director de Tics se obtuvo como resultado la necesidad de crear un manual que ayude a la gestión de incidentes de seguridad de la información.

La tesis [3], Nos indica el camino a seguir en el análisis y la gestión de incidentes de seguridad de la información, pero utilizando estándares diferentes a los que usaremos en esta propuesta los cuales son ITIL V3, Estos estándares están enfocados a la gestión de incidentes, y en este caso se utilizara para los incidentes de seguridad.

Además [3], nos indica que, al implementar una gestión de incidente basada en estándares internacionales en una entidad financiera ubicada en Bogotá, genera una serie de beneficios tales como: la estructuración de un proceso, la eficiencia de los resultados, responsabilidades claramente definidas y la validación misma del proceso para identificar mejoras en el mismo.

Por otra parte, en Ecuador [4] nos dice que con el diseño de políticas de seguridad informática que más se ajusten a las necesidades actuales de la Universidad, se pretende reducir el impacto al mínimo posible ante un riesgo de seguridad.

En conclusión y en base a las consultas antes mencionadas los principales criterios considerados en la propuesta para su posterior comprobación es la reducción de los procedimientos de respuesta ante un incidente de seguridad de la información utilizando un proceso estructurado bajo estándares internacionales de buenas prácticas.

1.2 DESCRIPCIÓN DEL PROYECTO

En vista que el departamento de Tics no cuenta con un manual de gestión de incidentes de seguridad de la información, el siguiente proyecto propone el diseño de un manual de gestión que agilice las acciones de respuesta del departamento en caso de sufrir un ciberataque que ponga en riesgo la seguridad de la información digital que descansa en los servidores o equipos de cómputo disponibles dentro de la Universidad.

El análisis sobre la gestión de incidentes de seguridad de la información estará fundamentado bajo los estándares de las normas ITIL V3 el cual nos establece tres etapas principales para el desarrollo del mismo. Las etapas comprenden:

- Análisis de la situación actual: Esta etapa comprende el estudio del accionar del personal perteneciente al departamento de Tecnologías de la información respecto a los casos de ciberataque que hayan ocurrido en la Universidad Estatal Península De Santa Elena
- Establecer roles: Servirá como un punto de partida para determinar las acciones a tomar o en caso sea necesario establezca contactos para delegar las acciones que se pondrán en práctica cuando ocurra un incidente, en esta etapa se generará un diagrama de flujo del proceso a seguir.
- Rediseño del proceso: Se establecen los procesos que se seguirán o mejorarán y se establecerá el esquema de trabajo para los diferentes roles

ITIL V3.

ITIL (Information Technology Infrastructure Library) Biblioteca de Infraestructura de Tecnologías de la Información, es un conjunto de mejores prácticas para la gestión de los servicios de TI. Algunas organizaciones consideran a ITIL como una metodología que implica roles, grupos, procesos que intervienen en el ciclo de vida del servicio, los cuales comprenden [5]:

- Estrategia del servicio
- Diseño del servicio
- Transición del servicio
- Operación del servicio
- Mejora continua del servicio

Gestión de Incidencias.

ITIL define una incidencia como “Una interrupción no planificada o una reducción de calidad de un servicio de TI. El fallo de un elemento de configuración que no haya afectado todavía al servicio también se considera una incidencia” [6]

Proceso de Gestión de Incidentes.

Según los estándares ITIL V3 el proceso a seguir en la gestión de incidentes es [7]:

1. Identificación
2. Registro
3. Categorización
4. Priorización
5. Diagnóstico inicial
6. Escalado
7. Investigación y diagnóstico
8. Resolución y restauración
9. Cierre

La línea de investigación de la carrera de informática con la que se ajusta mi investigación es Tecnologías y Gestión de la Información ya que está relacionada con temas de infraestructura y seguridad de las tecnologías de la información, tecnologías verdes, virtualización y computación en la nube, seguridad de la información, el Internet en las cosas a través de las redes de comunicación, sensores eléctricos y sistemas informáticos, sistemas de información geográfica, gestión de seguridad de la información que permitan generar información indispensable para la toma de decisiones. Además, se relaciona con temas de gestión de desarrollo de software para tecnologías de comercio electrónico, gestión de base de datos, inteligencia de negocios (minería de datos) con la finalidad de dar soporte a las decisiones en tiempo real a las empresas [8].

1.3 OBJETIVOS DEL PROYECTO

1.3.1 OBJETIVO GENERAL

Desarrollar un manual de gestión de incidentes de seguridad de la información mediante el uso de los estándares ITIL V3 para el departamento de Tecnologías de la Información de la Universidad Estatal Península de Santa Elena.

1.3.2 OBJETIVOS ESPECÍFICOS

- Analizar los procesos operativos en el departamento de Tics para incidentes de seguridad.

- Reestructurar los procesos de seguridad de la información en caso de un incidente adaptándolos a las normas ITIL V3.
- Elaborar un manual de políticas y procesos para la gestión de incidencias de seguridad de la información en el departamento de Tecnologías de la información.

1.4 JUSTIFICACIÓN DEL PROYECTO

Como menciona [1], en nuestros tiempos la información se ha convertido en uno de los recursos más importantes tanto a nivel empresarial como a nivel personal, por ello se han implementado normas las cuales definan los requisitos básicos que debe comprometerse a cumplir cualquier organización para salva guardar la información crítica para su negocio.

Por ende según [9], actualmente en el país el aumento de delitos informáticos permiten tener una percepción de las amenazas a los que están propensos los servidores y con ellos la información que en estos se guarda se ve expuesta a daños irreparables que pueden causar un retraso en las actividades de la Universidad Estatal Península De Santa Elena.

Con el objetivo de ayudar a mejorar la gestión de incidentes de la seguridad de la información dentro del departamento de Tecnologías de la Información de la Universidad Estatal Península de Santa Elena es necesario el desarrollo de un manual de gestión de incidentes que nos permita reestructurar los procesos y adaptarlos a normas y estándares internacionales que garanticen un buen accionar en caso de un ataque informático.

Dentro de estos estándares de buenas prácticas está definido ITIL V3, que especifica los lineamientos y normas para una efectiva y eficaz gestión de incidentes de seguridad de la información en todas las organizaciones que adapten los estándares y normas antes mencionados agilizando así el tiempo de respuesta ante un incidente que se pueda presentar.

La implementación de los estándares ITIL V3 para gestionar los incidentes de seguridad de la información, será un gran beneficio para el departamento de Tecnologías de la Información de la Universidad Estatal Península de Santa Elena, al utilizar procesos reestructurados y adaptados a las norma de buenas prácticas ITIL V3, empezado por establecer roles como un punto de inicio para el inmediato accionar o dado el caso delegar un responsable ante un incidente de seguridad de la información, reduciendo

considerablemente los riesgos de que la información de la universidad pueda ser vulnerada y disminuyendo de gran manera la pérdida de tiempo al momento de responder ante un ataque de la seguridad de la información hacia los servidores o equipos de la universidad

De esta forma la Universidad Estatal Península de Santa Elena al gestionar los incidentes de seguridad bajos los estándares ITIL V3 ayudara a mantener los tres pilares de la seguridad de la información los cuales son [10]:

- **Confidencialidad:** Requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas.
- **Integridad:** Supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.
- **Disponibilidad:** Supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos.

1.5 ALCANCE DEL PROYECTO

En busca de una mejora de la gestión de incidentes de seguridad de la información en el departamento de tecnologías de la información y comunicación de la Universidad Estatal Península De Santa Elena, este proyecto estará enfocado en la gestión de los siguientes ataques de seguridad [11].

Clase de incidente	Tipo De Incidente
Ataques	Modificación de sitios web (Defacement)
Daños Físicos	Daños o cambios físicos no autorizados a los sistemas y/o equipos.
Acceso no autorizado, robo o pérdida de equipos	Robo o perdida de equipos/perdida de datos
Código Dañino (Malware)	Infección Extendida
	Infección Única

Tabla 1 Clasificación de los incidentes según su tipo

Descripción de incidentes de seguridad de la información

Modificación de sitio web (Defacement): Vulnerabilidades explotadas con éxito en los sistemas de alojamiento (servidor web) o en las aplicaciones que permiten a un atacante modificar contenidos y páginas web. Estos ataques pueden involucrar la inserción de enlaces a sitios maliciosos y/o añadir contenidos que contienen el mensaje de atacante (políticos, difamatorios, etc.). [11]

Daños o cambios físicos no autorizados a los sistemas: Este tipo de incidentes se produce cuando un individuo sin autorización (interno o externo) consigue ganar acceso físico a los equipos y realiza cambios o daños no autorizados [11].

Perdida de datos: Pérdida o copia de datos que comprometan a seguridad e integridad de los sistemas de la organización, y que pueden ser consecuencia de la pérdida o robo de equipos que contengan datos como listas de usuarios, contraseñas, certificados digitales, credenciales, diagramas de red, documentación técnica de sistemas, etc. [11]

Robo o pérdida de equipos: Robo o pérdida de equipamiento TIC, como pueden ser equipos portátiles, cintas de copias de seguridad, equipamiento de redes, etc [11].

Infección Extendida: Un virus, gusano, caballo de Troya, rootkit, script, etc. que infecta exitosamente a un conjunto amplio de sistemas y en donde han fallado las medidas de detección y/o contención establecidas [11].

Infección Única: Un código dañino que solo afecta a un dispositivo, usuario o sistema [11].

Este proyecto no contempla los ataques de seguridad faltantes tales como [11]:

- **Ataque**
    - Ataque dirigido
- **Denegación del servicio (DoS)**
    - Exitosa
    - No Exitosa
- **Pruebas y reconocimientos**
    - Pruebas no autorizadas

- Alarmas de sistemas de monitorización

- **Abuso de privilegios y usos inadecuados**
  - Abuso de privilegios o de políticas de seguridad de la información
  - Uso indebido de la marca.

CAPITULO 2

2. MARCO TEORICO Y METODOLOGIA DEL PROYECTO

2.1 MARCO TEORICO

2.1.1 Normas ITIL

La Biblioteca de Infraestructura de Tecnologías de Información (ITIL sus siglas en inglés) es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general [12].

Aunque se desarrolló durante los años 1980, ITIL no fue ampliamente adoptada hasta mediados de los años 1990. Esta mayor adopción y conocimiento ha llevado a varios estándares, incluyendo ISO/IEC 20000, que es una norma internacional cubriendo los elementos de gestión de servicios de TI [12].

2.1.2 Objetivo de ITIL

El objetivo de ITIL es proporcionar a los administradores de sistemas de TI las mejores herramientas y documentos que les permitan mejorar la calidad de sus servicios, es decir, mejorar la satisfacción del cliente al mismo tiempo que alcanzan los objetivos estratégicos de su organización. Para esto, el departamento de TI debe ser considerado como una serie de procesos estrechamente vinculados. Pragmáticamente, ITIL cumple con la lógica de hacer que la TI sea útil para los empleados y clientes en lugar de lo opuesto [13].

2.1.3 Características de la librería

La principal causa de que ITIL se haya convertido desde la década de los 90 en un modelo de referencia y haya experimentado una expansión tan grande con respecto a otros modelos esta fundamentada por dos motivos [14]:

- Las características esenciales de esta librería.

- Su compatibilidad con respecto a la introducción de normas y/o estándares internacionales y otros modelos de gestión que estén funcionando en la organización.

A continuación, se detallan algunas de las características que han diferenciado a estos estándares de buenas prácticas:

- No tiene derechos de propiedad,
- Es de libre utilización. Cualquier empresa o persona puede ponerlo en práctica, incluso únicamente en las partes que quieran ser aplicadas.
- Estándar internacional.

2.1.4 Aplicación de la metodología ITIL para impulsar la gestión de TI

Un estudio realizado en Europa por la consultora Market Clarity, a instancias de BMC Software, revela que cada vez se aprecian más las ventajas de ITIL (Information Technology Infrastructure Library) a la hora de alinear la tecnología con los objetivos de negocio. Dicho estudio reflejó que un 70% de las 16 empresas encuestadas conocen esta metodología y los beneficios que ofrece [15].

2.1.5 ¿Qué es una incidencia?

Según ITIL, una incidencia es toda interrupción o reducción de la calidad no planificada del servicio. Pueden ser fallos o consultas reportadas por los usuarios, el equipo del servicio o por alguna herramienta de monitorización de eventos [16].

2.1.6 ¿Qué es un rol?

Un rol es un conjunto de responsabilidades y dominios de autoridad asignados a un puesto de trabajo. Un rol es un comportamiento frente a una actividad. Este rol se va a asociar a una persona física o a un equipo de personas.

Como regla general, un rol se define en un proceso o función. Algunos roles también se relacionan con los servicios. Vamos a identificar los roles que ostentan los clientes o usuarios.

2.1.7 Modelo de incidencia

Un modelo de incidencia permite optimizar el proceso de resolución de esta, como sabemos existen incidencias que no son nuevas, sino que ya se han presentado

anteriormente y que se repetirán en el futuro. Por esta razón varios organismos encuentran bastante útil la definición de un modelo de incidencias que puedan aplicar a incidencias recurrentes que comprometan la seguridad de la información [17].

A continuación, se presentan los puntos que un modelo de incidencia debería tener:

- Pasos a seguir para la resolución de la incidencia.
- Orden cronológico de los pasos.
- Responsabilidades
- Plazos para la resolución del incidente
- Procedimiento de escalado.

2.1.8 Principales actividades para la gestión de incidencias según ITIL V3

2.1.8.1 Detección

Cuanto más rápido se detecte una incidencia, su impacto será menor en lo que concierne a la seguridad de la información.

2.1.8.2 Registro

Todas las incidencias deben ser registradas independientemente una de otra, la información que generalmente se debe registrar es:

- Código único
- Categoría
- Prioridad
- Datos del usuario
- Descripción de la incidencia
- Estado
- Personal asignado a la resolución

2.1.8.3 Categorización

En esta actividad se establece el tipo exacto de la incidencia, en este documento la categorización estará dada por el gestor de primer nivel.

2.1.8.4 Priorización

La prioridad de una incidencia nos determina como se debe gestionar la misma, la prioridad suele depender de la urgencia o el impacto que pueda generar esta.

2.1.8.5 Diagnóstico inicial

Cuando el personal de soporte de primer nivel recibe una incidencia, realiza un diagnostico en base a los síntomas.

2.1.8.6 Escalado

Si el soporte de primer nivel no se ve capaz de solucionar el incidente, este asignara el incidente a un nivel superior

2.1.8.7 Investigación y diagnostico

Establecer exactamente que es lo que no funciona, cual sería el impacto y buscar una solución potencial al incidente,

2.1.8.8 Resolución

Una vez detectada la solución potencial del incidente, esta deberá ser aplicada y probada.

2.1.8.9 Cierre

Cuando se cierre la incidencia la resolución deberá ser documentada en la base de conocimiento para un posible reintento del mismo ataque.

2.2 METODOLOGÍA DEL PROYECTO

2.2.1 Metodología de Investigación

Para este proyecto se utilizará la metodología de investigación de tipo exploratorio, es decir se realizará la búsqueda de información y trabajos relacionados con esta línea de investigación con el objetivo de analizar y comparar la situación de otras empresas o entidades con la Universidad, con esta investigación se busca ofrecer un producto que se adapte a los requerimiento y necesidades de la universidad. Además, se realizará un estudio diagnóstico para conocer más a fondo la problemática que se abarcará en esta investigación.

El estudio diagnostico ayudara a conocer los procedimientos que se llevan a cabo dentro del departamento de Tics en caso de un incidente de seguridad de la información y de esta forma empezar a reconocer quien o quienes son las personas encargadas de la gestión de

estos incidentes y cuáles son los procesos que necesitaran reestructurarse y adaptarse a los estándares ITIL V3.

Esta propuesta tiene como objetivo mejorar los procesos de gestión de incidentes de seguridad de la información disminuyendo la cantidad de procedimientos o pasos a seguir durante un ciberataque.

2.2.2 TECNICAS DE RECOLECCION DE INFORMACIÓN

El método de recolección de información será mediante una entrevista al director del departamento de Tics de la Universidad Estatal Península de Santa Elena con el fin conocer los procesos que se llevan a cabo durante cada incidente de seguridad de la información mencionados en el alcance del proyecto.

2.2.3 METODOLOGÍA DE DESARROLLO

Con el objetivo de realizar una investigación de calidad en este proyecto, se plantea utilizar el desarrollo por etapas, debido a que permite desarrollar paso a paso los nuevos procesos basados en los estándares ITIL V3, así como la generación del manual en la etapa final.

Etapa de Análisis: Esta etapa comprende el estudio del accionar que el personal del departamento de Tecnologías de la Información y Comunicación haya tomado durante un incidente de seguridad de la información que haya ocurrido con anterioridad.

Etapa de establecimiento de roles: Establecer un punto de partida, asignando roles para determinar qué acciones se tomarán o dado el caso a que personas se delegarán en el momento que suceda un incidente de seguridad de la información.

Etapa de rediseño de los procesos: Se establecerán los procesos que se seguirán o mejorarán y el esquema de trabajo a seguir para cada rol.

2.3 Resultados

El desarrollo del manual de Gestión de incidentes de seguridad de la información para el departamento de Tics de la Universidad Estatal Península de Santa Elena permitirá conseguir los siguientes resultados:

- Obtener el documento de flujogramas de cada uno de los procesos que se utilicen en la gestión de incidentes de seguridad de la información.
- Optimización de procedimientos que forman parte de un proceso de gestión de seguridad de la información adecuándolos a las necesidades de la universidad.
- Describir de manera detallada todas las actividades que se desarrollaran en caso de que ocurra un incidente de los que se analizaran en esta propuesta de investigación.

Capítulo 3

3. Propuesta

3.1 Tema

MANUAL DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION BASADO EN LOS ESTANDARES ITIL V3 PARA LA UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA

3.2 Justificación

Para cada departamento de TI de cualquier organismo en general, es necesaria la implementación de estándares que acrediten las buenas prácticas que se están llevando a cabo de dicho departamento, y la Universidad Estatal Península de Santa Elena al dar un servicio educativo durante más de 22 años, debe adaptarse a la evolución de las nuevas tecnologías y buenas prácticas para mantenerse a la vanguardia en lo que concierne a la infraestructura tecnológica y estándares de buenas prácticas.

El departamento de TI de la universidad dispone de una infraestructura que le permite solventar la realización de sus actividades educativas de gestión interna, por esta razón es que el departamento se encuentra de manera frecuente en busca de mejorar la calidad de gestión de personal, así como de equipos que permiten brindan de forma más optima y con una mayor calidad los servicios disponibles en el departamento antes mencionado.

Este proyecto se justifica debido a la necesidad que tiene el departamento de TI de la Universidad Estatal Península de Santa Elena de un manual que permita gestionar los incidentes de seguridad de la información de una manera ptima al momento que este ocurra.

3.3 Objetivo

El objetivo de este manual es proporcionar los procedimientos detallados para la correcta gestión de incidencias de seguridad de la información que desarrolla el centro de soporte de la Universidad Estatal Península De Santa Elena (UPSE).

3.4 Ubicación

Institución: Universidad Estatal Península de Santa Elena.

Provincia: Santa Elena

Cantón: La Libertad.

Ilustración 1 Ubicación de UPSE en Google maps.

3.5 Actividades

A continuación, se detallan las actividades que se realizan en cada una de las etapas mencionadas en el documento.

Análisis de la situación actual

En esta etapa se procede a realizar un estudio de la situación actual y evaluar los procesos que realiza el área de soporte con respecto a los incidentes relacionados con la seguridad de la información, con el fin de identificar fallas o debilidades.

Con el proceso antes mencionado se llegó como conclusión al siguiente flujograma que nos indica cómo funciona el proceso actualmente, cabe recalcar que el proceso está bastante cerca de lo que es ITIL V3, pero con debilidades en puntos específicos y no orientado específicamente a incidentes de seguridad de la información.

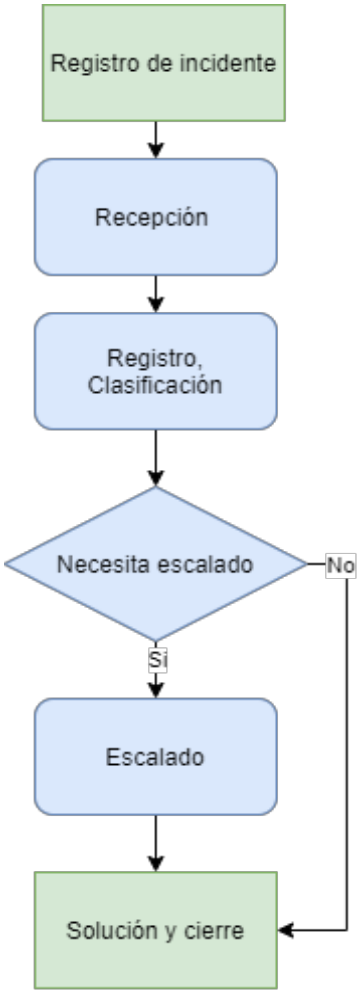


Ilustración 2 Proceso de gestión de incidentes actual.

Establecimiento de roles

En esta etapa, se determinaron los roles y las funciones que va a ejercer el personal perteneciente al departamento de TI de la Universidad Estatal Península de Santa Elena.

- Definir el centro de soporte
- Estructurar la jerarquía del centro del soporte
- Establecer el medio de comunicación para el reporte de incidentes relacionados con la seguridad de la información.
- Diseñar el flujograma correspondiente al proceso.

Rediseño del proceso

Se establecen los procesos que se optimizaran y seguirán en el caso de que se presente un incidente de seguridad de la información.

- Estipular los procesos de gestión de incidencias de seguridad de acuerdo con el tipo de ataque que afectaría a la universidad.
- Establecer acciones para generar el registro de reporte de incidentes.
- Establecer acciones para el registro de información generando así, una base de conocimientos que sirva de apoyo hacia futuros incidentes.
- Diseñar el manual de políticas y procedimientos del proceso de gestión de incidentes de seguridad de la información dentro de la Universidad Estatal Península De Santa Elena

Actividades Adicionales

Requerimientos de Proyecto
Se analizará el proceso a seguir para determinados incidentes que comprometan la seguridad de la información.
La investigación permitirá escalabilidad en base a una mesa de ayuda.
El procedimiento de desarrollo de la investigación deberá cumplir con las normas de buenas prácticas ITIL V3.
El manual debe permitir una respuesta inmediata ante determinados incidentes.
El manual se generará de tal forma que permita al usuario una ejecución intuitiva del proceso.

La investigación deberá ser simulada por una determinada herramienta web de gestión de incidentes.
Los usuarios solo podrán reportar incidentes por medio de la herramienta web.
La herramienta web tendrá una base de conocimiento que permite identificar si ya existe una solución dada al incidente presentado.
Se crearán las políticas generales del manejo gestión de incidentes de seguridad de la información
La investigación ayudara a mantener la confidencialidad, integridad y disponibilidad de la información.
Los procesos deberán ser graficados en flujogramas para un mejor entendimiento del personal de Tics.
Solo el personal perteneciente al departamento de Tics tendrá acceso a los tickets creados.
Los tickets tendrán una prioridad de acuerdo con el impacto que estos pueden causar a la información que descansa en los servidores o equipos pertenecientes a la Universidad.

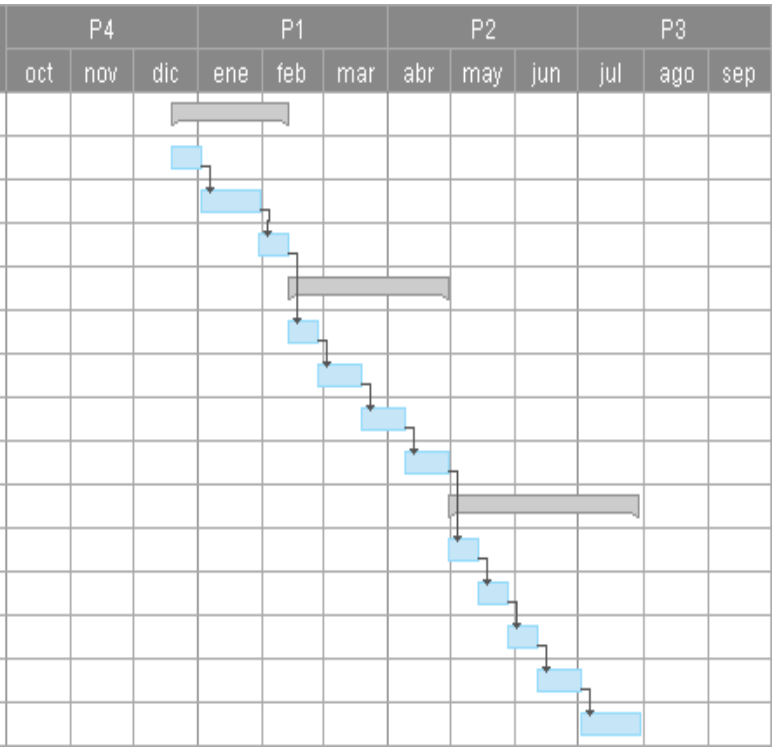
Tabla 2 Requerimientos de proyecto

3.6 Impacto

Con el constante esfuerzo por parte de la universidad para mejorar en todo aspecto, la inclusión de esta propuesta al relacionarse con los procesos de gestión de incidentes dentro del departamento de tecnologías de la información genera un impacto positivo al organizar, documentar y estandarizar determinados procesos dentro del departamento de TI esto con el fin de darle un salto de calidad a las operaciones dentro del mismo, incentivando a su vez a seguir estandarizando el resto de procesos que se manejan en el área de TI.

3.7 Cronograma

	Nombre de la tarea	Duració	Inicio	Finalizar
1	Análisis de la situación actual	40d	19/12/19	12/02/20
2	Comunicación con director de TI	2sem	19/12/19	01/01/20
3	Análisis de procesos actuales	4sem	02/01/20	29/01/20
4	Diseño de diagrama de flujo	2sem	30/01/20	12/02/20
5	Establecimiento de roles	55d	13/02/20	29/04/20
6	Definir el centro de soporte	2sem	13/02/20	26/02/20
7	Estructurar jerarquía de centro de soporte	3sem	27/02/20	18/03/20
8	Establecer medio de comunicación para el reporte de incidente	3sem	19/03/20	08/04/20
9	Diseño de diagrama de flujo	3sem	09/04/20	29/04/20
10	Rediseño de procesos	65d	30/04/20	29/07/20
11	Estipular los procesos que serán adaptados a ITIL V3	2sem	30/04/20	13/05/20
12	Establecer acciones para el reporte de incidentes	2sem	14/05/20	27/05/20
13	Establecer acciones para el registro de información (Base de conocimiento)	2sem	28/05/20	10/06/20
14	Adaptar los procesos a ITIL V3	3sem	11/06/20	01/07/20
15	Diseño del Manual de políticas y procedimientos.	4sem	02/07/20	29/07/20



Fuente: Henry Marin

Tabla 3 Cronograma de actividades

4. Conclusiones

- El análisis de la situación actual demostró que si existen procesos basados en normas de buenas prácticas, pero no definidos de manera formal.
- El uso de los estándares de buenas prácticas ITIL, también apoyara los procesos que actualmente son seguidos para la gestión de incidentes de servicios.
- El uso de la base de conocimientos proporcionara una retrospectiva sobre como han sido resueltos varios incidentes, apoyando de esta forma el rápido accionar en el momento que se presente un incidente.

5. Recomendaciones

- Diseñar o reestructurar los procesos para nuevos incidentes de seguridad de la información.
- Realizar inspecciones periódicas a la plataforma que se encuentra disponible para el reporte de incidentes con la finalidad de disminuir el riesgo de saturación del servicio.
- Capacitar a todo al nuevo personal perteneciente a la universidad sobre los estándares de buenas prácticas y sobre como reportar un incidente de seguridad de la información en la plataforma que se encuentre disponible.

Bibliografía

[1] Y. Tibaquira, «METODOLOGÍA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION,» Bogota, 2015.

[2] K. Gabriela y B. Edber, «ANALISIS EN SEGURIDAD INFORMATICA Y SEGURIDAD DE LA INFORMACION BASADO EN LA NORMA ISO/IEC 27001,» Guayaquil, 2015.

[3] Y. Tibaquira, Metodologia De Gestion De Incidentes De Seguridad De La Informacion Y Gestion De Riesgos Para La Plataforma SIEM De Una Entidad Financiera Basada En La Norma ISO/IEC 27035 E ISO/IEC 27005, BOGOTA, 2015.

[4] J. Muñoz, Diseño de Politicas de Seguridad Informatica Para La direccion De Tecnologias De la Informacion y Comunicacion, Cuenca, 2016.

[5] Tejada, Gestion de Servicios en el sistema informatico, IC Editorial, 2015.

[6] Bon, Gestion de Servicios TI basado en ITIL V3, 2008.

[7] J. V. J. Bon, Fundamentos de ITIL, Volume 3, Van Haren Publishing, 2008.

[8] F. d. S. y. Telecomunicaciones, «Facsistel,» [En línea]. Available: http://facsistel.upse.edu.ec/index.php?option=com_content&view=article&id=58&Itemid=463. [Último acceso: 28 Noviembre 2019].

[9] E. B. Kelly Bermudez, «Analisis en seguridad informatica y seguridad de la informacion basado en la norma ISO/IEC 27001,» Guayaquil, 2015.

[10] I. Excellence, «SGSI,» 1 Febrero 2018. [En línea]. Available: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/. [Último acceso: 3 Diciembre 2019].

[11] C. y. TB-Security, «Criterios comunes para la Gestión de Incidentes de Seguridad en el Esquema Nacional de Seguridad(ENS),» Ministerio de Defensa de España, 2012.

[12] D. Soto, «NextTech,» 20 Septiembre 2017. [En línea]. Available: https://nextech.pe/que-es-itil-que-beneficios-tiene-itil/. [Último acceso: 13 Agosto 2020].

[13] J.-F. Pillou, «CCM,» 16 Octubre 2008. [En línea]. Available: https://es.ccm.net/contents/602-itil-biblioteca-de-infraestructuras-de-tecnologias-de-informaci#:~:text=El%20objetivo%20de%20ITIL%20es,objetivos%20estrat%C3%A9gicos%20de%20su%20organizaci%C3%B3n.. [Último acceso: 9 Septiembre 2020].

[14] S. R. Huercano, «ITIL V3 Manual Integro,» [En línea]. Available: https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/GSDE01.pdf. [Último acceso: 26 Agosto 2020].

[15] M. P. Villamizar, «Aplicación de la metodología ITIL para impulsar la gestion de TI,» *Revista Espacio,* vol. 39, nº 9, p. 17, 2018.

[16] ServiceTonic, «Service Managment Software,» [En línea]. Available: https://www.servicetonic.com/es/itil/itil-v3-gestion-de-incidencias/#:~:text=Gesti%C3%B3n%20de%20Incidencias-,Qu%C3%A9%20es%20la%20Gesti%C3%B3n%20de%20incidencias%20y%20sus%20principales%20actividades,calidad%20no%20planificada%20del%20servicio.. [Último acceso: 05 Agosto 2020].

[17] ServiceTonic, «ServiceTonic,» [En línea]. Available: https://www.servicetonic.com/es/itil/itil-v3-gestion-de-incidencias/#:~:text=La%20Gesti%C3%B3n%20de%20Incidencias%20(Incident,fase%20de%20Operaci%C3%B3n%20del%20Servicio.&text=El%2

0principal%20objetivo%20de%20la,en%20las%20operaciones%20de%20negocio.. [Último acceso: 16 Septiembre 2020].

[18] L. Rosencrance, «TechTarget,» 23 Julio 2019. [En línea]. Available: https://searchdatacenter.techtarget.com/es/tutoriales/10-tipos-de-incidentes-de-seguridad-y-como-manejarlos. [Último acceso: 28 Noviembre 2019].

Anexos

Anexo 1: Entrevista dirigida al director de tecnologías de la información.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

ENTREVISTA DIRIGIDA AL DIRECTOR DEL DEPARTAMENTO DE TECNOLOGIA DE LA INFORMACION DE LA UNIVERSIDAD.

Objetivo. Obtener información sobre el departamento de tecnologías de la universidad, su conformación y su accionar en caso de un ataque de seguridad de la información.

Preguntas.

1. **¿Cuántas personas componen el departamento de Tics?**
2. **¿Qué personas pueden acceder al departamento de Tics?**
3. **¿Cuántos servidores tiene el departamento y como está funcionando cada uno?**
4. **¿Qué servicios de tecnología ofrece el departamento?**
5. **¿En el departamento existe un responsable o área encargada de la seguridad de la información?**
6. **¿Ha ocurrido algún incidente de seguridad durante su dirección del departamento de Tics?**
7. **¿Ha detectado alguna vez una vulnerabilidad en la seguridad de la información?**
8. **¿La universidad cuenta con un manual de política de seguridad de la información?**
9. **En caso de haber ocurrido un incidente de seguridad en el último año, describa lo ocurrido**

10. **¿Cuál es el procedimiento que se sigue en caso de un ataque a la seguridad de la información?**
11. **¿Existe el apoyo de las máximas autoridades en temas de tecnología?**