UNIVERSIDAD HISPANOAMERICANA

ESCUELA DE INGENIERÍA INFORMÁTICA

TESIS PARA OPTAR POR EL GRADO DE LINCENCIATURA EN

INGENIERÍA INFORMÁTICA

PROPUESTA DE UNA PÓLITICA DE MANEJO DE INCIDENTES EN EL DEPARTAMENTO DE TI DE INDUSTRIAL OLEAGINOSAS AMERICANAS S.A (INOLASA)

Sustentante:

Alondra María Arguedas González

Enero - 2021

Contenido

Tabla de imágenes

Tabla de cuadros

Tabla de Gráficos

CAPÍTULO I:

PLANTEAMIENTO DEL TEMA

1. ANTECEDENTES Y JUSTIFICACIÓN DEL PROYECTO

1.1 MARCO DE REFERENCIA EMPRESARIAL Y CONTEXTUAL

Industrial Oleaginosas Americanas S.A, conocida como INOLASA, se basa y es una empresa líder en la producción y comercialización de aceites vegetales, lecitina de soya e insumos alimenticios para animales.

Su origen se remite al año 1986, cuando José Ignacio González Hoffman, inversionista nicaragüense junto con unos socios le dan vida a tan prestigiosa organización. Esta ofrece un ambiente de trabajo seguro para sus colaboradores, el cual brinda confianza a cada uno de sus trabajadores ya que tiene un fuerte compromiso con el bien social y económico de Costa Rica y especialmente con su comunidad.

Las Oficinas Administrativas de la empresa se encuentran en San José, Uruca y tiene una Planta de Proceso en la Provincia de Puntarenas, contigua a Zona Franca Saret, Barranca Puntarenas.

La empresa es líder en la utilización de tecnología de punta, con esto la empresa se asegura de ofrecer productos de muy alta calidad a sus clientes, así mismo la empresa cuenta con constantes actualizaciones en el área tecnológica y brinda capacitaciones a sus colaboradores, además pasa por estrictos controles de calidad con el fin de enfocarse en las exigencias del mercado externo y dar seguimiento constante a la calidad total que la caracteriza.

> Cuenta con equipos de alta tecnología que le permiten procesar aproximadamente 1200 Toneladas Métricas de frijol de soya al día. Ha sido reconocida por la Asociación Americana de Soya como una de las plantas procesadoras de frijol de soya más eficiente en América Latina. También, ha sido reconocida por asociaciones como American Oil Chemists Society. Además, cuenta con una certificación FSSC22000 (Certificación de Seguridad Alimentaria). (INOLASA, s.f.)

Marco Estratégico

Misión

Proveer harina de soya para nutrición animal, aceites comestibles y otros productos competitivos de alta calidad para satisfacer a nuestros clientes, brindando servicio de excelencia y compromiso de producción segura y sostenible.

Visión

Ser líder regional de productos de alto valor agregado.

Valores

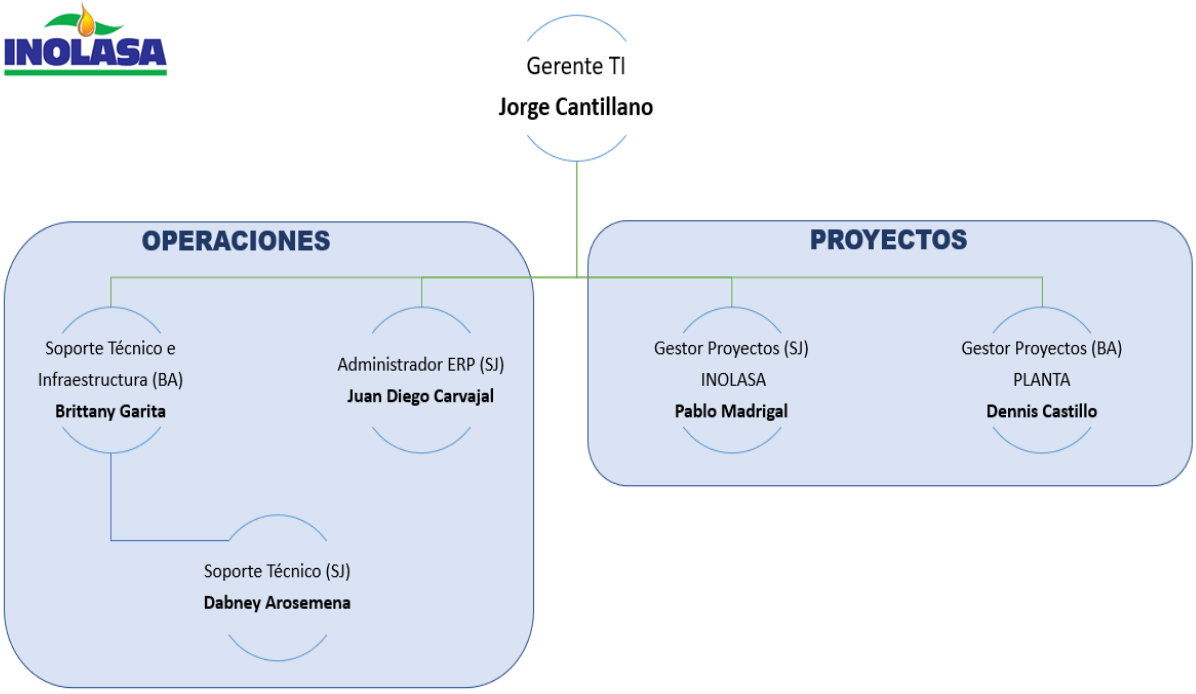
- Innovación
- Servicio al Cliente
- Respeto
- Calidad
- Pasión
- Seguridad
- Adaptabilidad

El objetivo general de INOLASA, es crecer en forma sana y sostenible aportando beneficios a sus accionistas, a sus empleados y a la sociedad como un todo. Las operaciones de la empresa se realizan de forma directa y a través de sus distribuidores en la región que comprende desde México hasta Panamá.

Organización:

Imagen número 1

Organigrama



Fuente: (Industrial Oleaginosas Americanas S.A, 2020, S.P.)

Historia de la organización:

A mediados de los 80, específicamente en 1986, Don José Ignacio González Hoffman, inversionista nicaragüense junto con unos socios crearon Industrial de Oleaginosas Americanas S. A. conocida como INOLASA con el fin de ofrecer al país y a la región centroamericana, productos derivados del frijol de soya, de alta calidad. Esta empresa emprendió sus funciones únicamente con un extractor y ahora es una de las empresas más

importantes en la zona de Puntarenas, brindando empleo a muchos Puntarenenses y al país en general.

Se encuentra ubicada en Barranca, Puntarenas, cerca de la costa Pacífica de Costa Rica, con oficinas administrativas en San José. En 1986 el sector de Barranca lucía muy diferente, la empresa estaba sola en este lugar junto a Montecillos que es otra empresa, con el pasar de los años se construyó La Zona Franca Saret, el IMAS, el INA y otras importantes instituciones.

El 17 de mayo de 1986 se realizó la primera venta de harina de soya en sacos, con un valor por quintal de 790 colones, la primera factura de esta venta fue realizada con una máquina manual. El primer cliente que compró a gran cantidad fue "Cobesa" que hoy en día es conocido como "Pipasa".

A inicios la empresa contaba con veinte colaboradores, conforme iba pasando el tiempo fue creciendo y así mismo la cantidad de empleados. También, al pasar los años iniciaron las exportaciones a países como El Salvador y Nicaragua; actualmente de exporta también a Panamá, México, Estados Unidos, China y Guatemala, además, provee a diferentes ganaderos y porcicultores con diversas fórmulas de alimento para consumo animal.

El primer gerente de planta el Ingeniero Pedro Lacayo Reyes y el gerente de producción el Ingeniero Julio Valdiviezo Fernández, fueron los encargados de incluir personal en el área de mantenimiento, producción y demás áreas. Actualmente Don Rodrigo Aguilar Torres, ya jubilado aún conserva un trabajo a medio tiempo en la empresa, era el controlador y también apoyaba en las contrataciones.

INOLASA desde sus inicios ha tenido un gran compromiso con la comunidad Puntarenense, hace donaciones de aceite a diferentes escuelas de la región, hogares de ancianos, hogares cristianos e iglesias, también ayuda a la municipalidad en actividades como carnavales, muy característicos de la zona.

La empresa reconoce el arduo trabajo de sus colaboradores y les brinda reconocimientos y regala de sus productos a las familias, haciéndoles sentir parte fundamental de la organización. Información brindada por personal interno de la empresa.

1.2. JUSTIFICACIÓN DEL PROYECTO

La tecnología avanza todos los días de manera acelerada, y las organizaciones deben adaptarse a su entorno interno y externo para poder permanecer en el mercado y evitar ser una más de las que desaparezca. Hoy en día es evidente el impacto que el uso de las Tecnologías de Información (léase en adelante TI) generan en las actividades empresariales y por ello es significativo que la empresa en estudio no se vea rezagada en este ámbito y es que, Córdova y Rojas consideran que "éstas son elemento clave para salir en el entorno competitivo en el que se desenvuelven actualmente las organizaciones." (Córdova y Rojas, 2019, p.4.)

La globalización y los cambios repentinos del mercado exigen a las organizaciones adecuarse al uso de la tecnología para lograr esa permanencia y competitividad a mediano y largo plazo en el nicho de mercado en el cual se enfocan sus actividades productivas y así desarrollar todo su potencial, por ende, es de suma importancia que las empresas busquen una mejora continua apoyándose en la tecnología ya que, de algún modo todos sus procesos productivos y planes de negocio se ven involucrados con los elementos tecnológicos en busca de la eficiencia y eficacia de sus funciones con el fin de lograr la satisfacción de sus clientes finales.

Como menciona el señor Nazar "el uso de las tecnologías transformadoras en las empresas radica en que los sistemas tecnológicos, a través del uso y análisis de datos, siempre están orientados a mejorar procesos y lograr resultados con mayor rapidez, eficiencia y certeza". Se considera preciso que la empresa enfoque recursos en mejorar y administrar los recursos tecnológicos que se encuentran a su alcance para lograr sus objetivos organizacionales. (Nazar, 2018, párr. 6)

INOLASA posee un Departamento de Tecnologías de Información que brinda soporte y asistencia a cada una de las operaciones diarias de la empresa, en este contexto el señor Alfonzo Gimeno expresa que, "la importancia de las Tecnologías de la Información y Comunicación (léase en adelante TIC) no reside en la tecnología en sí, sino en el hecho de que permita el acceso al conocimiento, la información y las comunicaciones". Estos elementos se consideran cada vez con mayor relevancia para lograr una interacción

económica apropiada y rentable con el mercado, por ende, este departamento es de suma importancia para la organización, debido a que atiende diariamente una gran cantidad de incidentes por el área de administración de Tecnologías de Información y al no llevar un control sobre cada una de estas incidencias en algunos elementos se ha vuelto difícil de manejar. (Gimeno, 2010, p.9.)

Una política para el correcto manejo de estas situaciones es la gestión de incidentes en las TI, permitirán un desempeño óptimo e integridad de los sistemas, además brindará soporte agilizando la resolución de problemas que surgen día a día, por medio de estándares y procedimientos que refuercen las actividades y brinden optimización del tiempo así mismo, con las mejores prácticas se logrará una coordinación de actividades, procesos y el logro de objetivos de forma estructurada con lo cual se apreciará a mediano y largo plazo el rendimiento en cada proceso, reducción de incidencias, planes correctivos y la satisfacción de los clientes; que sin duda alguna son el pilar fundamental para la existencia de la misma.

INOLASA es una empresa con muchos puntos a favor, sin embargo, no cuenta con reglamentación alguna para controlar los incidentes, esto es una necesidad con alta prioridad para esta organización ya que, actualmente ocupa mucho tiempo en realizar la actividad de atención a las incidencias, al implementar programas de mejora y políticas de seguimiento y control la mejora será notable y la resolución de los casos expuestos por los usuarios se atenderán de forma oportuna logrando la satisfacción de los mismos, logrando disminuir considerablemente las incidencias y por ende un ahorro de recursos económicos y de tiempo para la organización así como, la fiabilidad y lealtad de los clientes a largo plazo.

De igual forma la elaboración de estas políticas debe considerar al capital humano en la empresa, Sáenz manifiesta que, “La empresa ha de comunicar la existencia de una política de control expresa para que ésta no vulnere el derecho a la intimidad de los trabajadores”. Por lo cual el desarrollo e implementación de esta política debe ser clara, rigurosa y eficiente para mantener un mayor control de los incidentes y por ende su respectiva resolución, pero sin invadir la privacidad de sus trabajadores. (Sáenz, 2016, párr. 6)

2. DEFINICIÓN DEL PROBLEMA

2.1 **Problemática**

Un problema es: “Independientemente de su naturaleza, un problema es todo aquello que amerita ser resuelto” se basa en una serie de eventos y sus efectos, mismos que van a requerir de un análisis para lograr una resolución satisfactoria, la investigación es una parte importante de este proceso ya que, brinda herramientas para sustentar el proyecto. (Arias, 2012, p.34.)

La empresa Industrial Oleaginosas Americanas S.A no cuenta con un sistema o política que apoye el proceso de resolución de incidencias de los usuarios en cuanto al ámbito tecnológico. Todos los días los colaboradores del área de TI se encuentran con peticiones de atención a los problemas que los empleados tienen mientras laboran. La variedad de tipos de incidentes es amplia, los hay desde problemas con los equipos de cómputo, radios, teléfonos, problemas con el sistema Planificación de Recursos Empresariales (ERP) utilizado en la organización, problemas de almacenamiento, en los periféricos, así como problemas de usuarios, entre otros.

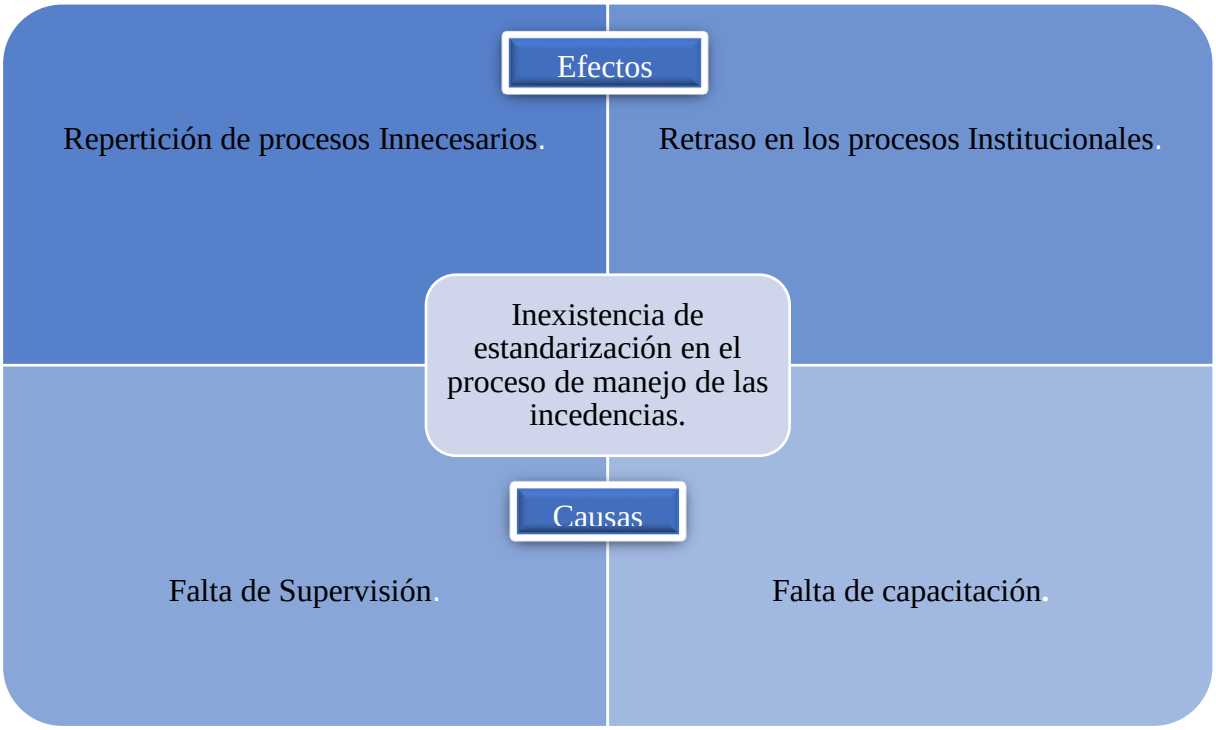
Tantos incidentes a diario impactan directamente en las funciones de la organización que si bien es cierto la empresa logra resolver manualmente los incidentes al ser tantos se puede perder información en el proceso sobre los casos, además, que el procedimiento manual retrasa las labores por motivo de tiempos de repuesta largos. En ocasiones se resuelven problemas que en otras circunstancias ya se habían resuelto y por carencia de un sistema que registre los pasos de la solución se pierde tiempo intentando buscar nuevamente la reparación a la incidencia.

Se pretende buscar una mejora sobre esta falta, implementando un control para las incidencias mismo que ayude a priorizarlas, enlistarlas para no perder información y que si sucede una eventualidad igual se pueda acceder a los pasos previamente registrados, un proceso estandarizado permitirá al departamento de TI gestionar de forma ordenada los incidentes para finalmente por medio de métricas permitirle a la alta gerencia la toma de decisiones sobre las áreas de mejora.

2.1.1. Diagrama de Causa- Efecto

Imagen número 2

Diagrama de Causa y Efecto



Fuente: Elaboración propia

Como análisis del diagrama anterior, la inexistencia de una política para el manejo de incidencias es producto de varias causas, entre ellas:

1. La falta de supervisión en el proceso de manejo de incidencias de los usuarios.
2. La falta de capacitación en temas relacionados con políticas y estándares para el control de las incidencias.

2.2. Problema General

A continuación, se expone el problema general del proyecto.

¿Cómo identificar las pautas para mejorar el proceso de atención a los incidentes de los usuarios de Servicios de Informática de INOLASA que permita la unificación de los pasos y disminución de situaciones adversas con el fin de desarrollar una propuesta de una política para el control de las incidencias?

2.2.1. Problemas Específicos

- ¿Es posible identificar el proceso de control de incidentes de los usuarios de Servicios de Informática con base a la situación actual?
- ¿Hay información relevante que permita describir el impacto que genera la falta de estandarización en dicho proceso?
- ¿Cómo definir un plan para la estandarización del proceso de control de incidentes para que el personal de TI realice la tarea de forma eficiente?
- ¿Se puede capacitar a los colaboradores del departamento de TI sobre las políticas necesarias para evitar situaciones no deseadas?

3. Objetivos

3.1 Objetivo General

Desarrollar una propuesta de un Modelo de Gestión basado en el Marco de Referencia ITIL V3 para dotar de herramientas de gestión, control y seguimiento del almacenamiento de incidentes del departamento de Tecnologías de Información de INOLASA

3.1.1. Objetivos Específicos.

- Identificar la situación actual del proceso de control de incidentes de acuerdo con la información recopilada sobre la atención a las situaciones adversas de INOLASA.

- Analizar las debilidades del proceso de incidentes dentro del departamento de Tecnologías de Información con el fin de priorizar los problemas en función del impacto que generen.
- Plantear una propuesta de gestión de incidencias en TI que permita la mejora de la situación actual utilizando como referencia las mejores prácticas en la industria.
- Plantear una propuesta de capacitación a los colaboradores para la aplicación del plan de gestión para el manejo de incidentes.

4. Alcance y Limitaciones

4.1 Alcance del Proyecto

A continuación, se describe en detalle el alcance planteado para lograr el cumplimiento de los objetivos del proyecto:

- El primer entregable del proyecto es un "Diagnóstico de la Situación Actual del Proceso de Control de Incidentes" tomando como base de conocimiento los problemas más comunes, así como las causas y los pasos para llegar a las soluciones con el fin de solventar futuras incidencias de manera eficiente.
- El segundo entregable es un "Análisis de Asignación de Prioridades de los Problemas" ya previamente detectados el cual determinará las debilidades y necesidades de dicho proceso dejando como evidencia el impacto real que se genera en la organización.
- Como tercer entregable se establece el "Planteamiento de una Propuesta de Gestión de Incidencias de TI" tomando en cuenta los hallazgos previos con el fin de alinearlas a las mejores prácticas en la industria del mercado.
- El cuarto entregable abarca un "Planteamiento de una propuesta de Capacitación" según las buenas prácticas, para los colaboradores que trabajan en dicho proceso, ayudándoles a la adaptación de cambios que permitan incrementar el nivel de eficiencia de los empleados como de los procesos.

4.1.1. Limitaciones del Proyecto

El proyecto estará limitado al establecimiento de una propuesta que le permita a la empresa decidir si desea implementar a futuro las soluciones.

La disposición del personal para atender y responder a las preguntas es una de las limitantes de la investigación.

En adición a las limitaciones del proyecto se podría definir también la ubicación geográfica de las Oficinas Administrativas de INOLASA se encuentran en la capital, San José.

CAPÍTULO ll:

MARCO TEÓRICO

En este capítulo se presenta la definición y conceptos, que respaldan lo desarrollado en este proyecto y que, además ofrece un mejor entendimiento al lector sobre el tema tratado, brindándole un panorama más amplio por medio de la sustentación de las teorías sobre los temas relacionados al problema en estudio.

CONTEXTO HISTÓRICO- ANTECEDENTES

Actualmente las tecnologías juegan un papel muy importante en las empresas, esta avanza de manera acelerada y las corporaciones deben evolucionar, innovar y hacerle frente a la nueva era digital, ya que con el pasar del tiempo estas dependen cada vez más de las TIC para satisfacer las necesidades y lograr los objetivos de la organización.

Las tecnologías de la información y la comunicación han transformado nuestra manera de trabajar y gestionar los recursos. Las TIC son un elemento clave para que nuestro trabajo sea más productivo: agilizando las comunicaciones, sustentando el trabajo en equipo, gestionando las existencias, realizando análisis financieros, y promocionando nuestros productos en el mercado.[1]

Conforme pasa el tiempo, mantener controlada la información en las diferentes tecnologías ha sido todo un tema de estudio, ya que, al manejarse grandes cantidades de datos e información importante, la gestión debe ser segura y eficiente.

Hace aproximadamente 30 años ocurrió un incidente en la historia de la informática, este afectó a más de 6 mil servidores, el primer malware auto replicable de la historia en la ARPANET (siglas en inglés de Advanced Research Projects Agency Network), fue realizado

[1] I Galo E. Cano-Pita, «Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones».

con el fin de averiguar el tamaño de esta en ese entonces e investigar contraseñas de otras computadoras usando una rutina de búsqueda que cambiaba los nombres de usuarios conocidos, este malware afectó a instituciones gubernamentales estadounidenses conectadas a ARPANET incluyendo el centro de investigación de la NASA.

> Fue en noviembre de 1988, un incidente de seguridad informática conocido como el "gusano de Internet" puso de rodillas a gran parte de Internet. La reacción a este incidente fue aislada y descoordinada, lo que resultó en muchos esfuerzos duplicados y en soluciones conflictivas. Semanas después, se formó el Centro de Coordinación (CERT). Poco después, el Departamento de Energía de los Estados Unidos formó la Capacidad Asesora de Incidentes de Computadoras (CIAC) para servir a sus constituyentes.
>
> Los expertos de la Universidad de California en Berkeley y del Instituto de Tecnología de Massachusetts actuaron rápidamente para capturar el gusano, analizar el programa y encontrar una solución. A la mañana siguiente, cuando aún no habían pasado 12 horas tras el descubrimiento del gusano, el equipo Computer Systems Research Group de Berkeley ya había desarrollado una serie de pasos para detener su propagación. Más tarde esa misma noche, en la Universidad de Purdue, se descubrió otro método para detener la infección, que fue ampliamente difundido.[2]

El Gusano Morris menciona la escritora Gonzáles es “un Malware que se auto-replica y se duplica para propagarse a equipos no infectados. Utilizan partes de un sistema operativo que

[2] «Martes de retrospectiva».

son automáticas e invisibles para el usuario… su replicación incontrolada consume recursos del sistema, lo que ralentiza o detiene otras tareas" (Gonzáles, 2020, párr 4.)

Este Virus se ha convertido en el malware que más alcance ha tenido y uno de los más importantes en la historia, si bien se dice que no este gusano no estaba libre de fallas y que fue un golpe de suerte que haya tenido éxito, lo cierto es que también dejó pérdidas económicas muy significativas.

> Dursegante los siguientes dos años, la cantidad de equipos de respuesta a incidentes continuó creciendo, cada uno con su propio propósito, financiamiento, requisitos de presentación de informes y participación. La interacción entre estos equipos experimentó dificultades debido a diferencias de idioma, zona horaria y estándares o convenciones internacionales. En octubre de 1989, un incidente importante llamado "gusano Wank" destacó la necesidad de una mejor comunicación y coordinación entre los equipos.[3]
>
> Los investigadores de Kasperki Lab coinciden en que "1989 apareció el gusano WANK en los sistemas de la red papelera basura del correo electrónico y. El gusano se propagaba y cambiaba los mensajes del sistema por gusanos contra los asesinos nucleares, invadiendo la computadora." (LAb, 2021, párr.5)
>
> Aproximadamente un año después de la aparición del gusano Morris, apareció el gusano WANK, el cual atacó a los sistemas VMS. Los sistemas VMS según son básicamente un sistema de administración de un sistema de video que puede administrar la información captada por las cámaras de vigilancia, al

[3] «FIRST History».

respecto el escritor Addati explica “están pensados para hacer mucho más fácil el trabajo de los operadores, permitiendo configurar y parametrizar ciertas automatizaciones, como pueden ser alarmas, mapas, interacción con relés o bien integrarse con otros sistemas ya existentes de una organización.” (Addati, 2014, p.3).

De igual forma aparecen en el juego las redes DEnet que según los autores Perdomo, Caizabuano y Altamirano se consideran que este programa tiene como función primordial “permitir la interconexión generalizada de diferentes computadoras principales y redes punto a punto, multipunto o conmutadas de manera tal que los usuarios puedan compartir programas, archivos de datos y dispositivos de terminal remotos.” (2018, p 110).

Los VMS, que corrían en las redes DEnet, aparentemente este otro gusano tampoco ocasionó grandes daños, a excepción del que realizó al infectar los equipos, y de obtener los privilegios adecuados sustituía desplegado del sistema por un anuncio que llenaba la pantalla con la palabra WANK (Worms Against Nuclear Killers), lo más sobresaliente de este gusano es que atacó una red compartida entre la NASA y el departamento de Energía de Estados Unidos, unos días antes de que la NASA lanzara su nave espacial Galileo, pero finalmente después de cuatro días el gusano fue contenido[4]

Así como estos, han existido muchos malware en la historia de la informática, esto lo que ha dado como respuesta es la gran dependencia de la TIC, así como el desarrollo de la seguridad

[4] Comprendamos, «Gusanos Informáticos».

informática, se fueron creando los Centro de Respuesta a Incidentes de Seguridad Computacionales.

Las CSIRT menciona el escritor Lanfranco es “Equipo de respuesta de incidentes de Seguridad Informática” es un equipo que ejecuta, coordina y apoya la respuesta a incidentes de seguridad que afectan a una comunidad objetivo” (Lanfranco, 2019,p.3)

Léase en adelante CSIRT) con el fin de gestionar los incidentes informáticos de alto impacto. Según la revista de la Universidad Nacional Autónoma de México el CSIRT es similar a un equipo de bomberos, entrenados para mitigar tan rápido como sea posible el incidente y que genere el mínimo impacto posible a la organización.

Es indispensable para las compañías idear estrategias preventivas y de soluciones en caso de que ocurra un incidente en la organización de cualquier tipo. Hoy en día la mayoría de las tecnologías en las empresas están conectadas entre sí, hacen uso de contraseñas y ejecutan procesos importantes los cuales pueden estar asociados a fallos e incidentes que paralicen sus funciones.

CONTEXTO TEÓRICO – CONCEPTUAL

Tecnología de Información y Comunicación:

Las Tecnologías de Información es un tema con mucho auge en la actualidad y es que, no es para menos, las personas se encuentran rodeadas de tecnología ya que, sin duda alguna facilita las tareas diarias. Para las empresas no es la excepción, TI es una herramienta útil con la cual pueden agilizar procesos y además obtener ventaja competitiva. Para la presente investigación se debe entender como TI al uso y manejo de computadoras y/o dispositivos electrónicos con los que se gestiona la información.

> Las TIC (Tecnologías de la Información y Comunicaciones) son las tecnologías que se necesitan para la gestión y transformación de la información, y muy en particular el uso de ordenadores y programas que permiten crear, modificar, almacenar, proteger y recuperar esa información. (Duarte, 2007)

> Las Tecnologías de la Información y la Comunicación (TIC) se desarrollan a partir de los avances científicos producidos en los ámbitos de la informática y las telecomunicaciones. Es el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido, video). (Gonzales, 2015)

Procesos de Negocio:

Los Procesos de Negocio son actividades estructuradas realizadas por el ser humano o bien por un dispositivo tecnológico, con el fin de obtener un resultado para lograr objetivos dentro de una organización.

Hitpass (2017) menciona que “un proceso de negocio son los que crean valor para un cliente, además, que es un conjunto de actividades que impulsadas por eventos y ejecutándolas con cierta secuencia”.

> Un proceso consiste en un conjunto de actividades que se ejecutan coordinadamente, en un entorno técnico y organizacional. Estas actividades, miradas en forma conjunta, logran un objetivo empresarial. Cada proceso de negocio es implantado específicamente por una sola organización, pero puede

> interactuar con los procesos de negocio ejecutados por otras organizaciones. (Weske, 2007)

Incidentes en Informática:

Un incidente en informática es un evento no deseado que deja repercusiones que afectan las operaciones de las empresas, estos afectan la integridad de la información y esto trae consigo muchas consecuencias más. Por otro lado, un error informático puede afectar la disponibilidad de la información paralizando las operaciones diarias la organización.

> Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad. (MINTIC, 2016)

> Un incidente de seguridad es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza. (Vieites, 2014)

Impacto Incidente:

Vieites (2014) meciona que “el impacto es la medición y valoración del daño que podría producir a la organización un incidente de seguridad”. Un incidente siempre dejará una repercusión en la empresa, sin embargo, estas se miden por el impacto que generen en esta, puede ser un impacto leve, moderado o alto.

Un análisis de impacto permite identificar los eventos que podrían afectar la continuidad de los sistemas críticos de la información y su impacto mediante la identificación de instalaciones físicas, identificación de sistemas de información, valoración de la criticidad de los sistemas de información y estimación del tiempo de recuperación de cada proceso, que nos permita determinar las estrategias de recuperación a partir de la prioridad y criticidad del proceso y su impacto sobre las operaciones. (Carlos Calderón, 2013)

Probabilidad:

> La probabilidad es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento. La frecuencia de ocurrencia implícita se corresponde con la amenaza. Para estimar la frecuencia podemos basarnos en datos empíricos (datos objetivos) del histórico de la empresa, o en opiniones de expertos o del empresario (datos subjetivos). (Intituto Nacional de Ciberseguridad, 2015)

Urgencia de Incidente:

La urgencia de incidente es el tiempo máximo de demora que tiene el usuario para resolver el accidente informático, además de cuánto tarda en resolverse y ordenados según su impacto en una lista de prioridad, sin embargo, no debe ser tomada como una lista definitiva.

Priorización de Incidentes:

Una vez que se haya determinado el impacto, la probabilidad y la urgencia de incidentes es importante, si bien es cierto todos los incidentes son importantes debe enlistarse los que más impacto generarían en la organización.

> La priorización de incidentes es un concepto de gestión de servicios de TI (ITSM) bien conocido, aunque a menudo poco valorado. La prioridad se compone de dos factores:
>
> - **Impacto** –el grado o cantidad de daño al negocio
> - **Urgencia** – qué tan rápido la empresa necesita una resolución
>
> La combinación de estos dos factores determina la prioridad de un incidente, según las necesidades del negocio. (Tedder, 2018)

La mayoría de los autores coinciden en que la priorización de incidentes está basada en la urgencia y el impacto de estos.

El ciclo de vida de la gestión de incidentes de TI

El proceso de gestión de incidentes se puede resumir de la siguiente manera:

- **Paso 1:** Registro del incidente.
- **Paso 2:** Categorización del incidente.
- **Paso 3:** Priorización del incidente.
- **Paso 4:** Asignación del incidente.

- **Paso 5:** Creación y gestión de tareas.
- **Paso 6:** Gestión y escalamiento del Acuerdo de Nivel de Servicio
- **Paso 7:** Resolución del incidente.
- **Paso 8:** Cierre del incidente. (Zoho Corp, 2020)

Incidentes de acuerdo con su contenido

Los incidentes tienen diferentes tipos de clasificaciones y entre ellas se encuentra por su contenido o el tipo de incidente al cuál se deberá enfrentar la organización. Entre algunos de ellos se encuentran:

- **Contenido abusivo**: son incidentes identificados como spam, contienen comentarios ofensivos, etc.
- **Contenido malicioso o malware**: software o firmware desarrollado para infiltrarse en un equipo o dañarlo sin conocimiento ni consentimiento del propietario, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo del propietario. Dentro de esta tipología se encuentran los virus, troyanos, gusanos, spyware, ransomware, etc. (Cloud, 2020)
- **Acceso indebido o intrusión**: Incidentes en los que se muestre acceso no permitido a cuentas privadas o aplicaciones.
- **Disponibilidad**: ataques que impiden el acceso a un sistema por el usuario (ataques de denegación de servicio).

- **Seguridad/Confidencialidad de la información**: problemas relacionados con el acceso a información y/o modificación no autorizada.
- **Fraude**: incidentes relacionados con usos no autorizados, derechos de autor, suplantación de identidad, phishing y robo de credenciales.
- **Helpdesk**: aquellos incidentes que realizan consultas técnicas envían mensajes informativos y peticiones judiciales.
- **Otros**: se incluyen en esta clasificación aquellas quejas sobre las que no se reportan evidencias o éstas no son contrastadas. (Cloud, 2020)

Amenaza:

Según (Intituto Nacional de Ciberseguridad, 2015) una amenaza es una circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

Seguridad Informática:

> Podemos definir la Seguridad Informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de los usuarios autorizados al sistema. (Vieites, 2014)

La Seguridad Informática se compone por prácticas que protegen, al usuario, a la organización, al cliente y toda persona involucrada que pueda verse afectada ante un ataque o descuido que atente contra la integridad de la información. Tomar medidas, tener un plan

piloto y una adecuada gestión es indispensable para los departamentos de TI de las organizaciones, así como debería serlo para el uso individual de toda persona que tenga acceso a los dispositivos tecnológicos.

Gestión:

Según (Westreicher, 2020) “La gestión es un conjunto de procedimientos y acciones que se llevan a cabo para lograr un determinado objetivo”. La acción de gestionar se realiza por medio de cuatro pasos, entre ellos se encuentra la planificación, la organización, la dirección y el control.

Gestionar es llevar a cabo planes con una secuencia con el fin de lograr los objetivos propuestos. Se puede gestionar los recursos, el tiempo, una empresa, el dinero, también incluye la gestión gubernamental. Los tipos de gestión que existen son:

- Gestión ambiental
- Gestión pública
- Gestión Empresarial
- Gestión del Conocimiento
- Gestión Social

Plan Gestión de Incidencias:

El Plan de Gestión de Incidencias tiene como objetivo la resolución pronta de los incidentes de manera esquematizada que brinde un mejor manejo de las actividades diarias y el trato a las personas involucradas. Es un plan estratégico que permite orientar los procesos de la organización brindando seguimiento y ayudando a disminuir los errores y riesgos.

Gestión de Servicios de TI:

La Gestión de Servicios de TI (ITSM), es planificar, controlar de tal manera que los objetivos de TI estén alineados con los objetivos de la organización. ITSM ayuda administrar los recursos de tecnológicos de la empresa, facilitar las operaciones, reducir los riesgos y principalmente proteger la información, además le brinda un enfoque estratégico para mantenerse atendiendo las necesidades de la empresa y lograr las metas propuestas.

> El personal de TI tiene que tratar muchos temas distintos como Incidencias, Problemas, Cambios y no pueden gestionar esto de la manera correcta. Los directores de cuentas tienen mucho que hacer para sus clientes, que quieren esto y aquello, y sus exigencias cambian cada día. Los directores de TI tienen que llevar una enorme variedad de tareas. Es, por lo tanto, necesario que organizaciones de TI ayuden a clarificar en todo esto. (Vilches, 2010)

Mejora Continua de procesos:

Para lograr mejorar un proceso es necesario conocerlo en su totalidad, desde las personas involucradas hasta el manejo de cada subproceso ya que, es un aspecto clave para brindarle a la organización oportunidades de mejora, por ende, para lograrlo es indispensable:

- Conocer el proceso, el objetivo y aporte que brinda a la empresa
- Identificar las debilidades y fortalezas del procedimiento
- Analizar las oportunidades de mejora
- Conocer las mejores prácticas para el proceso en estudio
- Realizar un plan de acción que esté alineado a los objetivos de la organización
- Implementar el plan de acción.

- Manual de procedimientos
- Seguimiento del proceso una vez implementado con el fin de verificar si la mejora aplicada brinda efecto sobre el proceso

ITIL:

> ITIL (Information Technology Infraestructure Library o Biblioteca de Infraestructura de Tecnologías de la Información) es un compendio de publicaciones, o librería, que describen de manera sistemática un conjunto de "buenas prácticas" para la gestión de los servicios de Tecnología Informática. (Huércano, Manual ITIL V3 Integro)
>
> ITIL nació en la década de 1980, a través de la Agencia Central de Telecomunicaciones y Computación del Gobierno Británico (Central Computer and Telecomunications Agency - CCTA), que ideó y desarrollo una guía para que las oficinas del sector público británico fueran más eficientes en su trabajo y por tanto se redujeran los costes derivados de los recursos TI. Sin embargo, esta guía demostró ser útil para cualquier organización, pudiendo adaptarse según sus circunstancias y necesidades. De hecho, resultó ser tan útil que actualmente ITIL recoge la gestión de los servicios TI como uno de sus apartados, habiéndose ampliado el conjunto de "buenas prácticas" a gestión de la seguridad de la información, gestión de niveles de servicio, perspectiva de negocio, gestión de activos software y gestión de aplicaciones. Estas buenas prácticas provienen de las mejores soluciones posibles que diversos expertos han puesto en marcha en sus organizaciones a la hora de

entregar de servicios TI, por lo que en ocasiones el modelo puede carecer de coherencia. (Huércano, Manual ITIL V3 Integro)

Normas ITIL V3:

La última versión vio la luz en 2007, denominada como ITIL v3. En esta versión se ha realizado un refresco (refreshment en palabras de la OGC), agrupando los elementos principales de ITIL en 5 volúmenes, que pueden encontrarse en la actualidad con los siguientes títulos (en inglés original) (Huércano, Manual ITIL V3 Integro)

- ITIL v3 Service Strategy (SS)
- ITIL v3 Service Design (SD)
- ITIL v3 Service Operation (SO)
- ITIL v3 Continual Service Improvement (CST)
- ITIL v3 Service Transition (ST)

- **Metodología ITIL V3:**

ITIL, Information Technology Infraestructure Library es un set de documentos donde se describen los procesos requeridos para la gestión eficiente y efectiva de los Servicios de Tecnologías de Información dentro de una organización. Son un conjunto de mejores prácticas y estándares en procesos para hacer más eficiente el diseño y administración de las infraestructuras de datos dentro de la organización. Es un "marco de trabajo" (framework) para la Administración de Procesos de TI. Esta metodología se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos

que cubren las actividades más importantes de las organizaciones. Garantizando así los niveles de servicio establecidos entre la organización y sus clientes. (JAURÈS, 2006)

Objetivos de ITIL V3:

El objetivo que persigue ITIL es diseminar las mejores prácticas en la gestión de servicios de Tecnologías de Información de forma sistemática y coherentemente. El planteo principal se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos. La idea subyacente es que, sin importar el rubro, la tecnología es cada vez más crítica para el negocio de cualquier empresa. Esto quiere decir que, si la tecnología no es administrada eficientemente, el negocio no funciona, lo que se vuelve más cierto al ser más dependiente de la infraestructura tecnológica. En este sentido, los estándares ITIL exigen un replanteamiento del área tecnológica y la definición de los elementos y procesos "críticos" dentro de la empresa. Esta metodología está especialmente desarrollada para reducir los costos de provisión y soporte de los servicios de TI, al mismo tiempo que se garantizan los requerimientos de la información en cuanto a seguridad manteniendo e incrementando sus niveles de fiabilidad, consistencia y calidad. (JAURÈS, 2006)

Fases de ITIL V3:

Las cinco fases del ciclo de vida de los servicios que propone ITIL V3 son las siguientes:

1) Estrategia de servicio: se ocupa del diseño, desarrollo e implantación de la gestión de servicios de TI como activo estratégico para la organización. El proceso de la estrategia de servicios comprende: la gestión de la cartera de servicios, la gestión financiera de TI y la gestión de la demanda.

2) Diseño del servicio: se encarga del diseño y desarrollo de los servicios y de los correspondientes procesos necesarios para apoyar dichos servicios. Entre los procesos del diseño de servicios figuran: la gestión del catálogo de servicios, la gestión de los niveles de servicio, la gestión de la disponibilidad, la gestión de la capacidad, la gestión de la continuidad de los servicios de TI, la gestión de la seguridad de la información y la gestión de proveedores.

3) Transición del servicio: se ocupa de la gestión y coordinación de los procesos, los sistemas y las funciones que se precisan para crear, comprobar e implantar servicios nuevos o modificados en las operaciones. Entre los procesos de transición del servicio figuran: la planificación y soporte de la transición, la gestión del cambio, la gestión de la configuración y los activos del servicio, la gestión del lanzamiento y el despliegue, la validación y comprobación del servicio, la evaluación y la gestión del conocimiento.

4) Operaciones de servicio: se ocupa de la coordinación, las actividades y los procesos necesarios para gestionar los servicios destinados a usuarios y clientes de empresas dentro de los niveles de servicio acordados. Los procesos de las operaciones de servicio son los siguientes: la gestión de eventos, el cumplimiento de peticiones, la gestión de incidencias, la gestión de problemas y la gestión del acceso.

5) Mejora continua: se ocupa de mejorar los servicios de forma constante para garantizar a las organizaciones que los servicios responden a las necesidades del negocio. La mejora continua trata sobre cómo mejorar el servicio, los procesos y las actividades de cada una de las fases del ciclo de vida. (Figuerola, 2012)

Beneficios de ITIL para las organizaciones:

La metodología de ITIL permite establecer roles y responsabilidades con el fin de mejorar la práctica, la comunicación y administración del proceso. Además, por medio de ITIL, las organizaciones pueden alinear los procesos a los objetivos de la organización, brindando de esta manera una mejora en la productividad, reducción de costos, mejora en los procesos de TI y por ende en la satisfacción del cliente.

Tener un proceso trabajando correctamente permite a la organización ser más eficiente y ayudarla a lograr las metas determinadas haciéndola crecer y madurar.

Proceso de Gestión de Incidencias:

Recepción y registro. El registro de la incidencia, tras su recepción por los canales habituales, debe incluir al menos los siguientes apartados:

- Servicios afectados.

- Posibles causas.

- Nivel de prioridad.

- Impacto.

- Recursos asignados para su resolución.

- Estado de la incidencia.

Este registro debe realizarse siempre que ocurra una incidencia, para que se lleve a cabo un seguimiento de la misma y pueda ser derivado a la gestión de problemas con una serie de datos informativos anexados; esto a la vez evita la pérdida de información, incrementando la eficiencia de las personas involucradas y del proceso. (Huércano, Manual ITIL V3 Integro)

Clasificación. La clasificación del incidente tiene como objetivo establecer su impacto en la organización y su prioridad de resolución. Dependiendo de su urgencia y su impacto se asignarán unos recursos y se establecerá un tiempo de resolución. Este tiempo, su impacto y su urgencia pueden variar a lo largo del análisis de la incidencia: pueden ampliarse por fallos en la estimación, como también recortarse, por soluciones temporales eficaces para el cierre de la incidencia. (Huércano, Manual ITIL V3 Integro)

Investigación y diagnóstico. La investigación de la solución dispone de dos fases:

- Comparación. Búsqueda en la base de datos (BBDD) de incidencias que tengan una raíz similar y, por lo tanto, una solución rápida y contrastada del problema. Si no existe ninguna, se pasará a la siguiente fase.
- Investigación y diagnóstico. Se analiza si el nivel 0 o primer nivel del centro de servicios tiene capacidad para resolver esta incidencia. Si no es así, se procederá a la asignación de esta o a su escalado (Huércano, Manual ITIL V3 Integro)

Escalado. El escalado es la asignación de la incidencia a un nivel superior del centro de servicios o a un superior jerárquico para la toma de decisiones de cambio en la forma de abordar la incidencia. Estos son los dos tipos de escalado existentes, y se definen de la siguiente manera:

- Escalado funcional: se utiliza un técnico o especialista de mayor nivel o conocimiento para su resolución.
- Escalado jerárquico: se deriva a un superior jerárquico la decisión de ampliar los recursos asignados o derivar finalmente la incidencia a otro tipo de resolución. (Huércano, Manual ITIL V3 Integro)

Seguimiento. El seguimiento de la incidencia tiene relación directa con el nivel en el que se haya resuelto. Si ha sido el primer nivel el que ha propuesto la solución, será responsabilidad de la Gestión de Incidencias o del Centro de Servicios; sin embargo, si la incidencia es derivada porque su resolución necesita de cambios, pasará a ser responsabilidad del proceso de Gestión de Cambios. (Huércano, Manual ITIL V3 Integro)

Para una mejor comprensión del lector se presentan seguidamente términos que serán empleados más adelante en la investigación.

Información se considera que información es un elemento clave para fundamentar ideas en cada ser humano de forma racional y le permite centrarse por medio de ello en la toma de decisiones, resolución de conflictos y el trabajo en equipo. Es por ello que la escritora Morales la define como "conjunto de datos que contiene un significado, y que una vez organizados aportan un conocimiento y la posibilidad de establecer una idea, objetivo o acción en torno a algo." (Morales, 2019, p.1)

A raíz de lo anterior se presume que la información genera conocimiento y este dependerá a su vez del valor, significancia y que cada persona le dé y el área a la que ha sometido su búsqueda de datos para la toma de decisiones.

La frecuencia según menciona la real Academia Española es “una repetición de un hecho o un suceso”. En la cotidianidad de la empresa pueden surgir una gran variedad de incidentes y esta debe resolver lo más pronto posible para lograr la satisfacción plena de sus clientes regulares a la vez que se reducen costos y se incrementa la credibilidad de la empresa. (Española, 2020)

Se considera que para que la empresa aprecie el valor del cambio se deben implementar área de mejoras. Para que ello el departamento de TI debe optimizar cada área que presente debilidad.

Áreas de Mejora hace referencia al “conjunto de aspectos de la organización de la actividad y sus interrelaciones que no funciona o funciona de manera inefectiva; es decir, no es eficaz y/o no es eficiente.” Estas áreas de mejora se cree que pueden mejorar tanto las capacidades de los trabajadores como los procesos que al final se verán reflejados con los resultados en el departamento y por tanto en la empresa en general. (Valles, 2016, p.1)

Para que los cambios sean eficientes y eficaces a la hora de implementación y seguimiento es necesario mantener un proceso de control de los estándares que permita validar, comprobar y verificar que toso está funcionando acorde a lo establecido, es decir que se cumplan los objetivos propuestos.

Procesos de Control, comenta la escritora Jauregui “consiste en la medición y corrección del desempeño para garantizar que los objetivos de la empresa y los planes diseñados para alcanzarlos se cumplan”. (2014, párr.1)

Al establecer procesos de control la empresa tendrá un mayor orden, control y accesibilidad en sus procesos; lo que a su vez permitirá realizar las correcciones oportunas en el momento

que se requiera y así lograr con mayor eficiencia y eficacia logra de objetivos y la satisfacción de sus usuarios finales.

Aunado a todo lo anterior se necesita implementar en la mentalidad de los trabajadores la idea que las mejores prácticas contribuirán al logro de los objetivos y evitar los disgustos de los clientes, dado que estas disminuyen los errores, maximizan los recursos y se obtienen los resultados esperados. Las **Mejores Prácticas** "hace referencia a toda experiencia guiada por principios, objetivos y procedimientos apropiados que se adecúan a una determinada normativa o a un parámetro consensuado, así como también toda experiencia que ha arrojado resultados positivos" (Montoro, 2020)

Blockchain empresas rastrear una transacción y trabajar con partes no confiables sin la necesidad de una parte centralizada (es decir, un banco). Esto reduce en gran medida la fricción en los negocios y tiene aplicaciones que comenzaron en las finanzas. (interactiva, 2020, párr.9)

CAPÍTULO lll:

MARCO METODOLÓGICO

TIPO DE INVESTIGACIÓN

La investigación busca y recolecta información, con el fin de comprender cómo se manejan y resuelven los incidentes, además de conocer la frecuencia con la que ocurren los incidentes y el impacto que estos generan para la organización, para de este modo definir las áreas de mejoras que agilicen el proceso como tal. Por la naturaleza de este estudio, el tipo de investigación a realizar corresponde a una investigación mixta.

Con la utilización del método cualitativo se pueden identificar los procesos de control de incidentes con los que cuenta la organización de tal manera que se permita analizar las causas, la funcionalidad, la eficiencia de dicho proceso con el fin de brindar soluciones según los resultados obtenidos. Además, investigar las mejores prácticas que brinda el mercado para el manejo y control de incidentes que se alinee a los objetivos de la organización.

Por otro lado, el método cuantitativo permite identificar la probabilidad y el impacto de los riesgos al no manejar correctamente los incidentes permitirá tener una percepción más exacta para que ayude a realizar un análisis estadístico que permita tomar mejores decisiones basadas en las necesidades y requerimientos de la organización.

Al comprender las necesidades del departamento de TI y de la organización basado en resultados tanto cualitativos como cuantitativos se abre camino para una propuesta de una política para el manejo de incidentes de la organización acertada.

ENFOQUE DE LA INVESTIGACIÓN

La investigación que se pretende realizar es basada en la mejora del proceso de control de incidentes en el departamento de TI de INOLASA, por lo cual será bajo el enfoque cuantitativo y cualitativo ya que, por medio de la recolección y el análisis de datos del proceso de actual del manejo de incidentes se procura proveer una propuesta de mejora basado en las mejores prácticas de gestión de incidentes, además tomando en cuenta la frecuencia, probabilidad e impacto que puedan generar a la empresa.

Como lo menciona (Sampieri, 2014) el enfoque cualitativo: Utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación.

Por otro lado, (Sampieri, 2014) menciona que: El enfoque cuantitativo refleja la necesidad de medir y estimar magnitudes de los fenómenos o problemas de investigación: ¿cada cuánto ocurren y con qué magnitud?

FUENTES DE INFORMACIÓN

Según (Marisol Maranto, 2015): Una fuente de información es todo aquello que nos proporciona datos para reconstruir hechos y las bases del conocimiento.

Las fuentes de información son una herramienta que colabora en la elaboración de la investigación, sustentando de manera teórica y práctica el desarrollo del proyecto. Las siguientes son las fuentes empleadas como apoyo a la investigación:

Fuentes Primarias

Como fuente primaria de información está la entrevista al encargado del Departamento de TI en INOLASA. Además, una entrevista a los usuarios finales, a quienes utilizan los equipos del departamento diariamente.

> Este sistema se emplea para la recopilación de información, cara a cara, para captar tanto las opiniones como los criterios personales, formas de pensar y emociones de los entrevistados. Mediante las entrevistas, se profundiza sobre los juicios emitidos para que el investigador realice más adelante las interpretaciones pertinentes. (Razo, 2020)

Fuentes Secundarias

Como fuentes secundarias se toma como todo aquel material teórico de libros, informes, sitios web, tesis o publicaciones que brindarán información básica y soporte a la investigación con el fin de validar cualquier comentario propio. Además, la información expuesta en el capítulo dos se recopiló de fuentes con notoriedad y credibilidad acerca de los temas relacionados a la gestión de incidentes. Las fuentes se encuentran debidamente referenciadas al final, en la sección de bibliografía.

Sujetos de Información

Los sujetos de información son aquellas personas que pueden brindar datos que sustenten y que estén relacionados con la investigación que se realiza. En esta investigación se tratará con los funcionarios del departamento de TI de INOLASA, así como el gerente de este departamento. Además, puede que en algún momento el criterio de algún funcionario fuera del departamento de TI sea vital y se requiera dicha intervención.

Técnicas y Herramientas de Recolección de Datos

Para esta investigación se detallan a continuación los instrumentos a utilizar para el análisis, la interpretación de los resultados y la toma de decisiones sobre este proyecto.

Entrevista

Como principal técnica en este trabajo debido a la facilidad de obtener información de primera mano, confiable y con la opción de que el sujeto pueda extenderse y brindar datos relevantes para la investigación.

La entrevista es aplicada a todo el departamento de TI tanto en la sede central como en la sede ubicada en Puntarenas, la entrevista se aplica debido a la situación actual del país y la ubicación de las sedes de manera remota, por medio de Teams, Skype o WhatsApp.

Encuesta

Como instrumento complementario a la investigación se procede a utilizar la encuesta, con el fin de que los usuarios finales brinden un criterio acerca del servicio, esto permitirá obtener la percepción sobre los servicios y de esta manera brindar conclusiones y exponer los beneficios que se obtendrían con esta investigación.

Al igual que la entrevista, las encuestas se realizan de manera remota, facilitando así la participación de los usuarios.

Variables de Investigación

Seguidamente se presenta el cuadro con las variables que conforman la investigación, en donde se establecen los indicadores que pueden medir aspectos concretos delimitando a la misma.

Cuadro número 1

Cuadro de variables

Objetivo Específico	Variable	Definición Conceptual
Identificar la situación actual del proceso de control de incidentes de acuerdo con la información recopilada sobre la atención a las situaciones adversas de INOLASA.	Realizar el estudio de la atención a las situaciones adversas	Definición de elementos para el estudio de atención a las situaciones adversas
Analizar las debilidades del proceso de incidentes dentro del departamento de Tecnologías de Información con el fin de priorizar los problemas en función del impacto que generen.	Priorizar los incidentes según el impacto que generen	Definición de los incidentes según el impacto que generan
Plantear una propuesta de gestión de incidencias en TI que permita la mejora de la situación actual utilizando como referencia las mejores prácticas en la industria.	Proponer una mejora para la situación actual basada en la Mejores prácticas	Definición de los elementos que mejoran la situación actual de acuerdo con las mejores prácticas
Plantear una propuesta de capacitación a los colaboradores para la aplicación del plan de gestión para el manejo de incidentes.	Proponer un plan de capacitación al personal para incrementar el nivel de eficiencia del proceso.	Definición de elementos importantes para las capacitaciones que ayuden a incrementar el nivel de eficiencia.

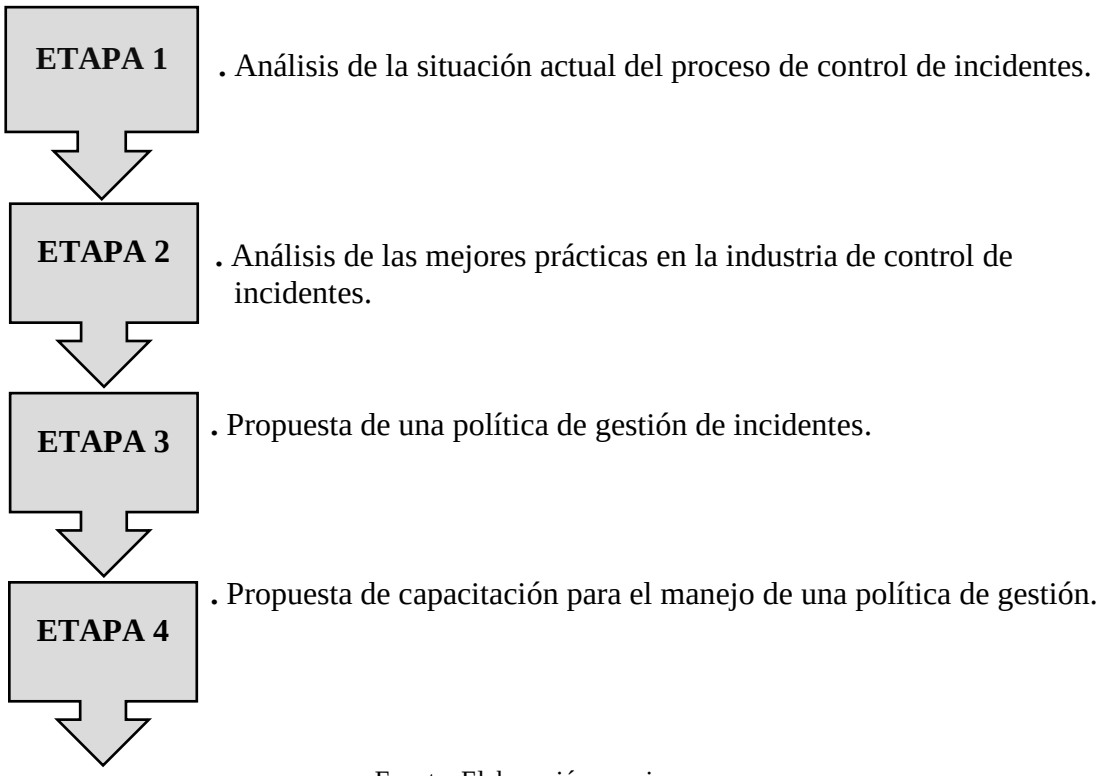
Fuente: elaboración propia

Diseño de Investigación

El diseño de la investigación nos permite establecer parámetros y además brinda una estructura al investigador con la cual realiza el proyecto por medio de etapas. Las etapas que conforman el diseño de la investigación ayudan a lograr el objetivo propuesto. A continuación, se muestra el conjunto de etapas para la propuesta de una política de manejo de incidentes en el departamento de TI de INOLASA.

Imagen número 3

Diagrama etapas del diseño de la investigación



Fuente: Elaboración propia

Cada una de esas etapas requiere de actividades para su realización, mismas que se detallan a continuación:

Etapa 1: Análisis de la Situación Actual

Para que el proyecto tenga sentido y genere valor para la organización es indispensable realizar un análisis tanto técnico como operacional dentro del departamento de TI de INOLASA. Analizar cómo gestionan los incidentes, la frecuencia y quiénes llevan esta tarea es fundamental para comprender las debilidades y las fortalezas de la empresa.

Por medio de entrevistas y encuestas lo que se busca es recopilar información que sustente y permita realizar un análisis de tal forma que se pueda estudiar las necesidades del proceso de control. Este paso es importante para realizar una propuesta acertada y beneficiosa para la empresa.

Etapa 2: Análisis de las mejores prácticas en la industria de control de incidentes

El objetivo de esta etapa es llegar a conocer las mejores prácticas existentes en la industria y sus características, de esta manera se seleccionarían la más apropiada para la empresa, basándose también, en las políticas líderes en el mercado, las más utilizadas y las mejores calificadas.

Como fuente de investigación se utilizará la bibliografía, se recopilará y estudiará la información más reciente y confiable con el fin de que brinde fuertes bases teóricas sobre las diferentes opciones disponibles en el mercado para que permita realizar una propuesta de valor a la organización.

Etapa 3: Propuesta de una política de gestión de incidentes

La finalidad de esta etapa consta de realizar una propuesta que se ajuste a las necesidades de la organización, tomando en cuenta los resultados obtenidos en el análisis de la situación actual por medio de un diagnóstico y un conjunto de herramientas y técnicas que determinen el estado del departamento de TI en cuanto a manejo de incidentes y además soportada en la teoría investigada a lo largo de este proyecto para que de esta manera la propuesta se adapte al proceso y logre cumplir los objetivos de dicho departamento.

Para lograr el éxito de esta selección se contará con la ayuda de los funcionarios del departamento de TI de INOLASA o involucrados que logren comprender el alcance y la necesidad de dicho sector, además tenga la disponibilidad de horario para aclarar preguntas que puedan surgir dicha selección.

Etapa 4: Propuesta de Capacitación para el manejo de una política de gestión

Como última etapa se tiene la propuesta de capacitación del personal involucrado en el proceso de control de incidentes con la finalidad de que se implemente la política propuesta de la manera correcta y permita obtener los resultados deseados. Capacitar a los funcionarios permitirá tener un marco de trabajo que además disminuya el margen de error haciendo el manejo de incidentes informáticos un proceso eficiente.

Matriz de Coherencia:

En esta sección se muestra una matriz de coherencia que permite al lector visualizar las relaciones entre objetivos, entregables, instrumentos y temas del marco teórico, ayudando de esta manera a entender el proceso metodológico desarrollado en la sección del diseño de la investigación.

Seguidamente se presenta la matriz de coherencia.

Cuadro número 2

Matriz de coherencia

Objetivo	Entregable	Etapa de la metodología del proyecto que posibilita la realización del entregable	Técnicas/métodos de recolección de la información	Instrumentos	Temas relacionados en el marco teórico
Identificar la situación actual del proceso de control de incidentes de acuerdo con la información recopilada sobre la atención a las situaciones adversas de INOLASA.	Análisis de la Situación Actual del proceso de control de incidentes	Etapa 1	Entrevista	Cuestionario	Proceso de Negocio Incidentes de Informática
Analizar las debilidades del proceso de incidentes dentro del departamento de Tecnologías de Información con el fin de priorizar los problemas en función del impacto que generen.	Análisis de la Situación Actual del proceso de control de incidentes	Etapa 1	Encuesta	Cuestionario	Impacto de Incidentes Probabilidad de impacto de incidentes Riesgos informáticos Clasificación de los incidentes informáticos
Plantear una propuesta de gestión de incidencias en TI que permita la mejora de la situación actual utilizando como referencia las mejores prácticas en la industria.	Análisis de las mejores prácticas en la industria de control de incidentes	Etapa 2 y 3	Entrevista	Cuestionario	Normas ITIL V3 Metodología de ITIL V3 Objetivo de ITIL V3 Normas ITIL

Plantear una propuesta de capacitación a los colaboradores para la aplicación del plan de gestión para el manejo de incidentes.	Análisis de los elementos a capacitar para el manejo correcto de una política de gestión	Etapa 3 y 4	Encuesta	Cuestionario	Gestión de Servicios de TI Plan de Gestión

Fuente: elaboración propia

CAPÍTULO lV:

DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

DIAGNÓSTICO ADMINISTRATIVO U OPERATIVO

El departamento de TI de INOLASA trabaja fuerte y de manera comprometida diariamente para mantener las operaciones de los demás departamentos y brindar soporte a los equipos tecnológicos con los que cuenta la empresa además de brindar soluciones informáticas a los problemas que se presenten.

Cada funcionario cuenta con un equipo tecnológico el cual tiene asignado un usuario y contraseña con la finalidad de mantener la seguridad, además INOLASA cuenta con la suscripción a Microsoft Office 365 proveyendo a cada colaborador de correo institucional y acceso a todas las aplicaciones que dicha plataforma ofrece tales como WORD, EXCEL (hoja de cálculo), POWER POINT(para realizar presentaciones), OUTLOOK(correo electrónico y agenda personal),por ejemplo la herramienta TEAMS que la utilizan para comunicarse; al igual que Yammer, Sharepoint con la cual pueden compartirse conocimiento y fortalecer el trabajo en equipo, aplicaciones como Word, PowerPoint para el día a día, Planner y One Drive también son de gran ayuda para el personal de INOLASA.

El servicio que brinda el departamento de TI a la organización es muy importante ya que, permite la obtención de la información inmediata y de manera segura, salvaguardando la integridad de los datos e información sensible de la organización.

La empresa cuenta con equipo tecnológico de calidad, el departamento de TI vela para que la organización invierta en equipo que ayude al mejoramiento de los procesos de negocio impactando directamente en la reducción de costos utilizando por ejemplo equipos amigables con el medio ambiente para mantener su producción segura y sostenible.

A inicios del 2020 el departamento de tecnología se ha visto en la obligación de mantener la organización trabajando debido a los cambios surgidos a nivel nacional por Covid-19, gracias a una rápida acción los departamentos han podido laborar de manera virtual, así mismo otras acciones necesarias como capacitaciones se han realizado en la virtualidad por medio de aplicaciones como Teams o Zoom.

DIAGNÓSTICO TÉCNICO

INOLASA es una empresa que siempre se enfoca en brindar calidad en sus productos, por ende, busca contar con los mejores equipos y la máxima tecnología posible para mejorar sus tareas diarias. El área de tecnología cuenta con personal con conocimiento en el tema, pero requiere de inversión en capacitación por parte de la alta gerencia, para reafirmar sus habilidades y brindar nuevas con ello, se dará más confianza al trabajador para realizar las funciones respectivas de su puesto y el logro de objetivos del mismo.

Al incrementar sus conocimientos y habilidades se considera como una ventaja competitiva ya que, todos los funcionarios conocen a la perfección las tareas y además conocen los puntos de mejora para trabajar en ello y obtener el máximo provecho de las fortalezas. El personal en el departamento de TI no es rotativo y esto respalda el alto grado de experiencia y lo calificados que están para los puestos que ocupan en la organización.

Una de las tareas del gerente de TI, es adquirir los mejores equipos para la organización, para lo cual esta persona realiza una toma de requerimientos, que se obtienen a través de los usuarios finales por medio de encuestas, entrevistas en donde se le cuestiona al usuario ¿para qué van a utilizar el producto? ¿Cómo lo van a utilizar?, ¿Qué va a almacenar?, posterior a eso se realizan las especificaciones, casos de uso e inspecciones además dependiendo del caso se utilizan prototipos, es decir una pequeña investigación para un análisis exhaustivo y de acuerdo con estos realiza un estudio para que la compra sea efectiva y conveniente para

la compañía. Entre algunas de las marcas de los dispositivos de computación que INOLASA tiende a preferir se encuentran DELL y LENOVO ya que según los requerimientos de la empresa y el departamento de TI se acoplan a las necesidades y se adaptan a la velocidad de avance tecnológico de la corporación.

En cuanto a Software, INOLASA utiliza un Sistema de Planificación de Recursos Empresariales (ERP) en este caso el que poseen es de Softland Exactus y Office 365 de Microsoft ya que, estos son modernos y tienen la capacidad de reunir los distintos procesos facilitando la colaboración, de esta manera se obtiene una mejor organización, optimización y mejora en los resultados.

El manejo de incidentes es un área de mejora que el gerente del departamento de TI tiene en la lista de prioridades, comprende la oportunidad de mejorar los procesos de cambio.

Actualmente se presentan entre 10 a 15 incidentes diarios de los cuales su mayoría podrían resolverse en un menor tiempo, si se contara con una política para gestionarlos. La empresa cuenta con una herramienta Service Desk que brinda un soporte importante de TI a la organización, que permitiría resolver los problemas ágilmente si se complementara con una política para la gestión de las incidencias. El ServiceDesk Plus de ManageEngine permite la gestión exhaustiva de incidentes y a pesar de los esfuerzos la resolución de incidentes necesita mejorarse ya que, no todos se concluyen de forma pronta y algunos requieren de más tiempo para ser corregidos, la organización espera con este medio y que otros factores como una normativa le permitan gestionar adecuadamente todo lo relacionado con el proceso de control de incidentes

Por otro lado, TI se encuentra muy bien respaldado con algunos equipos y dispositivos de repuestos o “extras” en caso de surgir algún inconveniente permitiéndoles reemplazar y avanzar con el trabajo. Esto se realiza en áreas previamente identificadas y críticas que deben mantener cierta continuidad de la operación.

DIAGNÓSTICO DE PERCEPCIÓN

Como se mencionó en el Capítulo lll de este trabajo, las técnicas empleadas para la recolección de datos fueron la entrevista y la encuesta, las cuales son necesarias para la interpretación de los datos y análisis de la situación actual de la organización incluyendo los elementos de los procesos administrativos y técnicos.

Una vez que se aplicaron las entrevistas, se analizaron y se clasificaron las respuestas en las siguientes categorías:

Procedimiento: Mediante las entrevistas realizadas para la recopilación de datos se obtuvo información general de las actividades y procesos que se manejan en el departamento de TI y al ser consultados sobre la manera en que se efectúa el proceso de manejo de incidentes se deduce que el usuario en el primer nivel interactúa con la herramienta Service Desk para reportar el incidente con una breve descripción y los “síntomas” o los detalles del problema, además el usuario especifica la categoría. Por consiguiente, el sistema le asigna un técnico de acuerdo con el tipo de incidente que haya sido reportado, el cual le brindará el soporte y el seguimiento. Por otro lado, también algunos de los incidentes son reportados vía llamada telefónica o correo, por lo cual el proceso es diferente, ya que el técnico toma los datos y realiza el proceso manualmente.

En algunas ocasiones cuando un técnico desconoce la solución se recurre a proveedores externos especialistas en el tema a resolver.

Recursos actuales de la empresa: Con la finalidad de garantizar la continuidad de los procesos de negocio, INOLASA cuenta con recursos valiosos para el este fin, como los es el recurso humano indispensable para realizar las tareas de cada puesto y sacar abante los objetivos de la organización. En cuanto al recurso financiero cuentan con un capital sólido

desde su fundación el cual se ha ido incrementando con el pasar de los años, en el caso de los recursos tecnológicos como computadoras, internet, impresoras teléfonos, intranet, Antivirus, software, Tablet y por último el recurso físico poseen su propio edificio, autos para el transporte de sus trabajadores, materia y maquinaria entre otros.

Por ejemplo, en la bodega, principalmente periféricos tales como monitores, impresoras, discos duros, módems. La empresa cuenta con estos equipos como manera de prevención, ya que en algunas ocasiones los procesos críticos no pueden esperar o retrasarse porque esto implica inactividad en tareas críticas de los departamentos, por ende, la manera más rápida y eficaz de resolver estos casos es reemplazar el equipo. Así mismo el personal de TI es el único con acceso a estos dispositivos dado que deben llevar el registro de los dispositivos dañados, los despachados del almacén y los que deben ir a reparación.

Tiempos de Repuesta: Al ser consultado el tema de los tiempos de respuesta a los incidentes los encuestados coinciden en el tiempo estimado de la atención a los incidentes siendo aproximadamente de una hora a máximo dos horas. Cabe destacar que también algunos casos toman mucho más tiempo, desde un día completo hasta una semana, esto contando el tiempo desde que el usuario lo reporta por medio de la herramienta o los otros medios mencionados anteriormente.

Frecuencia: Los resultados obtenidos muestran que la institución registra entre 10 a 15 incidentes diarios de los cuales la mayoría de los que se reportan son sobre autentificación por olvido de contraseñas, problemas con el correo institucional o falla en los periféricos. Por otro lado, tres de cada diez incidentes son de carácter urgente.

Conocimiento de temas: Este es un punto importante tanto para la organización como para los funcionarios del departamento de TI, porque como un recurso de competitividad y altos estándares todos los trabajadores del área de TI deben conocer sobre la gestión de la empresa, gestión de atención al cliente, los productos que la empresa ofrece, de igual forma manejar temas de redes móviles, intranets, políticas de seguridad, desarrollo de software esto porque permite la mejora continua tanto profesionalmente como personalmente.

INOLASA requiere de más esfuerzos y recursos económicos, de tiempo y humanos para lograr incorporar y aplicar un plan de capacitación a sus colaboradores, dirigida a todos sus

trabajadores pero en especial a los funcionarios del Departamento de Tecnología sobre actualizaciones y temas innovadores como por ejemplo ciberseguridad, redes 5G, Blockchain para verificar y dar seguimiento a sus transacciones aunado a esto mejorar en todo lo relacionado con atención al cliente o nuevos en el mercado, en la lista de tópicos de interés de la empresa se encuentran las actualizaciones sobre ERP, temas sobre la nube, realidad aumentada, transformación digital, experiencia al cliente, ética digital y muchos más. Estas capacitaciones deberían realizarse cada 6 meses aproximadamente o al menos una vez al año.

El personal de la empresa debería tener acceso a las capacitaciones de manera rotativa y en modalidades presencial y virtual para que de esa manera todos reciban la formación necesaria para incrementar y reforzar sus habilidades. Si bien es cierto una misma persona puede no tener experiencia en todas las áreas, la empresa tiene asignado un colaborador para cada una, según su nivel de experiencia, ya que cada colaborador tiene una especialización, permitiéndoles resolver la mayoría de los incidentes y en caso de que estos no puedan ser resueltos por los funcionarios, el gerente de TI toma medidas sobre el caso, en algunas ocasiones investiga y aprende sobre cómo solucionarlos o bien, por medio de contratación de proveedores expertos en el tema. Aquellos casos que no se logran resolver, son archivados en una base de datos para ser considerados como referente de mejora porque los altos gerentes saben que se pierde credibilidad con el cliente y deben a mediano plazo dar propuestas que ratifiquen la transparencia de esta ante los consumidores.

Satisfacción del personal: En términos generales, los funcionarios del departamento de TI se sienten satisfechos con todas las oportunidades que les brinda la empresa y los beneficios que ofrece trabajar en INOLASA. Sin embargo, no lo están en su totalidad con la manera en que se manejan los incidentes, ya que concuerda en que se pierde mucho tiempo y consideran que el tener una política formal sería de mucha ayuda en el día a día.

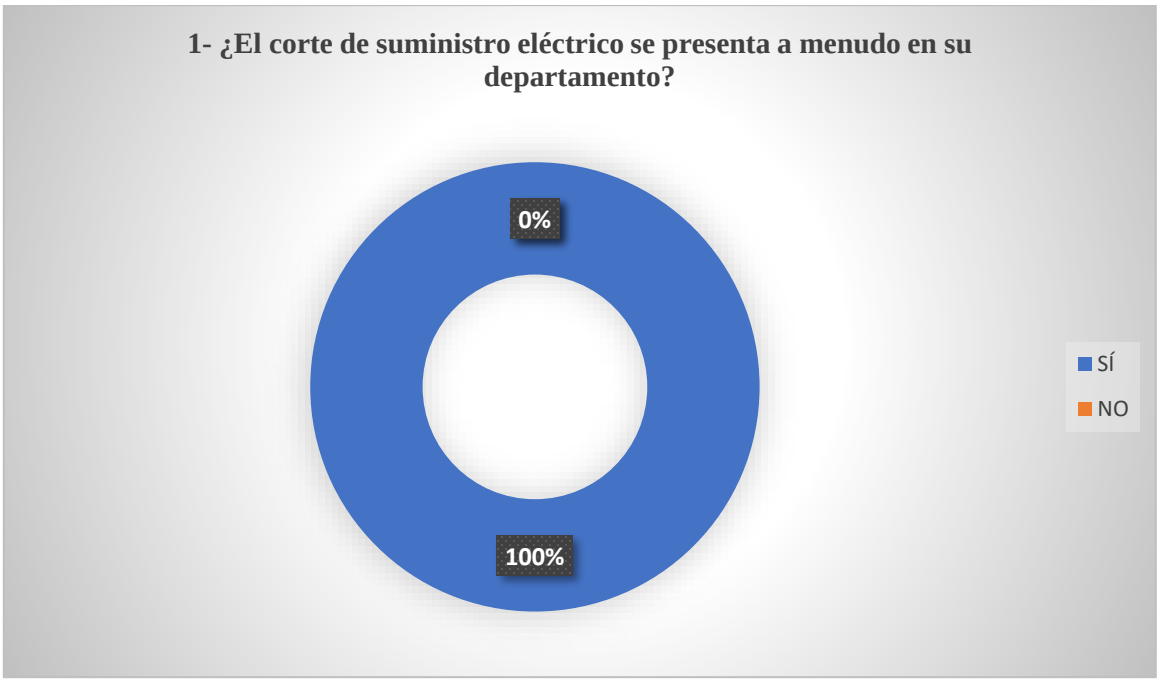
Como segunda herramienta para la investigación se utilizó la encuesta la cual estaba conformada por 26 preguntas en las cuales se buscó determinar los incidentes que propios de la organización, además, la frecuencia con que ocurren los incidentes y el tiempo aproximado de solución.

Finalmente se consulta sobre la satisfacción del personal del departamento de TI y su opinión con respecto a la implementación de una política que les ayude al proceso de control de incidentes y la calificación que le dan al nivel de conocimiento de sí mismos en temas importantes para solucionar los problemas.

Seguidamente se presenta el análisis de la información mediante gráficos.

Gráfico número 1

Frecuencia de cortes eléctricos en el departamento de TI

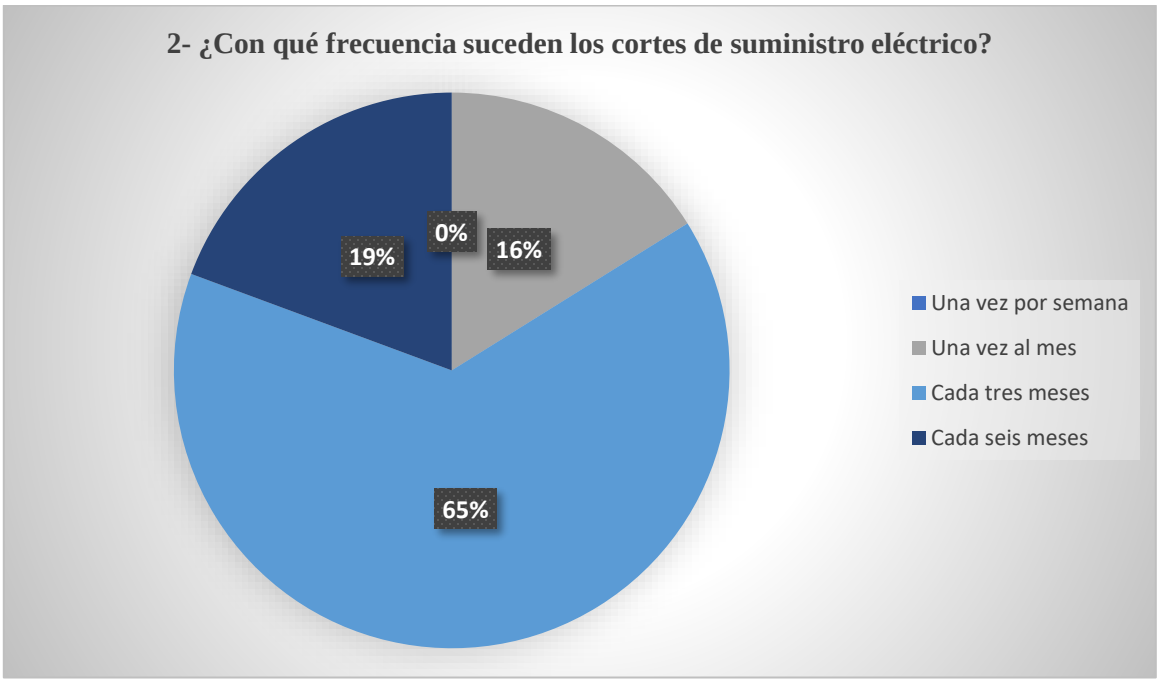


Fuente: elaboración propia

Al ser encuestados sobre si suceden incidentes de corte de suministro eléctrico, un 100% contestó que, si suceden en la organización, lo cual no les permite avanzar como quisieran. Lo implica un retraso en sus funciones cotidianas y de no haber guardado la información constantemente, esta podría perderse durante el apagón, incluso poner en riesgo el equipo hasta el grado de ser irreparable.

Gráfico número 2

Frecuencia con que se presentan cortes de suministros eléctricos

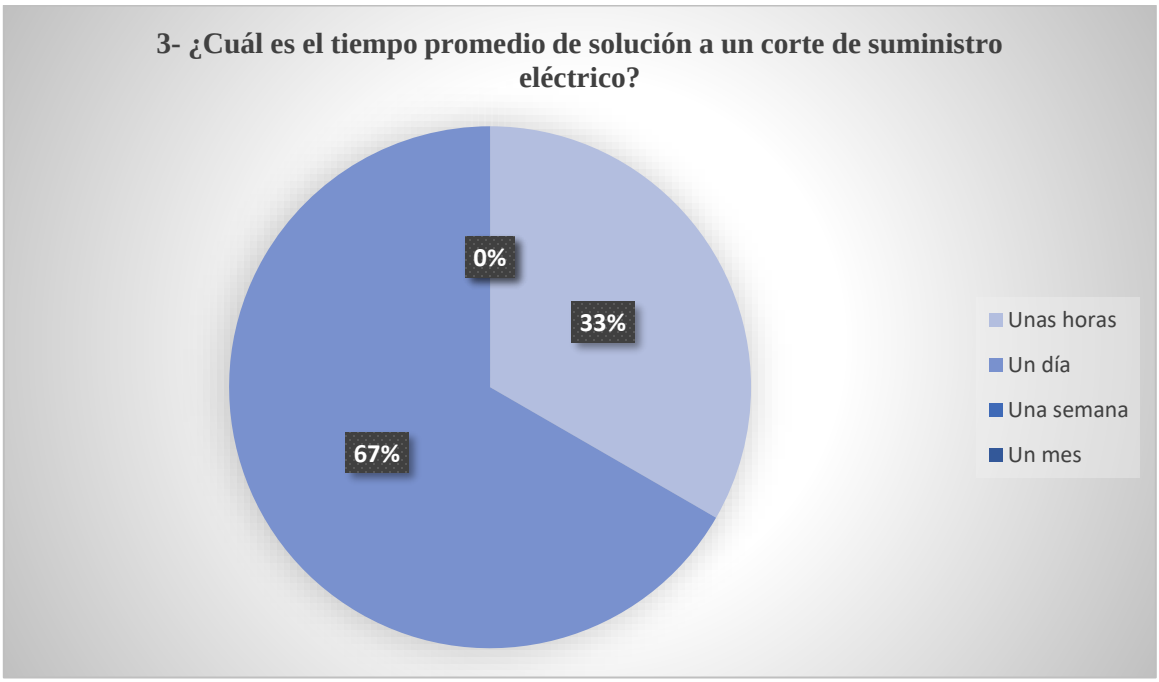


Fuente: elaboración propia

Como se muestra en el gráfico que un 65% de los entrevistados está de acuerdo en que cada tres meses se presente un corte de suministro, en tanto que un 16% consideran que al menos se da una vez al mes y un 19% considera que estos cortes se pueden presentar cada seis meses.

Gráfico número 3

Tiempo promedio de solución a un corte de suministro eléctrico



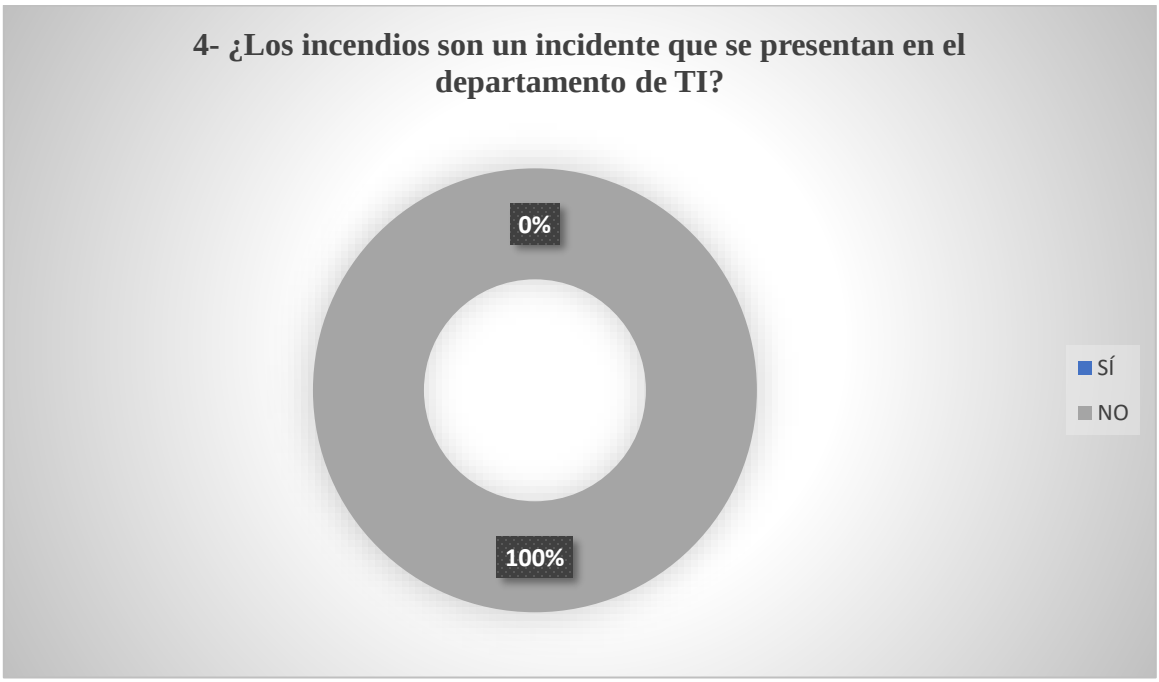
Fuente: elaboración propia

En el gráfico se detalla que un 67 % de los participantes de la investigación coinciden que el tiempo estimado para solucionar el corte de suministro eléctrico es de un día aproximadamente, en tanto una minoría 33% considera que, tan sólo requiere de unas horas para que este servicio se reestablezca.

Los participantes del estudio manifiestan que, al presentarse estos cortes de electricidad de forma inesperada, deben retrasar su trabajo y reorganizarlo una vez que el flujo normal de esta regresa.

Gráfico número 4

Los incendios son un incidente que se presenta en el departamento de TI



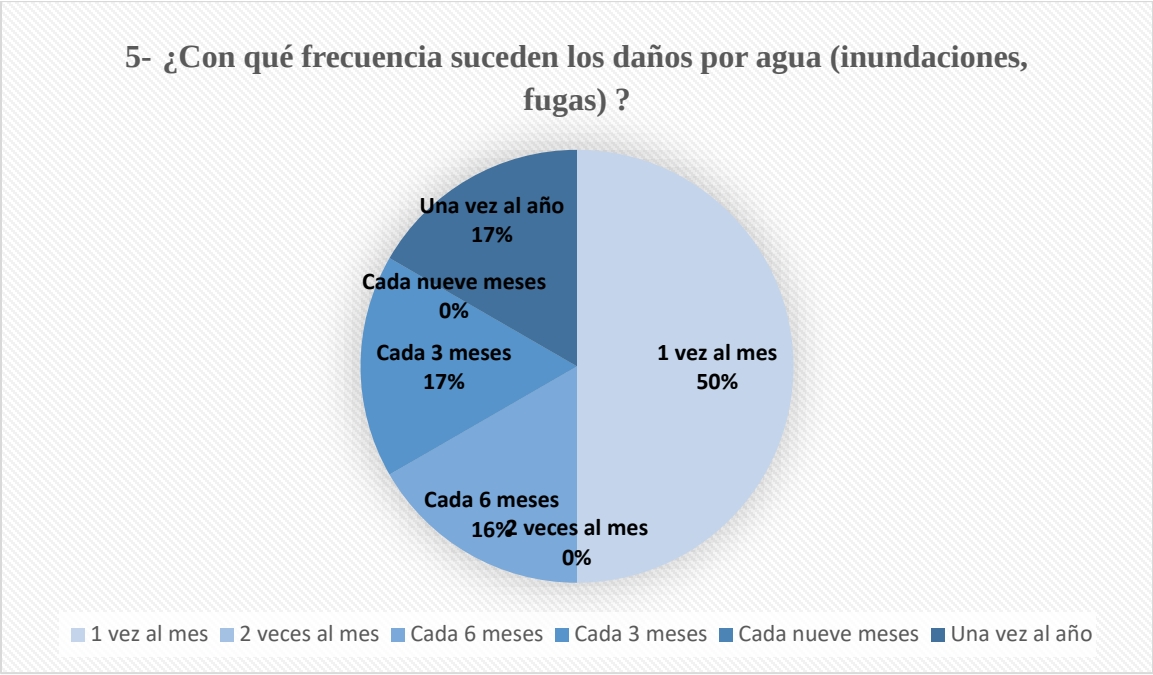
Fuente: elaboración propia

Al ser consultados sobre si los incendios son un incidente que ocurre en la organización, el 100% de los encuestados contestó que este tipo de acontecimiento no se presenta en la empresa.

Además, consideran que, debido a que la misma posee sistemas antiincendios y de igual forma se cuenta de protección a los equipos y respaldo de la información en caso de presentarse un problema de esta clase.

Gráfico número 5

Frecuencia con que se presentan daños por agua (inundaciones, fugas) en el departamento de TI

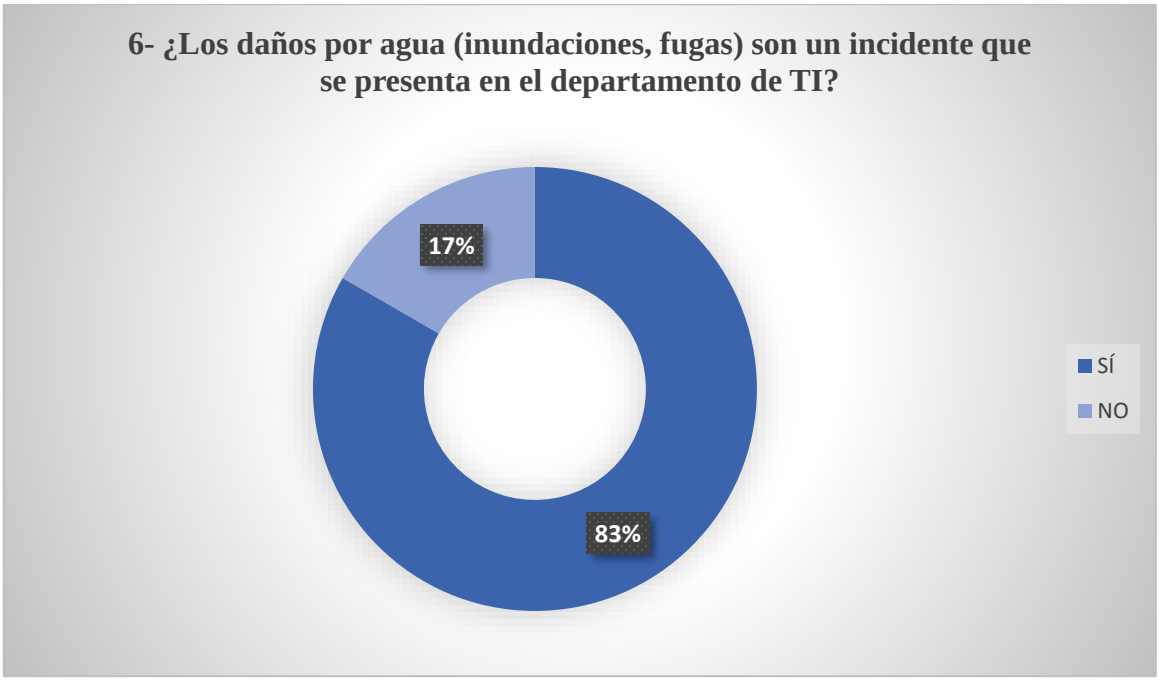


Fuente: elaboración propia

En el gráfico se muestra la frecuencia con la que ocurren los daños por agua (inundaciones, fugas). El 50% de los encuestados indicaron que este evento sucede una vez al mes, un 16% indica que cada 6 meses, un 17% ocurre cada 3 meses y un 17% comentó que sucede una vez al año. A esto le agregaron que depende de la temporada en la que se encuentre el país, ya que si surge algún temporal en cualquier época del año es posible que este problema se presente.

Gráfico número 6

Los daños por agua (inundaciones, fugas) son un incidente que se presenta en el departamento de TI



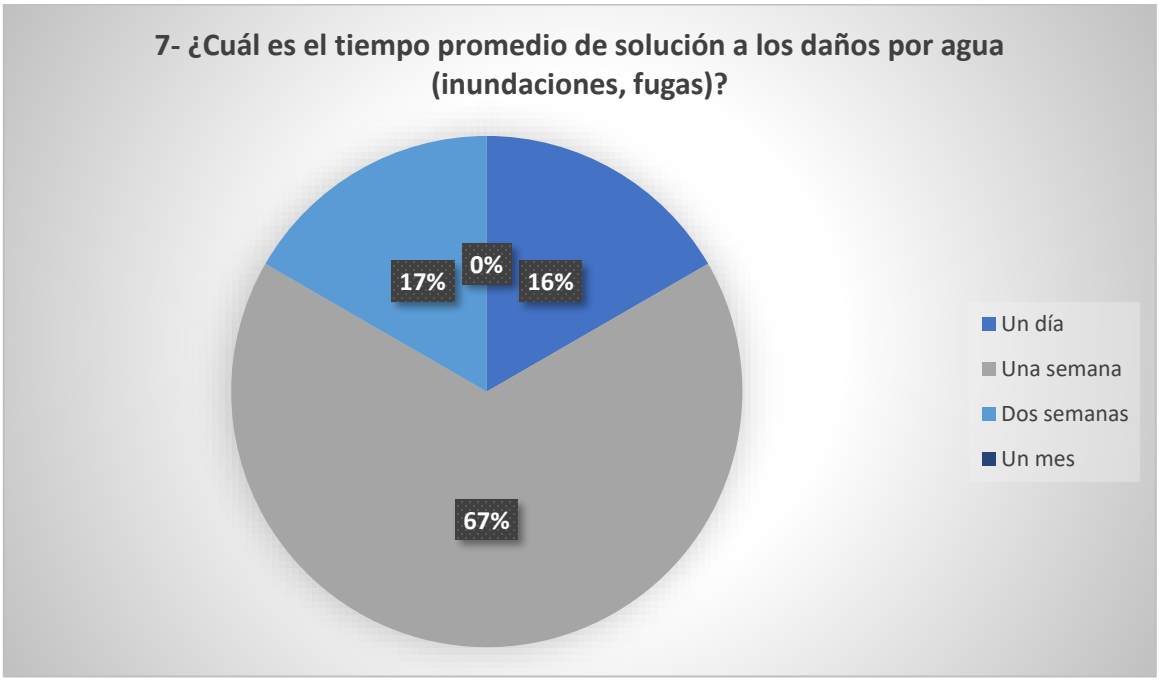
Fuente: elaboración propia

En cuanto a los daños por agua como inundaciones el 100% de los encuestados afirman que este incidente se presenta en la organización, ya que, se perciben algunas fugas en épocas lluviosas causando un deterioro en los equipos y hasta una posible pérdida.

Este hecho afecta tanto a los trabajadores como a la empresa en sí dado que, debe invertir recursos nuevamente para adquirir nuevo equipo o reparar los actuales.

Gráfico número 7

Tiempo promedio de solución a daños por agua

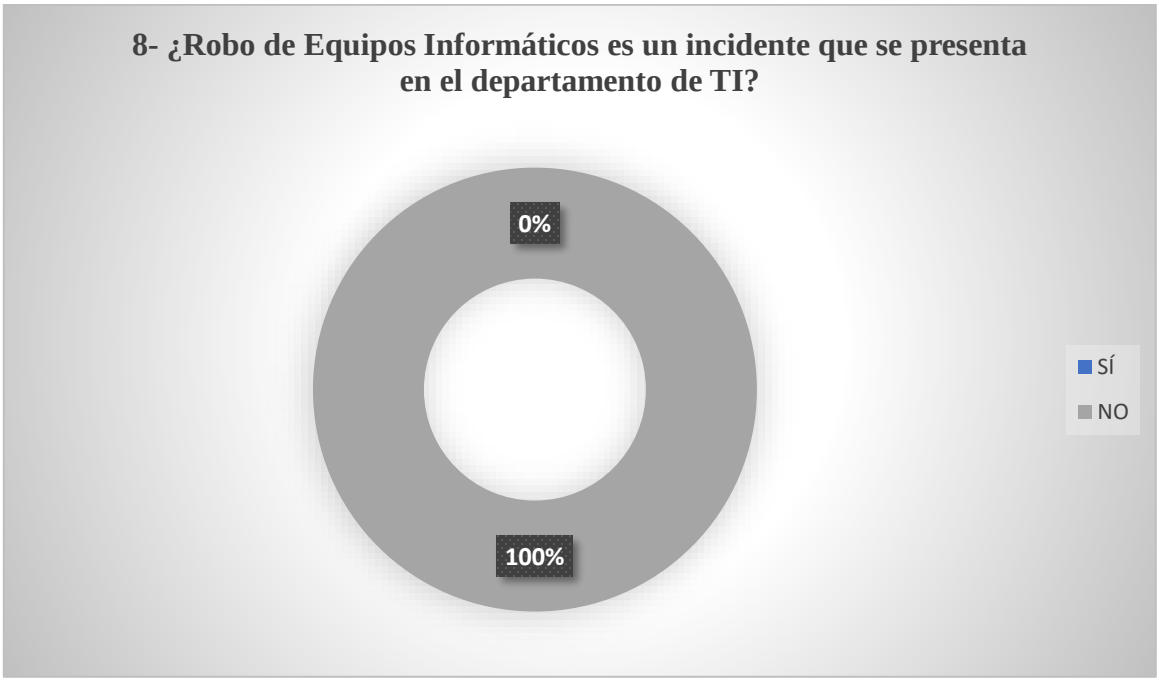


Fuente: elaboración propia

De acuerdo con los datos obtenidos se muestra que un 67% de los participantes considera que el tiempo estimado para brindar solución ante los incidentes causados por el agua (inundaciones, fugas) es de una semana, En tanto que un 17% considera que el tiempo para brindar solución a este inconveniente es de dos semanas y un 16% manifestó que es de tan solo un día.

Gráfico Número 8

Robo de equipos informáticos que se presentan en el departamento de TI

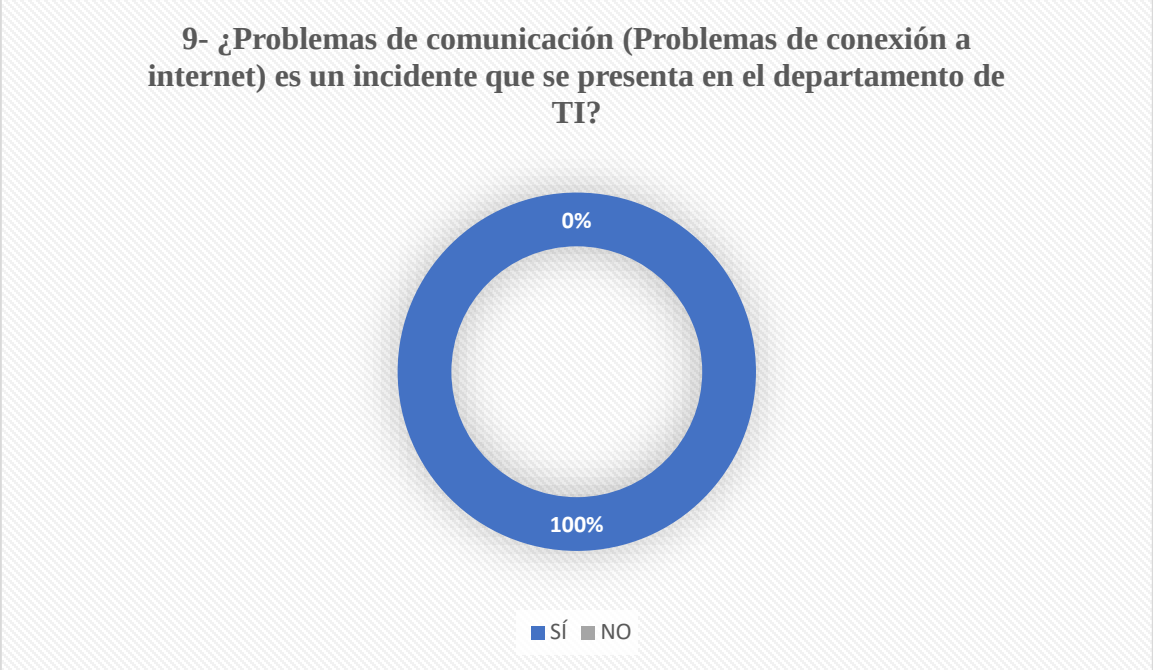


Fuente: elaboración propia

El Robo de Equipos Informáticos es un incidente que ataca a muchas organizaciones, por lo cual se decidió incluir al cuestionario esta pregunta, sin embargo, 100% de los encuestados contestaron que este problema no ocurre en el departamento de TI.

Gráfico número 9

Problemas de comunicación (conexión a internet) es un incidente que se presenta en el departamento de TI

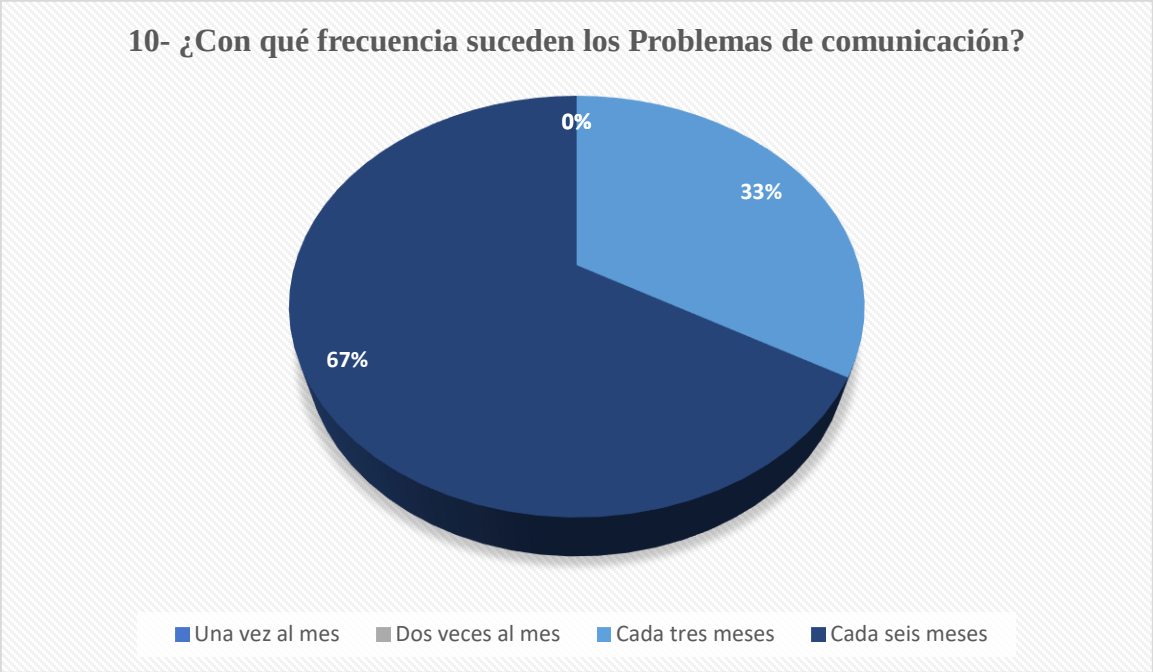


Fuente: elaboración propia

La organización trabaja con conexión a internet diariamente, es un punto clave e indispensable para la organización, si bien el departamento de TI tiene presente que esto dependerá casi en su totalidad al proveedor del servicio, los funcionarios del departamento de TI tienen en cuenta que los incidentes por Problemas de comunicación (Problemas de conexión a internet) pueden suceder de manera seguida y prolongada. Por ende, el 100% afirma que si sucede este tipo de incidente.

Gráfico número 10

Frecuencia con que suceden los problemas de comunicación

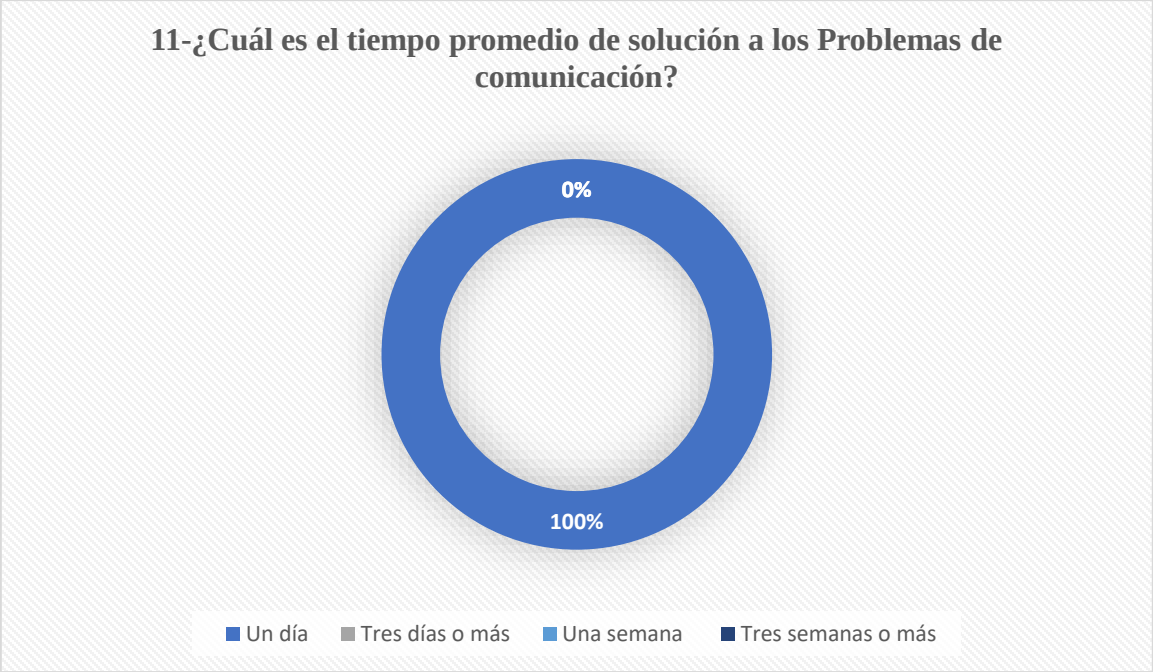


Fuente: elaboración propia

El dato que revela la siguiente pregunta sobre con qué frecuencia ocurre este incidente deja ver que la conexión a internet en el departamento de tecnología es bastante estable, ya que 67% de las personas encuestadas manifestaron que la frecuencia de este incidente es de seis meses. Por el contrario, 33% afirma que el hecho sucede cada tres meses.

Gráfico número 11

Tiempo promedio de solución a los problemas de comunicación

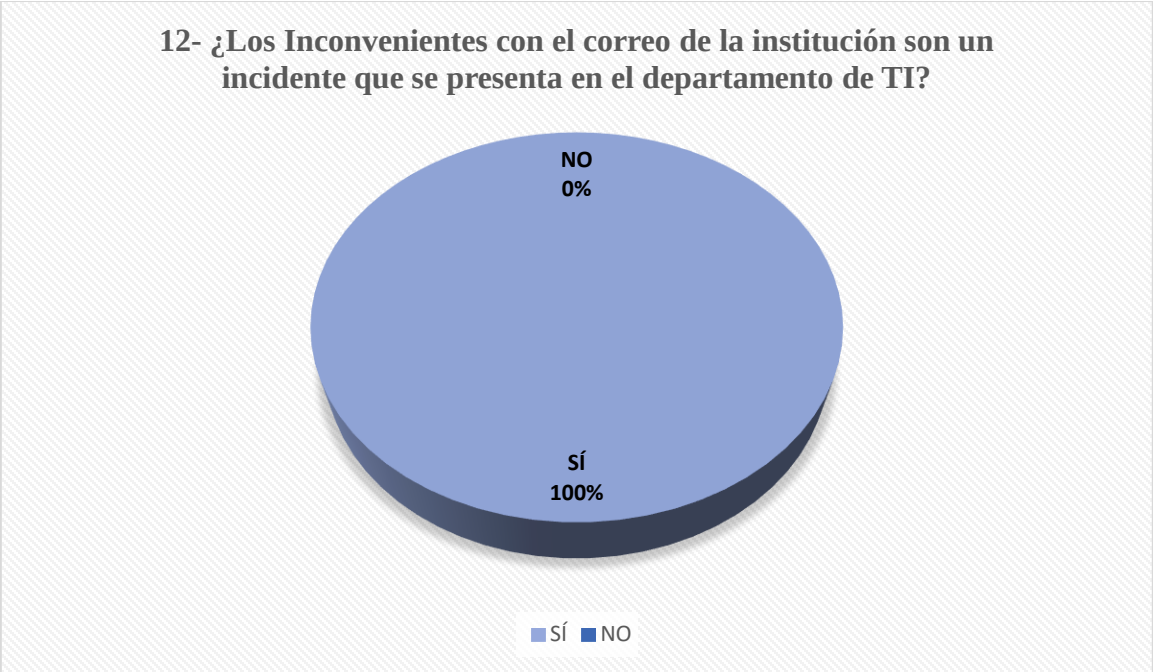


Fuente: elaboración propia

Además, el 100% de los encuestados mencionaron que el tiempo promedio de solución es de un día. Las respuestas muestran el nivel de conocimiento entre los funcionarios del departamento en temas de telecomunicaciones y redes, además de la prontitud con la que resuelven este tipo de problemas.

Gráfico número 12

Los inconvenientes con el correo de la institución son un incidente que se presenta en el departamento de TI

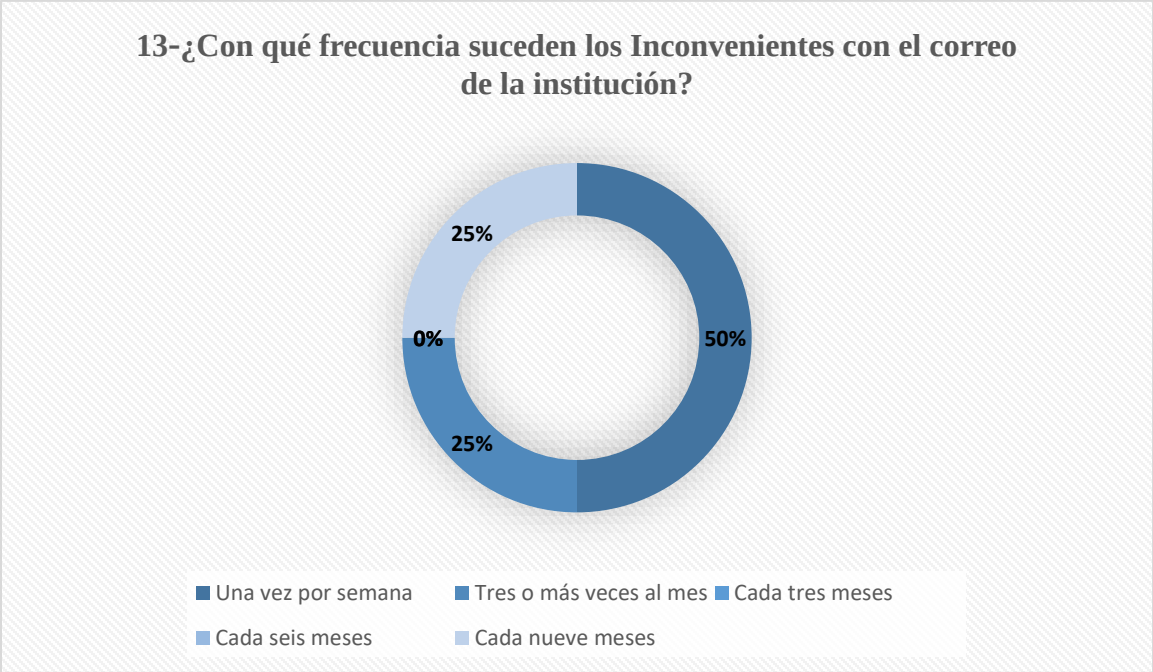


Fuente: elaboración propia

El correo institucional es un medio que se utiliza a diario en la organización y el departamento de TI no es la excepción, ya que, por este medio se comunican con los usuarios que no están familiarizados con el Service Desk y que requieren de sus servicios, por ende, la siguiente pregunta trata de dicho tema y como resultado a la pregunta de si surgían inconvenientes con el correo de la institución, un 100% contestó de forma positiva.

Gráfico número 13

Frecuencia con que suceden los inconvenientes con el correo de la institución



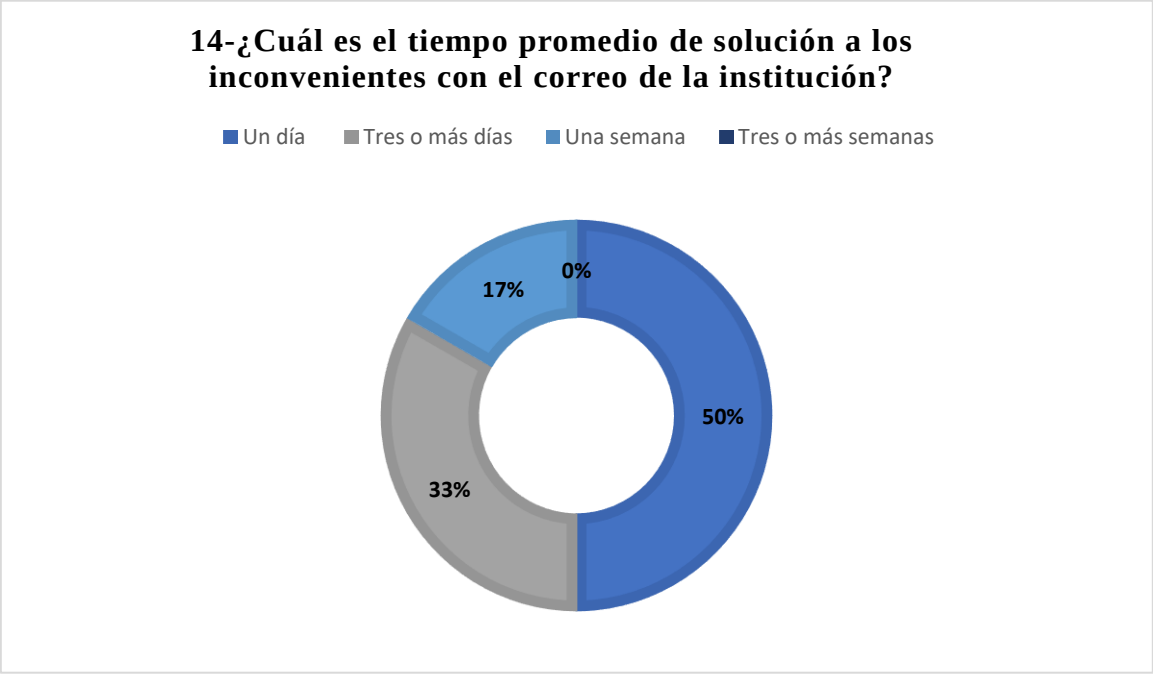
Fuente: elaboración Propia

Según los datos recabados, el 50% de los trabajadores considera que, este inconveniente ocurre cada semana, 25% menciona que tres o más veces al mes, 25% menciona que cada nueve meses. Esto ha sido con base a la percepción y la cantidad de incidentes que cada uno ha atendido de este tipo.

Dado que este incidente es un fenómeno recurrente se aprecia que los trabajadores ven afectadas sus labores cotidianas y por ende su rendimiento en el puesto de trabajo.

Gráfico número 14

Tiempo promedio de solución a los inconvenientes con el correo de la institución

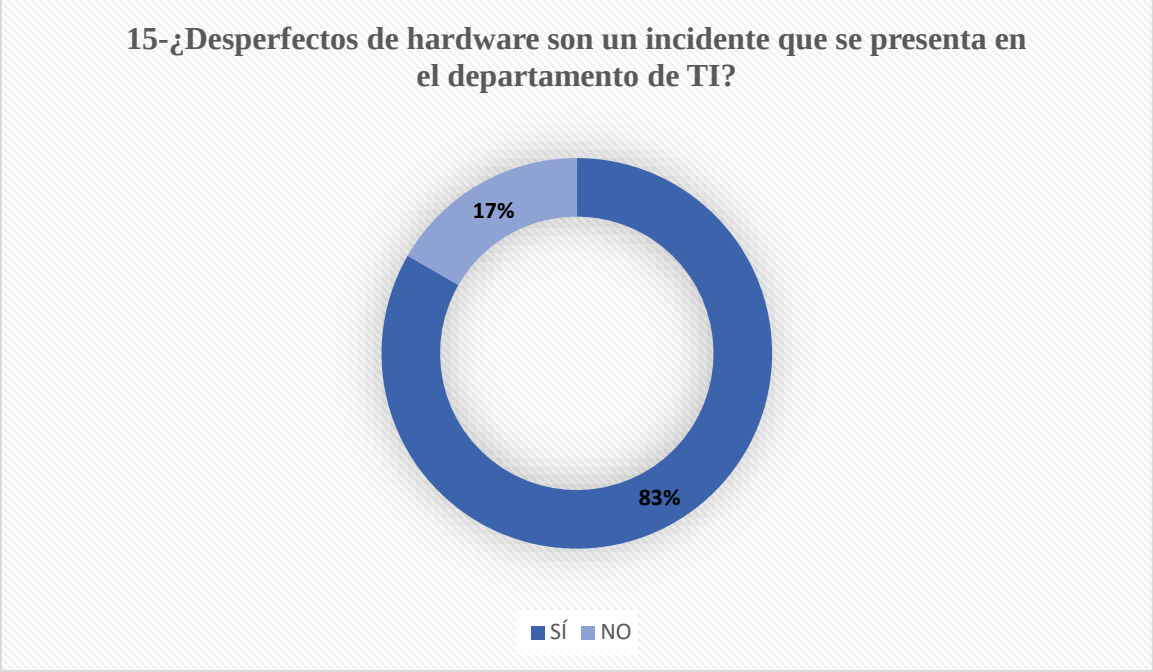


Fuente: elaboración propia

Según manifiestan los encuestados, el tiempo de solución a los inconvenientes con el correo de la institución, el 50% coinciden en tarde solo un día en darle solución a dichos inconvenientes, de igual forma un 33% afirman que se tarda aproximadamente entre tres o más días y el 17% mencionó que podría tener una duración de una semana. Cabe destacar que el tiempo de respuesta de solución a estos incidentes dependerá del tipo de problema, ya que solucionar el olvido de una contraseña durará menos que resolver un robo de identidad.

Gráfico número 15

Desperfectos de Hardware son un incidente que se presenta en el departamento de TI



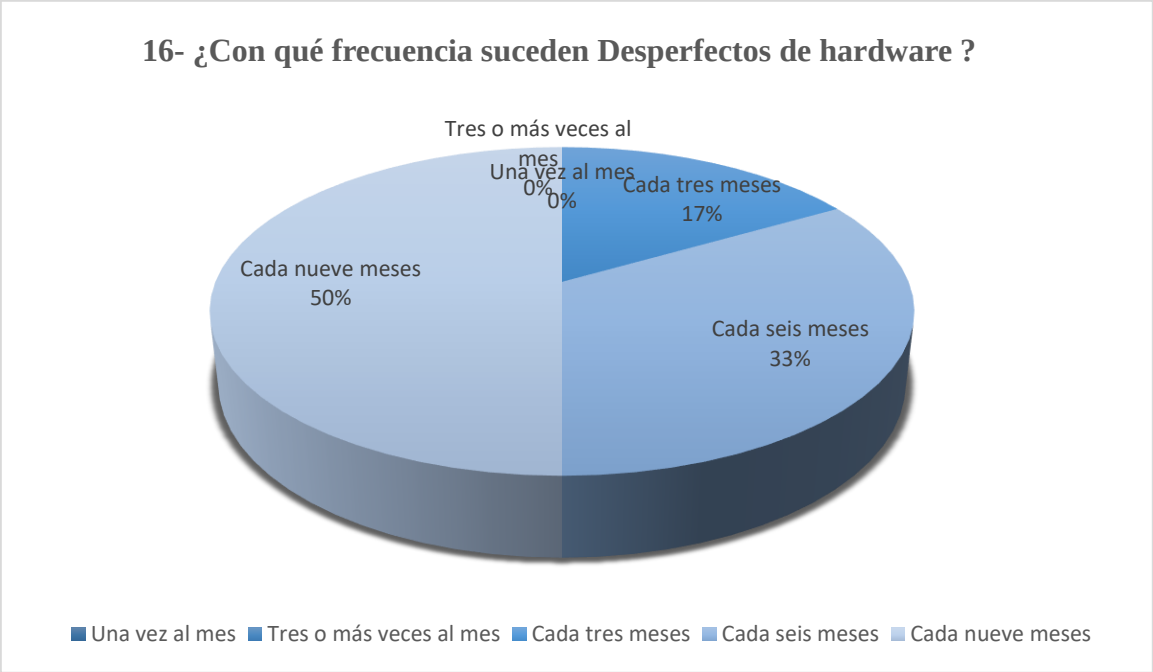
Fuente: elaboración propia

Los desperfectos de hardware son un incidente muy común en las organizaciones y debido a ello se preguntó sobre este tema, a lo cual un 83% menciona que, si surge esta problemática y un 17% respondió que no, tal como se aprecia en gráfico.

Se considera que estos desperfectos pueden ser ocasionados por daños de fábrica o por errores humanos como mala utilización y poco mantenimiento; pero sin importar la causa la solución debe rápida para garantizar la eficiencia y eficacia del sistema y por consecuente la satisfacción del cliente final.

Gráfico número 16

Frecuencia con que suceden desperfectos de Hardware



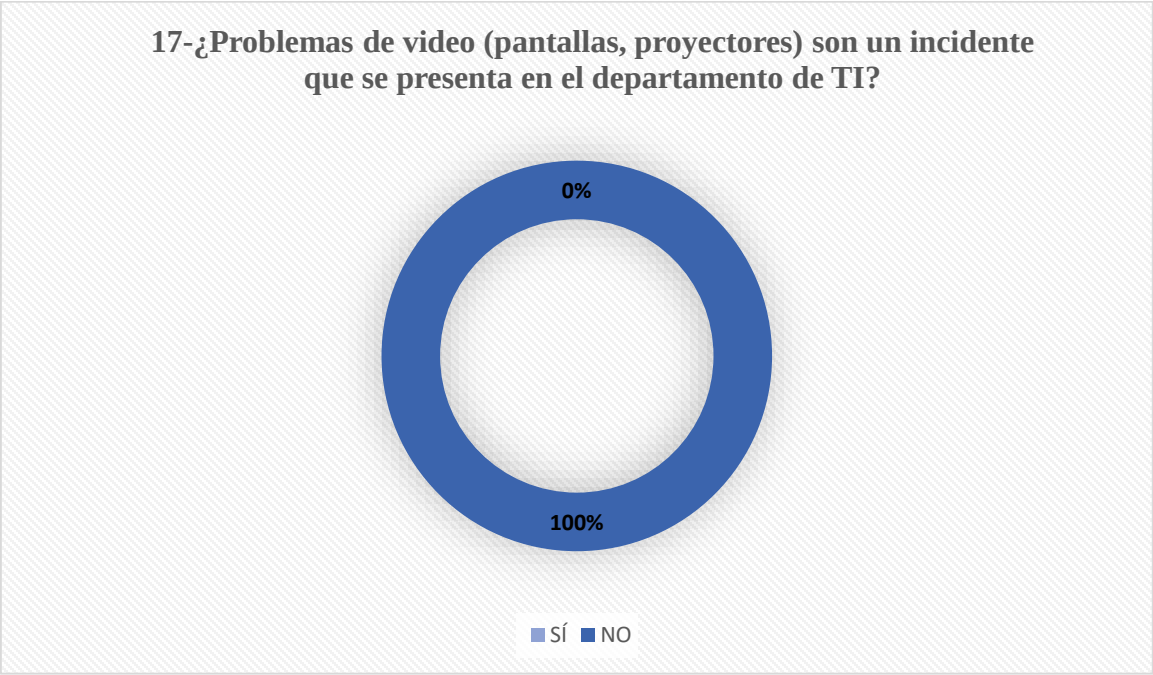
Fuente: elaboración propia

Con respecto a la frecuencia con que ocurren los desperfectos de hardware, el 50% de los encuestados afirma que sucede cada nueve meses, el 33% cada seis meses y el 17% de la muestra indicaron que ocurre cada tres meses.

Ante esta situación cabe resaltar que la información almacenada en los sistemas se ve comprometida al igual que la credibilidad de la empresa ante los clientes.

Gráfico número 17

Los problemas en equipo de video (pantallas, proyectores) son un incidente que se presenta en el departamento de TI



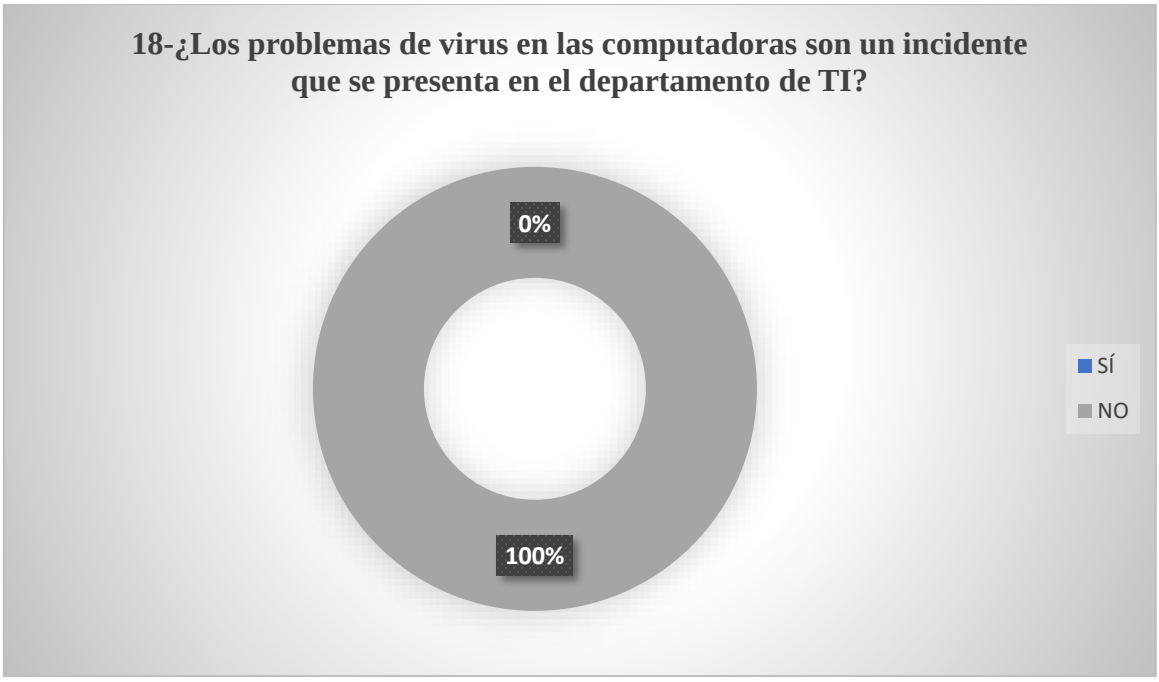
Fuente: elaboración propia

Con respecto a este ítem las respuestas otorgadas por los encuestados son muy favorables dado que el 100% de los encuestados mencionaron que no es un problema que suceda en la organización.

Se puede apreciar por tanto que al estar en perfecto estado y funcionamiento el uso de estos equipos brinda soporte durante las reuniones y contribuye de manera efectiva en las funciones de los colaboradores, por lo que la empresa acierta en este punto.

Gráfico número 18

Los problemas con virus en las computadoras son un incidente que se presenta en el departamento de TI

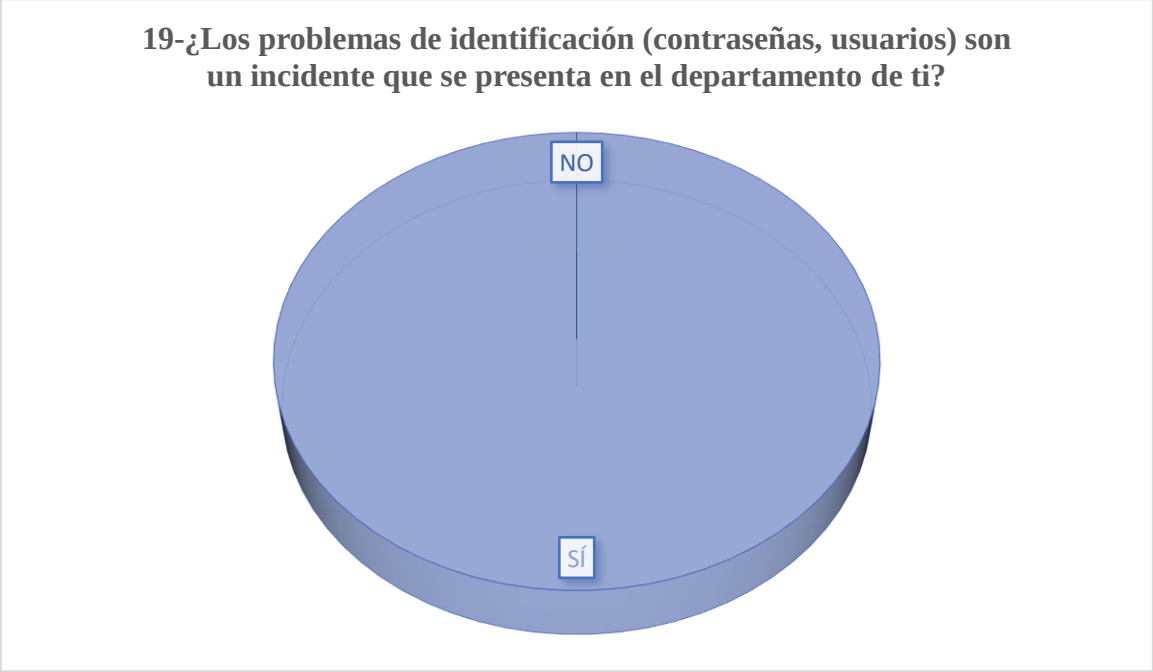


Fuente: elaboración propia

Al igual que la pregunta anterior el 100% de los participantes respondieron que no a la pregunta de si los problemas de virus en las computadoras era un incidente que ocurría en la organización, cabe destacar que el departamento de TI se esmera por la seguridad de cada usuario y brinda antivirus a cada dispositivo para evitar dichos incidentes.

Gráfico número 19

Los problemas de identificación (contraseñas, usuarios) son un incidente que se presenta en el departamento de TI

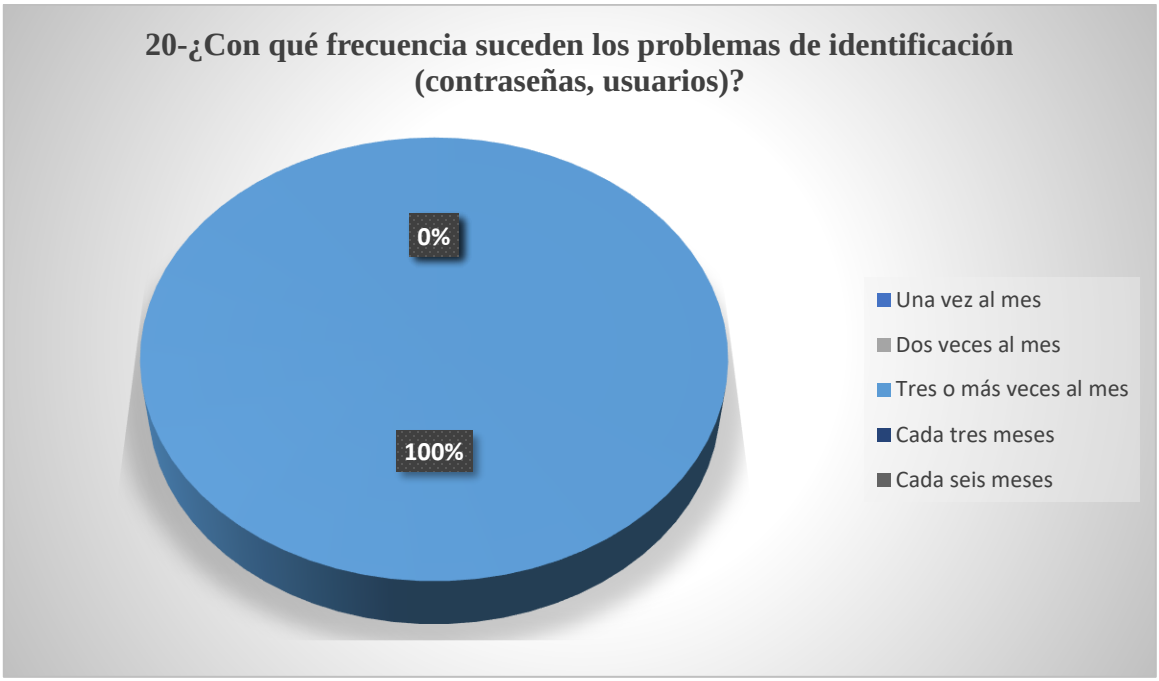


Fuente: elaboración propia

Un incidente muy frecuente en las organizaciones son los problemas de identificación (contraseñas, usuarios), ya que, muchos de los usuarios olvidan la contraseña de los dispositivos, del correo institucional o inclusive el nombre de usuario o correo. Por ende, se consultó al personal del departamento de TI si estos incidentes ocurrían en la empresa, a lo cual el 100% respondió de manera positiva.

Gráfico número 20

Frecuencia de los problemas de identificación (contraseñas, usuarios)

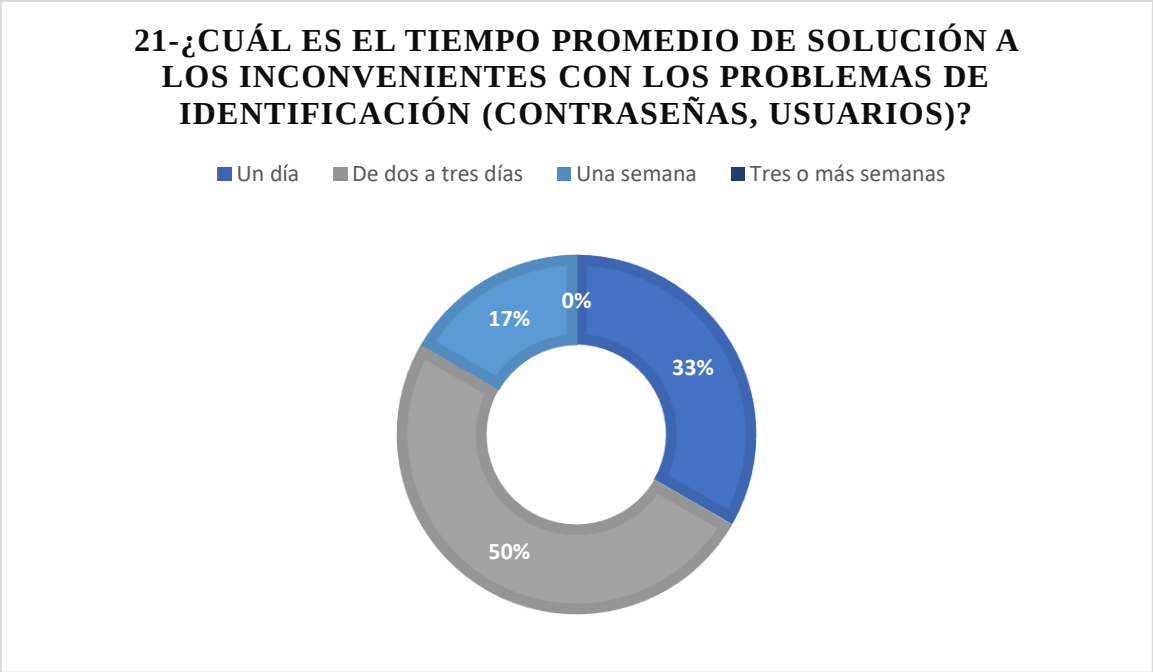


Fuente: elaboración propia

Como resultado a la pregunta relacionada con la frecuencia con la que ocurren los problemas de identificación, el 100% contestó que ocurre tres o más veces al mes, a esto agregaron que es uno de los incidentes más comunes y repetitivos.

Gráfico número 21

Tiempo promedio de solución a los inconvenientes con los problemas de identificación



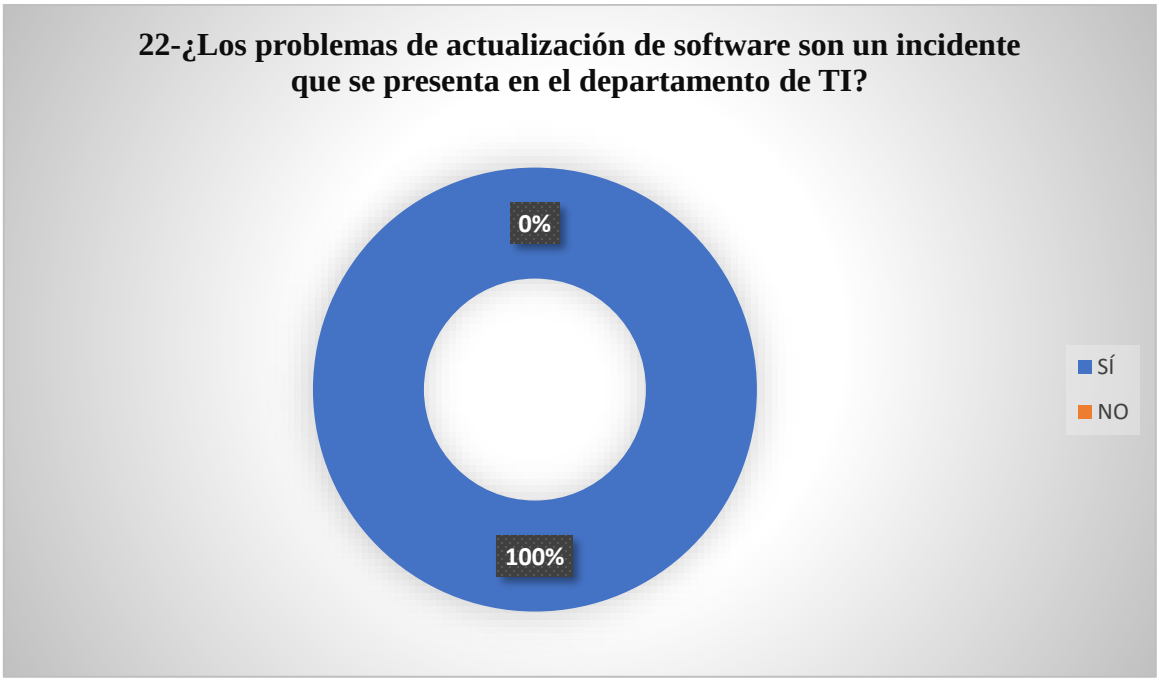
Fuente: elaboración propia

Sobre la consulta del tiempo promedio de solución a los inconvenientes con los problemas de identificación, un 50% considera que, el tiempo promedio es de dos a tres días, el 33% contestó que se dura un día en resolver el problema, un 17% afirma que una semana en resolver el incidente.

A pesar de ser por la seguridad de los datos, el aspecto de accesibilidad es importante para cumplir con los objetivos laborales y al verse retasado se asume que puede afectar la productividad del colaborador y por ende se deben solventar lo más pronto posible esta clase de inconvenientes.

Gráfico número 22

Los problemas de actualización de Software son un incidente en el departamento de TI

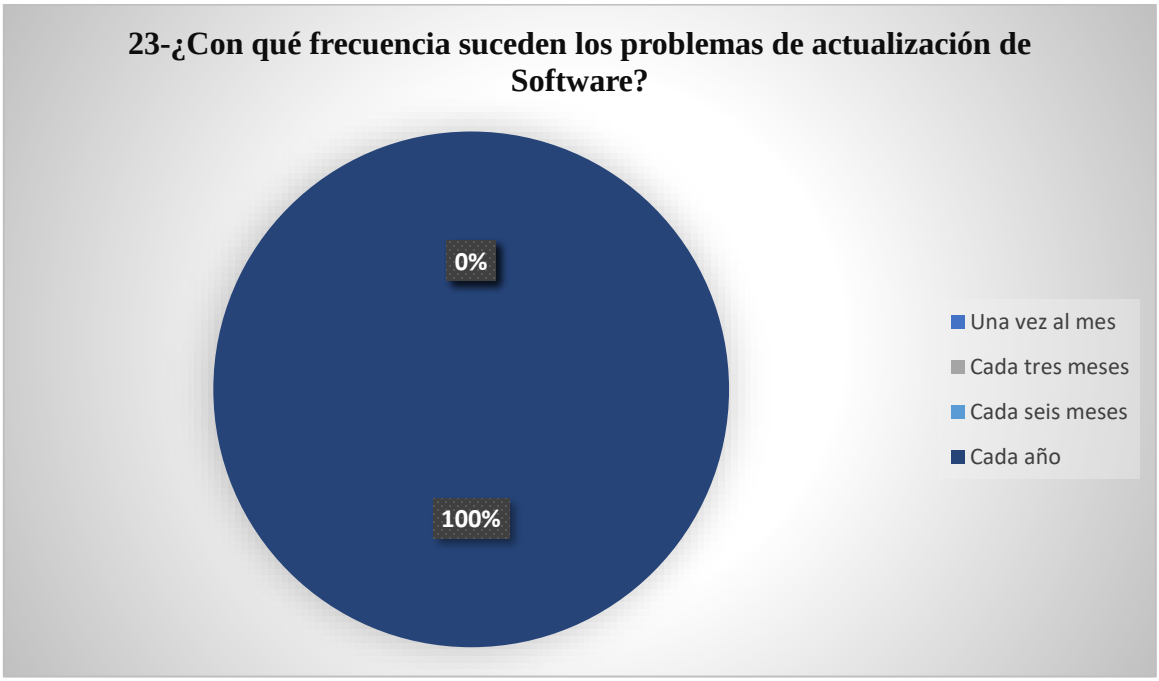


Fuente: elaboración Propia

Un Software actualizado le brinda a la empresa un excelente funcionamiento y una medida de seguridad de la información ya que, de estar desactualizados vuelve a los equipos vulnerables ante ataques, por lo cual se les preguntó sobre si los problemas de actualización son un incidente que suele suceder en la organización, a lo cual un 100% respondió que sí., pero que la empresa procura actualizarlos al menos una vez al año para ratificar su funcionamiento apropiado y que se puedan cumplir las funciones del puesto.

Gráfico número 23

Frecuencia con que suceden los problemas de actualización de Software

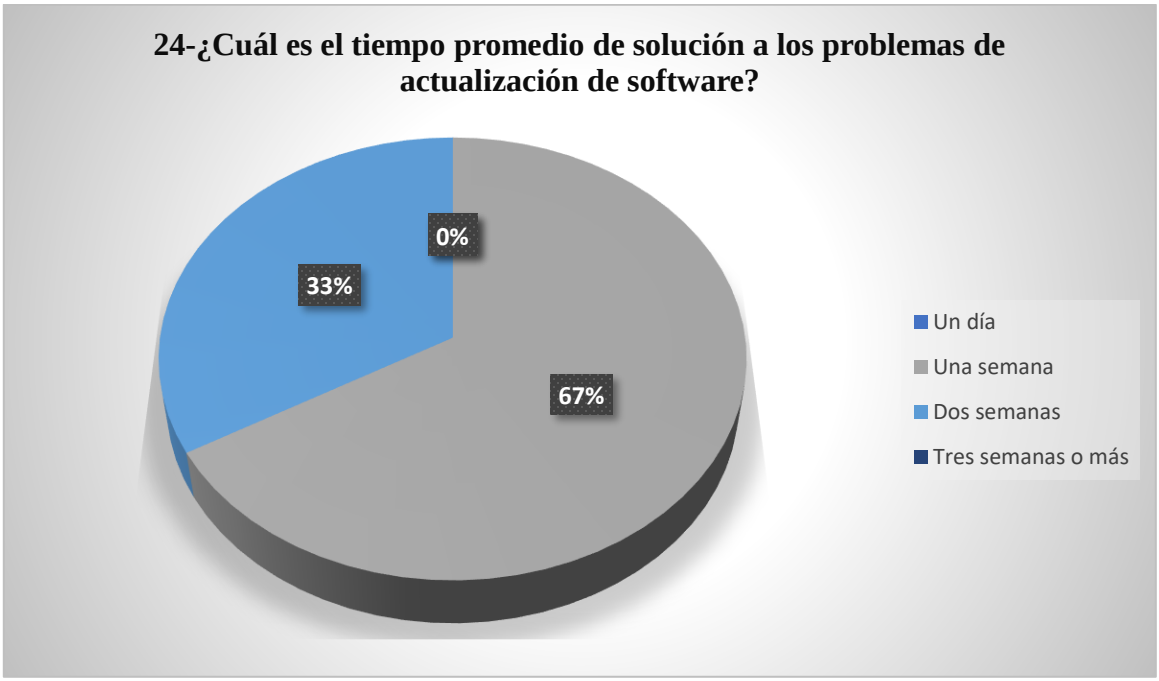


Fuente: elaboración propia

Se aprecia mediante la información anterior que el 100% de los encuestados consideran que al menos una vez al año se presentan problemas con las actualizaciones del Software, esto porque la empresa ya cuenta con fechas establecidas para realizar las actualizaciones en los equipos y por supuesto en aquellos que requieren de forma inmediata.

Gráfico número 24

Tiempo promedio de solución a los problemas de actualización a los problemas de Software



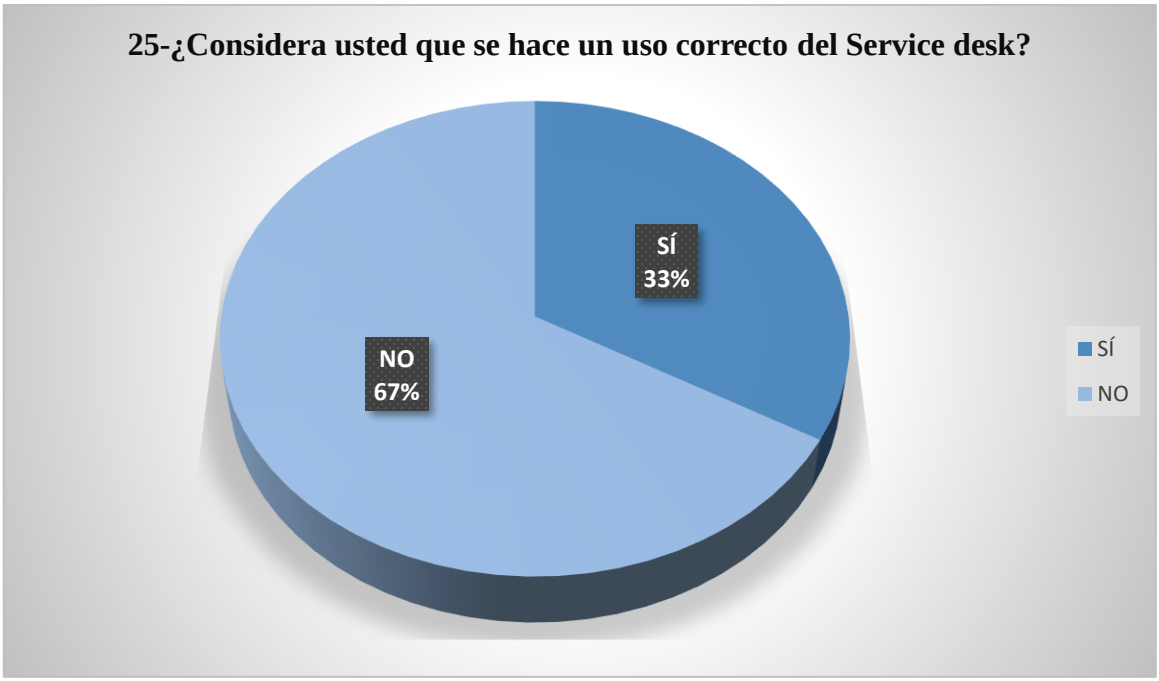
Fuente: elaboración Propia

Ante la pregunta sobre el tiempo de respuesta a los problemas de actualización de software, un 67% de los encuestado considera que se presentan en una semana y un 33% contestó que dos semanas.

Ya que, la labor de los trabajadores se basa en la utilización de las computadoras se percibe como positivo que resuelvan las situaciones de esta categoría en poco tiempo, aunque podría disminuirse y volverlo más eficiente.

Gráfico número 25

Se hace un uso correcto del Service Desk



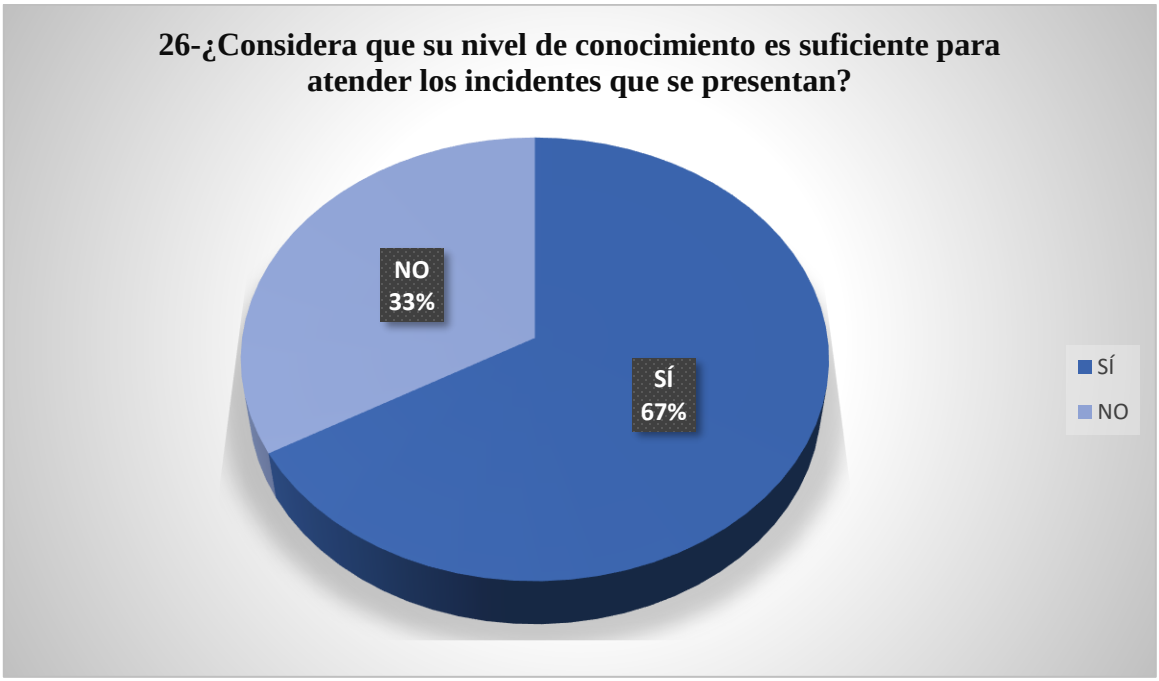
Fuente: elaboración propia

A la pregunta de si consideran que utilizan la herramienta Service Desk correctamente, el 67% contestó que no y el 33% dijo que sí.

Con esto la empresa asegura un trato apropiado y oportuno a sus clientes, además organizando y otorgando soporte internamente a la misma.

Gráfico número 26

Nivel de conocimiento para atender los incidentes que se presentan



Fuente: elaboración propia

Ante la consulta sobre el nivel de aprendizaje y entrenamiento que posee cada trabajador para brindar solución a los incidentes que se presentan en la organización un 67% consideró que poseen los conocimientos adecuados para brindar soluciones prontas, en tanto un 33% considera que no.

Adicionalmente, los que respondieron negativamente reforzaron la respuesta argumentando que no todos los temas los pueden saber ya que, a pesar de estar en constante actualización es muy difícil poder tener conocimiento de todos los temas y actualizaciones en el ámbito de la tecnología debido a que, avanza todos los días y existen temas que aún desconocen por completo.

En este punto se refuerza la necesidad de brindar las capacitaciones a los trabajadores y así incrementar sus conocimientos y que puedan responder rápidamente ante las necesidades de los clientes.

DETERMINACIÓN DE BRECHAS

La determinación de brechas se puede definir como el espacio entre donde se encuentra la empresa y donde quiere estar, es la diferencia entre el desempeño real y el deseado que esta presenta. Es importante realizar el análisis y conocer la determinación de brechas con la finalidad de enlistar las prioridades para facilitar y encaminar el proyecto y poder brindar buenos resultados para el departamento de TI y por consiguiente para la organización.

La estabilidad del personal es una gran ventaja ya que, no es rotativo y cuando hay un nuevo integrante se acopla fácilmente. Todos conocen a la perfección los procesos dentro del departamento, tienen muy buena comunicación entre sí, además se conocen entre ellos, trabajan en equipo, se motivan y se apoyan conjuntamente.

Lo ideal para el manejo de problemas informáticos sería optar por una política que ayude y refuerce el proceso de control de incidentes, ya que, aunque la empresa cuenta con la herramienta Service Desk, es indispensable tener una guía con las mejores prácticas en tecnología para el proceso, utilizando además su correcta aplicación.

Para obtener los mejores resultados en el objetivo propuesto en la presente investigación, se hará uso de los recursos tecnológicos, humanos y físicos que posee la organización y coloca a disposición de la investigadora. De igual forma se presenta una propuesta para los funcionarios de tecnología, la empresa afirma que este plan de mejora se implementará para contribuir a la mejora continua y agilizar las funciones del puesto, así como la consecución de objetivos a mediana y largo plazo de forma eficaz y eficiente, anudado a lo anterior manifiestan que, se le dará seguimiento a los cambios implementados.

CAPÍTULO V:

PROPUESTA DEL PROYECTO

En el siguiente capítulo se desarrollará la propuesta de la solución que ha sido contemplada a lo largo de este proyecto de investigación que ha sido acordada como entregable para INOLASA, empresa evaluada en este trabajo.

Catálogo de Servicios

En este apartado se muestran los servicios que ofrece el departamento de TI a la organización, con el fin de conocer el entorno, las tareas y formalizar el portafolio de servicios de la empresa.

Cuadro número 3

Servicios que brinda el departamento de TI a la organización

Nombre del Servicio	Descripción
Recuperación de contraseñas y usuarios	Cada equipo contiene como medida de seguridad un usuario y una contraseña, por lo tanto, el departamento de TI debe velar por ello y ayudar a recuperar los datos en caso de que el usuario olvide alguno o se presente algún otro incidente.
Instalación y mantenimiento de equipos (Hardware)	Cuando la organización adquiere equipo nuevo o alguno fue reparado, deben ser instalados y se deben mantener en óptimas condiciones para su uso adecuado.
Software Ofimático	Instalar y mantener en óptimas condiciones los programas de uso diario de la organización.
Software Administrativo	Instalar y mantener en óptimas condiciones el sistema financiero, así como la correcta gestión de la base de datos de la organización.
Redes y telecomunicaciones	Gestionar, dar acceso y brindar seguimiento a los dispositivos que requieren de comunicación en la organización
Gestión del correo institucional	Crear, gestionar y eliminar los correos de las cuentas institucionales según las necesidades de los usuarios y la organización.

Fuente: elaboración propia

Roles de Gestión de Solicitudes

A continuación, se describen los roles de gestión de solicitud:

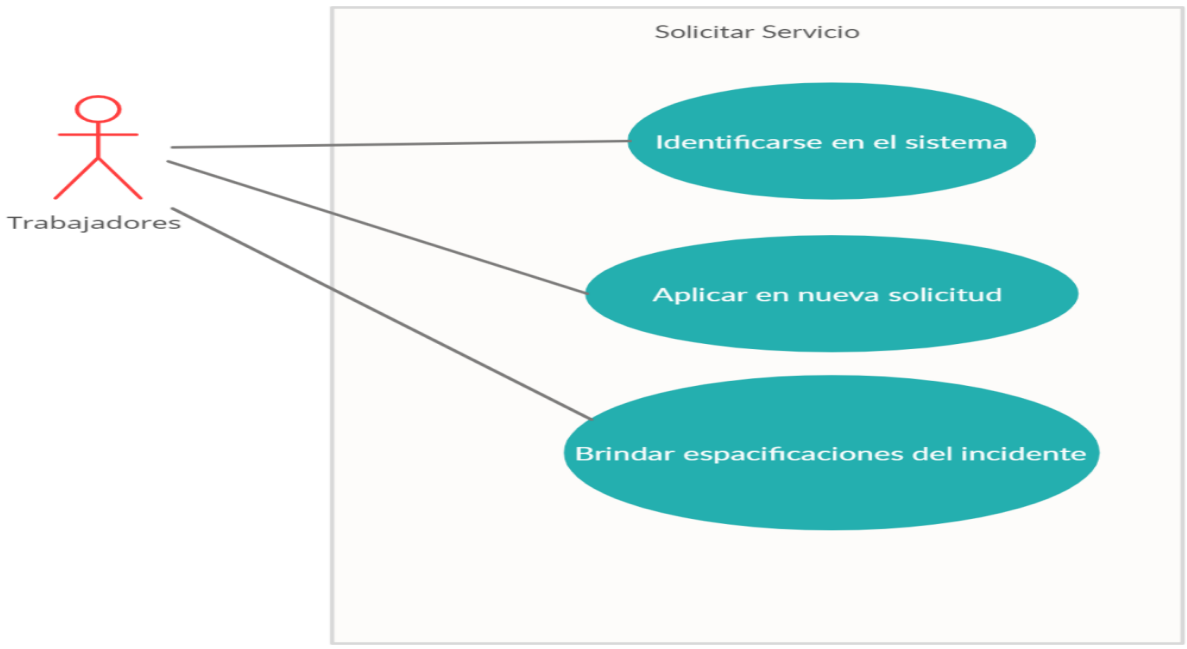
Cuadro número 4

Solicitante de servicio

Solicitante de Servicio	
OBJETIVOS	Solicitar el servicio
RESPONSABILIDADES	• Reportar el incidente por medio de la herramienta Service Desk • Especificar el problema y brindar información detallada • Brindar detalles sobre cómo afecta este incidente en las labores diarias
PERSONA ASIGNADA	Colaboradores de todos los departamentos

Imagen número 4

Diagrama de rol solicitante de servicio



Fuente: elaboración Propia

Cuadro número 5

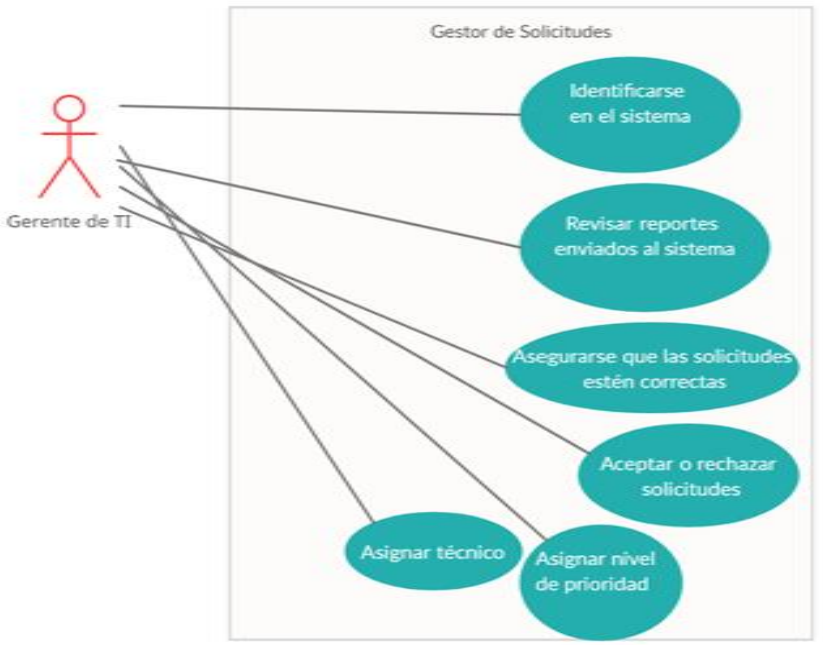
Gestor de solicitudes

Gestor de Solicitudes	
OBJETIVOS	Asegurar que se cumpla el proceso de cumplimiento de las solicitudes según lo estipulado
RESPONSABILIDADES	• Revisar los reportes enviados • Asegurarse de que las solicitudes contengan los datos y detalles completos • Aceptar o rechazar las solicitudes enviadas • Asignar nivel de prioridad • Designar un técnico al problema según el tipo y grado de dificultad del incidente
PERSONA ASIGNADA	Gerente de TI

Fuente: elaboración propia

Imagen número 5

Roles de gestor de solicitudes



Fuente: elaboración propia

Cuadro número 6

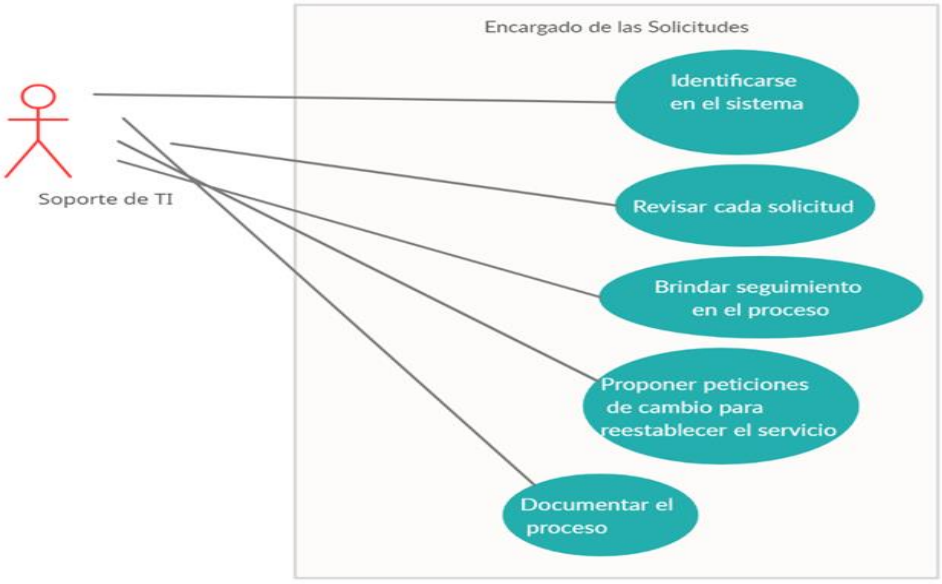
Encargado de las solicitudes

Encargado de las Solicitudes	
OBJETIVOS	Ser el primer contacto que atiende la solicitud
RESPONSABILIDADES	• Revisar cada una de las solicitudes • Brindar seguimiento a lo largo de todo el proceso de solución • Proponer peticiones de cambio para reestablecer el servicio • Documentar cada paso que surge una vez aceptada la solicitud
PERSONA ASIGNADA	Administrador de Aplicaciones Soporte técnico e infraestructura

Fuente: elaboración propia.

Imagen número 6

Rol de encargado de solicitudes

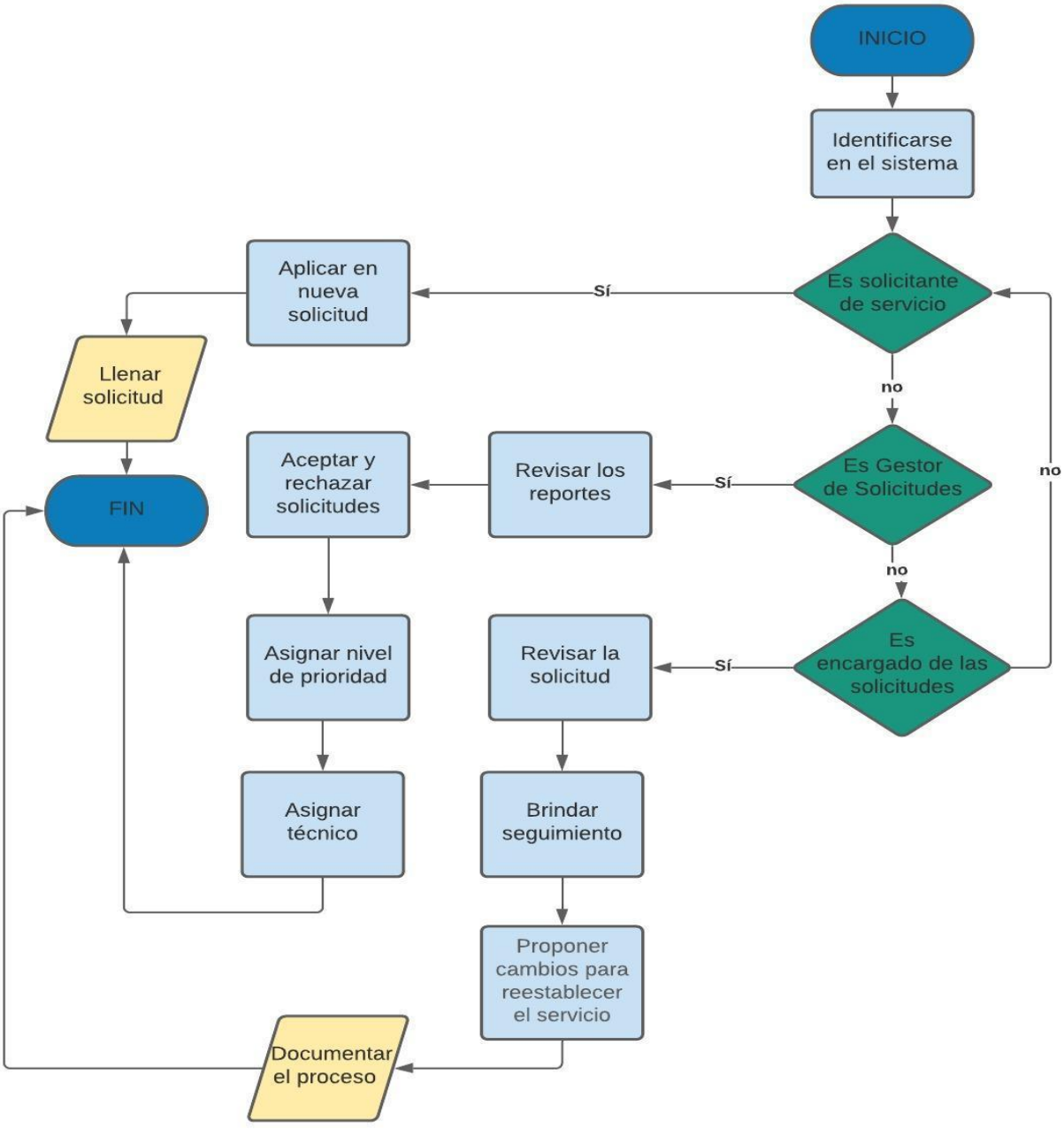


Fuente elaboración propia

A continuación, se muestra un diagrama de flujo en el cual se representa todo el proceso que siguen los roles de gestión de solicitudes y el flujo de la información que se genera.

Imagen número 7

Diagrama de flujo gestión de solicitudes y flujo de información



Fuente: elaboración propia

Roles de Gestión de Incidentes.

A continuación, se describen los roles de gestión de incidentes:

Cuadro número 7

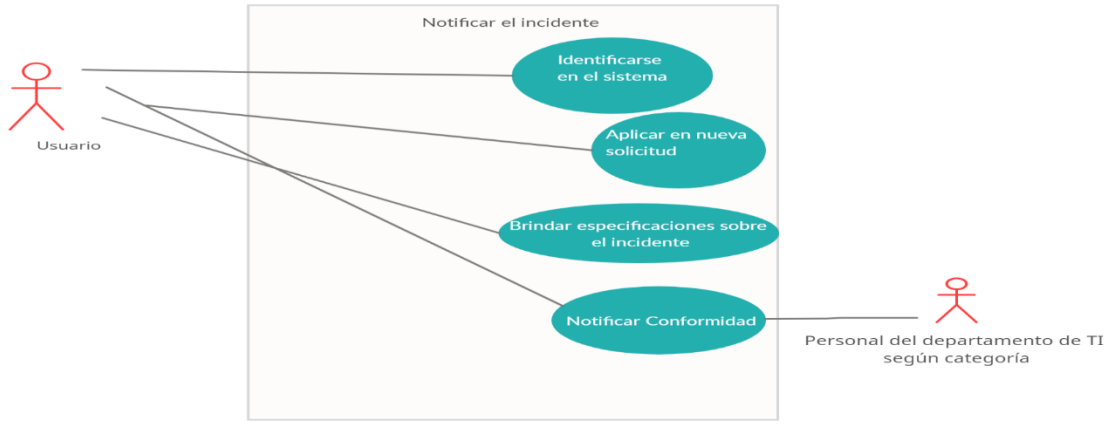
Roles de Usuario

USUARIO	
OBJETIVOS	Notificar el incidente en el menor tiempo posible con la mayor de las especificaciones
RESPONSABILIDADES	• Notificar inmediatamente el incidente • Hacer uso de la herramienta Service Desk para reportar el incidente • Realizar todas las anotaciones necesarias y detalladas sobre el incidente • Una vez el estado de la solicitud esté "resuelto" el usuario debe notificar conformidad o inconformidad con la solución
PERSONA ASIGNADA	Personal del departamento de TI calificado según el tipo o categoría de incidente

Fuente: elaboración propia

Imagen número 8

Rol notificador incidente



Fuente: elaboración propia

Cuadro número 8

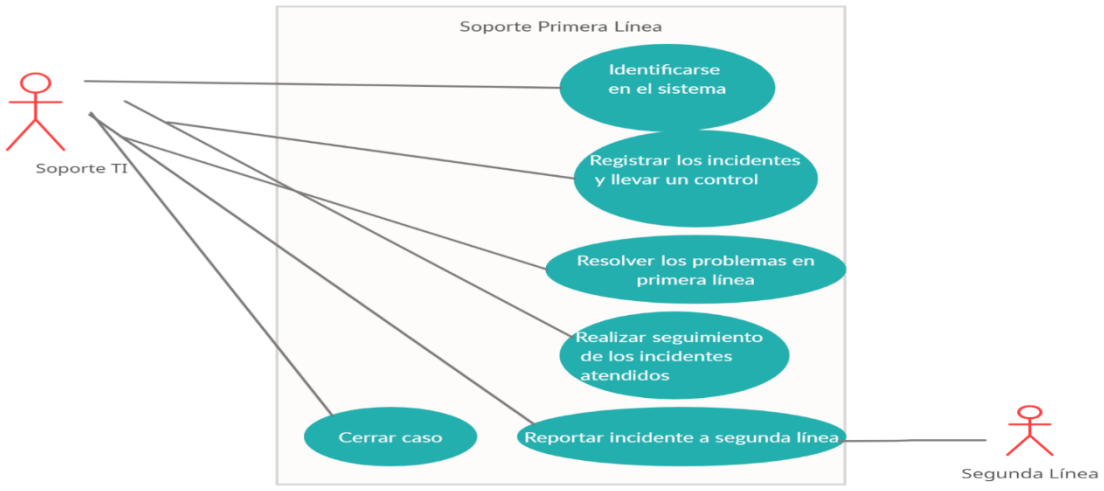
Soporte de primera línea

SOPORTE DE PRIMERA LÍNEA	
OBJETIVOS	Brindar solución a los incidentes como primer contacto
RESPONSABILIDADES	• Registrar los incidentes y llevar un control • Resolver los problemas en primera línea referentes a equipos de los usuarios finales • Realizar seguimiento de los incidentes atendidos • Reportar incidente en caso de no ser resuelto para que se eleve a segunda línea • Cerrar el caso del incidente
PERSONA ASIGNADA	Soporte técnico de TI

Fuente: elaboración propia

Imagen número 9

Soporte de primera línea



Fuente: elaboración propia

Cuadro número 9

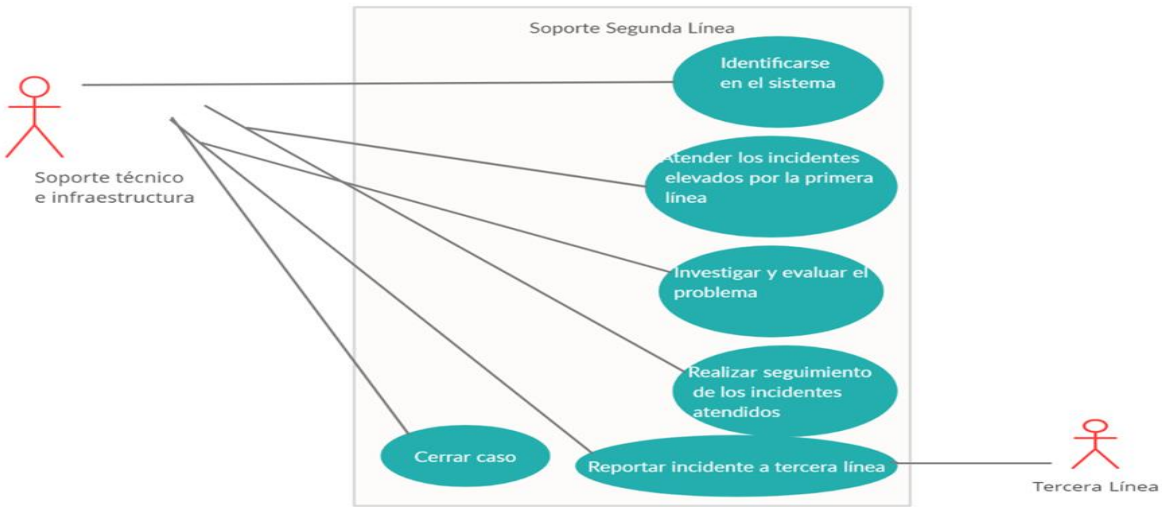
Soporte de segunda línea

SOPORTE DE SEGUNDA LÍNEA	
OBJETIVOS	Brindar solución a los incidentes como segundo contacto en caso de que la primera línea no lo pudo resolver
RESPONSABILIDADES	• Atender los incidentes elevados por la primera línea referentes a infraestructura de red • Investigar y evaluar el problema • Realizar seguimiento de los incidentes atendidos • Reportar incidente en caso de no ser resuelto para que se eleve a tercera línea • Cerrar el caso del incidente
PERSONA ASIGNADA	Soporte técnico e infraestructura

Fuente: elaboración Propia

Imagen Número 10

Rol de soporte de segunda línea



Fuente: elaboración propia

Cuadro número 10

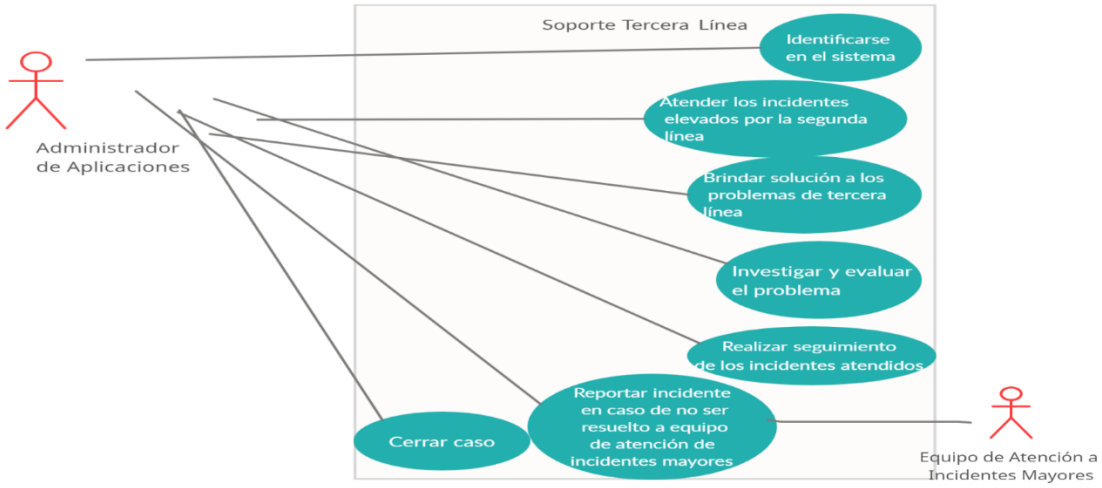
Soporte de tercera línea

SOPORTE EN TERCERA LÍNEA	
OBJETIVOS	Brindar solución a los incidentes como tercer contacto en caso de la segunda línea no lo pudo resolver
RESPONSABILIDADES	• Atender los incidentes elevados por la segunda línea • Brindar solución a los problemas referentes a Aplicaciones y el ERP • Investigar y evaluar el problema • Realizar seguimiento de los incidentes atendidos • Reportar incidente en caso de no ser resuelto para que se eleve al equipo de atención de incidentes mayores • Cerrar el caso del incidente
PERSONA ASIGNADA	Administrador de Aplicaciones

Fuente: elaboración propia

Imagen número 11

Rol de soporte de tercera línea



Fuente: elaboración propia

Cuadro número 11

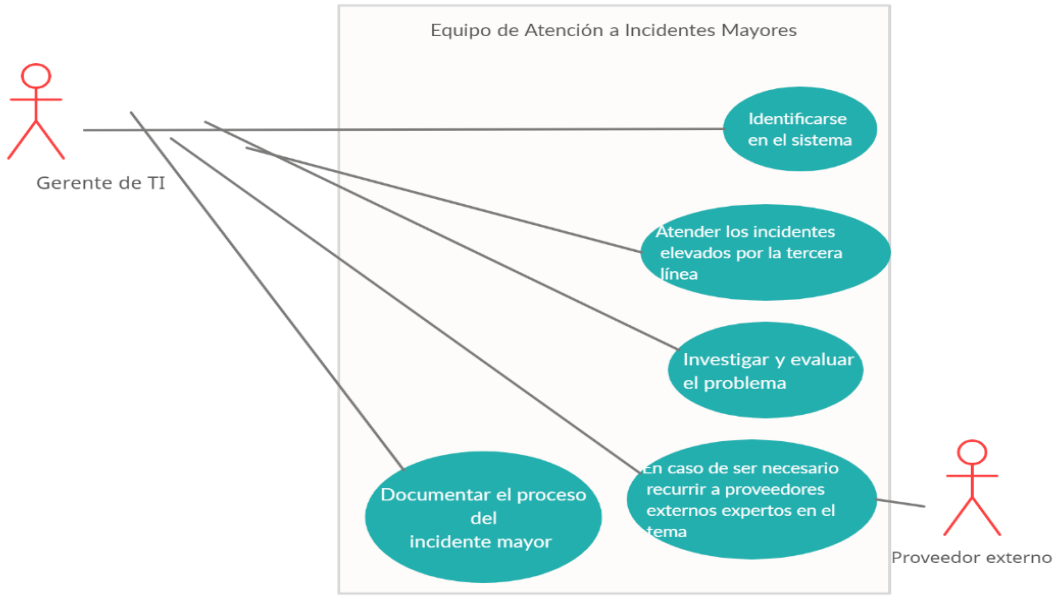
Equipo de atención a incidentes

EQUIPO DE ATENCIÓN A INCIDENTES MAYORES	
OBJETIVOS	Brindar solución a los incidentes mayores que no se lograron resolver en las líneas anteriores
RESPONSABILIDADES	• Atender incidentes mayores • Investigar y evaluar el incidente • En caso de ser necesario recurrir a proveedores externos expertos en el tema • Documentar el proceso del incidente mayor para el proceso de mejora continua
PERSONA ASIGNADA	Gerente de TI

Fuente: elaboración propia

Imagen número 12

Rol de equipo de atención de incidentes mayores

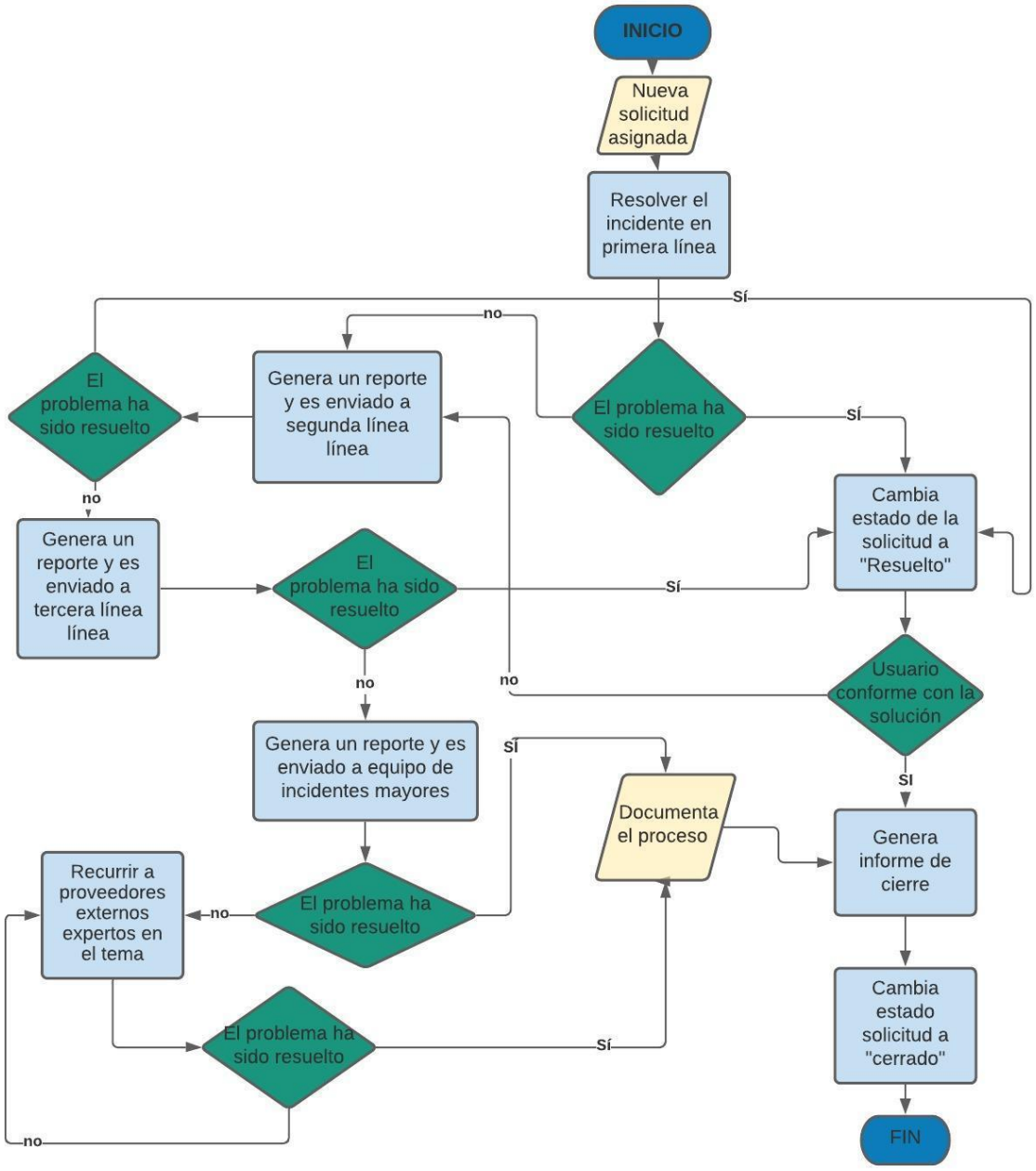


Fuente: elaboración propia

A continuación, se muestra un diagrama de flujo en el cual se representa todo el proceso que siguen los roles de gestión de incidentes y el flujo de la información que se genera.

Imagen número 13

Diagrama de flujo de los roles de gestión



Fuente: elaboración propia

Tiempo de Atención de Incidentes

El tiempo de atención de incidentes es el lapso que tiene el departamento de TI para revisar y analizar el incidente con la finalidad de brindarle una pronta respuesta al usuario, haciéndole saber si el problema está en proceso de solución. El horario de atención que brinda el equipo de tecnología a la solución de incidentes es de 8:00 am a 4:00 pm, en ese tiempo el usuario puede reportar incidencias y tener una pronta respuesta sobre si fue aceptada o rechazada la solicitud.

Por otra parte, el tiempo de resolución a los incidentes se refiere a la duración que les toma a los funcionarios del departamento de TI, solucionar el problema una vez que la solicitud fue aprobada.

Cuadro número 12

Prioridades y tiempos

Código de Prioridad	Prioridad	Tiempo de atención	Tiempo de Resolución
1	**Crítico**	**10 minutos**	**5 horas**
2	**Urgente**	**20 minutos**	**6 horas**
3	**Alta**	**30 minutos**	**Un día**
4	**Media**	**Un día**	**Un día**
5	**Baja**	**Dos días**	**Dos días**
6	**Mínima**	**Dos días**	**Una semana**

Fuente: elaboración propia

Estados de un Incidente:

El estado de un incidente permite conocer el punto o condición en el que se encuentra el mismo, de esta manera permite al usuario final saber la atención que le están brindando a la solicitud realizada.

Cuadro número 13

Estado de incidentes

Estado	Descripción
Abierto	Este estado indica que el incidente ha sido revisado y se encuentra en lista para ser asignado a soporte.
En progreso	En este punto el incidente se encuentra siendo investigado y en el proceso de resolución
Resuelto	Ha sido brindada una solución para el incidente, sin embargo, en este punto no se tiene la aprobación del usuario final
Cerrado	El problema ha sido resuelto y el usuario ha dado el visto bueno y puede trabajar con normalidad

Fuente: elaboración Propia

Estados de una solicitud:

Un estado de una solicitud permite a los funcionarios del departamento de TI y al usuario conocer la situación en la que se encuentra el reporte realizado.

Cuadro número 14

Estados de solicitud

Estado	Descripción
Borrador	En este estado la solicitud ha sido enviada y recibida, sin embargo, aún no ha sido revisada
En revisión	En este punto la solicitud está siendo revisada por el encargado de dicha tarea
Suspendido	Se suspenden las actividades debido a la realización de la solicitud
En espera de Autorización	La solicitud está en espera de aprobación
Aprobada	La solicitud ha sido aprobada
Rechazada	La solicitud ha sido rechazada
Cancelada	El usuario ha cancelado la solicitud
En proceso	Los funcionarios de TI se encuentran solucionando el incidente
Completada	La solicitud ha sido completada

Fuente: elaboración Propia

Definición de escalaciones y nivel de atención

En este apartado se definen las personas que participan durante el proceso de la resolución de los incidentes y la recepción de las solicitudes.

Cuadro número 15

Escalaciones y nivel de atención

Participante	Descripción
Usuario	La persona que reporta el incidente
Primer Nivel de Soporte	Es el nivel donde se atienden incidentes de soporte técnico a usuarios finales
Segundo Nivel de Soporte	En este nivel se atienden problemas referentes a infraestructura de red y comunicaciones
Tercer Nivel de Soporte	En este nivel se resuelve todo aquello relacionado a aplicaciones y ERP
Gerente de TI	La persona encargada de realizar autorizaciones y tomar decisiones en caso de ser necesarias
Equipo de Incidentes mayores y proveedores externos	Son incidentes que deben ser atendidos con la mayor brevedad y se requiere de un equipo más grande o bien, ayuda de proveedores y/o terceros

Fuente: elaboración propia

Cierre de incidentes y Solicitudes

El proceso de gestión de incidentes necesita un cierre formal, una vez que el usuario final haya determinado que el problema fue resuelto, debe realizarse el cierre por medio del Service Desk, el proceso a seguir es el siguiente:

Cuadro número 16

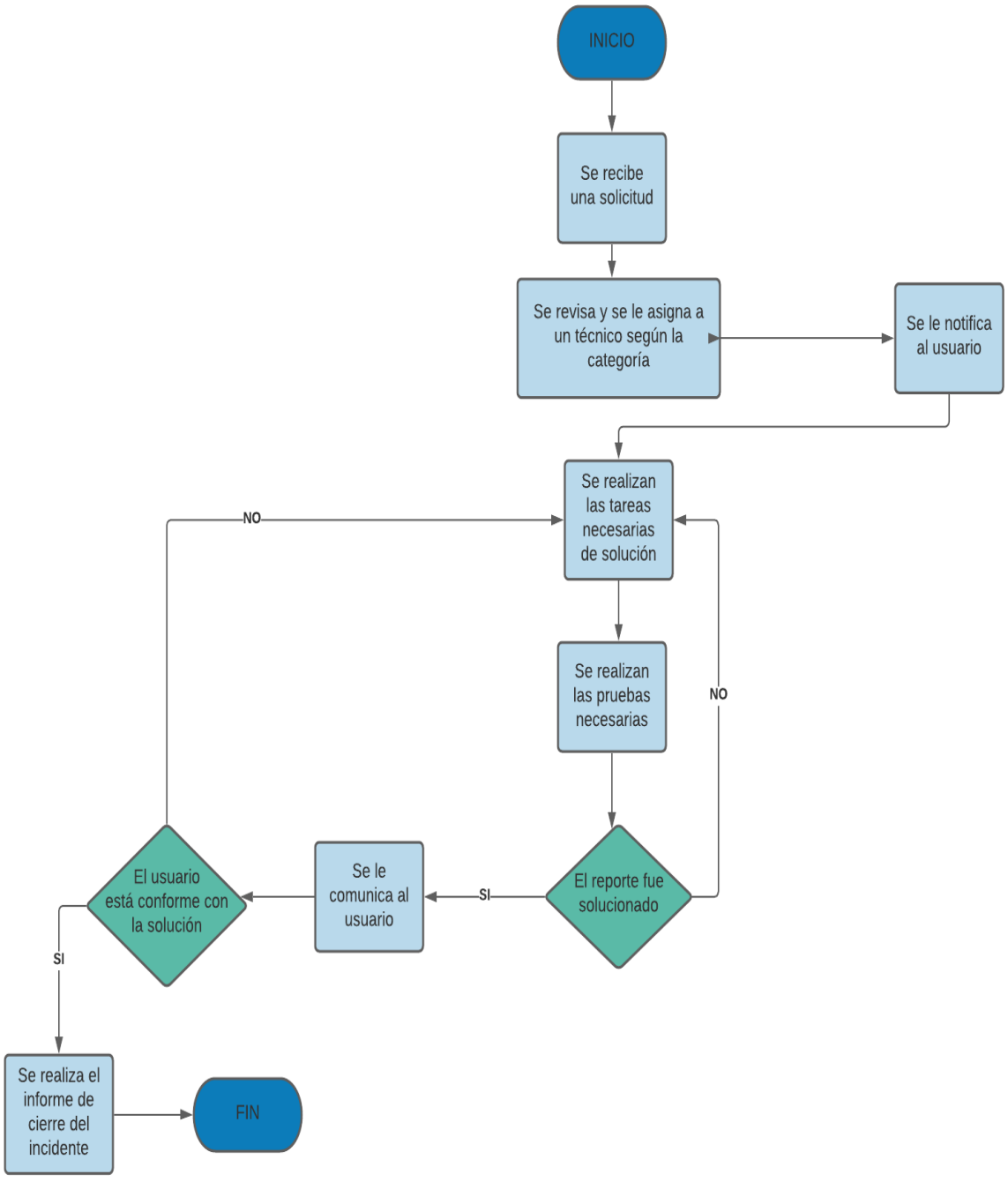
Cierre de incidentes y solicitudes

Etapa	Descripción
1. Identificar categorización	En esta etapa se verifica que la categorización dada inicialmente sea la misma una vez resuelto el problema. De lo contrario, se debe actualizar la categoría con la determinada durante el proceso de resolución.
2. Obtención de satisfacción del usuario	En esta etapa se recurre a herramientas como encuestas para conocer la satisfacción del personal.
3. Obtener documentación	Esta actividad consta de obtener toda la información del proceso de solución a la solicitud, todos los detalles y procedimientos que sucedieron durante el proceso, así como de los involucrados.
4. Determinar si es un incidente recurrente	En esta etapa es indispensable conocer si el problema ha sido resuelto desde su causa, esto con la finalidad de poder prevenirlo y poder tener un proceso de resolución en caso de que volviese a ocurrir.
5. Determinar requisitos financieros	Para cada uno de los reportes atendidos se debe documentar si tuvo algún costo monetario, de esta manera se controlan las solicitudes y se le pasa el reporte al área financiera.
6. Cierre formal	Un paso muy importante es realizar un informe con las especificaciones de cada incidente, en caso de que vuelva a suceder. Esto se realiza por medio de la herramienta Service Desk.

Fuente: elaboración propia

Imagen número 14

Diagrama de flujo cierre de incidentes y solicitudes



Fuente: elaboración propia

Propuesta de Implementación y Capacitación

En la siguiente sección se muestran los pasos a seguir para la implementación de la propuesta de gestión de incidentes para su adecuada utilización. Además, incluye una guía sobre las personas involucradas que deben ser capacitadas.

Propuesta de Implementación

- **Service Desk**

  Para esta herramienta es importante agregar y/o modificar algunos aspectos con el fin de que la herramienta vaya de la mano con la política propuesta, para lo cual se debe:

  1. Configurar el Service Desk de modo que soporte el catálogo de servicios
  2. Predeterminar los roles de gestión de incidentes dentro de la herramienta
  3. Incorporar los Roles de Gestión de Solicitudes
  4. Incluir el tiempo de atención a incidentes a la herramienta
  5. Establecer el estado de incidentes y de las solicitudes
  6. Configurar el proceso de cierre de las solicitudes

Cuadro número 17

Propuesta de implementación

PROPUESTA DE IMPLEMENTACIÓN	
ÁREA	ACCIÓN
Service Desk	• Configurar el Service Desk de modo que soporte el catálogo de servicios • Predeterminar los roles de gestión de incidentes en la herramienta • Incorporar los Roles de Gestión de Solicitudes • Incluir el tiempo de atención a incidentes a la herramienta • Establecer el estado de incidentes y de las solicitudes • Configurar el proceso de cierre de las solicitudes

Fuente: elaboración propia

Propuesta de Capacitación

Para lograr hacer uso correcto de la normativa es necesario que tanto el personal de TI como los usuarios finales utilicen de manera correcta el Service Desk, por lo cual deben estar familiarizados con cada módulo y saber los pasos a seguir en caso de que ocurra un incidente, es por ello que se establece una estructura detallada de qué puntos debe conocer cada persona según su rol:

- **Personal de TI:**
    1. **Gestor de las solicitudes**: Debe ser capacitado en el proceso y uso de la herramienta Service Desk de modo que conozca cómo deben ser realizadas las solicitudes para poder deducir si han sido completadas correctamente para, proceder a rechazar o aceptar el reporte. Además, el gestor de solicitudes tiene que saber cómo asignar el nivel de prioridad de cada solicitud para proceder a la asignación de un técnico registrado en el sistema.
    2. **Encargado de las solicitudes:** Capacitar en segunda instancia al encargado de las solicitudes el cual debe conocer el proceso en su totalidad ya que, que debe brindar seguimiento a cada solicitud para además documentar cada paso que surge durante el proceso el cual debe ser documentado dentro del Service Desk.
    3. **Gestor de Incidentes:** Al preparar al Gestor de Incidentes en el proceso y uso de la herramienta se asegura que las solicitudes se realicen correctamente, además este debe saber cómo y en qué pestaña debe llenar los controles mensuales de las solicitudes realizadas.
    4. **Soporte en primera línea:** Capacitar a los colaboradores de soporte en primera línea para que conozcan la herramienta y el proceso, ya que deben revisar las especificaciones de cada solicitud, saber dónde pueden ver los casos que tienen asignados y en caso de no poder resolverlos, informar sobre el proceso y enviarlo a segunda línea. Además, debe saber generar el informe de cierre.
    5. **Soporte en segunda línea:** Al capacitar al personal de segunda línea se asegura de que sepan dónde ver y qué deben hacer en caso de que la primera línea no

pueda resolver una solicitud, además en caso de no poder resolver el problema poder asignarlo a tercera línea. Además, debe saber generar el informe de cierre.

6. **Soporte en tercera línea:** Es indispensable que el personal de tercera línea conozca los mismos puntos mencionados en primera y segunda línea. Además, en caso de no poder resolver la solicitud generar un informe al personal de atención a incidentes mayores con todos los detalles estudiados.
7. **Equipo de atención a incidentes mayores:** Capacitar al personal que forma parte del equipo de atención a incidentes mayores con la finalidad de que puedan conocer el historial del caso en estudio, además se pueda informar sobre el proceso en gestión de dicho incidente y una vez resuelto el problema documentar todo el proceso en la herramienta y generar el informe de cierre del incidente.

❖ **Usuarios:**

Capacitar a los usuarios finales en el proceso que se debe seguir para la creación de solicitudes y el uso de la herramienta Service Desk. Los usuarios deberán saber cómo reportar correctamente un incidente, poder acceder a información para conocer sobre el incidente y saber dónde puede ver el proceso y el estado la solicitud realizada.

Cuadro número 18

Propuesta de capacitación

PROPUESTA DE CAPACITACIÓN	
PERSONAL	ACCIÓN
Personal de TI	• Capacitar al gestor de las solicitudes en el proceso y uso de la herramienta Service Desk • Capacitar en segunda instancia a los encargados de las solicitudes • Preparar al Gestor de los Incidentes en el proceso y uso de la herramienta Service Desk para velar que las solicitudes se realicen correctamente • Capacitar a los colaboradores de soporte en primera línea, segunda línea y tercera línea • Capacitar al personal que forma parte del equipo de atención a incidentes mayores

Usuarios	Capacitar a los usuarios finales en el proceso que se debe seguir para la creación de solicitudes y el uso de la herramienta Service Desk Los usuarios deberán saber: • Cómo reportar correctamente un incidente • Conocer el incidente • Saber dónde puede ver información sobre la solicitud realizada

Fuente: elaboración propia

CONCLUSIONES Y RECOMENDACIONES

En este apartado se presentan las concusiones y recomendaciones para la investigación.

Conclusiones

En este capítulo se describen las conclusiones que se obtienen al finalizar este proyecto, una vez realizado el estudio, analizado los resultados y tomado en cuenta la teoría sobre las metodologías que se implementaron se concluye que:

- Se identifica la situación actual del proceso de control de incidentes de acuerdo con la información recopilada según se muestra en el capítulo III de este documento, en el cual se reconoce claramente que el departamento de tecnología presenta una gran deficiencia en la gestión de incidentes, ya que el proceso no está respaldado por algún marco internacional o estándar que permita aplicar las mejores prácticas y un seguimiento optimo a los problemas que se presenten.
- A través del análisis realizado de la situación actual y la identificación de las debilidades en el capítulo III de este documento, se documentó la información relevante de los incidentes para deducir la clasificación, que permita analizar y priorizar todos lo relacionado con los incidentes según su frecuencia e impacto permitiendo definir las mayores debilidades del departamento.
- De acuerdo con el Marco Internacional ITILV3, se visualiza un claro vacío sobre las mejores prácticas por lo que es importante definir una propuesta, partiendo de las necesidades y requerimientos de la organización definidos en la investigación, los cuales se encuentran debidamente documentados para facilitar su uso y entendimiento.

- Una vez definida la propuesta, es necesario establecer un plan de capacitación al personal y usuarios involucrados en el proceso de control de incidentes, alineado a lo determinado en la investigación, con el objetivo de garantizar una adecuada implementación de la propuesta.

Recomendaciones

- Dadas las deficiencias identificadas en el proceso de control de incidentes se recomienda definir una propuesta basada en ITIL V3 que se encuentra dentro de las mejores prácticas que les permita desarrollar un nivel de servicio adecuado para la organización.
- Documentar la información importante sobre los incidentes que se presenten diariamente, que permita en un grado de madurez mayor en la gestión de incidentes desarrollar una Base de Conocimiento que permita implementar planes preventivos, definición de las incidencias de mayor impacto y disminución en los tiempos de respuesta.
- Implementar la propuesta de este proyecto como normativa de trabajo alineada con las mejores prácticas y alineada a los objetivos del departamento de TI para garantizar una correcta gestión de incidentes.
- Llevar a cabo la propuesta de implementación y la de capacitación de los colaboradores según su nivel de responsabilidad, así como a los usuarios finales, de acuerdo con los formatos establecidos, con el fin de obtener una correcta gestión de incidentes.

Bibliografía

Addati, G. A. (6 de 2014, p.3). *Área: Ingeniería Informática SISTEMAS VMS Y PSIM , Univesrsidad del Celma;Buenos Aires, revista virtual*. Obtenido de https://www.econstor.eu/bitstream/10419/110055/1/79211986X.pdf

Alba Córdova Vaca, L. R. (15 de 03 de 2019). *"TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TICS) APLICADAS A LAS ORGANIZACIONES EMPRESARIALES"*. Obtenido de https://www.hacienda.go.cr/Sidovih/uploads//Archivos/Articulo/tics-organizaciones-empresariales.pdf

Arias, F. G. (2012). *El proyecto de investigación introducción a la metodología científica. E-book.* Venezuela: EPISTEME,C.A.

Caicedo-Altamirano, V. P.-P.-C. (30 de 4 de 2018, p.110). *Arquitectura de redes de información. Principios y conceptos*. Obtenido de file:///C:/Users/Estudiante/Downloads/Dialnet-ArquitecturaDeRedesDeInformacionPrincipiosYConcept-6870909.pdf

Carlos Calderón, L. C. (2013). *Gestión de Incidentes y Gestión de la Continuidad del Negocio.* Colombia: Universidad Piloto de Colombia.

Cloud, E. (19 de 03 de 2020). *evaluandocloud.com*. Obtenido de evaluandocloud.com: https://evaluandocloud.com/tipos-incidentes-ciberseguridad/

Duarte, E. S. (2007). LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC) DESDE UNA PERSPECTIVA SOCIAL. *Revista Electrónica Educare*.

Española, R. A. (2020). *Definición de Frecuencia*. Obtenido de https://dle.rae.es/frecuencia

Figuerola, N. (2012). ITIL V3 ¿Por dónde empezar? En N. Figuerola, *ITIL V3 ¿Por dónde empezar?* (págs. 2-3). Buenos Aires.

Gimeno, V. A. (9 de 09 de 2010). *La influencia de las nuevas técnologías de la información y las comunicacipones y su repercución en las estrategia empresariales: la banca Online y su aplicación en en la cooperativas de crédito(Tesís doctoral)*. Obtenido de https://www.tesisenred.net/bitstream/handle/10803/52170/alfonso.pdf

Gonzales, E. A. (2015). Tecnologías de la Información y la comunicación. En E. A. Gonzales, *Tecnologías de la Información y la comunicación.* Lima, Perú: Fondo Editorial.

Gonzáles, Y. (17 de 09 de 2020, párr 4.). *¿Qué es un gusano informático? Tipos y ejemplos*. Obtenido de https://protecciondatos-lopd.com/empresas/gusano-informatico/

Guerrero, G. F. (1984). *Basico, Bloque.* Obtenido de https://s3. amazonaws. com/academia. edu. documents

Hitpass, B. (2017). *Business Process Management (BPM) Fundamentos y Conceptos de Implementación.* Santiago, Chile: BHH Ltda.

Huércano, S. R. (s.f.). Manual ITIL V3 Integro. En S. R. Huércano, *Manual ITIL V3 Integro.* Sevilla: Biable.

Huércano, S. R. (s.f.). *Manual ITIL V3 Integro.* Sevilla: Biable Management.

INOLASA. (s.f.). Obtenido de http://www.inolasa.com/index.html

interactiva, C. (2020, párr.9). *Las 7 principales tendencias tecnológicas para 2020*. Obtenido de https://computacioninteractiva.com/las-7-principales-tendencias-tecnologicas-para-2020/

Intituto Nacional de Ciberseguridad. (2015). Gestión de Riesgos, una guía de aproximación para el empresario. *incibe*, 3.

ISOTools. (s.f.). *ISOTOOLS EXCELLENCE*. Obtenido de Sistemas de Gestión de Riesgos y Seguridad: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/#:~:text=ISO%2027001%20es%20una%20norma,los%20sistemas%20que%20la%20procesan.&text=La%20Gesti%C3%B3n%20de%20la%20Seguridad,en%20la%20norma%20ISO%2027002.

Jauregui, M. (7 de 7 de 2014, párr.1). *Proceso de control básico*. Obtenido de https://aprendiendoadministracion.com/proceso-de-control-basico/

JAURÈS, P. R.-F. (2006). *METODOLOGÍA ITIL, Descripción, Funcionamiento y Aplicación.* Santiago: UNIVERSIDAD DE CHILE .

LAb, K. (2021, párr.5). *Enciclopedia Karpesky*. Obtenido de https://encyclopedia.kaspersky.es/knowledge/year-1989/

Lanfranco, E. (2019,p.3). *CSIRTs ¿De qué se trata?, modelos posibles,servicios y herramientas*. Obtenido de https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/4B%201.pdf

Marisol Maranto, M. E. (2015). *Fuentes de Información.* Universidad Autónoma del Estado de Hidalgo.

MINTIC, C. . (2016). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. *Seguridad y Privacidad de la Información*.

Montoro, M. (37 de 1 de 2020). *¿QUÉ SON LAS BUENAS PRÁCTICAS Y PARA QUÉ SIRVEN?* Obtenido de https://www.ats.edu.uy/buenas-practicas/

Morales, A. (9 de 12 de 2019, p.1). *Educación-Información*. Obtenido de https://www.todamateria.com/informacion/

Nazar, L. A. (03 de 05 de 2018). *Técnologias Transformadoras*. Obtenido de https://revistaempresarial.com/tecnologia/tecnologias-transformadoras/

Razo, C. M. (2020). Cómo elaborar y asesorar una investigación de tesis. En C. M. Razo, *Cómo elaborar y asesorar una investigación de tesis* (pág. 119). Mexico: Pearson Educación de México.

Rico, J. C. (s.f.). Gestión de la Seguridad. *S21Sec*.

Rioja, U. -U. (11 de 12 de 2019). *Universidad en Internet*. Obtenido de Universidad en Internet: https://www.unir.net/ingenieria/revista/iso-27001/

Sáenz, M. (20 de 01 de 2016). *El control empresarial del uso de las TIC se adapta a los nuevos tiempos*. Obtenido de https://www.observatoriorh.com/rr-ll/34778.html

Sampieri, R. H. (2014). *Metología de la Investigación.* México, DF: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Tedder, D. (19 de abril de 2018). *invgate*. Obtenido de invgate: https://blog.invgate.com/es/por-qu%C3%A9-una-matriz-de-priorizaci%C3%B3n-de-incidentes-es-importante#:~:text=La%20priorizaci%C3%B3n%20de%20incidentes%20es,la%20empresa%20necesita%20una%20resoluci%C3%B3n

Valdés, A. (1996). *Las normas ISO relacionadas con la documentación y la información.* La habana: ACIMED.

Valles, A. (07 de 2016, p.1). *Cómo se identifican áreas de mejora*. Obtenido de https://www.linkedin.com/pulse/c%C3%B3mo-se-identifican-%C3%A1reas-de-mejora-%C3%A0lex-vall%C3%A8s/?originalSubdomain=es

Vieites, Á. G. (2014). *Seguridad en Equipos Informáticos.* España: RA-MA.

Vilches, E. (2010). Guía de Gestión de Servicios basada en Fundamentos de ITIL v3. En E. Vilches, *Guía de Gestión de Servicios basada en Fundamentos de ITIL v3* (pág. 21). Madrid: Luarna Ediciones, S.L.

Weske, M. (2007). Business Process Management: Concepts, Languages, Architectures. En M. Weske, *Business Process Management: Concepts, Languages, Architectures.* Potsdam, Germany.

Westreicher, G. (07 de Agosto de 2020). *Economipedia*. Obtenido de Economipedia: https://economipedia.com/definiciones/gestion.html

Zoho Corp. (25 de junio de 2020). *MageneEngine*. Obtenido de MageneEngine: https://www.manageengine.com/latam/service-desk/itil-incident-management/que-es-la-gestion-de-incidentes-itil.html

Anexos

Anexo 1. Carta de aceptación de la empresa

03 de diciembre del 2020

A quien corresponda:

Por medio de la presente nuestra empresa INOLASA con cédula jurídica

3-101-058770 certifica que la estudiante ALONDRA ARGUEDAS GONZÁLEZ, de la Universidad Hispanoamericana, número de cédula 604370604 de la carrera de Ingeniería Informática, cuenta con la debida autorización para realizar su Proyecto de Final de Graduación en la Institución. Así mismo la institución y los colaboradores están en la mejor disposición para facilitar las tareas de investigación alusivas al tema.

Agradezco su atención, sin más se despide

Jorge Cantillano R.
Gerente Tecnología de Información
jcr@inolasa.com

Anexo 2. Cuestionario de incidentes

CUESTIONARIO DE INCIDENTES INFORMÁTICOS

Objetivo: Determinar los incidentes informáticos que se presentan en el departamento de TI de INOLASA.

La información es confidencial y los datos que se obtienen son estrictamente de uso interno.

MARQUE CON X.

¿Cuáles de los siguientes problemas informáticos se presentan a menudo en su departamento?

Corte de suministro eléctrico SÍ _____ NO_____

1. ¿Con qué frecuencia sucede el corte de suministro eléctrico en el departamento de TI?

___1 vez al mes
___2 veces al mes
___3 o más veces al mes
___Cada 3 meses
___Cada 6 meses
___Cada 9 meses
___Una vez al año

2. ¿Cuál es el tiempo promedio de solución cortes de suministro eléctrico?

___1 semana
___2 semanas
___3 semanas
___1 mes
___Más de un mes

3. Problemas con fuego(incendios) SÍ _____ NO_____

4. ¿Con qué frecuencia suceden problemas con incidentes de fuego?

___1 vez al mes
___2 veces al mes
___3 o más veces al mes
___Cada 3 meses
___Cada 6 meses
___Cada 9 meses
___Una vez al año

5. ¿Cuál es el tiempo promedio de solución a los incidentes causados por fuego?

___1 semana
___2 semanas
___3 semanas
___1 mes
___Más de un mes

6. Daños por agua (inundaciones, fugas) SÍ _____ NO_____

7. ¿Con qué frecuencia se presentan daños por agua (Inundaciones, fugas) en el departamento de TI? ___1 vez al mes ___2 veces al mes ___3 o más veces al mes ___Cada 3 meses ___Cada 6 meses ___Cada 9 meses ___Una vez al año	8. ¿Cuál es el tiempo promedio de solución a daños por agua? ___1 semana ___2 semanas ___3 semanas ___1 mes ___Más de un mes
9. Robo de Equipos Informáticos SÍ _____ NO_____	
10. Problemas de comunicación (Problemas de conexión a internet) SÍ _____ NO_____	
11. ¿Con qué frecuencia suceden los problemas de comunicación? ___1 vez al mes ___2 veces al mes ___3 o más veces al mes ___Cada 3 meses ___Cada 6 meses ___Cada 9 meses ___Una vez al año	12. ¿Cuál es el tiempo promedio de solución a los problemas de comunicación? ___1 semana ___2 semanas ___3 semanas ___1 mes ___Más de un mes
13. Inconvenientes con el correo de la institución SÍ _____ NO_____	
14. ¿Con qué frecuencia suceden los de inconvenientes con el correo en la institución? ___1 vez al mes ___2 veces al mes ___3 o más veces al mes ___Cada 3 meses ___Cada 6 meses ___Cada 9 meses ___Una vez al año	15. ¿Cuál es el tiempo promedio de solución los inconvenientes con el correo de la institución? ___1 semana ___2 semanas ___3 semanas ___1 mes ___Más de un mes
16. Desperfectos de hardware se presentan en la institución SÍ _____ NO_____	

17. ¿Con qué frecuencia suceden desperfectos con hardware? ___1 vez al mes ___2 veces al mes ___3 o más veces al mes ___Cada 3 meses ___Cada 6 meses ___Cada 9 meses ___Una vez al año	18. ¿Cuál es el tiempo promedio de solución a los desperfectos con hardware? ___1 semana ___2 semanas ___3 semanas ___1 mes ___Más de un mes
19. Problemas de video (pantallas, proyectores) se presentan en la institución SÍ _____ NO_____	
20. ¿Con qué frecuencia sucede este tipo de incidentes? ___1 vez al mes ___2 veces al mes ___3 o más veces al mes ___Cada 3 meses ___Cada 6 meses ___Cada 9 meses ___Una vez al año	
21. Problemas de virus en las computadoras son un incidente que se presenta en el departamento de TI. SÍ _____ NO_____	
22. Los problemas de identificación (contraseñas, usuarios) son un problema que se presenta en el departamento de TI SÍ _____ NO_____	
23. ¿Con qué frecuencia se presentan problemas de identificación de usuario? ___1 vez al mes ___2 veces al mes ___3 o más veces al mes ___Cada 3 meses ___Cada 6 meses ___Cada 9 meses ___Una vez al año	24. ¿Cuál es el tiempo promedio de solución a los inconvenientes con por identificación de usuarios? ___1 semana ___2 semanas ___3 semanas ___1 mes ___Más de un mes
25. Los problemas de actualización de software son un problema en el departamento de TI SÍ _____ NO_____	

26. ¿Con qué frecuencia con que suceden los problemas de actualización de software? ___1 vez al mes ___2 veces al mes ___3 o más veces al mes ___Cada 3 meses ___Cada 6 meses ___Cada 9 meses ___Una vez al año	27. ¿Cuál es el tiempo promedio de solución a los problemas de actualización de software? ___1 semana ___2 semanas ___3 semanas ___1 mes ___Más de un mes
28. ¿En el departamento de TI se hace uso correcto del Service Desk? SI_____ No_____	
29. ¿Considera que su nivel de conocimiento es suficiente para atender los incidentes que se presentan?	
¿Qué persona notifica el incidente? **¿A qué persona se le comunica el incidente?** **Otros incidentes**	

Muchas gracias, Dios le bendiga 😊

Anexo 3. Entrevista de incidentes informáticos

ENTREVISTA DE INCIDENTES INFORMÁTICOS **Objetivo:** Determinar los incidentes informáticos que se presentan en el departamento de TI de INOLASA. La información es confidencial y los datos que se obtienen son estrictamente de uso interno.
¿De qué forma trabajan actualmente cuando un usuario de algún otro departamento tiene un problema ya sea con un sistema o con una computadora?
¿Cómo se manejan los problemas cuando fallan equipos o periféricos y si se afectan los otros procesos o servicios?
¿Habían pensado anteriormente en implementar un sistema formal de gestión de incidencias?
¿Cuánto es el tiempo aproximado que les toma solucionar un problema o incidente?
¿Cuántas personas están encargadas de solucionar los incidentes?
¿Qué tan frecuente se presentan los incidentes?
¿Considera usted necesario tener una política para el manejo de esos incidentes?
En caso de no saber cómo resolver un incidente ¿a qué medios recurren?

Anexo 4. Carta de Tutor

CARTA DEL TUTOR

San José, 20 de julio de 2021

Maria Isabel Losilla Barrientos
Directora
Ingeniería Informática
Universidad Hispanoamericana
Sede Llorente

Estimada señora:

La estudiante **ALONDRA MARIA ARGUEDAS GONZALEZ**, cédula de identidad número 6-0437-0604, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado **"PROPUESTA DE UNA POLÍTICA DE MANEJO DE INCIDENTES EN EL DEPARTAMENTO DE TI DE INDUSTRIAL OLEAGINOSAS AMERICANAS S.A (INOLASA)"**, el cual ha elaborado para optar por el grado académico de Licenciatura en Ingeniería Informática.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a) Original del tema	10%	10
b) Cumplimiento de entrega de avances	20%	20
c) Coherencia entre los objetivos, los instrumentos aplicados y los resultados de la investigación	30%	30
d) Relevancia de las conclusiones y recomendaciones	20%	20
e) Calidad, detalle del marco teórico	20%	20
TOTAL		**100**

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

JULIAN RAQUEL CORDOBA SANABRIA (FIRMA)

Firmado digitalmente por JULIAN RAQUEL CORDOBA SANABRIA (FIRMA)
Fecha: 2021.07.20 19:12:09 -06'00'

Lic. Julián Córdoba Sanabria

Cédula 109640134

Anexo 5. Carta de Lector

CARTA DE LECTOR

San José, 23 de setiembre, 2021

Universidad Hispanoamericana
Sede Heredia
Carrera de Ingeniería Informática

Estimados señores,

La estudiante Alondra María Arguedas González, cédula de identidad 6-0437-0604, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "PROPUESTA DE UNA PÓLITICA DE MANEJO DE INCIDENTES EN EL DEPARTAMENTO DE TI DE INDUSTRIAL OLEAGINOSAS AMERICANAS S.A (INOLASA)" , el cual ha elaborado para obtener su grado de Licenciatura en Ingeniería Informática .

He revisado el contenido analizando, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación, considerando que, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atentamente,

ING. MARÍA ISABEL LOSILLA BARRIENTOS M.R.I.
Cédula: 1-0663-0662

Anexo 6. Declaración Jurada

DECLARACIÓN JURADA

Yo Alondra María Arguedas González, mayor de edad, portador de la cédula de identidad número 604370604 egresado de la carrera de Ingeniería Informática. de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura en Ingeniería Informática, juro solemnemente que mi trabajo de investigación titulado: Propuesta de una Política de manejo de Incidentes en el departamento de T.I de Industrial Oleaginosas Americanas (INOLASA)

es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público. en fe de lo anterior, firmo en la ciudad de San José, a los 20 días del mes de julio del año dos mil 21.

Arguedas

Firma del estudiante

Cédula 604370604.

Anexo 7. Autorización del CENIT

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 25/10/21

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Alondra María Arguedas González con número de identificación 604370604 autor (a) del trabajo de graduación titulado Propuesta de una Política de Manejo de Incidentes en el Departamento de TI de industrial Oleaginosas Americanas S.A (INOLASA) presentado y aprobado en el año 2021 como requisito para optar por el título de Licenciatura; (SI / NO) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

Arguedas 604370604
Firma y Documento de Identidad

ANEXO 1 (Versión en línea dentro del Repositorio)
LICENCIA Y AUTORIZACIÓN DE LOS AUTORES PARA PUBLICAR Y PERMITIR LA CONSULTA Y USO

Parte 1. Términos de la licencia general para publicación de obras en el repositorio institucional

Como titular del derecho de autor, confiero al Centro de Información Tecnológico (CENIT) una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, el autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito.

b) Autoriza al Centro de Información Tecnológico (CENIT) a publicar la obra en digital, los usuarios puedan consultar el contenido de su Trabajo Final de Graduación en la página Web de la Biblioteca Digital de la Universidad Hispanoamericana

c) Los autores aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) Los autores manifiestan que se trata de una obra original sobre la que tienen los derechos que autorizan y que son ellos quienes asumen total responsabilidad por el contenido de su obra ante el Centro de Información Tecnológico (CENIT) y ante terceros. En todo caso el Centro de Información Tecnológico (CENIT) se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

e) Autorizo al Centro de Información Tecnológica (CENIT) para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

f) Acepto que el Centro de Información Tecnológico (CENIT) pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

g) Autorizo que la obra sea puesta a disposición de la comunidad universitaria en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en las "Condiciones de uso de estricto cumplimiento" de los recursos publicados en Repositorio Institucional.

SI EL DOCUMENTO SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA O UNA ORGANIZACIÓN, CON EXCEPCIÓN DEL CENTRO DE INFORMACIÓN TECNOLÓGICO (CENIT), EL AUTOR GARANTIZA QUE SE HA CUMPLIDO CON LOS DERECHOS Y OBLIGACIONES REQUERIDOS POR EL RESPECTIVO CONTRATO O ACUERDO.