UNIVERSIDAD DE LAMBAYEQUE
FACULTAD DE CIENCIAS DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

DISEÑO DE MODELO DE GESTIÓN DE INCIDENTES DE TI PARA MEJORAR LOS PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD DE LAMBAYEQUE

PRESENTADA PARA LA OBTENCIÓN DEL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autores:

Leonardo Panta Miguel Angel

Regalado Delgado Edson

Asesor:

Castillo Zumarán Segundo José

Línea de Investigación:

Desarrollo y Gestión de los Sistemas de Información

Chiclayo – Perú

2020

Ing. Segundo José Castillo Zumarán
ASESOR

Mg. Enrique Santos Nauca Torres
PRESIDENTE

Ing. Jorge Tomás Cumpa Vásquez
SECRETARIO

Ing. Segundo José Castillo Zumarán
VOCAL

Dedicatoria

Dedico este proyecto y esfuerzo a mis padres, quienes fueron mi guía desde el inicio de mis días, por brindarme todo su apoyo y aliento durante todo momento de mi vida académica.

Agradecimientos

A Dios por la vida y sabiduría para alcanzar esta meta propuesta.

A mis padres por su constante apoyo, por su esfuerzo para darme la oportunidad de brindarme una carrera profesional.

Al ingeniero Ernesto Karlo Celi Arévalo por su gran apoyo brindado para el desarrollo de esta investigación.

Índice

RESUMEN IX
ABSTRACT X
I. INTRODUCCIÓN 1
II. MARCO TEÓRICO 5
2.1. Antecedentes Bibliográficos 5
2.2. Bases teóricas – científica 7
2.2.1. Incidente de seguridad de la información 7
2.2.2. Gestión de incidentes de seguridad de la información 10
2.2.3. Biblioteca de Infraestructura de Tecnologías de Información (ITIL) 12
2.2.4. ISO/IEC 27035:2011 17
2.2.5. Evaluación de la solución 19
2.3. Definición de términos básicos 19
2.4. Hipótesis 20
III. MATERIALES Y MÉTODOS 20
3.1. Variables y métodos 20
3.2. Tipo de estudio y diseño de investigación 21
3.3. Población y diseño de investigación 22
3.4. Métodos, técnicas e instrumentos de recolección de datos 23
3.5. Procesamiento de datos y análisis estadístico 23
IV. RESULTADOS 23
4.1. Análisis de la situación actual de la institución 23
4.1.1. Descripción de la institución 23
4.1.2. Distribución geográfica de la institución 25
4.1.3. Estructura organizacional de la institución 25
4.1.1. Servicios que ofrece la institución 27
4.1.2. Infraestructura tecnológica 27
4.1.3. Sistemas de Información 30
4.1.4. Conformación del personal de TI 31
4.1.5. Descripción del procedimiento actual de la gestión de incidentes de Tecnologías de la Información 31

4.2. Diseño del proceso de gestión de incidentes de Tecnologías de la Información 32
4.2.1. Preparación 32
4.2.2. Detección y reporte 33
4.2.3. Evaluación y análisis 35
4.2.4. Respuesta 47
4.2.5. Actividades Post-incidente 50
4.3. Diseño de procedimientos para la gestión de incidentes de Tecnologías de la Información 53
4.3.1. Diseño del flujo del proceso de gestión de incidentes de Tecnologías de la Información 53
4.3.2. Descripción de los roles en la gestión de incidentes de Tecnologías de la Información 54
4.3.3. Estados de un incidente en la gestión de incidentes de Tecnologías de la Información 54
4.3.4. Definición de indicadores en la gestión de incidentes de Tecnologías de la Información 57
4.4. Evaluación del Modelo 57
4.4.1. Resultados de la aplicación del instrumento 57
4.4.2. Evaluación de la fiabilidad del instrumento 61
4.4.3. Análisis de la Regresión Lineal Múltiple 62
V. CONCLUSIONES 68
VI. RECOMENDACIONES 69
VII. REFERENCIAS 70
VIII. ANEXOS 72

Índice de tablas

Tabla 1. Variables de la investigación 21
Tabla 2. Operacionalización de las variables de la investigación 21
Tabla 3. Distribución de usuarios de TI en la Universidad de Lambayeque 22
Tabla 4. Detalles de los servidores con los que cuenta la UDL 28
Tabla 5. Equipos de cómputo y red con los que cuenta la UDL 29
Tabla 6. . Software usado en la UDL 29
Tabla 7. Personal de la oficina de Cómputo e Informática 31
Tabla 8. Categorías de incidentes de seguridad de la información 35
Tabla 9. Priorización de las áreas de la UDL 37
Tabla 10. Escalas para determinar el nivel del impacto de los incidentes 38
Tabla 11. Escalas para determinar el nivel de urgencia de los incidentes 39
Tabla 12. Tiempos para la atención y cierre de los incidentes 39
Tabla 13. Mapa de calor para determinar el nivel de prioridad de un incidente en función del impacto y la urgencia 40
Tabla 14. Priorización de los incidentes 41
Tabla 15. Niveles de escalonamiento y responsables 44
Tabla 16. Niveles de escalonamiento de los incidentes 45
Tabla 17. Equipo de Respuesta a Incidentes 47
Ta**bla 18.** Resultados de la evaluación de la fiabilidad del instrumento (Alfa de Cronbach) ... 61
Tabla 19. Matriz de reducción de ítems evaluados 62
Tabla 20. Resultados de la evaluación del modelo por regresión múltiple 64
Tabla 21. Resultados del análisis de varianza del modelo 65
Tabla 22. Resultados del análisis de coeficientes del modelo 66

Índice de figuras

Figura 1. Componentes del proceso de riesgos 8
Figura 2. Procesos de ITIL 13
Figura 3. Relaciones en un incidente de seguridad de la información 17
Figura 4. Fases de la gestión de incidentes de seguridad de la información 18
Figura 5. Distribución de Facultades y Escuelas Profesionales 24
Figura 6. Ubicación de la UDL.....25
Figura 7. Organigrama de la UDL.....26
Figura 8. Organigrama del área de TI de la UDL.....27
Figura 9. Infraestructura de red de la UDL.....30
Figura 10. Flujo de decisiones entre los niveles de escalonamiento 43
Figura 11. Proceso de gestión de incidentes propuesto 53
Figura 12. Relaciones entre los estados de un incidente de Tecnologías de la Información....55
Figura 13. Actividades que dan origen a los estados de un incidente en el proceso de gestión de incidentes propuesto.....56
Figura 14. Resultados de los ítems (preguntas) del cuestionario de la dimensión Efectividad del diseño 57
Figura 15. Resultados de los ítems (preguntas) del cuestionario de la dimensión Usabilidad del modelo.....58
Figura 16. Resultados de los ítems (preguntas) del cuestionario de la dimensión Adaptabilidad del modelo.....59
Figura 17. Resultados de los ítems (preguntas) del cuestionario de la dimensión Satisfacción de usuarios 60

Resumen

La Universidad de Lambayeque es una institución educativa ubicada en la ciudad de Chiclayo que, como la mayoría de las casas de estudio, hacen uso de las Tecnologías de la Información para desarrollar sus procesos, dependiendo en gran medida de la disponibilidad de su infraestructura tecnológica. Por lo cual, la ocurrencia de cualquier incidente en alguno de sus sistemas informáticos, equipamiento o servicio informático afectará directamente en la prestación de servicios de la institución, perjudicando el normal funcionamiento de sus procedimientos, la seguridad de la información y la continuidad del negocio.

Tal realidad, fundamentó a desarrollar una investigación propositiva, la cual plantea diseñar un modelo de gestión de incidentes de TI para mejorar los procedimientos de seguridad de la información, comprendiendo el importante papel de dichos procedimientos para asegurar la disponibilidad de los procesos de la universidad. Para el diseño del modelo se utilizó como marco de referencia la norma ISO 27035 para la estructura del proceso y desarrollo de los procedimientos y el framework ITIL para definir los requisitos mínimos requeridos para la gestión de incidentes de TI.

El modelo propuesto fue evaluado a través de la aplicación de una encuesta de satisfacción destinada a los responsables de la Oficina de Cómputo e Informática, docentes de la Escuela Profesional de Ingeniería de Sistemas y al personal administrativo. Para el diseño de la encuesta se empleó la norma ISO 25010, de la cual se utilizó cuatro dimensiones: efectividad, usabilidad, adaptabilidad y satisfacción.

Palabras claves: mesa de ayuda, gestión de incidentes, seguridad de la información.

Abstract

The University of Lambayeque is an educational institution located in the city of Chiclayo that, like most of the houses of study, make use of Information Technologies to develop its processes, depending largely on the availability of its technological infrastructure. Therefore, the occurrence of any incident in any of its computer systems, equipment or computer service will directly affect the provision of services of the institution, damaging the normal operation of its procedures, information security and business continuity.

This reality, based on developing a proactive investigation, which proposes to design an IT incident management model to improve information security procedures, understanding the important role of such procedures to ensure the availability of university processes. For the design of the model, the ISO 27035 standard was used as a frame of reference for the structure of the process and development of the procedures and the ITIL model to define the minimum requirements required for the management of IT incidents.

The proposed model was evaluated through the application of a satisfaction survey for those responsible for the Office of Computing and Information Technology, teachers of the Professional School of Systems Engineering and administrative staff. For the design of the survey, the ISO 25010 standard was used, of which four dimensions were used: effectiveness, usability, adaptability and satisfaction.

Palabras claves: help desk, incident management, information security.

I. Introducción

En el mundo de hoy las organizaciones dependen de la tecnología para desarrollar sus actividades y lograr objetivos. La información generada por los procesos de las organizaciones es almacenada, procesada y transmitida diariamente a través de las redes internas y externas como Internet. Aunque el uso de la red de Internet les permite a las organizaciones poder desarrollarse con mayor facilidad, esta trae consigo amenazas de todo tipo que si no se controlan podrían conllevar a graves problemas de seguridad.

En el pasado, las amenazas convencionales de Internet eran relativamente claras, impuestas a través de archivos adjuntos de correo electrónico, software descargado, vulnerabilidades del navegador y sitios web fraudulentos. Incluso cuando las amenazas se hicieron más complejas, fácilmente podrían ser identificadas usando políticas, firmas y la defensa basadas en listas negras. Las amenazas de hoy son sigilosas por diseño y pueden ser lanzadas desde aplicaciones y sitios web legítimos y bien conocidos, incluyendo bancos, minoristas y grandes corporaciones que han sido comprometidas. (Norse Corporation, 2014, pág. 2)

Por otro lado, el paradigma clásico que se enfoca en proteger a la organización de las amenazas del exterior a través de la seguridad perimetral no basta para salvaguardar la confidencialidad, integridad y disponibilidad de la información ya que las amenazas, en el contexto actual, también vienen del interior de la organización. Teniendo esto en cuenta, nació el concepto de "defensa en profundidad" que convierte la seguridad de la información en algo más complejo y fiable.

"Las organizaciones han entendido que, si los mecanismos de protección implementados fallan, es necesario contar con procesos estructurados y personal especializado que maneje los incidentes de seguridad de información y restablezca los sistemas en el menor tiempo posible". (Andrade & Fuertes, pág. 17)

Según el Reporte de Seguridad de ESET Latinoamérica 2018, de cada cinco empresas en Latinoamérica como mínimo tres sufrieron por lo menos un incidente de seguridad (ESET Latinoamérica, 2018, pág. 15). A su vez la Encuesta Global de Seguridad de la Información 2017-2018 indica que para el 2021, la brecha en ciberseguridad alcanzará un costo aproximado de 6 billones de dólares, el doble calculado para el 2015. Los cual indica que los incidentes de seguridad son más frecuentes y con mayor impacto. (EY Perú, 2018, pág. 34)

Además, “actualmente las organizaciones luchan contra una serie de obstáculos: falta de agilidad, falta de presupuesto y falta de capacidad. Las cuales deben ser atendidas con urgencia ya que el panorama de amenazas está en constante crecimiento. Pues de eliminar estos obstáculos, las organizaciones tendrían una mejor respuesta ante cualquier incidente de seguridad”. (EY Perú, 2015, pág. 17)

En el plano nacional, algunos sectores de la industria cuentan con entes reguladores que recomiendan u obligan el uso de marcos y políticas de seguridad de la información. Sin embargo, no existen normas o leyes establecidas por el Ministerio de Educación (MINEDU) que regulen la seguridad de la información en este sector. Esto genera falta de conocimiento y desinterés sobre el tema en instituciones educativas.

Esto no libra a este tipo de instituciones de la implementación de políticas y procedimientos que aseguren los diversos datos que manejan, ya que existe la Ley peruana de Protección de Datos Personales (Ley N° 29733), dictada en el 2011, que obliga a las instituciones públicas y privadas que almacenan datos personales a garantizar un nivel suficiente de protección para dichos datos.

La mayoría de instituciones educativas (universidades, institutos, etc.) no han implementado políticas de seguridad de la información porque aún no han experimentado algún incidente de seguridad grave. Lo cual demuestra que las instituciones son reaccionarias y no preventivas, o que asumen que es un gasto injustificado.

En el caso de la Universidad de Lambayeque, esta cuenta con un área que alberga los servidores y demás infraestructuras que soportan las diferentes plataformas y servicios de la institución, llamada Cómputo e Informática. Además, esta tiene una unidad llamada Telemática encargada de dar solución a problemas de hardware y software y de dar mantenimientos a los diferentes activos de información. Según los datos recogidos en dichas áreas, desde años atrás han ocurrido incidentes de seguridad, que, aunque han sido controlados por ser leves, podrían causar graves daño a la institución si no existe prevención y gestión de estos.

Las causas de los incidentes de seguridad son diversas; entre estas se pueden encontrar la falta de políticas para el uso de los diferentes equipos y servicios como Internet, correo institucional, equipos informáticos, etc. La falta de procedimientos explícitos que permitan gestionar eficazmente dichos incidentes y la falta de planes de concientización a los colaboradores de la institución sobre temas de seguridad de la información.

El personal de la unidad de Telemática, encargado de dar solución a diversos incidentes en la institución, no cuenta con procedimientos establecidos para gestionarlos; lo cual nos hace saber que no existe un registro, seguimiento, priorización, clasificación y notificación de aquellos incidentes. Esto se debe tener muy en cuenta ya que las amenazas día a día se vuelven más sofisticadas y con mayor impacto.

Cabe mencionar que sí existen políticas de seguridad aplicadas en el área de Cómputo e Informática como listas de acceso, back ups, deshabilitación de puertos, entre otras. Estas políticas han sido aplicadas de acuerdo a las necesidades básicas de seguridad y no en base a un análisis previo de riesgos. Además, no hay una revisión ni actualización de políticas y controles.

Ante esta realidad, surge la necesidad de controlar los incidentes de seguridad que puedan ocurrir en cualquier organización mediante la aplicación de estándares y buenas prácticas, los cuales brindan un conjunto de recomendaciones y directrices que ayudan a dar una rápida y eficaz respuesta frente a los incidentes. Permitiéndoles a las organizaciones tener un mayor grado de seguridad y confianza.

Por tal motivo, se propuso diseñar un modelo para la gestión de incidentes de seguridad de la información, con el objetivo de prever y dar respuesta a las futuras amenazas que se materialicen. De esta forma ayudar a garantizar la confidencialidad, integridad y disponibilidad de la información y al mejoramiento y fortalecimiento continuo de esta.

Por lo tanto, el problema central de la investigación fue:

¿El diseño de un modelo para la gestión de incidentes de TI, puede contribuir a mejorar los procedimientos de seguridad de la información en la Universidad de Lambayeque?

Siendo la hipótesis de la presente investigación:

El diseño de un modelo de gestión de incidentes de TI, contribuirá a mejorar los procedimientos de seguridad de la información en la Universidad de Lambayeque.

En consecuencia, esta tesis tuvo como objetivo general demostrar de qué manera el diseño de un modelo para la gestión de incidentes de TI puede contribuir a mejorar los procedimientos de seguridad de la información en la Universidad de Lambayeque.

Además, los objetivos específicos fueron:

- Diagnosticar el estado actual de los incidentes de seguridad al interior de la Universidad de Lambayeque.
- Definir los requisitos y parámetros mínimos para la gestión de incidentes de Tecnologías de la Información: clasificación, priorización y escalonamiento de incidentes.
- Desarrollar los procedimientos para atender los diferentes incidentes de seguridad ocurridos en el interior de la Universidad de Lambayeque.
- Evaluar el modelo propuesto mediante una encuesta.

La justificación de esta investigación es que se contribuirá en la mejora del manejo de los incidentes en la Universidad de Lambayeque lo cual permite mantener la continuidad de los procesos. Además, porque se aplicaron las teorías y buenas prácticas para dar solución al problema.

II. Marco Teórico

2.1. Antecedentes Bibliográficos

A continuación, se presentan los antecedentes bibliográficos encontrados que se tomarán en cuenta en el desarrollo de esta investigación.

A nivel internacional

Cuzme M. y Pinargote R. (2015) en su investigación titulada "PLAN DE GESTIÓN DE INCIDENTES QUE AFECTAN A LOS EQUIPOS INFORMÁTICOS DE LA ESPAM MFL" desarrollada en la Escuela Superior Politécnica Agropecuaria de Manabí "Manuel Félix López" de Ecuador, tiene como objetivo elaborar un plan de gestión de incidentes que afectan a los equipos informáticos, estableciendo cursos de acción para reducir el impacto y mejorando la productividad de los usuarios. Los autores concluyeron que el inventariado de los equipos informáticos permitió establecer su disponibilidad y los riesgos a los que están expuestos los activos. Además, la evaluación de los incidentes permitió documentarlos y clasificarlos facilitando la respuesta a los mismos. Finalmente concluyó que un plan de gestión de incidentes permite un correcto manejo en los tiempos necesarios. Los autores recomendaron el inventario continuo de los activos informáticos, así como el registro de la información relevante de los incidentes tratados. Además, recomendó tomar conciencia de la importancia de acciones preventivas y también tener en cuenta las consideraciones regulatorias que tomen en su sector. Esta investigación es relevante para la presente tesis porque muestra el desarrollo de un plan de gestión de incidentes, aplicado en una institución educativa superior.

Cifuentes Obando, Juan Fernando (2017) en su investigación titulada "PROPUESTA DE AJUSTE AL MODELO DE GESTIÓN DE INCIDENTES DE LA EMPRESA CLARO COLOMBIA S.A. PARA EL MEJORAMIENTO CONTINUO DE LOS TIEMPOS DE RESPUESTA BASADO EN ITIL V3", desarrollada en la Universidad Santo Tomás de Colombia, tiene como objetivo proponer un ajuste al modelo de gestión de incidentes basado en ITIL V3 de la empresa Claro Colombia S.A. para disminuir los tiempos de respuesta de los incidentes asignados al grupo de Soporte en Sitio por parte de sus clientes internos. El autor concluyó que el ajuste realizado al modelo de gestión de incidentes de la empresa Claro Colombia S.A. le proporcionó al proceso de operación de servicio y en específico a la gestión de incidencias una mayor efectividad y simplicidad, en particular cuando los clientes internos creen un incidente en la mesa de servicio 123 MIC, mejorando así el servicio prestado y reduciendo los tiempos de respuesta. El autor recomendó analizar los incidentes que se escalan

a los demás grupos de asignación de la empresa Claro Colombia S.A. con el fin de hacer sugerencias de mejoras similares a las hechas para el grupo objeto de este análisis. Esta investigación es relevante para la presente tesis porque muestra la implementación de los procedimientos de ITIL v3 y con ello disminuir los tiempos de respuesta a incidentes.

A nivel nacional

Ayala Medrano, Miguel Angel (2017) en su investigación titulada "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR LOS PROCESOS DE GESTIÓN DEL RIESGO DE UN HOSPITAL NACIONAL", desarrollada en la Universidad Cesar Vallejo de Perú, tiene como objetivo evaluar la manera en que la implementación del Sistema de Seguridad de la Información influye en el proceso de gestión del riesgo en un Hospital Nacional. El autor concluyó que el riesgo se consigue disminuir de 3.72 a 3.09, representando el 16.96%. Por otro lado, se logra el aumento de los controles existentes en 76.19%. Por lo tanto, se determina que la implementación logró mejorar el proceso de gestión de riesgos. El autor recomendó establecer procedimientos de Evaluación y Tratamiento de Riesgos para mejorar el proceso de gestión de riesgos. Además, recomendó de forma general a toda institución relacionada a servicios de salud, implementar la metodología del Sistema de Gestión de Seguridad de la información. Esta investigación es relevante para la presente tesis porque muestra la aplicación del proceso de evaluación y tratamiento de riesgos para mejorar el proceso de gestión de riesgo.

Cruz D. y Fukusaki I. (2017) en su investigación titulada "DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA CLÍNICA MEDCAM PERÚ SAC", desarrollada en la Universidad San Martín de Porres, tiene como objetivo mitigar los riesgos a los que está expuesto los activos de la información de la clínica MEDCAM Perú SAC. El autor concluyó que la implementación del Sistema de Gestión de Seguridad de la Información a través de la identificación, diseño e implementación de controles permite mitigar los riesgos más críticos. Además, que la sensibilización es la pieza clave para este SGSI se puede implementar y mantener. El autor recomendó implementar gradualmente controles y aplicar mantenimientos periódicos a las políticas de seguridad. Además, recomienda planificar capacitaciones para los nuevos trabajadores y evaluar la factibilidad de la implementación de un plan de continuidad de negocios. Esta investigación es

relevante para la presente tesis porque muestra el diseño de un plan para mejorar la seguridad de una institución que da servicios de salud.

A nivel local

Gonzales Flores, Janett (2015) en su investigación titulada "IMPLEMENTACIÓN DEL MARCO DE TRABAJO ITIL V.3.0 PARA EL PROCESO DE GESTIÓN DE INCIDENCIAS EN EL ÁREA DEL CENTRO DE SISTEMAS DE INFORMACIÓN DE LA GERENCIA DE SALUD LAMBAYEQUE", desarrollada en la Universidad Católica Santo Toribio de Mogrovejo, tiene como objetivo apoyar al proceso de gestión de incidencias de TI en el área del Centro de Sistemas de Información (CSI) de la Gerencia Regional de Salud Lambayeque, mediante la implementación de las buenas prácticas del marco de trabajo ITIL v.3.0. El autor concluyó que con la implementación de las herramientas basadas en el marco de trabajo ITIL v3.0, se logró aumentar el número de incidencias resueltas con impacto sobre el usuario o negocio, reducir el tiempo destinado a la atención de las incidencias de las TI, reducir el tiempo de solución de las incidencias de las TI y aumentar la satisfacción de los usuarios respecto al servicio de atención y solución de incidencias de TI. Esto se logró gracias a la estandarización de procedimientos y el uso de controles; lo cual permite agilizar y facilitar la atención y solución de incidencias de TI. El autor recomendó una mejora continua de los procesos de gestión y analizar cada cierto tiempo la necesidad de implementar procesos de ITIL v3.0 faltantes para mejorar la calidad del servicio. Además, recomienda monitorizar constantemente las necesidades de los clientes y del negocio. Esta investigación es relevante para la presente tesis porque muestra la utilización de ITIL v3 en la gestión de incidentes de seguridad de la información.

2.2. Bases teóricas – científica

2.2.1. Incidente de seguridad de la información

La gestión de incidentes de seguridad de la información le permite a la organización prevenir y dar respuesta a incidentes que pueden poner en riesgo sus activos de información y por ende una perdida ya sea económica o en el peor de los casos, de imagen. Pero ¿a qué nos referimos cuando hablamos de incidentes?

Según la norma ISO/EIC 27000 (2014) "un incidente de seguridad de la información es un evento de seguridad no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de negocio y amenazando la seguridad de la información". (pág.

16) Afectando directamente sobre la confidencialidad, integridad y/o disponibilidad de la información.

Un incidente no deseado presenta tres componentes: amenazas, vulnerabilidades e impacto. Las vulnerabilidades indican la debilidad del activo que puede ser explotada por una amenaza. Si ninguno de estos componentes está presente, puede que no se produzca un incidente de seguridad ni que aparezcan riesgos. (Areitio Bertolín, 2008, pág. 56)

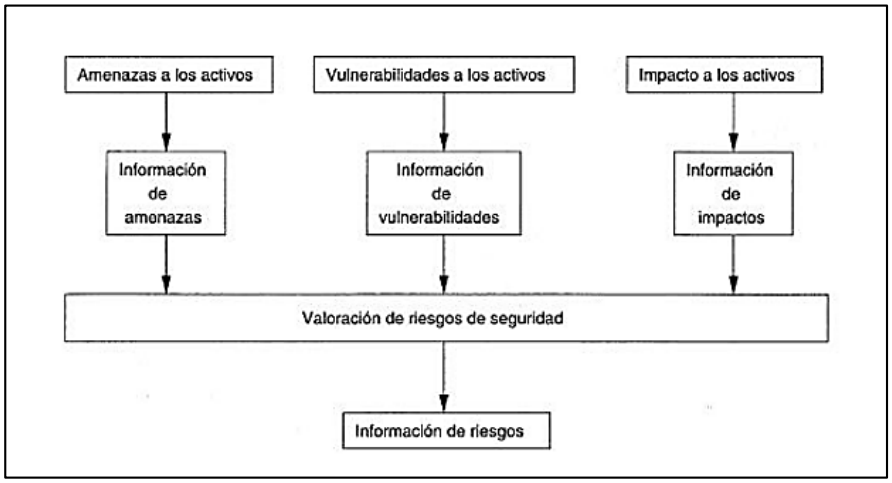


Figura 1. Componentes del proceso de riesgos.
Fuente: Areitio Bertolín, 2008.

Cuando queremos gestionar correctamente incidentes de seguridad, es necesaria optar por clasificar a todos estos. Dicha clasificación dependerá de varios factores, como:

- la naturaleza del incidente,
- la criticidad del/los sistemas/s afectado/s,
- el número de sistemas afectados,
- el impacto que el incidente puede tener en la organización desde el punto de vista legal, de imagen pública, y de prestación de servicio,
- los requerimientos legales y regulatorios.

Además, un incidente que incluya múltiples clases o tipologías debe ser clasificado por el evento de seguridad original o detectada inicialmente.

Son numerosos los tipos de incidentes de seguridad que pueden ocurrir en un sistema. Una posible clasificación sería la siguiente:

A. Acceso no autorizado: son ingresos y operaciones no autorizados a los sistemas, con éxito o no. Forman parte de esta categoría:

   - Robo de información.
   - Borrado de información.
   - Accesos no autorizados exitosos.
   - Alteración de la información.
   - Intentos recurrentes y no recurrentes de acceso no autorizado.
   - Abuso o mal uso de los servicios informáticos que requieren autentificación.

B. Código malicioso o malware: son incidentes que se infiltran en un sistema de información sin autorización del propietario. Son incidentes de código malicioso los siguientes:

   - Virus informático.
   - Troyano: código malicioso que se introduce en el sistema informático como un programa aparentemente legítimo e inofensivo pero que, al ejecutarlo, permite el acceso remoto del sistema a usuarios no autorizados.
   - Gusanos informáticos: código malicioso que, una vez ha accedido al sistema, se va duplicando a sí mismo. No altera los archivos ya instalados, pero supone un consumo de recursos importantes.
   - Ransomware: tipo de malware que una vez dentro de una red o sistema objetivo, se expande a otros equipos para finalmente "secuestrar" la información (archivos) mediante técnicas de criptografía y cobrar por el rescate de esta.

C. Denegación del servicio: eventos que producen la pérdida de un servicio en particular, impidiendo su ejecución normal. Suelen ser incidentes de denegación del servicio cuando en el sistema se nota que hay tiempos de respuesta muy bajo y servicios internos y externos inaccesibles sin motivos aparentes.

D. Pruebas, escaneos o intentos de obtención de información de un sistema de información: son eventos que intentan obtener información sobre las acciones que se producen en un sistema informático. Algunos de estos eventos son:

- Sniffers: aplicación cuya función es obtener la información que envían los distintos equipos de una red.
- Detección de vulnerabilidades: aplicaciones que buscan las vulnerabilidades de un sistema de información para aprovecharse de ello maliciosamente.

E. Mal uso de los recursos tecnológicos: eventos que atacan a los recursos tecnológicos de un sistema de información a causa de un mal uso de los mismos. Forman parte de este tipo de eventos:

- Violación de la normativa de acceso a internet.
- Abuso o mal uso de los servicios informáticos externo o internos.
- Abuso o mal uso del correo electrónico.
- Violación de las políticas, normas y procedimientos de seguridad información de una organización.

2.2.2. Gestión de incidentes de seguridad de la información

"La gestión de incidentes de seguridad tiene como objetivo calcular y utilizar adecuadamente los recursos necesarios para aplicar correctamente medidas de prevención, detección y corrección de incidentes de seguridad". (Chicano Tejada, 2014, pág. 60)

Así mismo, se debe garantizar que se aplica una metodología sólida para la gestión de incidentes de seguridad (establecer responsabilidades y procedimientos), a la vez que emplear procesos de mejora continua y métodos para la recogida de evidencias.

Existe un mecanismo que permite la monitorización de las incidencias de seguridad, cuantificación y costes asociados de las mismas, así como la recopilación de evidencias. Se establecerán procedimientos formales para informar y priorizar eventos de seguridad. Todo el personal afectado deberá conocer los procedimientos para informar de los diferentes tipos de eventos y debilidades que pudieran impactar en la seguridad de las aplicaciones informáticas que sirven de soporte a la tramitación telemática.

Se establecerán responsabilidades y procedimientos formales para manejar los eventos de seguridad y debilidades con eficacia una vez que estas hayan sido comunicadas. Además, se establecerá un proceso formal de mejora continua sobre toda la gestión de incidentes de seguridad y se recopilarán las evidencias necesarias por cada incidente con el fin de cumplir con la legalidad vigente. (Dirección de Informática y Telecomunicaciones, 2010, pág. 33)

Se establecen unas pautas generales a seguir para que esta gestión esté bien ejecutada:

- Preparación y prevención de los incidentes,
- Detección y reporte de los incidentes,
- Clasificación del incidente,
- Análisis del incidente,
- Respuesta al incidente,
- Registro del incidente,
- Aprendizaje.

Siguiendo estas fases de gestión de incidentes, las organizaciones pueden obtener numerosos beneficios, entre ellos:

- Rápida, eficiente y sistemática respuesta antes la aparición de incidentes.
- Rápida restauración del sistema informático garantizando la mínima pérdida de información posible.
- Generación de una base de datos con el histórico de los incidentes y de las medidas tomadas para una mayor rapidez ante próximos incidentes.
- Mejora continua de la gestión y tratamiento de incidentes.
- Eliminación de la aparición de incidentes repetitivos.
- Optimización de los recursos disponibles.
- Mayor productividad de los usuarios.
- Mayor control de los procesos del sistema de información y del proceso de monitorización del mismo.

La recolección y custodia de evidencias es crucial cuando el incidente ocurrido ha tenido un impacto considerable sobre la organización y aunque el motivo principal es ayudar a su resolución, también puede ser necesaria para iniciar procesos de naturaleza legal. En tales casos, es importante documentar claramente cómo se han obtenido y custodiado las evidencias, y siempre conforme a lo dispuesto en la legislación vigente.

La creación de un CSIRT le permite a una organización mantenerse preparada ante la ocurrencia de incidentes de seguridad de la información, ya que según ENISA (2006) “un CSIRT presta los servicios necesarios para ocuparse de estos incidentes y ayuda a los clientes del grupo al que atienden a recuperarse después de sufrir uno de ellos”. (pág. 62)

Uno de los sistemas para la gestión de incidentes son los Sistemas de Gestión de Información y Eventos de Seguridad (SIEM), estos son utilizados para el analizar eventos de seguridad informática en tiempo real y para recolectar y almacenar trazas de seguridad, permitiendo el análisis forense de incidentes y el cumplimiento de lo establecido en las regulaciones existentes. De acuerdo a un estudio de la consultora Gartner, el mercado de los sistemas SIEM se considera maduro y muy competitivo, encontrándose en una fase de adopción amplia donde múltiples desarrolladores de SIEM ofrecen las funciones básicas de gestión de trazas, monitorización de eventos y cumplimiento de regulaciones. (Montesino Perurena, Baluja García, & Porvén Rubier, 2013, pág. 44)

2.2.3. Biblioteca de Infraestructura de Tecnologías de Información (ITIL)

Hoy, las organizaciones dependen de las TI para satisfacer sus objetivos corporativos y sus necesidades de negocios, entregando valor a sus clientes. Para que esto ocurra de una forma gestionada, responsable y repetible, la empresa debe asegurar que los servicios recibidos de alta calidad de TI deben:

- Satisfacer las necesidades de la empresa y los requisitos de los usuarios.
- Cumplir con la legislación.
- Asignarse y entregarse de forma eficaz y eficiente.
- Revisarse y mejorarse de forma continua.

El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas. El rol de ITIL es brindar orientación en el nivel organizacional más bajo que pueda aplicarse. Debajo de ese nivel, para implementar ITIL en una organización se requieren los conocimientos específicos de sus procesos de negocio para ajustar ITIL a fin de lograr una eficacia óptima. (IT Governance Institute y Oficina Gubernamental de Comercio, 2008, pág. 25)

El ciclo de vida comprende:

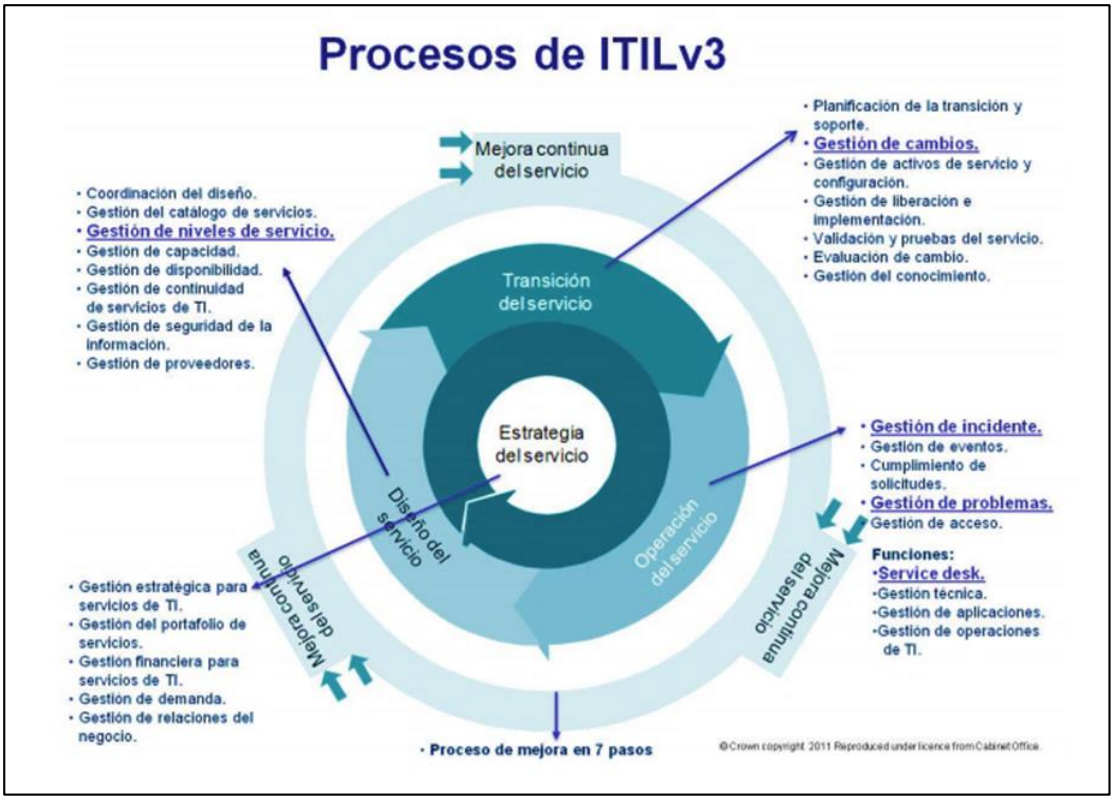


Figura 2. Procesos de ITIL.
Fuente: Universidad TecVirtual del Tecnológico de Monterrey, 2012.

A. Estrategia de Servicio

"La perspectiva, la posición, los planes y patrones que un proveedor de servicios necesita ejecutar para cumplir con los resultados del negocio de una organización". (OGC, 2011a, pág. 51).

Estos procesos tienen la finalidad de optimizar el negocio y son los siguientes:

- Gestión estratégica para servicios de TI, que es responsable de definir y mantener la perspectiva, posición, planes, y patrones de una organización con respecto a sus servicios y la gestión de los mismos.
- Gestión del portafolio de servicios, que se encarga de las decisiones de realizar un servicio o no. Estas decisiones atañen a los servicios y a la asignación de los activos de servicio.
- Gestión financiera para servicios de TI, que se encarga de gestionar los fondos y de asegurar su buena administración.
- Gestión de demanda, que analiza las fuentes de la demanda de un servicio para identificar sus patrones, es decir, busca anticipar o influenciar la demanda.

- Gestión de relaciones del negocio, que permite enlazar al proveedor y al cliente con la estrategia misma.

Estos procesos ayudan a determinar cuáles servicios son viables y cuáles no.

B. Diseño de Servicio

"Incluye el diseño de los servicios, las prácticas regulatorias, las políticas y procesos requeridos para llevar a cabo la estrategia del proveedor de servicios y facilitar la introducción de servicios en ambientes que tienen soporte". (OGC, 2011b, pág. 37)

Estos procesos ayudarán al diseño de un servicio nuevo o la mejora de uno ya existente:

- Coordinación del diseño, encargado de coordinar todas las actividades de diseño de servicios, procesos y recursos.
- Gestión del catálogo de servicios, se encarga de proporcionar y mantener el catálogo de servicios y de asegurar que esté disponible para aquellos que estén autorizados a acceder a él.
- Gestión de niveles de servicio, responsable de negociar acuerdos de nivel de servicios alcanzables y de asegurar que estos se cumplan.
- Gestión de capacidad, responsable de asegurar que la capacidad de los servicios de TI y la infraestructura de TI puedan cumplir con los requerimientos acordados, relacionados con la capacidad y el desempeño de una manera rentable y oportuna.
- Gestión de disponibilidad, se encarga de asegurar que los servicios de TI cumplan con las necesidades actuales y futuras de disponibilidad del negocio de una manera rentable y oportuna.
- Gestión de continuidad de servicios de TI, se encarga de gestionar los riesgos que podría afectar seriamente los servicios de TI.
- Gestión de seguridad de la información, responsable de asegurar que la confidencialidad, integridad y disponibilidad de los activos, información, datos y servicios de TI de una organización satisfagan las necesidades acordadas del negocio.
- Gestión de proveedores, responsable de asegurar que todos los contratos y acuerdos con proveedores apoyen las necesidades del negocio y que todos los proveedores cumplan sus compromisos contractuales.

C. Transición de Servicio

"Incluye una serie de procesos que son la guía para el desarrollo y la mejora de las capacidades para hacer la transición de servicios nuevos o modificados en ambientes que tienen soporte". (OGC, 2011c, pág. 43)

Y se asegura que los servicios nuevos, modificados o retirados satisfagan las expectativas del negocio, tal como se documenta en las etapas de estrategia y diseño del servicio dentro de su ciclo de vida.

Incluye los siguientes procesos:

- Planificación de la transición y soporte, provee la planeación para la transición del servicio y coordinación de los recursos que sean requeridos.
- Gestión de cambios, se encarga de controlar el ciclo de vida de todos los cambios, permitiendo que se realicen cambios que son beneficiosos, minimizando la interrupción de servicios de TI
- Gestión de activos de servicio y configuración, responsable de asegurar que los activos requeridos, para entregar servicios, estén debidamente controlados, y que haya información precisa y confiable sobre esos activos.
- Gestión de liberación e implementación, responsable de la planificación, programación y control de la construcción, prueba e implementación de liberaciones y de proporcionar nuevas funcionalidades que son requeridas por el negocio al tiempo que protege la integridad de los servicios existentes.
- Validación y pruebas del servicio, responsable de la validar y probar un servicio de TI nuevo o modificado.
- Evaluación de cambio, es un proceso genérico que considera si el desempeño es aceptable, genera valor, es adecuado y si se puede proceder a la implementación.
- Gestión del conocimiento, responsable de asegurar que la información correcta sea entregada en el lugar apropiado o a la persona adecuada en el tiempo correcto para la toma de decisiones informadas.

D. Operación de Servicio

“La fase de operación del servicio coordina y lleva a cabo las actividades y procesos requeridos para entregar y gestionar servicios en los niveles acordados con los usuarios de negocio y clientes”. (OGC, 2011d, pág. 35)

Esta fase también gestiona la tecnología que se utiliza para entregar y operar los servicios de soporte. Incluye los siguientes procesos y funciones:

Procesos:

- Gestión de eventos, tiene como propósito detectar eventos, darles sentido y determinar las acciones de control adecuadas. Es la base para el monitoreo y control operacional.
- Gestión de incidente, asegura que se restablezca la operación normal de servicio lo antes posible y se minimice el impacto al negocio.
- Cumplimiento de solicitudes, responsable de proporcionar un canal para recibir las solicitudes de los usuarios y servicios estándares, y mantener la satisfacción de usuarios y clientes con eficiencia y manejo profesional de todas las solicitudes de servicio.
- Gestión de problemas, previene proactivamente la ocurrencia de incidentes y minimiza el impacto de los incidentes que no se pueden prevenir.
- Gestión de acceso, responsable de permitir que los usuarios hagan uso de los servicios de TI, datos u otros activos. La gestión de acceso ayuda a proteger la confidencialidad, integridad y disponibilidad de los activos, garantizando que sólo los usuarios autorizados pueden accederlos o modificarlos.

Funciones:

- Service desk, es el único punto de contacto entre el proveedor de servicios y los usuarios. Un service desk típico maneja incidentes y solicitudes de servicio y también maneja la comunicación con los usuarios.
- Gestión técnica, responsable de proporcionar las competencias técnicas para dar soporte a los servicios de TI y a la gestión de la infraestructura de TI. La gestión técnica define los roles de los grupos de soporte, así como las herramientas, procesos y procedimientos requeridos.

- Gestión de operaciones de TI, responsable de realizar las actividades diarias necesarias para gestionar los servicios TI y dar el soporte a la infraestructura de TI. Esta gestión incluye el control de operaciones de TI y la gestión de instalaciones.
- Gestión de aplicaciones, da soporte a los procesos de negocio de la organización ayudando a identificar requerimientos de funcionalidad y utilidad para el software de aplicación.

2.2.4. ISO/IEC 27035:2011

Esta norma forma parte de los estándares relacionados a la Seguridad de la Información. En especial esta norma se enfoca en la implementación de procesos para la gestión de incidentes de seguridad de la información. Su implantación permite establecer procedimientos para prevenir, tratar y responder ante cualquier evento que afecte los activos e información de la organización.

Una amenaza actúa de forma no deseada para explotar vulnerabilidades de los sistemas de información, servicios o redes, produciendo la ocurrencia de eventos de seguridad de la información y por ende causar potencialmente algún incidente no deseado a los activos de información expuestos por dichas vulnerabilidades.

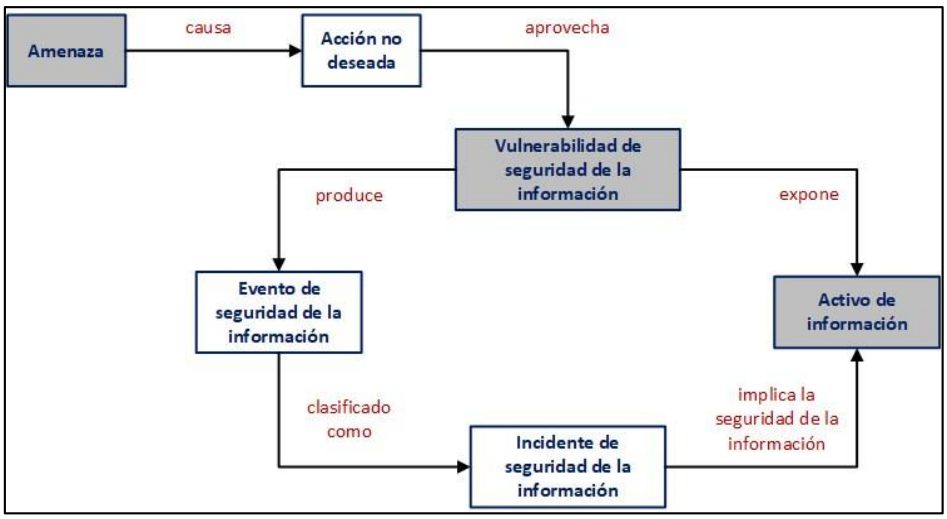


Figura 3. Relaciones en un incidente de seguridad de la información.
Fuente: Adaptado de International Organization for Standardization, 2013.

El establecer políticas de seguridad de la información o controles por sí solo no da la garantía de una protección de la información, sistemas de información, servicios o redes. Las vulnerabilidades residuales pueden hacer a la seguridad ineficaz y permitir la existencia de incidentes de seguridad que podrían producir diferentes grados de daños a la organización.

Además, constantemente las amenazas evolucionan, de este modo aumentando el grado de riesgo que afronta la organización. Por lo tanto, es necesario que toda organización tenga un enfoque estructurado y planificado para:

- Detectar, informar y evaluar los incidentes de seguridad de la información.
- Responder a incidentes de seguridad de la información, incluida la activación de controles apropiados para la prevención, reducción y recuperación de los impactos (por ejemplo, en el apoyo a las áreas de gestión de crisis).
- Reportar vulnerabilidades de seguridad de la información que aún no han sido explotadas para causar eventos de seguridad de la información y posiblemente incidentes de seguridad de la información, y evaluarlos y tratarlos apropiadamente.
- Aprender de los incidentes y vulnerabilidades de seguridad de la información, instituir controles preventivos y mejorar el enfoque general de la gestión de incidentes de seguridad de la información.

La gestión de incidentes de seguridad de la información se compone de cinco fases:

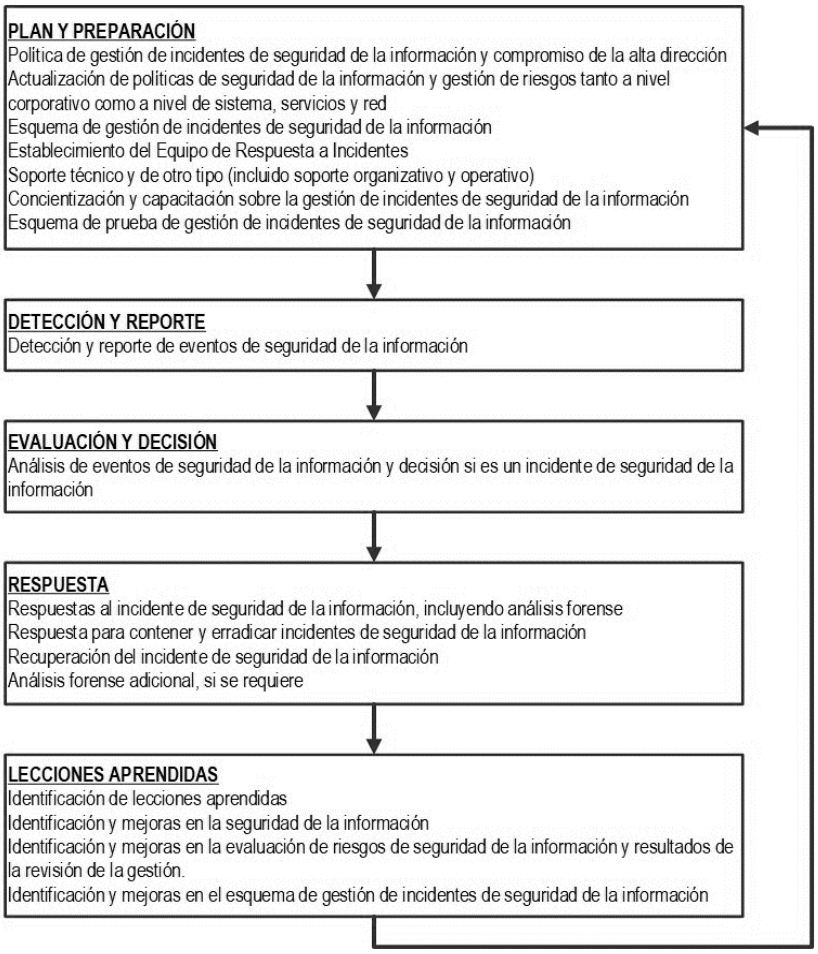


Figura 4. Fases de la gestión de incidentes de seguridad de la información. Fuente: ISO, 2013.

2.2.5. Evaluación de la solución

Ya que esta investigación tiene como objetivo mejorar el proceso de gestión de incidentes con el diseño de un modelo de gestión de incidentes de Tecnologías de la Información, se ha tenido que decidir qué marcos de trabajo se adoptará para cumplir los objetivos propuestos. Por tal, se utilizará el estándar ISO/IEC 27035 el cual permite la implementación de sistemas de gestión de incidentes de seguridad de la información, ya que es necesario gestionar cualquier tipo de incidente que pueda materializarse y dañar a la universidad.

Adicionalmente es necesaria la mejora constante de los servicios de gestión de incidentes dados por la institución, por ende, ITIL v3.0 es la mejor propuesta para un enfoque de mejora de servicios.

2.3. Definición de términos básicos

- Amenaza: potencial causa de un incidente no deseado, que puede resultar en daño a un sistema u organización. (International Organization for Standardization, 2014, pág. 11)
- Ataque: intentar destruir, exponer, alterar, inutilizar, robar o ganar acceso no autorizado o hacer uso no autorizado de un activo. (International Organization for Standardization, 2014, pág. 1)
- Clasificación de incidente: proceso de asignar un incidente a una clase o tipo en base a criterios de priorización, tiempo de resolución y recursos necesarios. (International Organization for Standardization, 2014, pág. 8)
- Escalamiento: mecanismo utilizado para asegurar la resolución oportuna de un incidente, de modo que cada nivel asume cierto grado de complejidad. (International Organization for Standardization, 2014, pág. 11)
- Evento de seguridad: ocurrencia detectada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas, o una situación desconocida hasta el momento y que puede ser relevante para la seguridad. (International Organization for Standardization, 2014, pág. 3)
- Incidente de seguridad: único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa

de comprometer las operaciones de la organización y de amenazar la seguridad de la información. (International Organization for Standardization, 2014, pág. 5)

- Monitorear: acción que permite supervisar o controlar las operaciones realizadas utilizando medios físicos o a través de aplicaciones de software. (International Organization for Standardization, 2014, pág. 7)
- Priorización de incidente: secuencia con la que un problema o incidentes tiene que ser resuelto objetivamente, basándose en impacto y urgencia. (International Organization for Standardization, 2014, pág. 9)
- Proceso: conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados. (International Organization for Standardization, 2014, pág. 9)
- SIEM: (Security Information and Event Management – Gestión de Eventos y Seguridad de la Información) es un enfoque de la gestión de la seguridad que pretende dar una visión holística de la seguridad de Tecnologías de la Información de una organización. Un SIEM combina la gestión de la seguridad de la información (SIM – Security Information Management) y la gestión de eventos de seguridad (SEM – Security Event Management) en un sistema de gestión integral de seguridad. (Tibaquira Cortes, 2015, pág. 15)
- Sistema de Información: aplicaciones, servicios, activos de Tecnología de la Información, u otros componentes de manejo de información. (International Organization for Standardization, 2014, pág. 4)
- Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas. (International Organization for Standardization, 2014, pág. 13)

2.4. Hipótesis

El diseño de un modelo de gestión de incidentes de TI, contribuirá a mejorar los procedimientos de Seguridad de la Información en la Universidad de Lambayeque.

III. Materiales y métodos

3.1. Variables y métodos

Tabla 1. Variables de la investigación.

Variable Independiente	Modelo de gestión de incidentes de TI
Variable Dependiente	Incidentes de seguridad de la información

Fuente: Elaboración propia.

El siguiente cuadro muestra los indicadores a tener en cuenta en el momento de la medición:

Tabla 2. Operacionalización de las variables de la investigación.

Variable	Dimensión	Indicador	Instrumento para la evaluación	Escala
Modelo de gestión de incidentes de TI	Efectividad del diseño	Nivel de efectividad de los procedimientos y parámetros	Cuestionario	Escala Likert de 5 niveles
		Nivel de integración del modelo en la gestión de incidentes de la organización		
	Usabilidad del modelo	Grado de adecuación del modelo a las necesidades de la institución	Cuestionario	Escala Likert de 5 niveles
		Grado de usabilidad del modelo		
	Adaptabilidad del modelo	Nivel de adaptación al entorno operativo de la institución	Cuestionario	Escala Likert de 5 niveles
	Satisfacción de usuarios	Nivel de satisfacción por la información resultante del modelo	Cuestionario	Escala Likert de 5 niveles
Incidentes de seguridad de la información	Nivel de mejora en el proceso de gestión incidentes de seguridad	Satisfacción	Cuestionario	Escala Likert de 5 niveles

Fuente: Elaboración propia.

3.2. Tipo de estudio y diseño de investigación

Esta investigación se ha tipificado de la siguiente manera:

- Descriptiva: porque se detalló la situación actual de la Universidad de Lambayeque con relación a sus políticas y procedimientos para gestionar incidentes de TI y cómo se estuvo llevando a cabo los procesos de seguridad actualmente.
- Propositiva: porque esta investigación no tuvo como objetivo implementar el modelo de gestión de incidentes de TI, por las limitaciones que existen. Por lo cual, quedó como una propuesta de solución a los problemas de gestión de incidentes en la Universidad de Lambayeque.
- Correlacional: porque el modelo propuesto se evaluó en relación a su impacto sobre la gestión de incidentes de seguridad de la información.

El diseño del modelo lógico para la contrastación de la hipótesis es del tipo relacional, porque se tiene como propósito medir el grado de relación que existe entre las dos variables definidas:

X r Y

X: modelo de gestión de incidentes de TI

Y: incidentes de seguridad de la información en la Universidad de Lambayeque

r: grado de influencia (impacto) de la variable X sobre Y

3.3. Población y diseño de investigación

Las áreas de la institución (funcionarios de estas) que están directamente relacionadas y tiene la capacidad y autoridad de evaluar el modelo de gestión propuestos son:

Tabla 3. Distribución de usuarios de TI en la Universidad de Lambayeque.

Tipo de usuario	**N° de usuario**
Personal de la oficina de Cómputo e Informática	4
Docentes de la Escuela Profesional de Ingeniería de Sistemas	6
Personal Administrativo	10
TOTAL	**20**

Fuente: Elaboración propia.

Ya que en la siguiente tesis se pretendió evaluar el diseño de un modelo de gestión, se determinó desarrollar un cuestionario para dicha evaluación. Por lo cual, se seleccionó al

personal responsable de gestionar las Tecnologías de la Información y docentes con el conocimiento y la experiencia en el tema.

3.4. Métodos, técnicas e instrumentos de recolección de datos

Las técnicas para la recolección de datos fueron las siguientes:

a. Encuesta: se aplicó una encuesta a los funcionarios, docentes y personal administrativo, los cuales evaluaron el modelo de gestión propuesto en base a las dimensiones establecidas. La selección de los profesionales se basó en la capacidad y autoridad para gestionar las Tecnologías de la Información (Anexo N° 3).

b. Análisis documental: se revisó documentos estratégicos, administrativos y legales pertenecientes a la institución. Además, se realizó la revisión de la norma 27035.

c. Entrevistas: las entrevistas sirvieron para obtener información de los procedimientos para la evaluación y seguimientos de los controles establecidos para la protección de los activos tecnológicos considerados en esta investigación. Las entrevistas se aplicaron a funcionarios, los cuales tenían responsabilidad y autoridad en la gestión de la seguridad de TI y de la información.

3.5. Procesamiento de datos y análisis estadístico

Para el procesamiento de datos se hizo uso del software IBM SPSS Statistics y Microsft Excel y la Regresión Lineal Múltiple como metodología para la contrastación de la hipótesis.

IV. Resultados

4.1. Análisis de la situación actual de la institución

4.1.1. Descripción de la institución

La Universidad de Lambayeque está ubicada en la ciudad de Chiclayo. Es una institución académico-administrativa privada, orientada a la formación académica de personas.

Fue creada el 14 de enero del 2010 mediante la resolución N° 10-2010-CONAFU, expedida por la ex Comisión Nacional para la Autorización de Funcionamiento de las Universidades (CONAFU) y dentro del marco de la nueva Ley Universitaria (Ley N° 30220).

La Universidad de Lambayeque cuenta con dos facultades y cinco escuelas profesionales, tal como se muestra en la siguiente imagen:

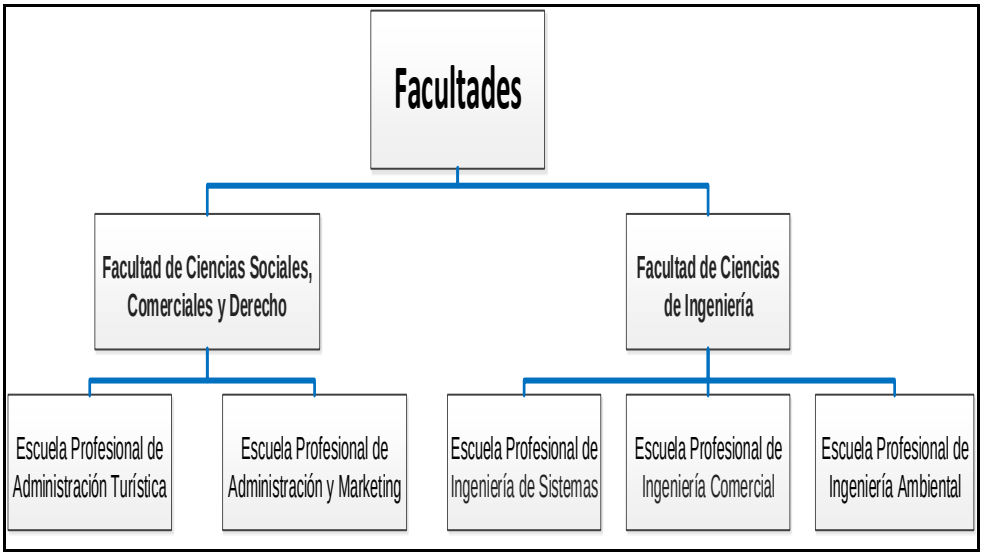


Figura 5. Distribución de Facultades y Escuelas Profesionales.
Fuente: Elaboración propia.

La Universidad de Lambayeque cuenta con un área administrativa/ejecutora de apoyo, llamada Cómputo e Informática, encargada del procesamiento y tratamiento de información proveniente de los órganos internos de dicha institución.

Las principales funciones de dicha área son las siguientes:

- Mantener la confidencialidad, integridad y disponibilidad de los sistemas informáticos e información que hace uso las áreas administrativas y académicas.
- Procesar información de acuerdo a la ejecución de procedimientos y planes estudiantiles.
- Desarrollar funcionalidades en los sistemas informáticos de acuerdo a los requerimientos del área administrativa y académica.
- Solucionar errores y dar mantenimiento a los sistemas informáticos.
- Apoyar, verificar y coordinar las actividades de procesamiento de matrícula, emisión de actas, estadística académica y los exámenes de admisión de la universidad.
- Brindar apoyo a los diversos sistemas administrativos y académicos en el procesamiento automático de datos.
- Gestionar la información de pagos de pensiones y matrículas con las entidades bancarias.
- Emitir informes periódicos relacionados con el área de su competencia.

El área de Cómputo e Informática tiene una unidad llamada Telemática, la cual se encarga de:

- Dar solución a problemas de hardware y software en los equipos informáticos.
- Asistir y manejar los incidentes de TI que se generan en las diferentes áreas.
- Manejar la logística de la parte técnica informática.
- Dar mantenimiento a los equipos informáticos.

4.1.2. Distribución geográfica de la institución

La Universidad de Lambayeque se ubica geográficamente en la calle Tacna N° 065, en el distrito de Chiclayo, provincia de Chiclayo. Tal como se muestra en la imagen.

Figura 6. Ubicación de la UDL.
Fuente: Google Maps, 2019.

4.1.3. Estructura organizacional de la institución

La Universidad de Lambayeque cuenta con la siguiente estructura organizacional.

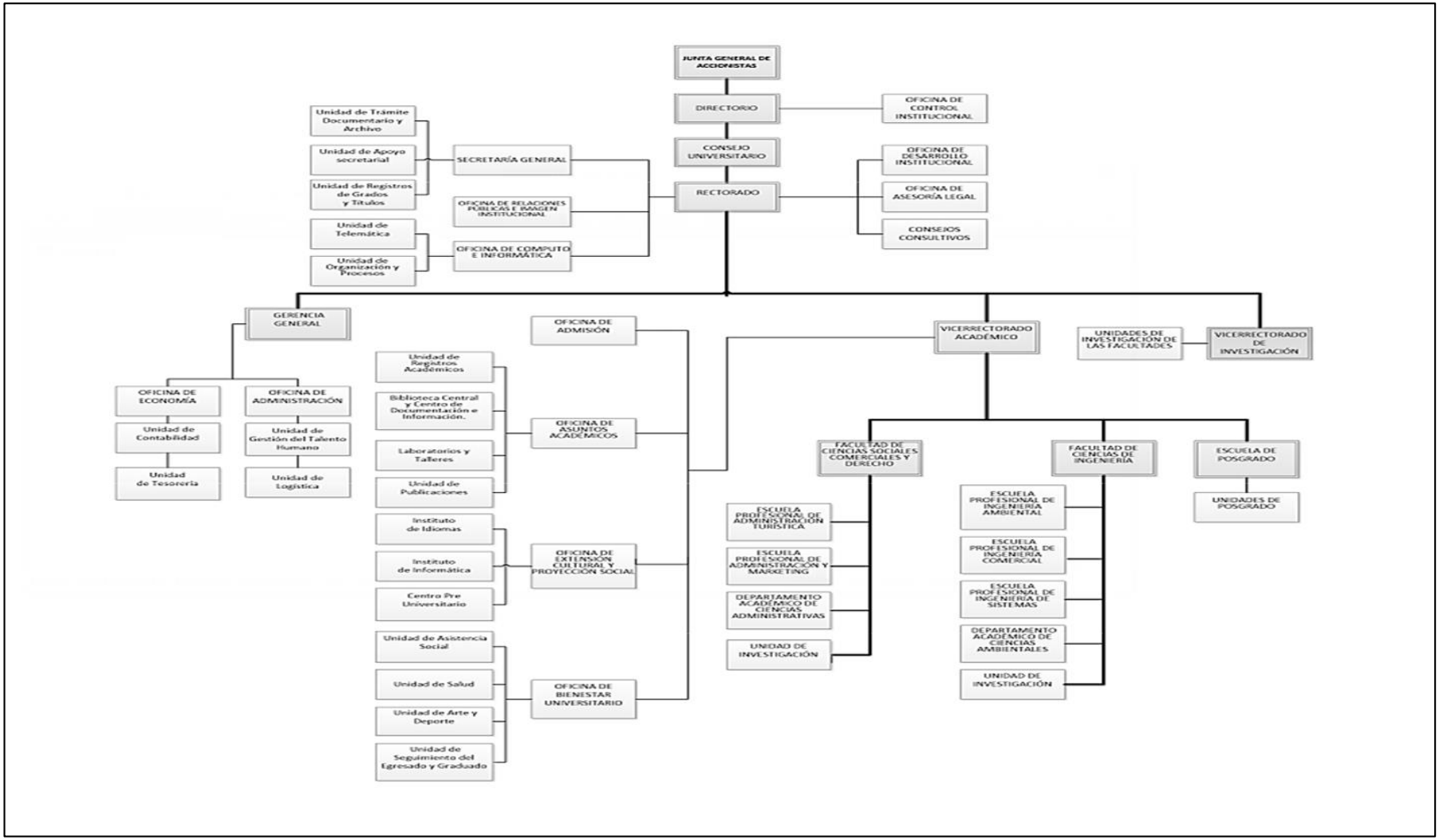


Figura 7. Organigrama de la UDL.
Fuente: Plan Estratégico, 2017.

Como se puede observar, la oficina de Cómputo e Informática es una unidad orgánica dependiente directamente del Rectorado. Por lo tanto, tiene un alto grado de participación, negociación y responsabilidad en el más alto nivel de la institución. Su ámbito de operación es a nivel de toda la institución.

La oficina de Cómputo e Informática está compuesta por dos unidades: Unidad de Organización y Procesos y Unidad de Telemática.

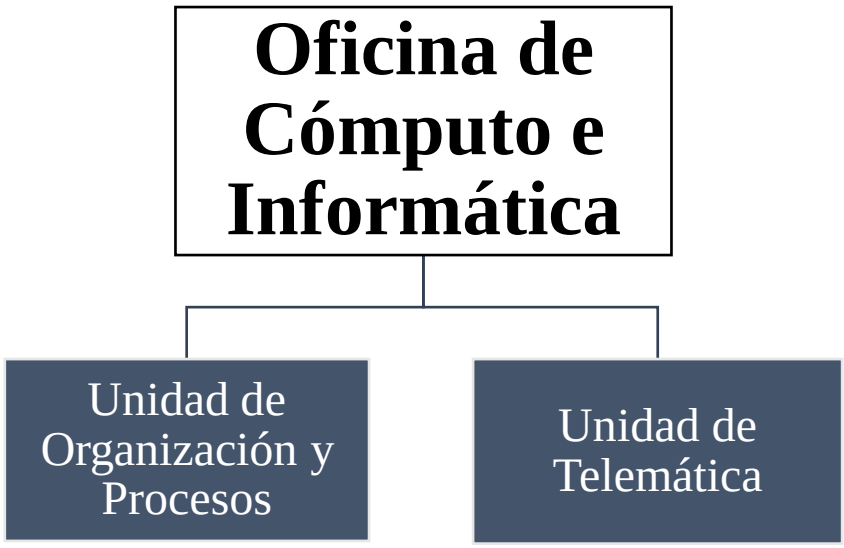


Figura 8. Organigrama del área de TI de la UDL.
Fuente: Plan Estratégico, 2017.

4.1.1. Servicios que ofrece la institución

Dentro de sus principales servicios figuran:

- Página web
- Servidor FTP
- Servidor de archivos (repositorio)
- Aplicación web académica (estudiantes)
- Alquiler de aulas y laboratorios multimedia
- Acceso a Internet, etc.

4.1.2. Infraestructura tecnológica

La Universidad de Lambayeque cuenta con una infraestructura tecnológica detallada en los siguientes cuadros.

a. Hardware

Actualmente la institución cuenta con la siguiente infraestructura tecnológica:

Tabla 4. Detalles de los servidores con los que cuenta la UDL.

N°	Sistema operativo	Descripción		Servicio
1	OpenSuse 42.1	FABRICANTE	HP	Servidor de Gestión Académica
		MODELO	ProLiant DL380	
		PROCESADOR	Intel Xeon CPU X5550 @ 2.67 GHz (2 sockets)	
		MEMORIA	2 GB	
		TIPO DE SISTEMA	OS de 32 bits	
2	OpenSuse 42.1	FABRICANTE	HP	Servidor de Campus Virtual
		MODELO	ProLiant DL380	
		PROCESADOR	Intel Xeon CPU X5550 @ 2.67 GHz (2 sockets)	
		MEMORIA	2 GB	
		TIPO DE SISTEMA	OS de 32 bits	
3	OpenSuse 42.1	FABRICANTE	HP	Biblioteca
		MODELO	ProLiant DL380	
		PROCESADOR	Intel Xeon CPU X5550 @ 2.67 GHz (2 sockets)	
		MEMORIA	2 GB	
		TIPO DE SISTEMA	OS de 32 bits	
4	OpenSuse 42.1	FABRICANTE	HP	Instituto de Idiomas
		MODELO	ProLiant DL380	
		PROCESADOR	Intel Xeon CPU X5550 @ 2.67 GHz (2 sockets)	
		MEMORIA	2 GB	
		TIPO DE SISTEMA	OS de 32 bits	
5	OpenSuse 42.1	FABRICANTE	HP	Instituto de Informática
		MODELO	ProLiant DL380	
		PROCESADOR	Intel Xeon CPU X5550 @ 2.67 GHz (2 sockets)	
		MEMORIA	2 GB	
		TIPO DE SISTEMA	OS de 32 bits	
6	OpenSuse 42.1	FABRICANTE	HP	
		MODELO	ProLiant DL380	

	PROCESADOR	Intel Xeon CPU X5550 @ 2.67 GHz (2 sockets)	Base de Datos Principal
	MEMORIA	2 GB	
	TIPO DE SISTEMA	OS de 32 bits	

Fuente: Elaboración propia.

Además, cuenta con el siguiente equipamiento:

Tabla 5. Equipos de cómputo y red con los que cuenta la UDL.

Dispositivo	**Cantidad**
ESTACIONES DE TRABAJO	200
SWITCHS	28
ACCESS POINTS	12
MODEMS – ROUTERS	3

Fuente: Elaboración propia.

b. Software

Tabla 6. Software usado en la UDL.

Tipo	**Software**
SERVIDOR	Linux OpenSuse 42.1
CLIENTE	Windows 7 Ultimate y Windows XP
GESTOR DB	MYSQL
LENGUAJE DE DESARROLLO	Python – Framework Django 1.8 y 3.4
ANTIVIRUS	Norton Antivirus, Panda Antivirus y Kaspersky Antivirus.
FIREWALL	Linux Zentyal

Fuente: Elaboración propia.

c. Redes y comunicaciones

Actualmente la institución cuenta con tres líneas de internet:

- Fibra 25 Mbps: usada exclusivamente para los servicios web (aplicaciones) que ofrece la institución.

- DSL 40 Mbps y HFC 60 Mbps: usadas para el acceso a internet de las redes administrativa y académica, configuradas con balanceo de carga.

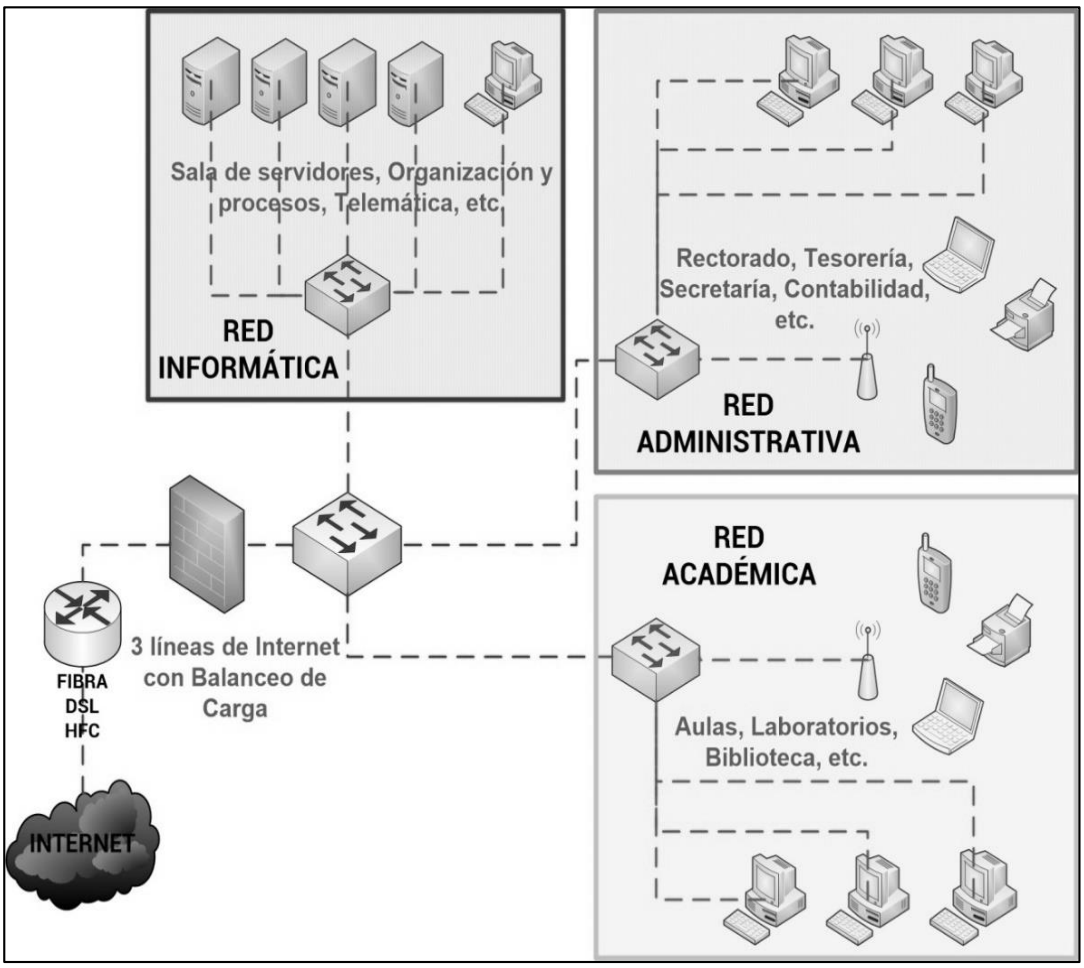


Figura 9. Infraestructura de red de la UDL.
Fuente: Elaboración propia.

4.1.3. Sistemas de Información

La Universidad de Lambayeque cuenta con sistemas de información transaccionales tales como:

a. Sistema de Gestión Académica (Acadsis)
b. Sistema de Biblioteca
c. Sistema de Trámite Documentario
d. Sistema del Instituto de Idiomas
e. Sistema del Instituto de Informática
f. Campus Virtual (alumnos y docentes)

Cabe mencionar que todos los sistemas informáticos han sido desarrollados por la oficina de Cómputo e Informática y que el acceso interno a estos está controlado mediante listas de direccionamiento lógico que gestiona el firewall.

4.1.4. Conformación del personal de TI

La oficina de Computo e Informática cuenta con un personal que suple los puestos de:

Tabla 7. Personal de la oficina de Cómputo e Informática.

Recurso humano	Cantidad
Jefe de área	1
Desarrollo de sistemas	
○ Analista programador	1
○ Programador de apoyo	1
Telemática	
○ Especialista en soporte	1
Organización y Procesos	
○ Analista de organización y procesos	1
TOTAL	**5**

Fuente: Elaboración propia.

4.1.5. Descripción del procedimiento actual de la gestión de incidentes de Tecnologías de la Información

Actualmente no existe un procedimiento estandarizado o aprobado para la gestión de incidentes de seguridad de la información. Sin embargo, para dicha gestión se aplica un procedimiento que se ha establecido "empíricamente" como consecuencia de la exigencia de dar solución a dichos incidentes. La actual gestión se desarrolla de la siguiente manera:

- El usuario que detecta un incidente o evento anormal, contacta al encargado de la unidad de Telemática a través de una llamada o de un correo electrónico y reporta el evento.
- El encargado de la unidad de Telemática acude al área, realiza unas preguntas al usuario que reportó para iniciar el diagnóstico y procede a manipular el equipo de cómputo para comprobar la ocurrencia de los eventos.

- El encargado de la unidad de Telemática, luego de diagnosticar y de acuerdo a la gravedad, dará solución al incidente en la misma área o llevará el equipo a la oficina de la unidad de Telemática.
- En caso el incidente no pueda ser resuelto, solicitará ayuda a su jefe superior.

El encargado de la unidad de Telemática es el responsable, según sus funciones, de dar respuesta a los diferentes incidentes y problemas en equipos de cómputo que ocurran en la institución.

En conclusión, el actual procedimiento no cuenta con etapas como registro, clasificación, escalonamiento o lecciones aprendidas. La falta de planificación e implementación de procedimientos alineados a estándares y buenas prácticas para la gestión de incidentes de seguridad, es debida en gran medida a que aún no han sido afectados por incidentes que hayan generado gran impacto. Sin embargo, en este contexto en que día a día grandes empresas de diferentes sectores son víctimas de incidentes, es vital saber cómo actuar y responder ante la materialización de una amenaza.

4.2. Diseño del proceso de gestión de incidentes de Tecnologías de la Información

Los siguientes parámetros se desarrollaron y definieron colectivamente con las unidades de Organización y Procesos y Telemática. Además, para la construcción de los requisitos y definición de las fases del modelo se tuvo en cuenta el estándar ISO 27035 y el framework ITIL v3:

4.2.1. Preparación

Para lograr una correcta operación del proceso de gestión de incidentes de seguridad de la información se debe desarrollar actividades de planificación y preparación. Estas actividades previas se refieren a medidas proactivas que le permitan a la institución estar preparados para una gestión de incidentes eficaz.

Por lo cual, es necesario que el personal responsable de administrar las Tecnologías de la Información y la alta dirección, con el apoyo de las diferentes áreas de la institución, desarrollen las siguientes actividades:

A. Formular y producir una política de gestión de incidentes de seguridad de la información.

B. Desarrollar un plan para la ejecución de análisis de riesgos y la posterior gestión de los mismos.
C. Establecer un equipo de respuesta a incidentes.
D. Establecer un plan para la actualización de software.
E. Asegurar las plataformas tecnológicas y redes.
F. Establecer un plan de concientización y comunicación sobre la gestión de incidentes y sus beneficios a todo el personal.

Además, es necesario contar con herramientas y sistemas hardware y software especializado y dedicado al manejo de incidentes que permitan recolectar información/evidencia, analizar, mitigar y erradicar amenazas.

Es importante también para robustecer la gestión de incidentes tener recursos que facilitarán la fase de análisis como:

- Contar con un diagrama de red que permita ubicar rápidamente los recursos de TI.
- Preparar una Línea – Base del comportamiento de red normal que incluya: horarios de utilización, puerto – protocolo de red, IP que generan mayor cantidad de tráfico, etc.
- Listado de puertos conocidos y de puertos usados para lanzar ataques.
- Contar con información de sistemas críticos: dirección IP, configuración, usuarios, nombre, parches, etc.
- Contar con un sistema que permita Gestionar los Eventos e Incidentes de Seguridad (SIEM).

4.2.2. Detección y reporte

Esta es la primera fase operativa de la gestión de incidentes de seguridad de la información que tiene como objetivo desarrollar procedimientos claros de comunicación y un punto de contacto (Mesa de Ayuda) el cuál recibirá las alertas y reportes de los usuarios ante un posible incidente de seguridad.

Un administrativo, docente, estudiante o tercero que tiene la sospecha o certeza de la ocurrencia de algún incidente de seguridad, tendrá que completar el formato “Reporte de Incidente de Seguridad de la Información” (Anexo A) y entregar físicamente o enviarlo por el correo

electrónico a la unidad de Telemática para que Mesa de ayuda realice el registro y la toma de decisiones correspondientes.

La persona que diligencia el formato "Reporte de Incidente de Seguridad de la Información" debe hacerlo con la mayor cantidad posible de información. Los campos del formato son:

- Fecha de reporte: fecha en la que se procede a diligenciar y entregar el reporte a la unidad de Telemática. Se debe tener en cuenta el formato DD/MM/AAAA.
- Hora de reporte: hora en la que se procede a diligenciar y entregar el reporte a la unidad de Telemática. Se debe tener en cuenta el formato HH:MM.
- Nombres y apellidos: nombre completo del administrativo, docente, estudiante o tercero que diligencia el reporte.
- Cargo: cargo del administrativo, docente, estudiante o tercero que diligencia el reporte.
- Área/oficina: área u oficina a la que pertenece el administrativo, docente, estudiante o tercero que diligencia el reporte.
- Correo electrónico: correo electrónico del administrativo, docente, estudiante o tercero que diligencia el reporte.
- Teléfono institucional: número de teléfono institucional del administrativo o docente que diligencia el reporte.
- Teléfono personal: número de teléfono personal del administrativo, docente, estudiante o tercero que diligencia el reporte.
- Fecha en la que observó el incidente: fecha en la que el administrativo, docente, estudiante o tercero observó la ocurrencia del incidente a reportar. Se debe tener en cuenta el formato DD/MM/AAA.
- Hora en la que observó el incidente: hora en la que el administrativo, docente, estudiante o tercero observó la ocurrencia del incidente a reportar. Se debe tener en cuenta el formato HH:MM.
- Opciones del tipo de incidente reportado: se debe seleccionar y marcar aquellas opciones que se considere han ocurrido. En caso ninguna de las opciones represente al incidente que se quiere reportar, se debe marque la opción "otro" y hacer una pequeña descripción.

- Descripción del incidente: en este campo el administrativo, docente, estudiante o tercero debe responder a las siguientes preguntas: ¿Qué ocurrió? ¿Cómo ocurrió? ¿Tomó alguna acción?

Una vez recibido el reporte, por cualquiera de las vías disponibles, Mesa de Ayuda deberá asegurarse que el incidente aún no haya sido registrado. Esto con el fin de evitar duplicaciones innecesarias.

De confirmar que el incidente no esté registrado, Mesa de Ayuda debe registrar el formato "Reporte de Incidente de Seguridad de la Información", solicitar cualquier explicación a la persona que reportó el incidente y recopilar información necesaria disponible de diferentes fuentes, si fuera necesario. Luego de esto, Mesa de Ayuda debe proceder a realizar la evaluación para determinar si la solicitud de reporte amerita clasificarse como un incidente o es una falsa alarma (falso positivo). Si se determinara que es una falsa alarma, Mesa de Ayuda debe informar sobre esta decisión a la persona que diligenció el reporte.

Además, si se detecta que el incidente pudiera afectar a otros usuarios, es importante que sean notificados inmediatamente para que comprenda que su flujo de trabajo puede verse afectado.

4.2.3. Evaluación y análisis

4.2.3.1. Categorización de los incidentes

La siguiente categorización de incidentes de seguridad de la información se diseñó teniendo en cuenta el tipo de amenaza y las formas más comunes de estos. Adicionalmente se ha incluido en esta lista, incidentes acontecidos en el interior de la institución, con el fin de abarcar una mayor cantidad de incidentes a gestionar. Dicho lo anterior, está no es una categorización exhaustiva y puede requerir la incorporación de nuevos elementos según sea necesario.

Tabla 8. Categorías de incidentes de seguridad de la información.

Categoría	Tipo de incidente
ACCESO NO AUTORIZADO	Suplantación de identidad del usuario
	Acceso no autorizado al sistema o red
	Interceptación de datos/información
	Robo o pérdida de activo de información

	Escaneos de vulnerabilidades/activos
	Explotación de vulnerabilidades
	Ataque de fuerza bruta
	Defacement Web
	Compromiso de cuentas de usuarios
	Exposición de datos personales
MODIFICACIÓN NO AUTORIZADA	Manipulación de configuraciones
	Manipulación de registros/logs de sistemas
	Modificación no autorizada de información
	Destrucción no autorizada de información
COMPROMISO DE LA DISPONOBILIDAD	Denegación de servicio
	Error humano
	Fallo del servicio de Internet o eléctrico
	Fallo (hardware/software)
	Uso inadecuado
USO INAPROPIADO DE RECURSO	Incumplimiento de políticas de SI
	Incumplimiento de requisitos legales
MULTICOMPONENTE	Difusión de software dañino (Malware)
	Ransomware
	Phishing
	Spam
	Daños por agua, fuego, electricidad
	Desastres naturales
	Sabotaje

Fuente: Elaboración propia.

4.2.3.2. Priorización del origen del incidente

Cuando hablamos del origen de un incidente, nos referimos al área o unidad donde este ha ocurrido. Como es evidente, no todas las áreas o unidades dentro de una institución tiene la misma importancia, ya que algunas manejan información crítica o la interrupción de esta afecta directamente un proceso core. Es por ello lo importante de clasificar cada área de la institución.

Además, esta clasificación nos permite, a la hora de tomar decisiones frente a un incidente, una mayor precisión en la asignación de recursos y mantener la continuidad de los procesos críticos de la universidad.

El siguiente cuadro muestra la priorización de las distintas áreas dentro de la universidad. Este cuadro se desarrolló con ayuda del Jefe de la oficina de Cómputo e Informática:

Tabla 9. Priorización de las áreas de la UDL.

Área	Sub-Área	Nivel Prioridad
DIRECTORIO	Oficina de Control Institucional	Alta
RECTORADO	Secretaria General	Crítica
	Oficina de Relaciones Públicas e Imagen Institucional	Alta
	Oficina de Cómputo e Informática	Crítica
	Oficina de Desarrollo Institucional	Media
	Oficina de Asesoría Legal	Alta
	Consejos Consultivos	Baja
GERENCIA GENERAL	Oficina de Economía	Crítica
	Oficina de Administración	Crítica
VICERRECTORADO ACADÉMICO	Oficina de Admisión	Media
	Oficina de Asuntos Académicos	Alta
	Oficina de Extensión Cultural y Proyección Social	Alta
	Oficina de Bienestar Universitario	Baja
	Faculta de Ciencias Sociales, Comerciales y Derecho	Media
	Faculta de Ciencias de Ingeniería	Media
	Escuela de Postgrado	Media
VICERRECTORADO DE INVESTIGACIÓN	Oficina de Investigación de las Facultades	Baja

Fuente: Elaboración propia.

4.2.3.3. Priorización de los incidentes

Para un correcto seguimiento, determinación de criticidad y asignación adecuada de recursos es importante establecer grados de criticidad e impacto que produciría un incidente de seguridad en la institución.

La priorización de un incidente se calcula en base a dos variables:

- **Impacto**: define la repercusión del incidente de acuerdo al daño que causa a los procesos del negocio y/o de la cantidad de usuarios perjudicados. A continuación, se muestra los niveles establecidos para este modelo:

Tabla 10. Escalas para determinar el nivel del impacto de los incidentes.

Impacto	Valor	Definición
CRÍTICO	4	Incidente que afecta la continuidad de uno o más procesos críticos y/o la mayoría de unidades de trabajos.
ALTO	3	Incidente que afecta determinadas funciones de los procesos críticos y/o a un grupo de unidades de trabajos o usuarios con funciones críticas.
MEDIO	2	Incidente que afecta a uno o más procesos no críticos de la institución y/o a un grupo de usuarios con funciones no críticas.
BAJO	1	Incidente que afecta de manera mínima a algún proceso no crítico y/o a algunas estaciones de trabajos.

Fuente: Elaboración propia.

- **Urgencia**: define el tiempo máximo que un usuario puede esperar a la resolución de un incidente, sin que sufra consecuencias importantes. En la siguiente tabla se muestra los niveles de urgencias establecidos para este modelo:

Tabla 11. Escalas para determinar el nivel de urgencia de los incidentes.

Urgencia	Valor	Definición
CRÍTICA	4	Incidente que requiere atención y la restauración de manera inmediata de uno o más procesos críticos.
ALTA	3	Incidente que requiere atención rápida ya que ha perjudicado parcialmente uno o más procesos críticos.
MEDIA	2	Incidente que requiere atención media por involucrar la continuidad parcial o total de un proceso no crítico.
BAJA	1	Incidente que no advierte atención de inmediato ya que no afecta la continuidad de ningún proceso de la institución.

Fuente: Elaboración propia.

A cada grado de urgencia se le ha asignado un tiempo determinado. Esta asignación permite distribuir adecuadamente los tiempos para la gestión de los incidentes y llevar un mejor control y seguimiento de sus estados.

A continuación, se muestra un cuadro con los tiempos máximos de atención y de cierre de un incidente, el cual fue elaborado con el personal de la oficina de Cómputo e Informática, teniendo como referencia los tiempos estándares recomendados y la criticidad del incidente:

Tabla 12. Tiempos para la atención y cierre de los incidentes.

Urgencia	Tiempos máximos	
	Atención	**Cierre**
Crítica	5 minutos	1 hora
Alta	15 minutos	2 horas
Media	30 minutos	3 horas
Baja	45 minutos	4 horas

Fuente: Elaboración propia.

Teniendo los valores definidos se aplicará la siguiente fórmula para establecer la escala de priorización de incidentes:

Nivel prioridad = IMPACTO x URGENCIA

En el siguiente cuadro se muestra los resultados del diagrama de prioridades de incidentes establecido para la Universidad de Lambayeque:

Tabla 13. Mapa de calor para determinar el nivel de prioridad de un incidente en función del impacto y la urgencia.

Nivel de Prioridad			Urgencia			
			Crítica	Alta	Media	Baja
			4	3	2	1
Impacto	Crítico	4	**16**	**12**	**8**	**4**
	Alto	3	**12**	**9**	**6**	**3**
	Medio	2	**8**	**6**	**4**	**2**
	Bajo	1	**4**	**3**	**2**	**1**

CRÍTICO | MAYOR | MEDIO | MENOR

Fuente: Elaboración propia.

El siguiente cuadro muestra la priorización de los incidentes establecidos en la Universidad de Lambayeque y los tiempos máximos determinados tanto para la atención como para el cierre de mismo. Esta priorización se desarrolló con el personal de la oficina de Cómputo e Informática.

Tabla 14. Priorización de los incidentes.

Tipo de incidente	Tiempo de atención	Tiempo de cierre	Nivel prioridad
Acceso no autorizado al sistema o red	5 minutos	1 hora	CRÍTICO
Robo o pérdida de activo de información			
Explotación de vulnerabilidades			
Modificación no autorizada de información			
Exposición de datos personales			
Fallo del servicio de Internet o eléctrico			
Difusión de software dañino (malware)			
Destrucción no autorizada de información			
Ransomware			
Suplantación de identidad de usuario	15 minutos	2 horas	MAYOR
Escaneos de vulnerabilidades/activos			
Manipulación de configuraciones			
Denegación de servicio			
Incumplimiento de políticas de SI			
Interceptación de datos/información	30 minutos	3 horas	MEDIO
Ataque de fuerza bruta			
Compromiso de cuentas de usuarios			
Manipulación de registros/logs de sistemas			
Error humano			
Fallo (hardware/software)			
Uso inadecuado			
Incumplimiento de requisitos legales			
Phishing			
Daños por agua, fuego, electricidad			
Defacement Web	45 minutos	4 horas	MENOR
Spam			
Desastres naturales			
Sabotaje			

Fuente: Elaboración propia.

4.2.3.4. Escalonamiento

El escalonamiento implica establecer las instancias necesarias para resolver un incidente, es decir, disponer de diferentes niveles de atención, en caso el incidente no sea resuelto en primera línea.

Los tipos (criterios) de escalonamiento son:

- Escalonamiento funcional: implica la necesidad de involucrar a otra persona con mayor conocimiento.
- Escalonamiento jerárquico: implica la necesidad de involucrar a otra persona con mayor nivel de autoridad que tome decisiones no asignadas a ese nivel.
- Escalado por capacidad: implica la necesidad de otra persona o área con mayores recursos para responder a incidentes más complejos.

En la Universidad de Lambayeque se establecieron tres niveles de atención:

- Primer Nivel: a cargo de Mesa de Ayuda, el cual brindará inicialmente soporte en línea. Mesa de Ayuda es responsable de dar seguimiento a cada incidente hasta su cierre, así la atención sea escalada a otro nivel.
- Segundo Nivel: a cargo del encargado de la unidad de Telemática. Responsable de la gestión de la red, del sistema antivirus y de dar soporte técnico a los equipos de la universidad.
- Tercer Nivel: a cargo jefe de la oficina de Cómputo e Informática y desarrolladores. Cuenta con capacidad para negociar con proveedores externos y con todas las áreas de la universidad.

La siguiente imagen muestra el flujo que toma la respuesta a un incidente entre los diferentes niveles de escalonamiento establecidos:

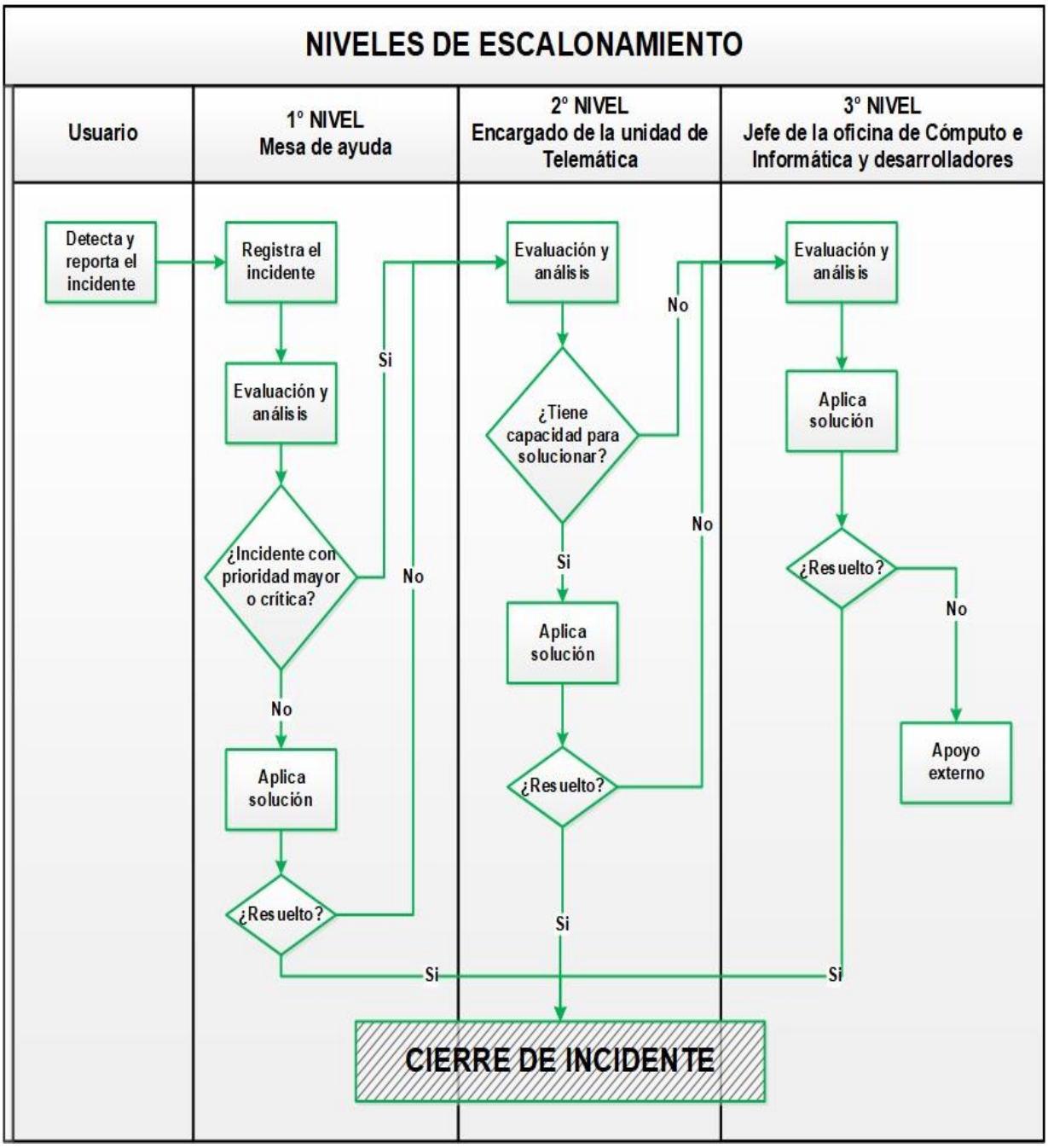


Figura 10. Flujo de decisiones entre los niveles de escalonamiento.
Fuente: Elaboración propia.

A continuación, se muestra un cuadro con los niveles de escalonamiento de acuerdo al nivel de prioridad del incidente para la toma de decisiones. Además, dicho cuadro se debe tener en cuenta para la notificación o información de los incidentes:

Tabla 15. Niveles de escalonamiento y responsables.

Origen de notificación de incidente	**Responsable de registro y seguimiento**	**Nivel de prioridad**	**Responsable de la gestión**
- Usuario - Jefe de Cómputo e Informática - Sistemas de detección de incidentes/eventos	Mesa de Ayuda (punto de contacto)	Crítico	Encargado de Telemática, Jefe de Cómputo Informática y desarrolladores (Notifica a la alta dirección)
		Mayor	Encargado de Telemática
		Media	Mesa de Ayuda y Encargado de Telemática
		Menor	Mesa de Ayuda

Fuente: Elaboración propia.

En el siguiente cuadro se detalla el escalonamiento que se hará a cada incidente, de acuerdo a su tipo:

Tabla 16. Niveles de escalonamiento de los incidentes.

			Nivel 1	**Nivel 2**	**Nivel 3**
Nivel de Prioridad	**Incidente**	**Tiempo de Atención 5 minutos**	**Tiempo de Cierre 0 minutos**	**Tiempo de Cierre 20 minutos**	**Tiempo de Cierre 40 minutos**
CRITICO	Acceso no autorizado al sistema o red	Mesa de Ayuda	Mesa de Ayuda	Encargado de la Unidad de Telemática	Jefe de la Oficina de Cómputo e Informática y Desarrolladores
	Robo o pérdida de activo de información				
	Explotación de vulnerabilidades				
	Modificación no autorizada de información				
	Exposición de datos personales				
	Fallo del servicio de Internet o eléctrico				
	Difusión de software dañino (malware)				
	Destrucción no autorizada de información				
Nivel de Prioridad	**Incidente**	**Tiempo de Atención 15 minutos**	**Tiempo de Cierre 0 minutos**	**Tiempo de Cierre 60 minutos**	**Tiempo de Cierre 60 minutos**
MAYOR	Suplantación de identidad de usuario	Mesa de Ayuda	Mesa de Ayuda	Encargado de la Unidad de Telemática	Jefe de la Oficina de Cómputo e Informática y Desarrolladores
	Escaneos de vulnerabilidades/activos				
	Manipulación de configuraciones				
	Denegación de servicio				
	Incumplimiento de políticas de SI				

Nivel de Prioridad	**Incidente**	**Tiempo de Atención 30 minutos**	**Tiempo de Cierre 60 minutos**	**Tiempo de Cierre 60 minutos**	**Tiempo de Cierre 60 minutos**
MEDIO	Interceptación de datos/información	Mesa de Ayuda	Mesa de Ayuda	Encargado de la Unidad de Telemática	Jefe de la Oficina de Cómputo e Informática y Desarrolladores
	Ataque de fuerza bruta				
	Compromiso de cuentas de usuarios				
	Manipulación de registros/logs de sistemas				
	Error humano				
	Fallo (hardware/software)				
	Uso inadecuado				
	Incumplimiento de requisitos legales				
	Phishing				
	Daños por agua, fuego, electricidad				
Nivel de Prioridad	**Incidente**	**Tiempo de Atención 45 minutos**	**Tiempo de Cierre 60 minutos**	**Tiempo de Cierre 90 minutos**	**Tiempo de Cierre 90 minutos**
BAJO	Defacement Web	Mesa de Ayuda	Mesa de Ayuda	Encargado de la Unidad de Telemática	Jefe de la Oficina de Cómputo e Informática y Desarrolladores
	Spam				
	Desastres naturales				
	Sabotaje				

Fuente: Elaboración propia.

4.2.4. Respuesta

4.2.4.1. Equipo de Respuesta a Incidentes

Para la fase de respuesta, es esencial contar con personal que cuente con experiencia y habilidades necesarias para manejar incidentes. Por lo cual, se debe establecer un grupo de profesionales que formen el Equipo de Respuesta a Incidentes. En el siguiente cuadro se detalla la conformación de dicho equipo:

Tabla 17. Equipo de Respuesta a Incidentes.

Equipo de Respuesta a Incidentes de Seguridad de la Información
1. Jefe de la oficina de Cómputo e Informática
2. Desarrolladores de aplicaciones y sistemas informáticos
3. Encargado de la unidad de Telemática
4. Encargado de Mesa de Ayuda
5. Operador de Mesa de Ayuda
6. Responsable del activo de información afectado

Fuente: Elaboración propia.

4.2.4.2. Respuesta a incidentes

En este punto es importante tener en cuenta lo siguiente:

- Mesa de Ayuda debe consultar la base de datos de incidencias para determinar si el actual incidente coincide con algún otro ya resuelto y aplicar el procedimiento establecido.
- Mesa de Ayuda debe determinar si la resolución del incidente escapa a sus capacidades. Si este fuera el caso, aplicar los protocolos de escalonamiento existentes y dejará a cargo la solución a algún integrante del Equipo de Respuesta a Incidentes, el cual será notificado automáticamente.
- El encargado de la unidad de Telemática debe recolectar evidencia del incidente reportado que pueda facilitar suficiente información en caso se requiera una investigación post incidente.

- Mesa de Ayuda debe de mantener una comunicación fluida con el encargado de aplicar la solución, con el objetivo de actualizar el estado del incidente. Para que de este modo los implicados dispongan de información exacta sobre el mismo.
- Mesa de Ayuda llevará el control del tiempo máximo de solución establecido a un incidente, mediante alertas enviadas por email, mensajes de texto o llamadas.
- En los casos en que algún sistema crítico sea afectado gravemente por un incidente, se debe considerar la congruencia de activar el Plan de Continuidad del Negocio.
- Si el incidente se presentara reiteradamente y no se halla una solución determinante al mismo, se procederá a notificar a la Gestión de Problemas para su análisis detallado.

4.2.4.3. Contención

Esta actividad busca contener y mitigar los efectos del incidente con la finalidad de que estos no se extiendan y pueda causar más daños a la información o activos de información. Provee de tiempo al equipo de respuesta a incidente para desplegar una estrategia de solución a medida.

Es por ello que se debe plantear estrategias, las cuales dependerán en gran medida de los siguientes factores:

- Recursos para desarrollar la estrategia.
- Duración de la solución.
- Necesidad de mantener la evidencia.
- Capacidad de mitigación de la estrategia frente al incidente.
- Criticidad de los activos afectados.
- Posible modo de actuación del atacante.

Algunas de las medias para contener los efectos de incidentes son:

- Aislar o desconectar un equipo o parte de una red del resto de redes de la organización.
- Si fuera el caso de un equipo crítico, se puede filtrar solo el tráfico legítimo a través de un firewall entre ese equipo y el resto de red.
- Si se logra conocer detalles técnicos del incidente, vectores de ataque, comportamiento, etc., es probable desarrollar medias ajustadas a cada circunstancia.
- Contactar con el fabricante del producto para obtener información sobre la instalación de parches u obtener soluciones alternativas.

- Suspender el acceso lógico y físico de usuarios a sistemas o información crítica. Además, cambiar las contraseñas de las credencias o apoyar a los usuarios a que lo hagan de una forma segura.

4.2.4.4. Erradicación

La erradicación implica el desarrollo de tareas planificadas que permitan eliminar cualquier rastro que ha dejado el incidente. Estas tareas deberán ser desarrollas según las características y efectos del incidente, especificando los responsables de la ejecución de dichas tareas.

Factores a tener en cuenta en el desarrollo de medidas para la erradicación:

- Experiencias anteriores.
- Pérdida económica.
- Posibles implicaciones legales.
- Efectividad de la estrategia.
- Recursos necesarios para aplicar la estrategia.
- Determinación de los procesos o activos comprometidos.

Algunas de las medias para erradicar los efectos de incidentes son:

- Análisis del antivirus a todo el sistema y particiones del disco duro.
- Comprobar la integridad de los datos mediante uso de hashes.
- Restaurar conexiones y privilegios de las credenciales paulatinamente.

4.2.4.5. Recuperación

La recuperación tiene como objetivo lograr el restablecimiento total de los servicios, el funcionamiento normal de los procesos y evitar que otros incidentes se sucedan con la misma causa. Esto implica no solo el desarrollo de medidas activas, sino también la aplicación de controles regulares.

Algunas medidas de recuperación son:

- Reinstalación de sistemas y servicios de una forma adecuada con el uso de copias seguras.
- Instalación de último parches y actualización de seguridad.

- Revisión de controles y medidas de seguridad.
- Test de los sistemas para detectar fallas y eventos que afecten la seguridad.

Durante el desarrollo de todo el proceso de respuesta es sumamente importante extraer datos y documentarlos adecuadamente, con el objetivo de diligenciar el Informe de Resolución de Incidente y elaborar las lecciones aprendidas.

Asimismo, es necesario desarrollar las siguientes actividades:

1. Ingresar el proceso de resolución a la base de datos de gestión de incidentes de seguridad de la información.
2. Confirmar la solución del incidente a los usuarios. Mesa de Ayuda es el encargado a través de un correo electrónico.
3. Si fuera necesario, la recategorización del incidente. A cargo de Mesa de Ayuda, además se deberá actualizar el Informe de Resolución de Incidente.
4. Cerrar el incidente. Mesa de Ayuda tiene a cargo esta actividad.

4.2.5. Actividades Post-incidente

4.2.5.1. Uso de datos e informe final

Los datos y evidencias extraídas en la solución de un incidente deberán almacenarse para generar reportes e información requerida en futuras investigaciones y producir e implementar controles preventivos más eficaces. Este almacenamiento debe ser hecho por el encargado de la unidad de Telemática.

Entre estos datos tenemos:

- Daños producidos.
- Número de incidentes reportados y gestionados.
- Constancia de ataques.
- Perjuicios generados por los incidentes.
- Recursos asignados a los incidentes.
- Vectores de ataque.
- Activos de información comprometidos.

El Informe de Resolución de Incidente deberá ser diligenciado por Mesa de Ayuda y el encargado de la unidad de Telemática, los cuales, se valdrán de los datos obtenidos durante el proceso de solución. Este informe debe facilitar la comprensión de las decisiones y medidas adoptadas a cualquier involucrado en la gestión del incidente. Asimismo, el informe debe incluir recomendaciones sobre mejoras de seguridad para evitar incidentes similares.

El Informe de resolución de incidente contiene los siguientes puntos:

1. Fecha de ocurrencia del incidente
2. Hora de ocurrencia del incidente
3. Fecha de notificación del incidente
4. Hora de notificación del incidente
5. Apellidos y nombres de la persona que reportó el incidente
6. Área donde labora la persona que reportó el incidente
7. Ocurrencia del incidente
8. Detalles del incidente
9. Daños producidos por el incidente
10. Tipo de incidente
11. Impacto del incidente
12. Urgencia del incidente
13. Nivel de criticidad del incidente
14. Nivel de escalonamiento
15. Declaración de incidente
16. Análisis de causa del incidente
17. Estados del incidente
18. Fecha de solución
19. Detalle de la solución
20. Recomendaciones para reforzar la seguridad

Luego que Mesa de Ayuda de por acabo la diligencia del informe, este se deberá enviar al jefe de la oficina de Cómputo e Informática mediante correo electrónico para su respectiva verificación y aprobación.

4.2.5.2. Lecciones aprendidas

El desarrollo de lecciones aprendidas implica el enfoque de ver más allá de un incidente, es decir, valerse de los datos extraídos en el actual proceso para obtener información que ayude a identificar la necesidad de controles o cambios de enfoque. Por lo cual, las lecciones aprendidas juegan un papel importante en la mejora del proceso de gestión de incidentes. Entre ellas podemos tomar en cuenta las siguientes:

- Desarrollar un plan de capacitación para los funcionarios de la institución sobre incidentes de seguridad, especialmente si se ha detectado amenazas con gran posibilidad de materializarse.
- Identificar tendencias o patrones.
- Identificar áreas de preocupación.
- Identificar donde se podrían implementar medidas preventivas para reducir la probabilidad de incidentes futuros.
- Identificar nuevos tipos de incidentes y amenazas.
- Identificar inconsistencia en los procedimientos.

4.2.5.3. Actualización de controles de seguridad de la información

El jefe de la oficina de Cómputo e Informática es el encargado de revisar cada Informe de Resolución de Incidente, específicamente las recomendaciones que aparecen en este. Es después de esta revisión donde se puede identificar si es necesario nuevos controles o modificar alguno de los existentes. Sin embargo, no todas las recomendaciones o requisitos de control pueden ser factibles desde el punto de vista financiero u operacional, por lo que se puede incluir como un objetivo a largo plazo mientas se desarrolla una solución más viable.

4.2.5.4. Manejo de evidencia

Es posible que luego del cierre de un incidente sea necesario realizar un análisis forense, por lo tanto, es importante que se apliquen controles que garanticen la confidencialidad, integridad y disponibilidad a la hora de almacenar evidencia. El encargado de la unidad de Telemática tiene la responsabilidad del almacenamiento físico de las evidencias bajo condiciones seguras y transparentes.

4.3. Diseño de procedimientos para la gestión de incidentes de Tecnologías de la Información

4.3.1. Diseño del flujo del proceso de gestión de incidentes de Tecnologías de la Información

A continuación, se describirá el flujo del proceso propuesto para la gestión de incidentes de TI que servirá como guía para la prevención, respuesta y mejora continua en la Universidad de Lambayeque. Para diseñar el proceso se tuvo en cuenta las características y capacidades con la que cuenta la oficina de Cómputo e Informática, por lo cual, este se diseñó a un nivel inicial. Además, se tuvo en cuenta el estándar ISO 27035.

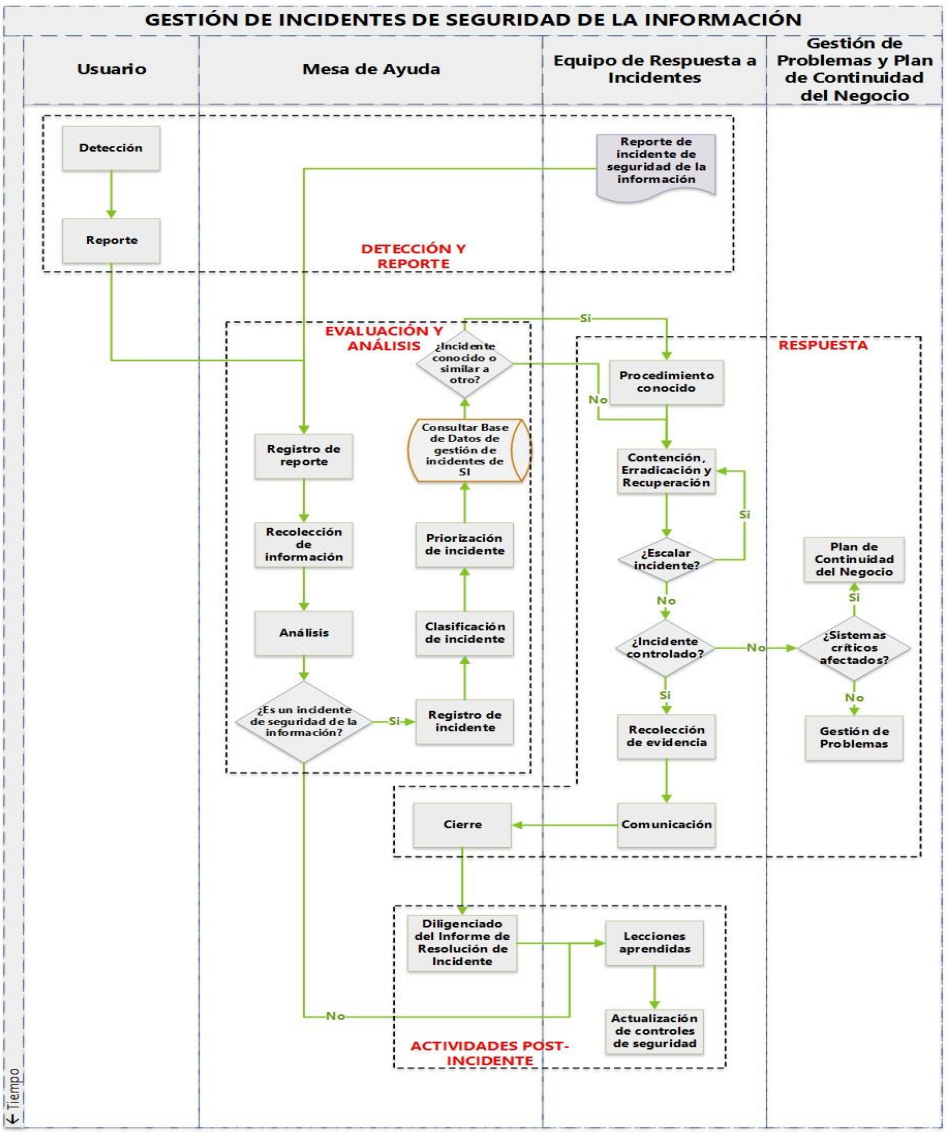


Figura 11. Proceso de gestión de incidentes propuesto.
Fuente: Elaboración propia.

4.3.2. Descripción de los roles en la gestión de incidentes de Tecnologías de la Información

Los roles en la gestión de incidentes de Tecnologías de la Información son:

- Usuario: persona (administrativo, docente, estudiante o tercero) que hace uso de algún servicio o activo de información de la universidad.
- Mesa de Ayuda: es el encargado del proceso. Tiene como objetivo monitorear y vigilar la correcta ejecución del proceso de gestión y obtener los datos necesarios para la evaluación del proceso. Además, es el encargado de registrar, atender y resolver incidentes en primera instancia.
- Equipo de Respuesta a Incidentes: grupo de personas con mayor experiencia en manejo de Tecnologías de la Información encargado de dar solución a incidentes de diferentes niveles de priorización.

4.3.3. Estados de un incidente en la gestión de incidentes de Tecnologías de la Información

En un inicio el registro, control y seguimiento de los incidentes se desarrollará mediante una plantilla en Microsoft Excel, lo cual no impide que más adelante se logre adquirir un software especializado para estos fines. Los estados de un incidente son:

1. Abierto
2. Cancelado
3. Asignado
4. En proceso
5. Detenido
6. Solucionado
7. Cerrado

En la siguiente figura se muestra la relación entre los estados de un incidente:

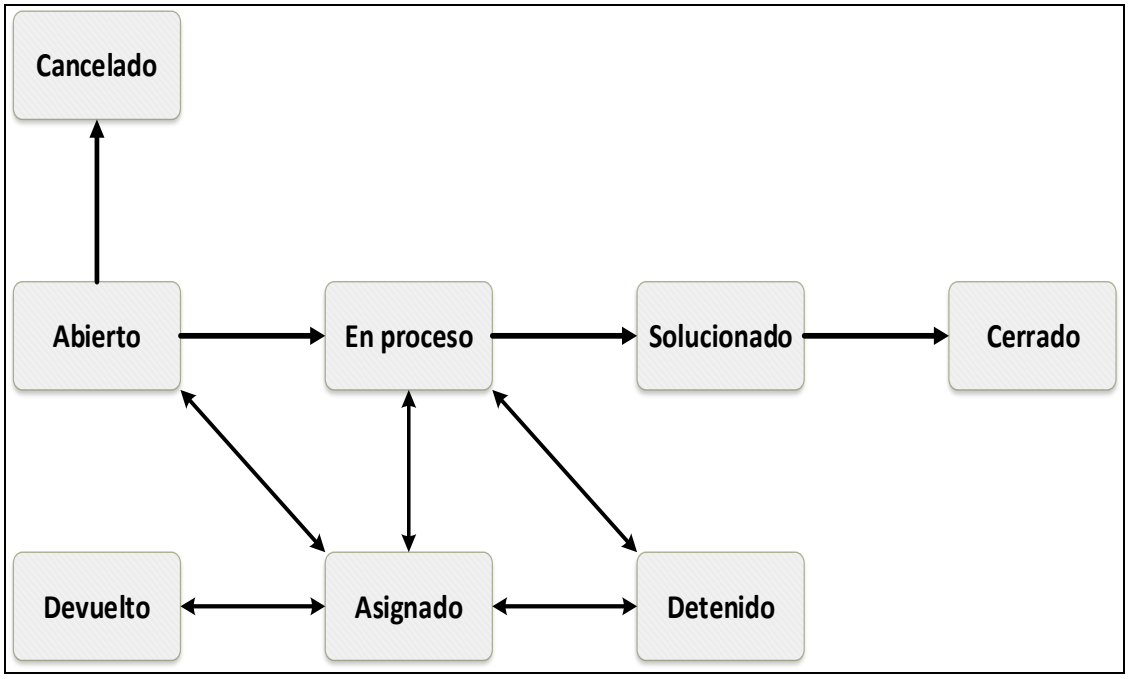


Figura 12. Relaciones entre los estados de un incidente de Tecnologías de la Información.
Fuente: Elaboración propia.

Esta propuesta de relaciones entre los estados de un incidente permite evitar la ocurrencia de inconsistencia y ayuda al cumplimiento del proceso, ya que define el flujo entre un estado y otro y la lógica entre la secuencia de las actividades.

En la siguiente figura se detalla las actividades que originan cambios en el estado de un incidente:

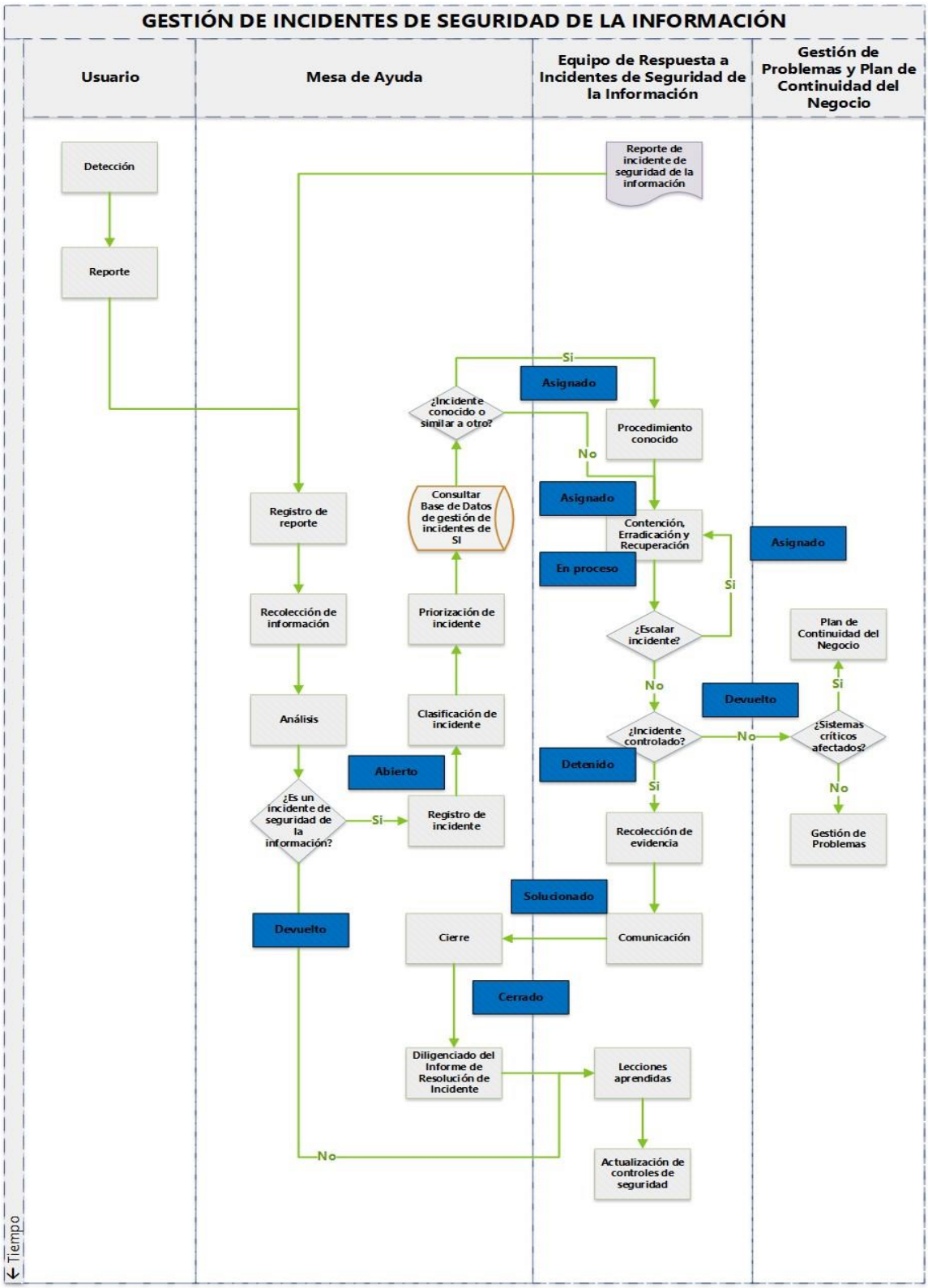


Figura 13. Actividades que dan origen a los estados de un incidente en el proceso de gestión de incidentes propuesto.
Fuente: Elaboración propia.

4.3.4. Definición de indicadores en la gestión de incidentes de Tecnologías de la Información

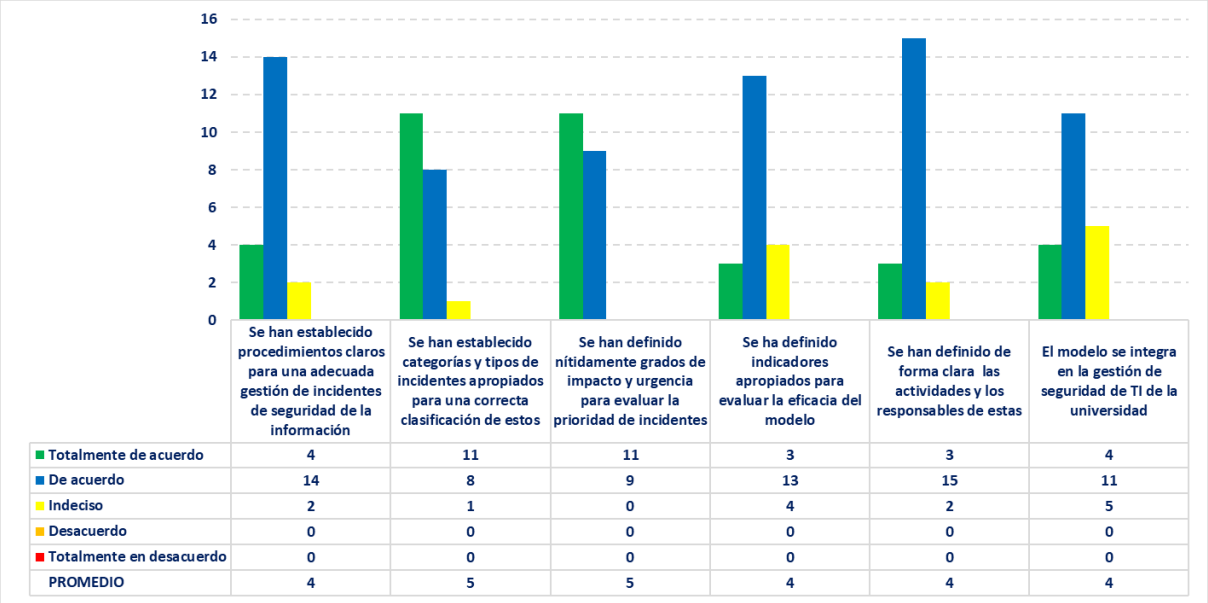
Para poder medir el desempeño del proceso se ha considerado contar con las siguientes métricas en un intervalo mensual:

- Número total de incidentes reportados, clasificados por tipo de prioridad.
- Número de incidentes asignados a grupos de soporte clasificados por tipo de prioridad.
- Número de incidentes solucionados por nivel de soporte.
- Porcentaje de incidentes solucionados clasificados por tipo de prioridad.

4.4. Evaluación del modelo

4.4.1. Resultados de la aplicación del instrumento

A continuación, se muestran los resultados obtenidos de la aplicación de la encuesta al personal administrativo y docentes de la Escuela Profesional de Ingeniería de Sistemas:



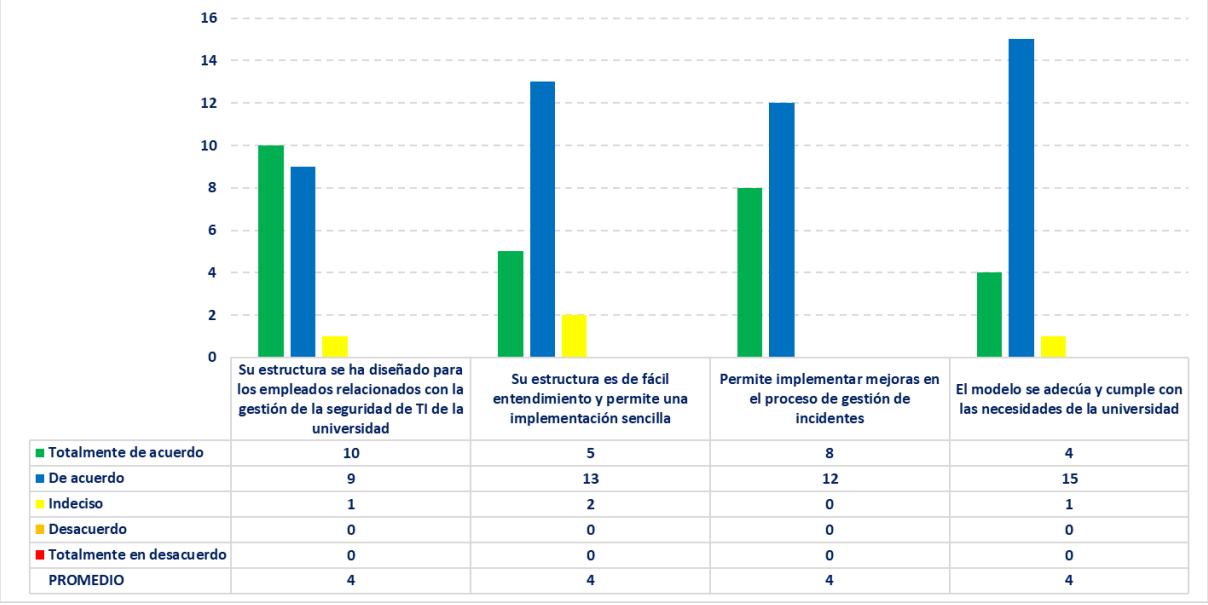
	Se han establecido procedimientos claros para una adecuada gestión de incidentes de seguridad de la información	Se han establecido categorías y tipos de incidentes apropiados para una correcta clasificación de estos	Se han definido nítidamente grados de impacto y urgencia para evaluar la prioridad de incidentes	Se ha definido indicadores apropiados para evaluar la eficacia del modelo	Se han definido de forma clara las actividades y los responsables de estas	El modelo se integra en la gestión de seguridad de TI de la universidad
Totalmente de acuerdo	4	11	11	3	3	4
De acuerdo	14	8	9	13	15	11
Indeciso	2	1	0	4	2	5
Desacuerdo	0	0	0	0	0	0
Totalmente en desacuerdo	0	0	0	0	0	0
PROMEDIO	4	5	5	4	4	4

Figura 14. Resultados de los ítems (preguntas) del cuestionario de la dimensión Efectividad del diseño. Fuente: Elaboración propia.

De la figura mostrada se puede observar que del total de encuestados:

1. El 20% (4 encuestados) está totalmente de acuerdo, el 70% (14 encuestados) está de acuerdo y el 10% (2 encuestados) está indeciso respecto a los procedimientos establecidos para una adecuada gestión de incidentes.

2. El 55% (11 encuestados) está totalmente de acuerdo, el 40% (8 encuestados) está de acuerdo y el 5% (1 encuestado) está indeciso respecto a las categorías y tipos de incidentes establecidos para una correcta clasificación.
3. El 55% (11 encuestados) está totalmente de acuerdo y el 45% (9 encuestados) está de acuerdo respecto a los grados de impacto y urgencia establecidos para evaluar la prioridad de los incidentes.
4. El 15% (3 encuestados) está totalmente de acuerdo, el 65% (13 encuestados) está de acuerdo y el 20% (4 encuestados) está indeciso respecto a los indicadores definidos para evaluar la eficacia del modelo.
5. El 15% (3 encuestados) está totalmente de acuerdo, el 75% (15 encuestados) está de acuerdo y el 10% (2 encuestados) está indeciso respecto a la claridad de las actividades y los responsables de estas definidas.
6. El 20% (4 encuestados) está totalmente de acuerdo, el 55% (11 encuestados) está de acuerdo y el 25% (5 encuestados) está indeciso respecto a la integración del modelo de gestión a la UDL.

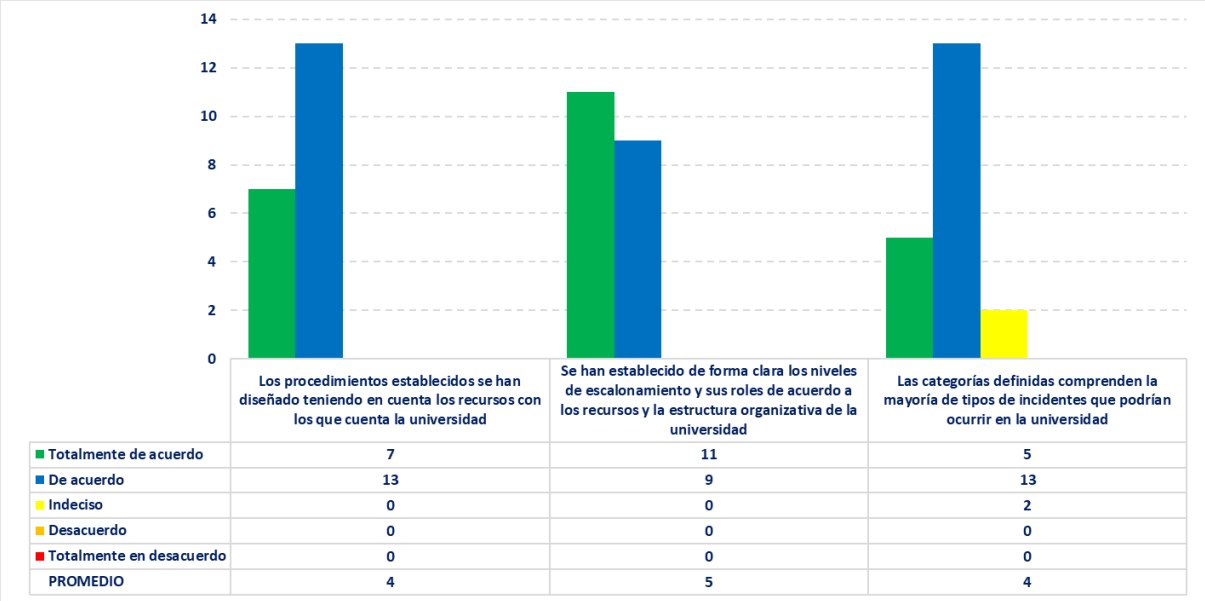


	Su estructura se ha diseñado para los empleados relacionados con la gestión de la seguridad de TI de la universidad	Su estructura es de fácil entendimiento y permite una implementación sencilla	Permite implementar mejoras en el proceso de gestión de incidentes	El modelo se adecúa y cumple con las necesidades de la universidad
Totalmente de acuerdo	10	5	8	4
De acuerdo	9	13	12	15
Indeciso	1	2	0	1
Desacuerdo	0	0	0	0
Totalmente en desacuerdo	0	0	0	0
PROMEDIO	4	4	4	4

Figura 15. Resultados de los ítems (preguntas) del cuestionario de la dimensión Usabilidad del modelo.
Fuente: Elaboración propia.

De la figura mostrada se puede observar que del total de encuestados:

1. El 50% (10 encuestados) está totalmente de acuerdo, el 45% (9 encuestados) está de acuerdo y el 5% (1 encuestado) está indeciso respecto a la estructura del modelo y la usabilidad de este para los empleados que gestionan la seguridad de TI en la UDL.
2. El 25% (5 encuestado) está totalmente de acuerdo, el 65% (13 encuestados) está de acuerdo y el 10% (2 encuestados) está indeciso respecto al fácil entendimiento e implementación sencilla del modelo.
3. El 40% (8 encuestados) está totalmente de acuerdo y el 60% (12 encuestados) está de acuerdo respecto a la implementación de mejoras del modelo al proceso de gestión de incidentes de la UDL.
4. El 20% (4 encuestados) está totalmente de acuerdo, el 75% (15 encuestados) está de acuerdo y el 5% (1 encuestado) está indeciso respecto a la adecuación y cumplimiento del modelo a las necesidades de la UDL.



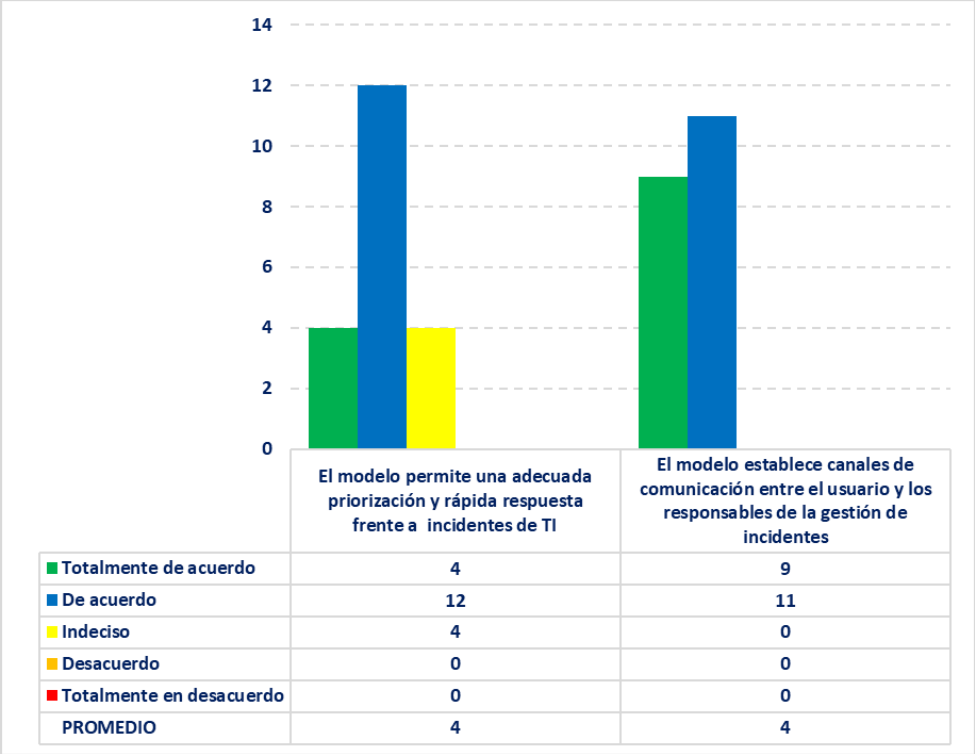
	Los procedimientos establecidos se han diseñado teniendo en cuenta los recursos con los que cuenta la universidad	Se han establecido de forma clara los niveles de escalonamiento y sus roles de acuerdo a los recursos y la estructura organizativa de la universidad	Las categorías definidas comprenden la mayoría de tipos de incidentes que podrían ocurrir en la universidad
Totalmente de acuerdo	7	11	5
De acuerdo	13	9	13
Indeciso	0	0	2
Desacuerdo	0	0	0
Totalmente en desacuerdo	0	0	0
PROMEDIO	4	5	4

Figura 16. Resultados de los ítems (preguntas) del cuestionario de la dimensión Adaptabilidad del modelo. Fuente: Elaboración propia.

De la figura mostrada se puede observar que del total de encuestados:

1. El 35% (7 encuestados) está totalmente de acuerdo y el 65% (13 encuestados) está de acuerdo respecto al diseño de los procedimientos y los recursos con los que cuenta la UDL.

2. El 55% (11 encuestados) está totalmente de acuerdo y el 45% (9 encuestados) está de acuerdo respecto a los niveles de escalonamiento y roles establecidos y los recursos y estructura de la UDL.
3. El 25% (5 encuestados) está totalmente de acuerdo, el 65% (13 encuestados) está de acuerdo y el 10% (2 encuestados) está indeciso respecto a la comprensión de las categorías definidas de los posibles incidentes en la UDL.



	El modelo permite una adecuada priorización y rápida respuesta frente a incidentes de TI	El modelo establece canales de comunicación entre el usuario y los responsables de la gestión de incidentes
Totalmente de acuerdo	4	9
De acuerdo	12	11
Indeciso	4	0
Desacuerdo	0	0
Totalmente en desacuerdo	0	0
PROMEDIO	4	4

Figura 17. Resultados de los ítems (preguntas) del cuestionario de la dimensión Satisfacción de usuarios.
Fuente: Elaboración propia.

De la figura mostrada se puede observar que del total de encuestados:

1. El 20% (4 encuestados) está totalmente de acuerdo, el 60% (12 encuestados) está de acuerdo y el 20% (4 encuestados) está indeciso respecto al modelo y la adecuada priorización y respuesta de incidentes.
2. El 45% (9 encuestados) está totalmente de acuerdo y el 55% (11 encuestados) está de acuerdo respecto a los canales de comunicación establecidos entre los usuarios y los responsables de la gestión de incidentes.

4.4.2. Evaluación de la fiabilidad del instrumento

Se estimó el nivel de fiabilidad del instrumento (cuestionario) usando el Alfa de Cronbach, para determinar si las respuestas de cada ítem tienen significancia y son válidos. Esto es necesario ya que si el instrumento es poco confiable no es posible determinar la relación entre dos o más variables.

George & Mallery (2003) sugiere tener en cuenta las siguientes escalas para evaluar los coeficientes de Alfa de Cronbach:

- Coeficiente alfa >0.9 es excelente
- Coeficiente alfa >0.8 es bueno
- Coeficiente alfa >0.7 es aceptable
- Coeficiente alfa >0.6 es cuestionable
- Coeficiente alfa >0.5 es pobre
- Coeficiente alfa <0.5 es inaceptable

Se obtuvieron los siguientes resultados:

Tabla 18. Resultados de la evaluación de la fiabilidad del instrumento (Alfa de Cronbach).

Estadísticas de fiabilidad	
Alfa de Cronbach	**N de elementos**
,725	20

Resumen de procesamiento de casos

		N	%
Casos	Válido	20	100,0
	Excluido[a]	0	,0
	Total	20	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Los resultados muestran que el coeficiente es de 0.725, confirmando de esta forma, que la encuesta aplicada es aceptable. Por lo tanto, los datos son confiables y se pueden procesar estadísticamente.

4.4.3. Análisis de la Regresión Lineal Múltiple

Se hizo uso la Regresión Lineal Múltiple debido a que la hipótesis de la presente investigación pretende estudiar posible relación entre las variables del modelo (independientes) y la variable dependiente, como se muestra a continuación:

- Variable Independiente (X_i): Modelo de gestión de incidentes de TI basado en Efectividad del diseño(X_1), Usabilidad del modelo(X_2); Adaptabilidad del modelo(X_3) y Satisfacción de usuarios(X_4).
- Variable Dependiente (Y): Incidentes de seguridad de la información.

Por lo tanto, el modelo a evaluar es un modelo de regresión múltiple de la forma:

$$Y = C_0 + C_1X_1 + C_2X_2 + C_3X_3 + C_4X_4 + E$$

El objetivo de este análisis es construir una función que permite estimar el valor futuro de la variable dependiente y contrastar si son estadísticamente relevantes los factores que hemos elegidos como predictores (dimensiones). Para lo cual, se siguieron los siguientes pasos:

A. Reducción de ítems de cada dimensión evaluada

La variable independiente: Modelo de gestión de incidentes de TI presenta la siguiente matriz de reducción de ítems evaluados:

Tabla 19. Matriz de reducción de ítems evaluados.

Dimensión	Ítems		Ítem reducido
Efectividad del diseño (X_1)	Usted considera que los procedimientos establecidos para la gestión de incidentes de seguridad de la información son claros	P1	X_1 = (P1 + P2 + P3 + P4 + P5 + P6)/6
	Usted considera que las categorías y tipos de incidentes establecidos permiten una adecuada clasificación de estos.	P2	

	Respecto a la evaluación de prioridad de incidentes, ¿los grados de impacto y urgencia se han definido nítidamente?	P3	
	Para la evaluación de la eficacia del modelo, ¿se han establecido indicadores apropiados para tal fin?	P4	
	Respecto a los procedimientos establecidos, ¿se han definido de forma clara las actividades y los responsables de cumplirlas?	P5	
	Usted considera que el modelo se integraría con facilidad en la gestión de seguridad de Tecnologías de la Información de la universidad	P6	
Usabilidad del modelo (X_2)	Respecto a la estructura del modelo, ¿usted considera que ha sido diseñada para los empleados relacionados con la gestión de seguridad de Tecnologías de la Información de la universidad?	P7	X_2 = (P7 + P8 + P9 + P10)/4
	¿Está usted de acuerdo con la siguiente afirmación? "La estructura del modelo es de fácil entendimiento y permite una implementación sencilla".	P8	
	Usted considera que el modelo permite implementar mejoras en el proceso de gestión de incidentes.	P9	
	Respecto a la usabilidad del modelo, ¿usted considera que se adecúa y cumple con las necesidades de la universidad?	P10	
Adaptabilidad del modelo (X_3)	Respecto a los procedimientos establecidos, ¿usted considera que han sido diseñados teniendo en cuenta los recursos con los que cuenta la universidad?	P11	X_3 = (P11 + P12 + P13)/3
	Se han establecido de forma clara los niveles de escalonamiento y sus roles de acuerdo a los recursos y estructura organizativa de la universidad.	P12	

	¿Está usted de acuerdo con la siguiente afirmación?: "Las categorías definidas comprenden la mayoría de tipos de incidentes que podrían ocurrir en la universidad".	P13	
Satisfacción de usuarios (X_4)	Usted considera que el modelo permite una adecuada priorización y rápida respuesta frente a incidentes de Tecnologías de la Información.	P14	X_4 = (P14 + P15)/2
	Usted considera que se han establecido canales de comunicación entre el usuario y los responsables de la gestión de incidentes de Tecnologías de la Información.	P15	

Fuente: Elaboración propia.

B. Aplicación de la metodología de Regresión Lineal Múltiple

A continuación, se muestran los resultados obtenidos en la aplicación de la metodología de Regresión Lineal Múltiple:

Tabla 20. Resultados de la evaluación del modelo por Regresión Lineal Múltiple.

Resumen del modelo[b]

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Durbin-Watson
1	,777[a]	,603	,498	,218	2,265

a. Predictores: (Constante), Satisfacción, Efectividad, Usabilidad, Adaptabilidad

b. Variable dependiente: Y

En el cuadro observamos el resultado de R cuadrado (coeficiente de determinación) que nos permite estimar la proporción o porcentaje de la variación de la variable dependiente que es explicada por una o más variables predictoras (dimensiones), es decir, refleja el nivel de interpretación de un modelo para la variable que pretende explicar. El rango para R cuadrado debe estar entre 0 y 1, siendo el valor esperado el más cercano a 1. El cuadro muestra un valor de 0.603, siendo este un resultado aceptable por su proximidad a 1. Por lo tanto, se demuestra la relación

entre las variables predictoras (dimensiones) y la variable dependiente. Ya que el nivel de explicación es aceptable, entonces es fiable analizar la relación entre dichas variables.

Además, el resultado de la prueba de Durbin-Watson que nos da un valor para determinar la independencia de errores, pero no una significancia. El valor esperado de la prueba Durbin-Watson es que sea lo más cercano a 2, en este caso tenemos un valor de 2.265 que es bueno. El rango que se debe tener en cuenta para aceptar el resultado de la prueba de Durbin-Watson es entre 1.85 y 2.30. La interpretación de este resultado es que no existe dependencia de las observaciones recogidas, es decir no existe autocorrelación. Por lo tanto, se demuestra que la recogida de la información fue aleatoria, evitando así invalidar por completo las conclusiones del análisis estadístico (obteniendo conclusiones erróneas). Ya que en un modelo de Regresión Lineal Múltiple se supone que no debe existir autocorrelación.

C. Análisis de varianza (ANOVA)

Los resultados del ANOVA se muestran en el siguiente cuadro:

Tabla 21. Resultados del análisis de varianza del modelo.

ANOVA[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	1,086	4	,272	5,705	,005[b]
	Residuo	,714	15	,048		
	Total	1,800	19			

a. Variable dependiente: Y

b. Predictores: (Constante), Satisfacción, Efectividad, Usabilidad, Adaptabilidad

Como el modelo de regresión que estamos trabajando es saber si las cuatro variables independientes están prediciendo la variable dependiente, entonces trabajaremos con los resultados del modelo que se muestra en la tabla ANOVA.

Aquí se observa que hay una significancia menor al 0.05 ($0.005 \leq 0.05$) y la interpretación en términos de hipótesis es que el modelo que estamos probando mejora significativamente la predicción de la variable dependiente.

D. Análisis de coeficiente de la ecuación de regresión

Tabla 22. Resultados del análisis de coeficientes del modelo.

Coeficientes[a]

Modelo		Coeficientes no estandarizados		Coeficientes estandarizados			95.0% intervalo de confianza para B	
		B	Error estándar	Beta	T	Sig.	Límite inferior	Límite superior
1	(Constante)	5,427	,849		6,395	,000	3,618	7,235
	Efectividad	,097	,125	,152	,772	,452	-,171	,364
	Usabilidad	-,294	,136	-,421	-2,166	,047	-,583	-,005
	Adaptabilidad	-,471	,122	-,766	-3,853	,002	-,732	-,211
	Satisfacción	,367	,108	,655	3,404	,004	,137	,597

a. Variable dependiente: Y

De los resultados del análisis de coeficientes obtenidos concluimos que tres de las variables son las que más aportan para explicar la varianza de la variable dependiente: Usabilidad (X_2), Adaptabilidad (X_3) y Satisfacción (X_4). Siendo la variable Satisfacción (X_4) la que más aporta a la explicación con un valor de 0.367.

De la misma tabla, también podemos observar los valores T y su significancia, que son valores que nos demuestran que tanto podemos generalizar el modelo de predicción a la población, son: T = -2.166, -3.853 y 3.040. Sin embargo, las significancias para estos mismos coeficientes respectivamente son: sig. = 0.047, 0.002 y 0.004, lo que significa que las variables al tener una significancia mayor a 0.05 se pueden incluir en el modelo.

Además, se puede observar que la variable Efectividad (X_1) es la que menos aporta a la explicación de la variable dependiente (al modelo), ya que el valor de su significancia es mayor a 0.05 (0.452 > 0.05).

Por lo tanto, de los resultados de la tabla de coeficientes se puede concluir que nuestro modelo de regresión es:

$$\boldsymbol{Y = C_0 + C_2X_2 + C_3X_3 + C_4X_4 + E}$$

$$\boldsymbol{Y} = 5.427 - 0.294\ \mathbf{X_2} - 0.471\ \mathbf{X_3} + 0.367\ \mathbf{X_4} + E$$

$$\boldsymbol{Y} = 5.427 - 0.294 * \boldsymbol{usabilidad} - 0.471 * \boldsymbol{adaptabilidad} + 0.367 * \boldsymbol{satisfacción}$$

Discusión

En esta investigación al demostrar la relación entre el modelo de gestión de incidentes de TI propuesto y los incidentes de seguridad de la información de la Universidad de Lambayeque, se pudo encontrar en el análisis de ANOVA que el valor de la significancia (0.005) es menor que 0.05. Lo cual nos da a entender que las variables independientes (predictores) mejora significativamente la predicción de la variable dependiente. Esto quiere decir que la definición de parámetros para la clasificación, priorización y escalonamiento y los procedimientos para responder incidentes, tienen relación con una gestión de incidentes de seguridad de la información eficaz. Además, los resultados obtenidos en el análisis de coeficientes nos indica que las variables que más aportan al modelo son Usabilidad, Adaptabilidad y Satisfacción, siendo esta última la que tiene un mayor grado de aporte a la explicación de la varianza de la variable dependiente. Lo cual indica, que el modelo permite una adecuada priorización y rápida respuesta a incidentes y que establece canales de comunicación claros.

Frente a lo mencionado, se acepta la hipótesis de investigación, la cual refiere la contribución del diseño de un modelo de gestión de incidentes de TI a la mejora de los procedimientos de seguridad de la información en la Universidad de Lambayeque.

Estos resultados son corroborados por Gonzales (2015) quien en su investigación llega a la conclusión que la implementación del framework ITIL v3 permitió mejorar la gestión de incidentes, específicamente en reducir los tiempos destinados a la atención y solución y en la satisfacción de los usuarios respecto al servicio de atención y solución de incidentes. Así también Cuzme y Pinargote (2015) concluyen que el desarrollo de un plan de gestión de incidentes permite establecer procedimientos de resolución, con el fin de tratar a los incidentes de forma correcta y en el tiempo establecido. En consecuencia, se coincide que es de suma importancia que las instituciones mantengan un control y registro adecuado de los incidentes de seguridad, detallando los procedimientos necesarios. Es decir, procedimientos para la clasificación, priorización, escalado y respuesta a incidentes.

En tal sentido, de todo lo estudiado y analizado en la presente investigación se determinó que la Universidad de Lambayeque depende en gran medida de su infraestructura tecnológica. A

pesar de ello, no se cuenta con ningún plan de prevención o manejo de riesgos e incidentes, quizás por el motivo de ser una institución relativamente pequeña.

La ausencia de procedimientos de respuesta a incidentes, específicamente el registro, da lugar a no tener datos claros y precisos sobre el historial de ocurrencia de estos incidentes. Por lo cual, es importante plantear procedimientos reducidos y claros. En consecuencia, se diseñó un modelo de gestión de incidentes con los datos necesarios para un adecuado análisis y respuesta.

Así mismo, se encontró vulnerabilidades en la parte del software ya que aún se hace uso del OS Windows XP y 7, el cual, ya no tiene soporte por el desarrollador, aumentando de esta forma el riesgo de materializarse una amenaza. En ese sentido, es necesario desarrollar un análisis de riesgos para tener información clara y real de las amenazas que podrían afectar el normal funcionamiento de la universidad.

V. Conclusiones

1. Se logró definir la situación actual de la Universidad de Lambayeque, identificando y describiendo los procesos, arquitectura e infraestructura tecnológica, personal, entre otros; que permitieron diagnosticar el estado actual en cuanto a gestión de incidentes se refiere.

2. Previo al diseño del proceso de gestión de incidentes, se hizo un análisis para determinar los parámetros imprescindibles para la implementación de un modelo de gestión de incidentes, concluyendo que era necesario definir los siguientes parámetros: categorización de los incidentes, priorización de los incidentes mediante los niveles de impacto y urgencia y la estructuración de los grupos de soporte, teniendo en cuenta los recursos y organización de la oficina de Cómputo e Informática.

3. Se diseñó los procedimientos de gestión de incidentes basado en la norma ISO 27035, teniendo en cuenta las funciones, roles y recursos de la oficina de Cómputo e Informática. Además, se determinaron métricas básicas para su evaluación.

4. El modelo de regresión, explica el 60.3% de la varianza de la variable dependiente, lo que prueba que las dimensiones seleccionadas son adecuadas. El valor de la prueba de Durbin-Watson de 2.265 demuestra que hay independencia de errores, es decir, que el

instrumento aplicado para la recopilación de información es válido. Además, el resultado de ANOVA, del modelo de regresión con las cuatro variables, demuestra que mejora significativamente la predicción de la variable dependiente ya que sig. (0.005) es menor que 0.05. Se acepta la hipótesis. Por lo cual, de los resultados de la evaluación del modelo propuesto, se concluye que el modelo de gestión de incidentes de TI permite mejorar los procedimientos de seguridad de la información, cumpliendo con las buenas prácticas de ITIL e ISO 27035.

VI. Recomendaciones

1. Se recomienda revisar cada cierto tiempo las categorías y tipos de incidentes con el fin de agregar nuevas formas de estos e implementar la gestión de problemas según los requerimientos de ITIL.

2. Crear un plan de capacitación para el personal administrativo sobre los procedimientos de gestión de incidentes, así como, al personal dedicado a gestionar los incidentes sobre módulos especializados de ITIL y seguridad de la información.

3. Implantar un sistema informático especializado en gestión de incidentes que permita automatizar las actividades del proceso.

4. Aplicar la metodología del análisis de riesgos sobre los activos de información para determinar las amenazas y los daños que estas pueden causar.

VII. Referencias

Agencia Europea de Seguridad de las Redes y de la Información. (2006). *Cómo crear un CSIRT Paso a Paso.*

Andrade, R., & Fuertes, W. (s.f.). *Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática (CSIRT). Caso de estudio: ESPE.*

Areitio Bertolín, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid: Cengage Learning Paraninfo, S.A.

Ayala Medrano, M. A. (2017). *Sistema de Gestión de Seguridad de Información para mejorar el proceso de gestión del riesgo en un Hospital Nacional.* Lima.

Chicano Tejada, E. (2014). *Gestión de incidentes de seguridad informática.* (1° ed.). Málaga: IC Editorial.

Cifuentes Obando, J. F. (2017). *Propuesta de ajuste al modelo de gestión de incidentes de la empresa Claro Colombia S.A. para el mejoramiento continuo de los tiempos de respuesta basados en ITIL v3.* Bogotá.

Cruz Diaz, M. A., & Fukusaki Infantas, S. (2017). *Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica Medcam Perú SAC.* Lima.

Cuzme Romero, M. G., Pinargote Anchundia, R. E., & Sabando Loor, E. (2015). Plan de gestión de incidentes que afectan a los equipos informáticos de la ESPAM MFL. *Informática y Sistemas,* 24-30.

Darren George, P. M. (2003). SPSS for Windows Step by Step. Boston: Allyn & Bacon.

Dirección de Informática y Telecomunicaciones. (2010). *Manual de seguridad. Aplicación de Tramitación Telemática.* DEPARTAMENTO DE JUSTICIA Y ADMINISTRACIÓN PÚBLICA, Platea.

ESET Latinoamérica. (2018). *ESET Security Report 2018 Latinoamérica.*

EY Perú. (2015). *Encuesta Global de Seguridad de la Información 2014 "Perspectivas sobre Gobierno, Riesgo y Cumplimiento ".*

EY Perú. (2018). *Encuesta Global de Seguridad de Información 2017-2018 "Recuperando la ciberseguridad: prepárese para enfrentar los ataques cibernéticos".* Ernst & Young Global Limited, Perú.

Gonzales Flores, J. A. (2015). *Implementación del marco de trabajo ITIL v.3.0 para el proceso de gestión de incidencias en el área del centro de sistemas de información de la Gerencia de Salud Lambayeque.* Chiclayo.

International Organization for Standardization. (2011). *Information technology — Security techniques — Information security incident management.*

International Organization for Standardization. (2014). Information technology — Security techniques — Information security management systems — Overview and vocabulary.

International Organization for Standarization. (2013). *Information technology— Security techniques — Code of practice for information security controls.*

IT Governance Institute y Oficina Gubernamental de Comercio. (2008). *Alineando CobiT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio de la empresa.*

Montesino Perurena, R., Baluja García, W., & Porvén Rubier, J. (Enero-Abril de 2013). Gestión automatizada e integrada de controles de seguridad informática. *Revista de Ingeniería Electrónica, Automática y Comunicaciones, XXXIV*, 40-58.

Norse Corporation. (2014). How Advanced Attacks Get Past. 2.

OGC. (2011a). *ITIL® Service Strategy.*

OGC. (2011b). *ITIL® Service Design.*

OGC. (2011c). *ITIL® Service Transition.*

OGC. (2011d). *ITIL® Service Operation.*

Tibaquira Cortes, Y. A. (2015). *Metodología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma SIEM de una entidad financiera basada en la norma ISO/IEC 27035 e ISO/IEC 27005.* Bogota.

Universidad TecVirtual del Tecnológico de Monterrey. (2012). *Conceptos básicos para la ceritificación en ITIL.*

VIII. Anexos

Anexo N° 1: Formato para el reporte de incidentes de Seguridad de la Información propuesto.

Anexo N° 2: Responsables de las actividades del proceso de gestión de incidentes propuesto.

Anexo N° 3: Cuestionario para evaluar el diseño del modelo propuesto (instrumento).

Anexo N° 1: Formato para el reporte de incidentes de Seguridad de la Información propuesto.

Fecha de reporte: Hora de reporte:

DATOS DE LA PERSONA QUE REPORTA

Nombres y apellidos:

Cargo:

Área/Oficina:

Correo electrónico:

Teléf. institucional: Teléf. personal:

INFORMACIÓN SOBRE EL INCIDENTE

Fecha en la que se observó el incidente:

Hora en la que se observó el incidente:

De las lista que se muestra a continuación seleccione y marque con una **X** las opciones que considere se presentaron

__ Suplantación de identidad de usuario
__ Acceso no autorizado al sistema o red
__ Interceptación de datos/información
__ Robo o pérdida de activo de información
__ Escaneos de vulnerabilidades/activos
__ Explotación de vulnerabilidades
__ Ataque de fuerza bruta
__ Defacement Web
__ Compromiso de cuentas de usuarios
__ Exposición de datos personales
__ Manipulación de configuraciones
__ Manipulación de registros/logs de sistemas
__ Modificación no autorizada de información
__ Destrucción no autorizada de información
__ Otro (describa):

__ Denegación de servicio
__ Error humano
__ Fallo del servicio de Internet o eléctrico
__ Fallo (hardware/software)
__ Uso inadecuado
__ Incumplimiento de políticas de SI
__ Incumplimiento de requisitos legales
__ Difusión de software dañino (malware)
__ Ransomware
__ Phishing
__ Spam
__ Daños por agua, fuego, electricidad
__ Desastres naturales
__ Sabotaje

Descripción del incidente (¿qué ocurrió? ¿cómo ocurrió? ¿tomó alguna medida?):

_____

_____

_____

* Diligencie este formato y entréguelo personalmente o envíelo por correo electrónico a la Oficina de Cómputo e Informática.

* Si el incidente se trata de un fraude mediante correo electrónico (phishing), no elimine el mensaje, póngase en contacto telefónicamente con Mesa de Ayuda y reenvíe el mensaje a los correos que se le indicará.

* Para cualquier inquietud o consulta comuníquese con Mesa de Ayuda.

Anexo N° 2: Responsables de las actividades del proceso de gestión de incidentes propuesto.

Actividad	Responsable	Descripción
Reportar el incidente	Administrativos, docentes, estudiantes o terceros. Mesa de Ayuda	Las personas que tengan acceso a la información o activos de información y se dan cuenta que se está presentando un ataque a los activos de la institución o tienen conocimiento de alguna persona que está violando las políticas de seguridad, deberá de reportar el evento o incidente directamente en la oficina de Cómputo e Informática o mediante el diligenciado del Reporte de Incidente de Seguridad de la Información
Registrar el incidente	Mesa de Ayuda	Mesa de Ayuda, luego de confirmar la ocurrencia, deberá registrar el incidente asignándole una categoría y tomando los datos del reporte diligenciado por el usuario.
Evaluar el impacto y urgencia del incidente	Mesa de Ayuda - Encargado de la unidad de Telemática	Mesa de Ayuda deberá realizar la evaluación del impacto considerando los activos afectados, las áreas alcanzadas, el pronóstico de expansión y los daños causados. Para determinar los niveles de impacto y urgencia se tendrán en cuenta las tablas N° 10 y 11.
Identificar el nivel de prioridad del incidente	Mesa de Ayuda y Encargado de Telemática	Deberán determinar el nivel de prioridad del incidente considerando el nivel de impacto y de urgencia. Se tendrá en cuenta los niveles establecidos en la tabla N° 13.
Escalar el incidente	Mesa de Ayuda	Mesa de Ayuda deberá controlar los tiempos establecidos a cada nivel para dar solución al incidente. Por tanto debe tener en cuenta los niveles de escalonamiento establecidos.
Aplicar estrategias de Contención	Mesa de Ayuda Encargado de la unidad, de Telemática y Jefe de la oficina de Cómputo e Informática	Se debe tener en cuenta los siguientes factores: - Recursos para desarrollar la estrategia. - Duración de la solución. - Necesidad de mantener la evidencia. - Capacidad de mitigación de la estrategia frente al incidente. - Criticidad de los activos afectados. - Posible modo de actuación del atacante.
Aplicar estrategias de Erradicación	Mesa de Ayuda, Encargado de unidad de Telemática y Jefe de la oficina de Cómputo e Informática	Se debe tener en cuenta los siguientes factores: - Experiencias anteriores. - Pérdida económica. - Posibles implicaciones legales. - Efectividad de la estrategia. - Recursos necesarios para aplicar la estrategia. - Determinación de los procesos o activos comprometidos.
Aplicar estrategias de Recuperación	Mesa de Ayuda, Encargado de la unidad de Telemática y Jefe de la oficina de Cómputo e Informática	La determinación de las estrategias de Recuperación depende de los daños ocasionados por el incidente. Por lo cual, es necesario realizar un análisis del daño generado.
Recolectar evidencia	Encargado de la unidad de Telemática	Se obtendrá información de la red, de los equipos afectados y declaraciones de personas que han presenciado o han sido afectadas por el incidente.

Realizar análisis post-incidente	Mesa de Ayuda, Encargado de la unidad de Telemática y Jefe de la oficina de Cómputo e Informática	Dentro las actividades post-incidentes tenemos: - Generar reportes e información para desarrollar controles. - Diligenciar el Informe de Resolución de Incidente. - Actualizar controles de seguridad. - Desarrollar planes de capacitación para los usuarios. - Manejar la evidencia obtenida en el proceso para futuros análisis si esto fuera necesario.
Diligenciar el Informe de Resolución de Incidente	Mesa de Ayuda	Una vez se haya cerrado el incidente, Mesa de Ayuda deberá de diligenciar el informe recopilando información de las diferentes personas que han participado en la resolución del incidente. Luego este informe debe ser enviado al jefe de la oficina de Cómputo e Informática para su aprobación.

Anexo N° 3: Cuestionario para evaluar el diseño del modelo propuesto (instrumento)

PREGUNTA	NIVEL DE CONFORMIDAD				
1. Usted considera que los procedimientos establecidos para la gestión de incidentes de seguridad de la información son claros.	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
2. Usted considera que las categorías y tipos de incidentes establecidos permiten una adecuada clasificación de estos.	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
3. Respecto a la evaluación de prioridad de incidentes, ¿los grados de impacto y urgencia se han definido nítidamente?	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
4. Para la evaluación de la eficacia del modelo, ¿se han establecido indicadores apropiados para tal fin?	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
5. Respecto a los procedimientos establecidos, ¿se han definido de forma clara las actividades y los responsables de cumplirlas?	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
6. Usted considera que el modelo se integraría con facilidad en la gestión de seguridad de Tecnologías de la Información de la universidad.	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
7. Respecto a la estructura del modelo, ¿usted considera que ha sido diseñada para los empleados relacionados con la gestión de seguridad de Tecnologías de la Información de la universidad?	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5

8. ¿Está usted de acuerdo con la siguiente afirmación? "La estructura del modelo es de fácil entendimiento y permite una implementación sencilla".	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
9. Usted considera que el modelo permite implementar mejoras en el proceso de gestión de incidentes.	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
10. Respecto a la usabilidad del modelo, ¿usted considera que se adecúa y cumple con las necesidades de la universidad?	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
11. Respecto a los procedimientos establecidos, ¿usted considera que han sido diseñados teniendo en cuenta los recursos con los que cuenta la universidad?	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
12. Se han establecido de forma clara los niveles de escalonamiento y sus roles de acuerdo a los recursos y estructura organizativa de la universidad.	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
13. ¿Está usted de acuerdo con la siguiente afirmación?: "Las categorías definidas comprenden la mayoría de tipos de incidentes que podrían ocurrir en la universidad".	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
14. Usted considera que el modelo permite una adecuada priorización y rápida respuesta frente a incidentes de Tecnologías de la Información.	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5
15. Usted considera que se han establecido canales de comunicación entre el usuario y los responsables de la gestión de incidentes de Tecnologías de la Información.	Totalmente en desacuerdo 1	Desacuerdo 2	Indeciso 3	De acuerdo 4	Totalmente de acuerdo 5

16. ¿Qué tan satisfecho está usted con el diseño del modelo propuesto para la gestión de incidentes de seguridad de la información?	<table><tr><td>Totalmente en desacuerdo 1</td><td>Desacuerdo 2</td><td>Indeciso 3</td><td>De acuerdo 4</td><td>Totalmente de acuerdo 5</td></tr><tr><td></td><td></td><td></td><td></td><td></td></tr></table>