UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍA DE LA INFORMACIÓN

TRABAJO DE TITULACIÓN

Trabajo de Integración Curricular , previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

"Plan de respuesta a incidencias de seguridad informática (IRP) para la Dirección de Tecnologías de la información de la UPSE"

AUTOR

Jesús Daniel Rosales Reyes

PROFESOR TUTOR

LSI. Daniel Quirumbay Yagual, MSIA.

LA LIBERTAD – ECUADOR

2020

AGRADECIMIENTO

Agradezco a mis padres que siempre me han brindado todo su apoyo en cualquier momento, por haberme formado con valores y también haberme ayudado con recursos materiales para poder cumplir esta etapa de vida universitaria. Por ustedes estoy aquí.

A mis hermanos porque también fueron parte fundamental en este largo camino que tuve que recorrer.

A mi tutor Msia. Daniel Quirumbay por brindarme la oportunidad, tiempo y el apoyo necesario durante el desarrollo de esta investigación, también como docente por compartir sus conocimientos y ayudarme con temas que no sabía.

A resto de mis docentes que también formaron parte de mi etapa universitaria, cada uno me brindaron sus conocimientos y aportó en mi desarrollo como profesional.

Jesús Rosales Reyes

APROBACIÓN TUTOR

En calidad de tutor de la propuesta tecnológica con título “Plan de respuesta a incidencias de seguridad informática (IRP) para la Dirección de Tecnologías de la información de la UPSE”, presentado por el señor egresado ROSALES REYES JESUS DANIEL estudiante de la carrera de Tecnología de la Información, me permito declarar que luego de haber orientado, analizado y revisado, es aprobado en todas sus partes.

Particular que informo para los fines consiguientes.

Lsi. Daniel Quirumbay Yagual, MSIA
Docente Tutor

La Libertad, 07 de octubre del 2020

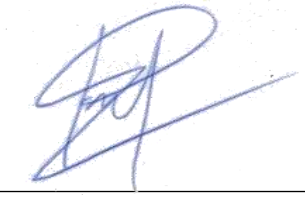
TRIBUNAL DE GRADO

Ing. Samuel Bustos Gaibor, MSc.
DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Ing. Jaime Orozco Iguasnia, Mgt.
DOCENTE ESPECIALISTA

LSI. Daniel Quirumbay Yagual, MSIA.
DOCENTE TUTOR

Ing. Alicia Andrade Vera, Mgt.
DOCENTE GUÍA UIC



Jesús Daniel Rosales Reyes
ESTUDIANTE

RESUMEN

Para establecer un equipo de respuesta a incidentes de seguridad informático (CSIRT) académico en la Universidad Estatal Península de Santa Elena (UPSE) es necesario contar un plan de respuesta a incidentes de seguridad informática (IRP), la presente propuesta tecnológica tiene como finalidad establecer pautas para un IRP para iniciar el proceso de la creación del CSIRT-UPSE y adicional a esto la implementación de una página web donde se acogerá las incidencias informáticas que ocurran en la facultad de sistemas y telecomunicaciones (FACSISTEL), de esta manera el departamento de TIC obtendrá un registro de incidencias de seguridad informática debido que actualmente no cuenta con uno. Para alcanzar este objetivo se utilizó diferentes herramientas de código abierto y distintas metodologías y técnicas de recolección de información.

Como producto final se obtuvo una página web CSIRT-UPSE, donde se encuentra embebido la herramienta especializada para recibir tickets de incidencias informáticas REQUEST TRACKER todo esto teniendo conexión con el plan de respuesta a incidencias de seguridad informática para el uso y las acciones correctas a tomar.

Para demostrar los beneficios de contar un plan de incidencias informáticas, la página web CSIRT-UPSE y el Request Tracker los servidores se crearon de manera local.

Palabras claves: plan de contingencia informático, sistema gestor de tickets, CSIRT, Reportes de incidencias

ABSTRACT

To establish an academic computer security incident response team (CSIRT) at the Santa Elena Peninsula State University (UPSE), it's necessary to have a computer security incident response plan (IRP), the present technological proposal takes as a purpose to establish rules for an IRP with that it's possible to initiate the process of the creation of the CSIRT-UPSE and additional to this the implementation of a web page where one will receive the computer incidences that happen in the faculty of systems and telecommunications (FACSISTEL), this way the TIC department will obtain a record of incidences of computer safety owed that at present isn't provided with one. To achieve this objective, different open source tools were used and different methodologies and techniques of compilation of information.

As a final product, a CSIRT-UPSE web page was obtained, in which the specialized tool to receive tickets from computer incidences REQUEST TRACKER is embedded all this having connection with the plan of response to incidents of computer security for the use and the correct actions to take.

To demonstrate the benefits of counting a plan of computer incidences, the web page CSIRT-UPSE and Request Tracker the servants were created in a local way.

Keywords: computer contingency plan ticket management system, CSIRT, Incident reports

DECLARACIÓN

El contenido del presente Trabajo de Graduación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

_____

JESÚS DANIEL ROSALES REYES

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

En los últimos años las actividades maliciosas asociadas a la tecnología se han incrementado, la rápida y eficaz respuesta es clave en organizaciones públicas y privadas por tal motivo entran en operación los CSIRT, la implementación de un plan de respuesta de incidencias (IRP) junto con un equipo de profesionales de seguridad de TI que tienen el conocimiento para detectar y manejar los incidentes, con el objetivo de poder hacerle frente a amenazas de seguridad y ayudar a mitigar las vulnerabilidades que podrían presentarse [1]. La Universidad Estatal Península de Santa Elena (UPSE) para brindar un servicio de calidad debe estar en constante crecimiento y una clave del éxito es adaptarse a la nueva era digital, en utilizar tecnologías de la información para automatizar sus servicios lo que conlleva que más información sea relevante, y aun siendo una institución prestigiosa no se salva de estar expuesto a ataques informáticos con fines maliciosos.

El presente trabajo de investigación se enfocó en implementar un plan de respuesta a incidencias de seguridad informática donde abarca cómo manejar un evento especifico de la manera más efectiva, como está conformado un CSIRT las funciones de cada uno y mantener un historial de todas las incidencias que se han registrado para evitar incidentes similares a futuro. Este documento de propuesta tecnológica, consta de dos secciones:

El capítulo I se detalla el antecedente, descripción objetivos, justificación, alcance, metodologías empleadas en el proyecto y resultados esperados.

El capítulo II detalla el marco teórico, contextual y conceptual que son pilares para entender la propuesta tecnológica planteada, también se detalla las pautas del plan de respuesta a incidentes de seguridad informática, la implementación de la herramienta para el registro de incidencias y resultados de la investigación realizada.

CAPÍTULO I

FUNDAMENTACIÓN

1.1 ANTECEDENTE

Trabajar en reforzar la seguridad informática de una entidad pública o privada se transforma en uno de los procesos esenciales para que las entidades logren asegurar el buen desempeño de la misma [2]. La mayor amenaza que se enfrenta la sociedad actualmente es el creciente y recurrentes incidencias de seguridad informática en los sistemas de información. Estas incidencias informáticas que a veces no son de manera involuntaria, se desarrollan todo el tiempo y simbolizan un desafío complicado de realizar para la sociedad. En circunstancias de ataques intencionados el desafío es aún más complicado porque debido al fácil acceso a internet encontrar herramientas para realizar ataques informáticos resulta más simple además que cada vez son más sofisticadas [3].

La Universidad Estatal Península de Santa Elena (UPSE) ubicado en la provincia de Santa Elena cantón La Libertad cuenta con una página web de información para usuarios dentro y fuera de la institución, además de aplicaciones Web para los estudiantes, docentes, administrativos y bienestar universitario con un servicio de calidad. La UPSE con el avance tecnológico ha aumentado el nivel de riesgo ante incidencias informáticas amenazando la disponibilidad e integridad por causas de actividades maliciosas o mal manejo de los propios recursos.

Los ataques informáticos no tienen preferencia suelen llegar para grandes o pequeñas infraestructuras por igual y de manera inesperada, no se pueden predecir es por eso que actuar de manera rápida y eficaz son piezas fundamentales para evitar posibles daños a futuros.

El crecimiento e innovación de los servicios tecnológicos ha facilitado las tareas cotidianas de instituciones, empresas y sociedad en general, sin embargo, de manera paralela los delitos informáticos aumentan [4], surgiendo nuevas amenazas a tal punto de causar pérdidas de datos e interrupciones en los procesos que se realizan en dicha entidad.

El primer Equipo de Respuesta a incidencias de Seguridad Informática (CSIRT, del inglés Computer Security Incident Response Team) fue creado en 1988 con la aparición del gusano Morris (Creado por Robert Tappan Morris) que afectó casi el 10% de los sistemas conectados al ARPANET (Advanced Research Projects Agency Network) que la DARPA (Defense Advanced Research Projects Agency) impulsó con la iniciativa del CSIRT en la Universidad de Carnegie Mellon [5].

En una publicación emitida el 15 de abril del 2019 por el diario El Universo ratifica que algunas instituciones del estado recibieron en los últimos días más de 40 millones de asaltos cibernéticos donde no hubo robo de información. Los asaltos surgieron en Estados Unidos, Reino Unido y también de Ecuador; entre las entidades atacadas están Cancillería de Ecuador, Presidencia de la República, Banco Central del Ecuador, ministerios y GAD´s [6]. Un CSIRT es un equipo especialista en seguridad de la información que proporciona servicios y apoyo a un grupo en particular (la comunidad de destino) con el fin de prevenir, manejar y responder a las incidencias informáticas. En Estados Unidos las siglas CERT (Equipo de Respuesta ante Emergencias Informáticas) se acostumbra a utilizar en vez de CSIRT [7], en China conocido CNCERT o CNCERT/CC [8], en España conocido como CSIRT es que cumple con la definición genérica ofrecida por la ENISA, FIRST o Trusted Introduced [9].

Figura 1: CSIRT nacionales dentro de los Estados Miembros de la OEA

En varios países de Latinoamérica se han implementado CSIRT para dar la debida atención necesaria a requerimientos de seguridad informática [1], en Ecuador tiene el nombre de EcuCERT (Equipo de respuesta a incidencias informáticas del Ecuador) [10]. En cada país algunas Universidades han creado su CSIRT Académico de forma exitosa, favoreciendo el uso de las buenas prácticas de seguridad y la formación de un personal apto para mejorar y fortalezca las unidades de seguridad de la información. El país tiene dos universidades, el denominado CSIRT-UTPL que es el Equipo de Respuesta a Incidencias de Seguridad Informática, el cual está ubicado en la Universidad Técnica Particular de Loja y el CSIRT-EPN Centro de respuesta a incidencias informáticas de la Escuela Politécnica Nacional.

Una característica de los CSIRT a nivel local y global es la compartición de información al público general, se comunican entre ellos de los ataques informáticos que tienen y de esta manera ayudan mutuamente para buscar una solución rápida en caso de que sea un ataque grave. Se publican las soluciones para que otros CSIRT se basen en esto cuando tengan problemas iguales o similares.

La UPSE actualmente no dispone de personal que esté al tanto de las actividades que se emiten antes las incidencias informáticas. Por tal motivo con la implementación del CSIRT en la UPSE se tendría personal capacitado para dar la atención necesaria antes posibles amenazas o fallos que se presenten en las plataformas web, tanto como estudiantes y personal administrativo pueden enviar reportes a través del portal del CSIRT que tendría la UPSE.

Sabiendo la brecha digital que existe en el país, la carencia de leyes frente accidentes de seguridad informática y la poca capacitación en temas de seguridad; la utilización de CSIRT académicos sería de gran impulso para ofrecer a la sociedad lineamientos que le permitan: identificar las inseguridades de la infraestructura tecnológica, limitar el impacto de las amenazas informáticas, llevar a cabo métodos para la rehabilitación frente a accidentes informáticos y seleccionar estándares para garantizar la confidencialidad, integridad y veracidad de los datos. La utilización de un CSIRT contribuirá a:

- Creación de plan de respuesta a incidencias (IRP)
- Establecer métodos de respuesta a accidentes de seguridad informáticos estructurados que permitan reducir el impacto negativo de amenazas a los elementos y servicios tecnológicos de la UPSE.
- Brindar un punto de contacto a la comunidad académica de la UPSE y a la sociedad en general, para el acompañamiento en la utilización de prácticas de seguridad y procesos para el manejo de accidentes de seguridad informática.

El plan de respuesta a incidencias (IRP) se trata de un componente crítico en las políticas de ciberseguridad, que le garantizará que una organización pueda responder en forma apropiada en caso de que sufrir ataques informáticos [11]. Crear el IRP es lo primero que debe hacer un CSIRT. Las organizaciones que carecen de experiencia pueden contratar a un consultor para ayudar a redactar el plan. Es importante que el equipo tenga personal completo y participe en la creación del plan, incluso si se realiza con un consultor externo, para que el equipo CSIRT tenga familiaridad y un sentido de propiedad. Cada miembro del equipo debe revisar el plan de respuesta a incidencias detalladamente. El plan sea fácilmente accesible para todo el personal del CSIRT ayudará a garantizar que, cuando aparezca una incidencia se seguirán los procedimientos correctos.

1.2 DESCRIPCIÓN DEL PROYECTO

El presente proyecto contará con la creación del IRP para el CSIRT-UPSE que debe incluir tres elementos para una buena gestión óptima que son:

1.2.1 Plan integral

1.2.1.1 Preparación

Estos son los pasos que su equipo de respuesta a incidencias debe tomar para prepararse para las incidencias de seguridad informática:

- Desarrollar políticas para implementar en caso de una incidencia de seguridad informática (virus, malware, acceso no autorizado a infraestructura)
- Revisar la política de seguridad y realice una evaluación de riesgos.
- Priorizar los problemas de seguridad, conozca sus activos más valiosos y concéntrese en incidencias críticos de seguridad

1.2.1.2 Identificación

- Identificar y evaluar la incidencia.
- Decidir la gravedad y el tipo de incidencia.
- Documentar las acciones tomadas, esta información se puede usar más adelante como evidencia si la incidencia llega a un tribunal de justicia.

1.2.1.3 Contención

Una vez que el equipo aísla una incidencia de seguridad, el objetivo es detener más daños. Esto incluye:

- **Contención a corto plazo:** una respuesta instantánea, para que la amenaza no cause más daño.
- **Copia de seguridad del sistema:** hacer una copia de seguridad de todos los sistemas afectados antes de borrarlos en caso de que la situación lo amerite.
- **Contención a largo plazo:** arreglar temporalmente los sistemas afectados para que puedan usarse en la producción. Mientras esto ocurre tomar medidas para evitar que la incidencia se repita o se intensifique: instalar parches de seguridad en los sistemas afectados y asociados, eliminar las cuentas y puertas traseras creadas por los atacantes, modificar las reglas del firewall y cambiar las rutas para que la dirección del atacante sea nula, etc.

1.2.1.4 Erradicación

Esto se hace de la siguiente manera:

- Aislar la raíz del ataque para eliminar todas las instancias del software.
- Realizar análisis de malware para determinar la extensión del daño.
- Dar tiempo para asegurarse de que la red sea segura.

1.2.1.5 Recuperación

Asegurar de que los sistemas afectados no estén en peligro y puedan restablecerse a sus condiciones de trabajo. El propósito de esta fase es devolver los sistemas afectados al entorno de producción, para garantizar que no conduzcan a otra incidencia. Asegúrese de que no ocurra otra incidencia restaurando los sistemas a partir de copias de seguridad limpias, reemplazando los archivos comprometidos con versiones limpias, reconstruyendo los sistemas desde cero, instalando parches y cambiando las contraseñas.

1.2.1.6 Documentación

El equipo debe identificar cómo se gestionó y erradicó la incidencia. Qué acciones tomaron para recuperar el sistema atacado, las áreas donde el equipo de respuesta necesita mejoras y las áreas donde fueron efectivas. Los informes sobre las incidencias que se presentaron proporcionan una revisión clara de toda la incidencia y podrán usar en reuniones, como puntos de referencia para comparar o como información de capacitación.

1.2.2 Equipo

Para prepararse y atender la incidencia, debe formar un equipo centralizado de respuesta a incidencia, responsable de identificar las brechas de seguridad y tomar medidas de respuesta. El equipo debe incluir:

- **Líder del equipo:** coordina todas las acciones del equipo y garantiza que el equipo se concentre en minimizar los daños y recuperarse rápidamente. Prioriza las acciones durante el aislamiento, análisis y contención de una incidencia. Supervisa todas las acciones y guía al equipo durante incidencias de alta gravedad.
- **Analistas de seguridad:** equipo de analistas de seguridad que trabajan en todos los departamentos para aislar y corregir fallas en los sistemas, soluciones y aplicaciones de seguridad de la organización. Recomiendan medidas específicas para mejorar la postura general de seguridad.

- **Investigador principal:** aísla la causa raíz, analiza toda la evidencia, gestiona otros analistas de seguridad y realiza una recuperación rápida del sistema y el servicio.
- **Investigadores de amenazas:** proporcionan el contexto de una inteligencia de incidencias y amenazas. Utilizan esta información y registros de incidencia anteriores para crear una base de datos de inteligencia interna. En muchos equipos de seguridad son herramientas automatizadas.
- **Representación legal:** una incidencia puede convertirse en cargos penales. Por lo tanto, debe tener recursos humanos y orientación legal.

1.2.3 Herramienta

Uno de los elementos para la óptima gestión a incidencias debe incluir herramientas para el manejo antes mencionada, como adición al plan de respuesta a incidencias de seguridad informática el CSIRT debe de contar con una plataforma web para eso se creará un prototipo en donde habrá servicios de seguridad: boletines de alerta y aviso, manejo de vulnerabilidades y la sección de reportar una incidencia.

La implementación de la aplicación web que será administrado por Tics podrá ser utilizado por docentes y estudiantes que conforman la facultad de sistemas y telecomunicaciones dichos usuarios pueden reportar incidencia que ocurren con los equipos informáticos de la facultad o sus portátiles personales. Esto permitirá crear un grupo de investigación en relación a la seguridad informática y de la información. No se le considerará como etiquetera técnica, la página de la UPSE ya cuenta con soporte técnico [12], esta aplicación web se enfoca a riesgos informáticos o auditoria forense, para evitar el registro de reportes innecesario el personal encargado de administrar la aplicación web reconocerá que dicho reporte de incidencia sea relacionado a ciberseguridad y no de soporte técnico.

CSIRT-UPSE brindará servicios que están relacionado con su misión, los servicios prestados son: servicios proactivos y servicios reactivos. Los servicios reactivos son los servicios más importantes que brinda un CSIRT, responden a las incidencias de seguridad cibernética que ocurre en su propia infraestructura. Los principales tipos de servicios reactivos son la gestión de incidencia y la respuesta de la vulnerabilidad.

Los servicios proactivos tienen como objetivo mejorar los procesos y la seguridad de la infraestructura para prevenir incidencia de seguridad o disminuir el impacto cuando ocurre una incidencia. Los principales tipos de servicios proactivos son realización de seguimiento, la distribución de alertas y el ofrecimiento de servicios de investigación y desarrollo.

El tiempo de respuesta del mismo dependerá de la gravedad de la incidencia reportado, si el reporte es de alto nivel que no se pueda resolver de manera local, se pedirá ayuda a CEDIA que tiene registrado a otros CSIRT, le solicitará una consulta de la solución al problema si el ataque ha sido registrado anteriormente en otro lado o en dicho caso si es un reporte nuevo se registrará para su posterior solución. Si el reporte informático es de bajo nivel, se trabajará localmente, pero de igual manera quedará registrado para que otros CSIRT que tengan el mismo problema a futuro puedan ayudarse, la información registrada solo se publicará la alerta, mas no la divulgación de los datos de la institución caso contrario si el alto mando de dicha institución lo autoriza para que la información sea de conocimiento público.

La base para que cualquier organización pueda operar de una forma confiable en materia de seguridad informática comienza con la definición de políticas basadas en las buenas prácticas y adecuados estándares internacionales. Los usuarios de la UPSE se encuentran estructurado en 4 grupos de políticas de seguridad, que están alineadas con el Estándar Británico ISO/IEC:27002, plantillas del SysAdmin Audit, Networking and Security Institute (SANS) y Open Web Application Security Project (OWASP).

Los cuatros grupos de política de seguridad son:

- General
- Seguridad de la Red
- Seguridad de la Infraestructura Tecnológica
- Seguridad de la Aplicación

Para el desarrollo del sistema web se utilizará las siguientes herramientas:

- **Joomla:** “es un sistema de administración de contenido (CMS) de código abierto para publicar contenido web, se basa en un marco de aplicación web modelo-vista-controlador que le permite crear aplicaciones en línea potentes”
- **XAMPP:** es un paquete de software libre, que consiste principalmente en el sistema de gestión de bases de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script PHP y Perl.
- **Visual Paradigm:** “Herramienta de diagrama de caso de uso UML
- **Request tracker:** “es un sistema de seguimiento de tickets (Help Desk) escrito en Perl que se utiliza para coordinar tareas y administrar solicitudes entre una comunidad de usuarios”

1.3 OBJETIVO DEL PROYECTO

1.3.1 Objetivo general

Implementar un plan de respuestas a incidencias de seguridad informática aplicando estándares y buenas prácticas definidas, para reducir los riesgos informáticos del departamento de TIC de la Universidad Estatal Península de Santa Elena.

1.3.2 Objetivos específicos

- Desarrollar un prototipo de una plataforma web con el uso de herramientas OpenSource para reportar las incidencias identificadas por la comunidad universitaria.
- Reducir el tiempo de notificación de incidencias informáticas reportadas, para establecer acciones a realizar que ayuden a la solución de las mismas.
- Aplicar el plan de incidencias para problemas de seguridad informática reportadas.
- Obtener reportes de los resultados obtenidos de incidencias de seguridad informáticas resueltos.

1.4 JUSTIFICACIÓN

Un plan de respuesta a incidencias puede proporcionar una base sólida para futuros esfuerzos de seguridad, puede ayudar a mitigar el impacto de las amenazas de

seguridad. A medida que las amenazas cibernéticas crecen en número y sofisticación, es una realidad necesaria en cualquier organización [13].

La falta de un plan de respuesta a incidencias puede conducir a tiempos de recuperación más largos y a un mayor costo. El trabajo diario de los usuarios de una organización está vinculado directamente al uso de las tecnologías en los cuales se exponen a ciertos tipos de ataques comunes que son virus, troyanos y amenazas de mayor nivel como los ransomware y rootkits que inutilizar los sistemas informáticos de una entidad, mismas amenazas que pueden llegar a extraer y borrar archivos confidenciales.

El departamento de TIC actualmente se encarga del área de infraestructura de red, soporte técnico y las incidencias informáticas los mismos que son atendidos cuando alguien los reporta, pero no existe registros estadísticos, hay reglas que tienen que ser conocidas y aplicadas en cada grupo, pero estas no son aplicadas por el personal, no cuentan un área formal para llevar a cabo el estudio de incidencias y el rastreo de los mismos.

La implementación del plan de respuesta tiene como propósito de dar inicio a estudios e investigaciones sobre delitos informáticos que ocurrirán y luego se archivaran, los cuales no han podido ser tramitados por falta de un registro histórico. El CSIRT-UPSE va a realizar la mayor parte de las acciones en respuesta a un hecho, lo más importante es que el plan sea fácil de encontrar durante el pánico de una crisis potencial y fácil de entender.

Como parte de la herramienta se optó por la creación de una aplicación web debido que la UPSE actualmente no cuenta con un sistema que permita la comunicación de reportar incidencias entre usuarios y el personal de TIC, se podrían iniciar actividades de detección, prevención y seguimiento a actos delictivos informáticos para la preservación de las herramientas tecnológicas que posee la universidad, por lo tanto, establecer esta tecnología es parte del plan de respuesta a incidencias de seguridad informática (IRP).

El tema propuesto está alineado a los objetivos del Plan Nacional de Desarrollo "Toda una Vida" y también contribuye de esta manera a la línea de investigación de Desarrollo de Software planificadas por la Facultad de Sistemas y Telecomunicaciones "arquitectura de redes, routing, ingeniería de tráfico, tratamiento de información, tecnologías de comunicación, análisis de señales, algoritmos de cifrado".

Eje 3: Más sociedad, mejor Estado

Objetivo 7: Incentivar una sociedad participativa, con un Estado cercano al servicio de la ciudadanía.

Política 7.3

Fomentar y fortalecer la auto-organización social, la vida asociativa y la construcción de una ciudadanía activa y corresponsable, que valore y promueva el bien común [14].

Política 7.9

Promover la seguridad jurídica y la defensa técnica del Estado [14].

Objetivo 9: Garantizar la soberanía y la paz, y posicionar estratégicamente al país en la región y el mundo.

Política 9.1

Promover la paz sostenible y garantizar servicios eficientes de seguridad integral [14].

Política 9.3

Crear y fortalecer los vínculos políticos, sociales, económicos, turísticos, ambientales, académicos y culturales, y las líneas de cooperación para la investigación, innovación y transferencia tecnológica con socios estratégicos de Ecuador [14].

1.5 ALCANCE DEL PROYECTO

La propuesta está enfocada en la creación del IRP para el CSIRT-UPSE que el departamento de TIC está elaborando, uno de sus elementos menciona el desarrollo o utilización de una herramienta, en este caso se desarrollará el prototipo de una

página web para el CSIRT-UPSE y el área de pruebas donde se dará los respectivos testeos de la herramienta tecnológica que llevará a cabo en la facultad de sistemas y telecomunicaciones.

Los módulos que se desarrollará para la implementación del prototipo son:

- Alerta y avisos: En esta sección de la página web se encontrará todo lo relacionado a seguridad informática que promueve la buena práctica hacia los usuarios, también información actualizada de los hechos ocurridos de incidencias informáticas detectadas para tener la debida precaución a futuro.
- Manejo de incidencias: Todo acontecimiento informado a CSIRT va a ser ingresado y registrado en el sistema de administración de incidencias de seguridad informáticos (Request Tracker) como: visus, malware y acceso no autorizado a infraestructura. Más adelante se sigue un desarrollo de parte de técnicos expertos para saber la validez del acontecimiento informado, saber el nivel de amenaza que puede representar este en los sistemas afectados definiéndose además un nivel de prioridad para la atención de este hecho.

Al terminar cada evaluación, se envía un archivo al contacto designado de la institución con el resultado de esta revisión, con la intención de que conozcan el estado y las recomendaciones a tomar para que mejoren el servicio o corrijan algún inconveniente que se ha suscitado. El propósito de este sistema es crear un ambiente seguro para ubicar inconvenientes que pudieran existir en la institución y esas incidencias informáticas logren ser por consiguiente corregidos.

1.6 METODOLOGÍA

Para esta iniciativa se incluirá metodologías de la investigación que contienen una sucesión de técnicas o procesos a continuar para la ejecución de un estudio científico, realizar búsquedas bibliográficas, con el propósito de investigar la implementación de un CSIRT en la provincia de Santa Elena, de los cuales no se consiguió información. Con toda prueba circunstancial manifiesta por hecho que

esta iniciativa se utilizará una investigación exploratoria al no existir un estudio antes de la implementación de un CSIRT en la UPSE.

Se utilizará la metodología de investigación diagnóstica con el objetivo de conocer los procesos dentro de la organización, será esencial para hallar requerimientos de información y abarcar la situación actual en lo relacionado a seguridad informática en la universidad.

Población

- Personal de TICS de la UPSE
- Personal académico y administrativo de la UPSE
- Estudiantes de la facultad de sistemas y telecomunicaciones de la UPSE

Recolección de información

Las técnicas son los procedimientos e instrumentos que utilizamos para acceder al conocimiento. Encuestas, entrevistas, observaciones y todo lo que se deriva de ellas [15]. La técnica de recolección de datos a utilizar será las encuestas (Ver Anexo 1).

1.6.1 Variables -Hipótesis

- Tiempo en que se demora al percatarse en la aparición de una incidencia informático presente.
- Tiempo de respuesta para la ejecución de una posible solución ante la incidencia informático que se manifestó.

1.6.2 Resultados de encuestas

Pregunta 1: Tiene conocimiento básico de buenas prácticas de seguridad informática?

Respuesta	Frecuencia	Porcentaje
Si	83	59,43 %
No	57	40,71 %
TOTAL	140	100 %

Tabla 1: Conocimientos básicos de buenas prácticas de seguridad informática

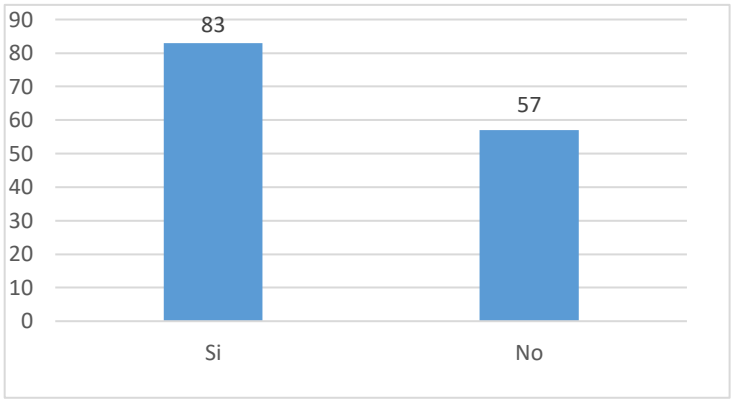


Figura 2: ***Conocimientos básicos de buenas prácticas de seguridad informática***

Análisis

Según la información recolectada un 59,43% tienen conocimientos básicos de seguridad informática mientras que el 40,71% no cuentan con conocimientos básicos sobro seguridad informática.

En base a esta encuesta realizado a una muestra de la población podemos observar que la mayoría si tiene conocimientos y analizando los porcentajes se concluye que se necesita tener un medio de información para brindar ayuda de buenas prácticas de seguridad informática.

Pregunta 2: Seleccione que equipos informáticos es el que más utiliza dentro de la facultad de sistemas y telecomunicaciones.

Respuesta	Frecuencia	Porcentaje
Equipos informáticos de los laboratorios de la facultad	15	10,71%
Equipos informáticos personales	16	11,43%
Ambos	109	77,86%
TOTAL	140	100%

Tabla 2: Equipos informáticos más utilizados

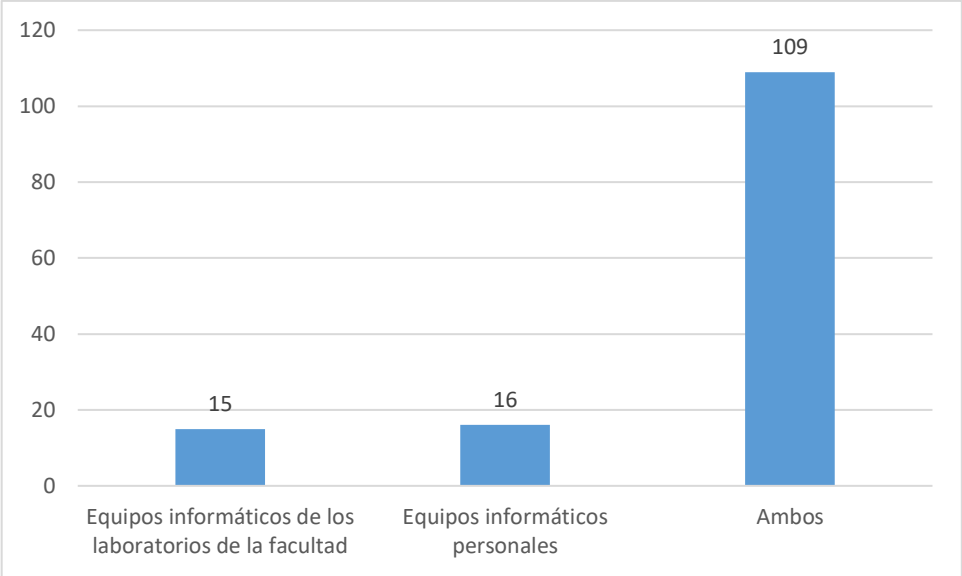


Figura 3: Equipos informáticos más utilizados

Análisis

La información recolectada muestra que el 77,86% de los usuarios utilizan sus equipos informáticos personales y también los equipos del laboratorio de la facultad.

Se puede deducir que tanto los equipos informáticos de los laboratorios y los equipos personales de los usuarios están propenso a sufrir alguna incidencia informática.

Pregunta 3: ¿Has sufrido incidencias informáticas en los laboratorios de la facultad o en sus equipos informáticos?

Respuesta	Frecuencia	Porcentaje
Si	83	66,43 %
No	47	33,57 %
TOTAL	140	100 %

Tabla 3: Incidencias informáticas en los laboratorios o equipos informáticos de los usuarios

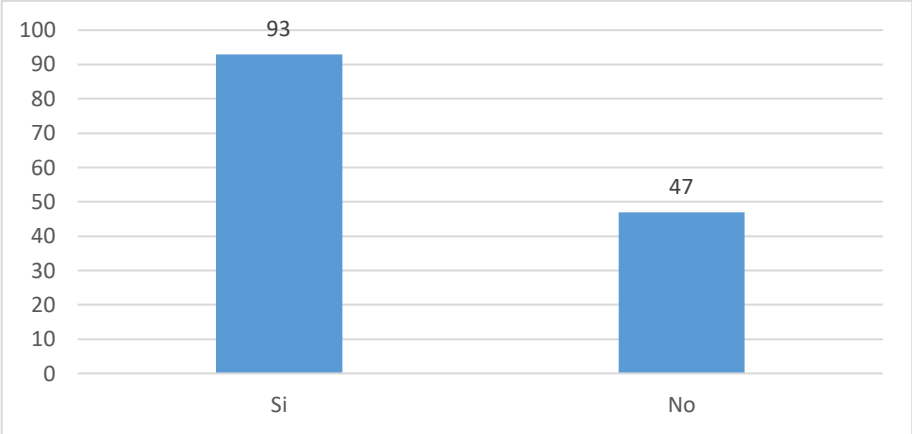


Figura 4: Incidencias informáticas en los laboratorios o equipos informáticos de los usuarios

Análisis

Un 66,43% de los usuarios manifiestan que han sufrido una incidencia informática dentro de la facultad.

En base a la encuesta realizada existieron incidencias informáticas y debido a ciertos factores esas incidencias no fueron registrados o alertados por parte de los usuarios.

Pregunta 4: ¿Qué medio usa actualmente para comunicarse con el área de servicios TIC cuando necesita ayuda ante una situación de incidencia informática?

Respuesta	Frecuencia	Porcentaje
Correo electrónico	22	15,71 %
Teléfono	4	2,86 %
Herramienta especializada de gestión de incidencias	0	0,00 %
De manera personal	114	81,43 %
TOTAL	140	100 %

Tabla 4: Medios para comunicar incidencias informáticas

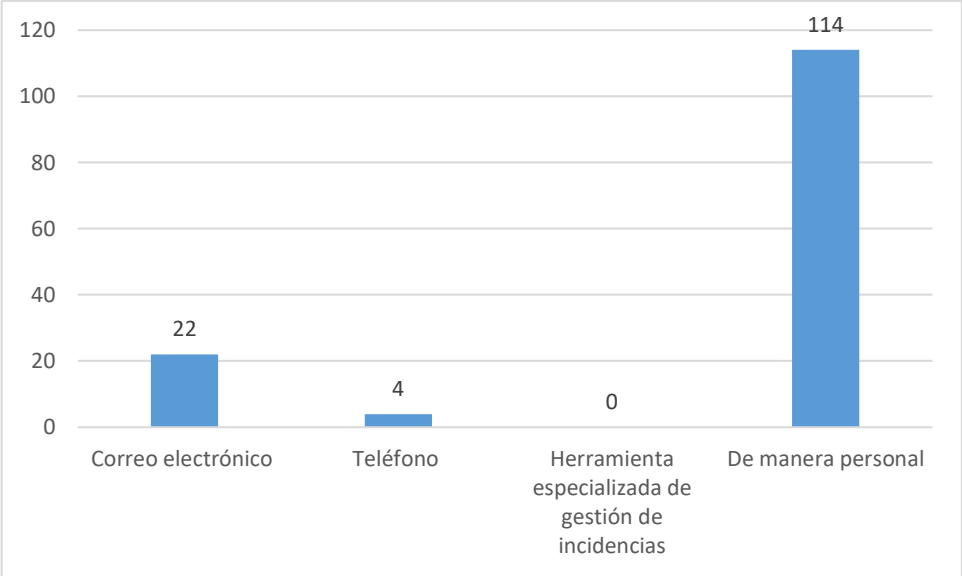


Figura 5: Medios para comunicar incidencias informáticas

Análisis

La información recolectada muestra que un 81,43% de los encuestados manifiestan que para informar una incidencia informática lo hacen de manera personal siendo este el medio más utilizado, a continuación, con un 15,71% los usuarios utilizan el correo electrónico, le sigue por vía telefónica un 2,86% y finalmente un 0% de los usuarios no utilizan una herramienta especializada de gestión de incidencias.

El análisis conlleva que la implementación del Request Tracker ayudaría al momento de reportar una incidencia informática para reducir el tiempo que podría tardarse al momento de utilizar otras vías de comunicación

Pregunta 5: A partir de que usted comunica su incidencia, ¿cuánto tiempo transcurre hasta que el servicio técnico lo contacta?

Respuesta	Frecuencia	Porcentaje
De 0 a 30 minutos	19	13,57 %
De 31 a 60 minutos	32	22,86 %
De 1 a 2 horas	43	30,71 %
Más de 2 horas	46	32,86 %
TOTAL	140	100 %

Tabla 5: Tiempo que transcurre para que la incidencia reportada sea detectada

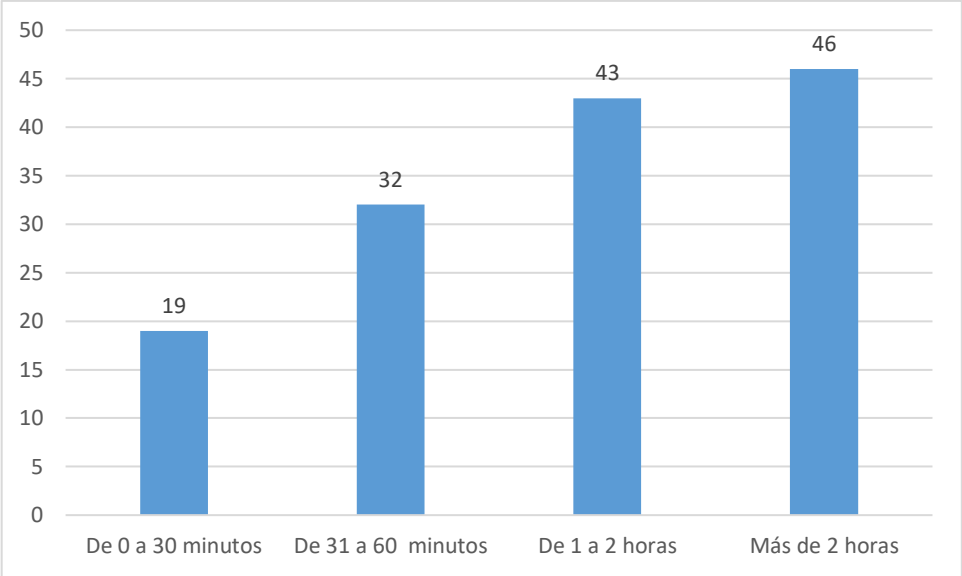


Figura 6: Tiempo que transcurre para que la incidencia reportada sea detectada

Análisis

El 32,86% de los encuestados manifiestan que se tarda más de 2 horas hasta que un personal de Tics atienda su comunicado.

Debido que el personal de tics cumple con diferentes roles no cuenta con un equipo enfocado para las incidencias de seguridad informática.

Pregunta 6: ¿Cuánto tiempo toma al departamento de TIC en atender sus requerimientos?

Respuesta	Frecuencia	Porcentaje
30 minutos	13	9,29 %
1 hora	28	20 %
2 horas	79	56,43 %
Más de 2 horas	20	14,29 %
TOTAL	140	100 %

Tabla 6: Tiempo que transcurre para atender los requerimientos

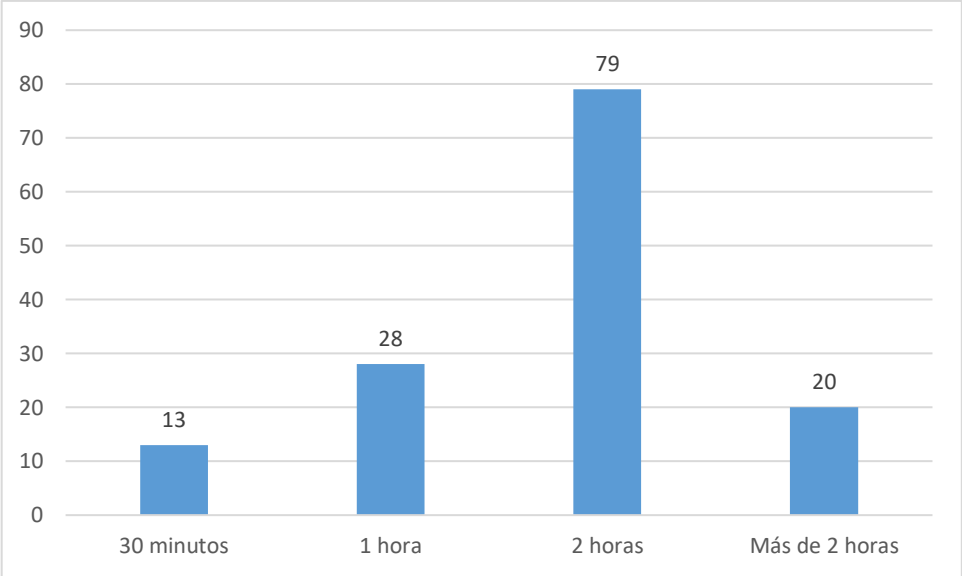


Figura 7: Tiempo que transcurre para atender los requerimientos

Análisis

Un 56,43% de los usuarios encuestados manifiestan que tardan en dar solución un aproximado de 2 horas dependiendo que tan grave sea la situación.

Con la implementación del sistema Request Tracker junto con el plan de contingencia ese tiempo puede reducirse sin tomar en cuenta los factores de (conocimiento y complejidad) debido que podrán acceder a un historial de incidencias y buscar las soluciones de manera más rápida.

Pregunta 7: ¿Estaría de acuerdo en utilizar una plataforma web para solicitar ayuda ante un personal capacitado si esto implica una mejora en el tiempo de atención y satisfacción en una situación de incidencia informático?

Respuesta	Frecuencia	Porcentaje
Si	138	98,57 %
No	2	1,43 %
TOTAL	140	100 %

Tabla 7: Usuarios dispuesto a utilizar la plataforma web

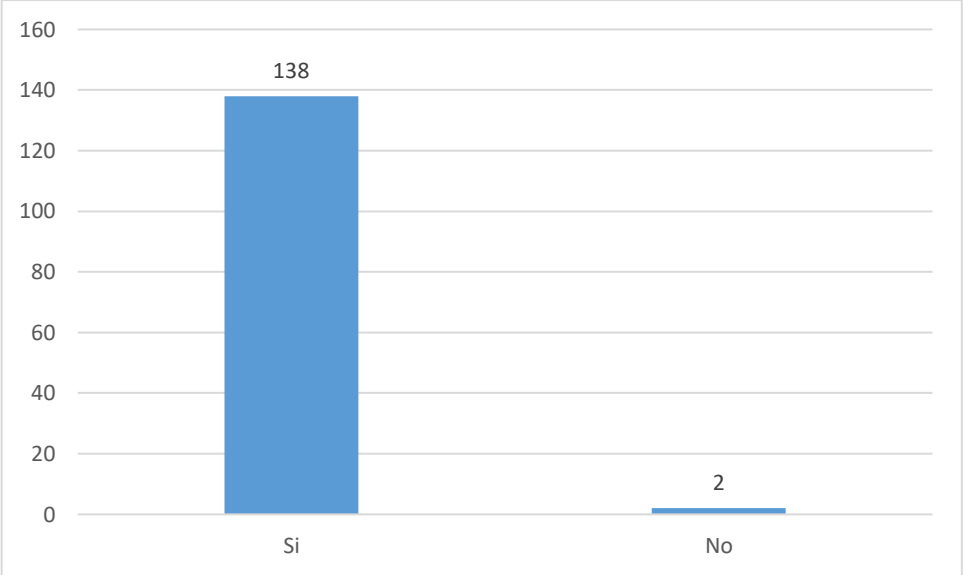


Figura 8: Usuarios dispuesto a utilizar la plataforma web

Análisis

El 98,57% de los encuestados manifiestan que estarían dispuesto a usar una plataforma web.

Cómo se puede observar la mayoría de las personas encuestadas están de acuerdo con la implementación de la plataforma web junto con el aplicativo web Request Tracker)

1.6.3 Metodología de prueba de intrusión en la NIST SP 800-115

Para determinar la eficacia de los procesos del IRP es evaluar frente a objetivos específicos de seguridad. La Guía Técnica para Evaluaciones y Pruebas de Seguridad de la Información NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment), simulan ataques del mundo real en un intento de identificar modos de evadir las características de seguridad de una aplicación, sistema o red de datos [16].

Se lo divide en cuatro fases que son:

Fase de planificación

Se identifican las reglas que deben seguirse durante la prueba de intrusión y objetivos a alcanzar. En esta fase no se realiza ningún tipo de prueba de seguridad.

Fase de descubrimiento

Se realiza el descubrimiento de vulnerabilidades a partir de la información recopilada de servicios, base tecnológica y otras informaciones que permitan realizar búsquedas en bases de datos de vulnerabilidades.

Fase de ejecución

Fase principal del proceso en donde se realiza la comprobación de las vulnerabilidades previamente descubierto. Si un ataque es exitoso, debe aislarse y documentarse cuidadosamente la vulnerabilidad y proponerse medidas para mitigarla

Fase de documentación y reportes

Se desarrolla en paralelo con el resto de las fases del siguiente modo:

- En la fase de planificación se documenta el plan de evaluación o las reglas de interacción.
- En la fase de descubrimiento se almacenan los reportes generados por los escaneadores de vulnerabilidades e informaciones útiles obtenidas a través de otros medios.
- En la fase de ejecución se almacenan los reportes generados por las herramientas de explotación de vulnerabilidades.

Al concluir la prueba de intrusión, se genera un reporte con la descripción de las vulnerabilidades encontradas, presenta una puntuación de riesgos y brinda una guía sobre como mitigar las debilidades descubiertas.

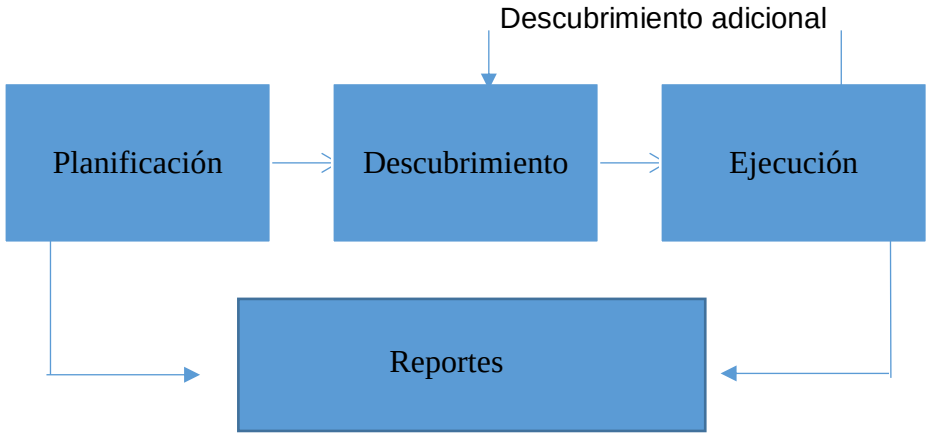


Figura 9: Pasos de la metodología prueba de intrusión NIST SP 800-115

Metodología de Desarrollo del Software

El desarrollo de un programa conlleva un conjunto de actividades y resultados asociados que generan un producto de software, existen modelos de desarrollo que representa un proceso desde una visión particular y de esta forma brindan a los desarrolladores una guía sobre ese proceso para organizar la ejecución de dichas actividades [17].

Para el desarrollo de este proyecto se utilizará el modelo incremental debido que se puede presentar cambios durante la realización del software [18], este modelo permite adaptarse a las necesidades de la universidad que siempre está en proceso de mejoras.

Cada iteración tiene cuatro fases: análisis, diseño, implementación y prueba. Al finalizar una iteración se evaluará y corregirá errores en caso de tener para cumplir con las necesidades de la institución, llegando al punto de finalizar todas las iteraciones por ende concluyendo con el software.

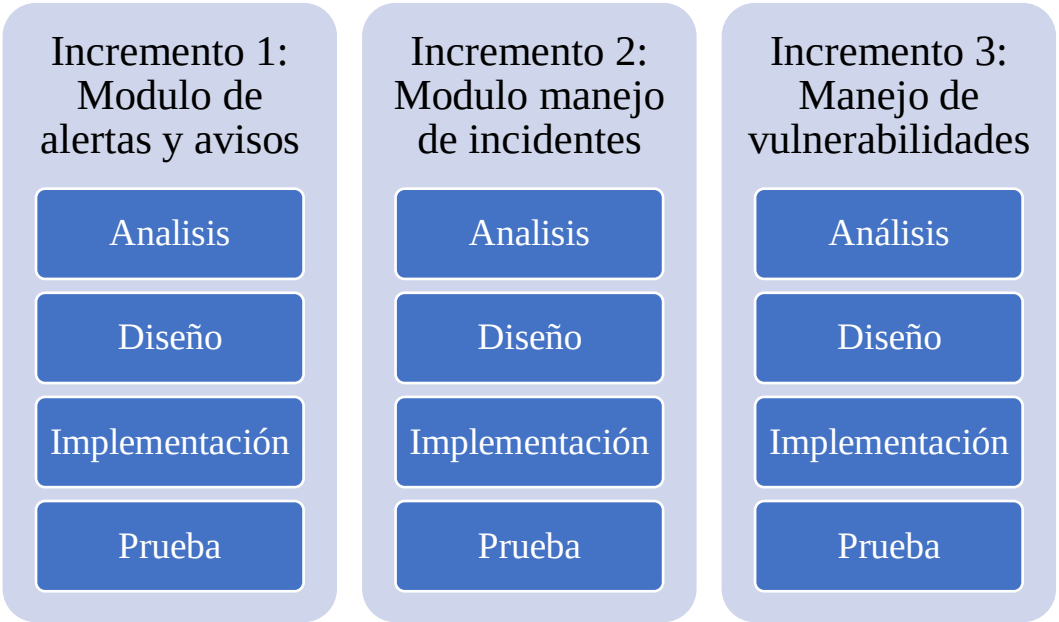


Figura 10: Fases modelo incremental

1.7 RESULTADOS ESPERADOS

Resultados que se espera lograr

- Realizar pruebas de funcionalidad a la herramienta implementada de tal forma que contribuya y se ajuste a los requerimientos de la organización.
- Reducir el tiempo que conlleva el proceso de notificación de una incidencia informática.
- Estandarizar las respuestas efectivas a las incidencias de seguridad informáticas para que el daño causado por estos sea mínimo.
- Reportes estadísticos donde contenga datos relevantes como el tipo de incidencias de seguridad informática registrado, nivel de criticidad y el tiempo estimado de solución para futuros usos.

CAPITULO II

LA PROPUESTA

2.1 MARCO CONTEXTUAL

La Universidad Estatal Península de Santa Elena, se encuentra ubicada en la Avda. principal La Libertad - Santa Elena, cantón La Libertad provincia de Santa Elena, a una latitud sur 2° 13′ 59.63″ y latitud oeste 80° 52′ 40.45″. Las pruebas se llevarán a cabo en la facultad de sistemas y telecomunicaciones.

Figura 11: Ubicación UPSE matriz

2.2 MARCO CONCEPTUAL

2.2.1 Consecuencia de la falta de seguridad informática

La seguridad informática radica en asegurar que los recursos del sistema de información (material informático o programas) de la organización se utilicen de una manera determinada, y que el acceso y modificación de la información contenida en él solo sea válido para usuarios de confianza y autorizado [19].

La gran importancia que se debería otorgar a todos los aspectos relacionado con la seguridad informática en una organización. La expansión de los virus y códigos maliciosos y su rápida distribución, así como los miles de ataques de incidencias de seguridad informática que ocurren cada año, han generado mucha atención en este tema [19].

Es necesario tener en cuenta otras características o cuestiones relacionados cuando se habla de seguridad informática [19]:

- Cumplimiento de las regulaciones legales aplicables a cada sector o tipo de organización, dependiendo del marco legal de cada país.
- Control en el acceso a los servicios brindados y la información guardada por un sistema informático.
- Control en el acceso y utilización de archivos protegidos por la ley: contenido digital con derechos de autor, archivos con datos de carácter personal, etc.
- Identificación de los autores de la información o de los mensajes.
- Registro del uso de los servicios de un sistema informático, etc.

Las consecuencias de una mala seguridad informática los riesgos varían de acuerdo a la naturaleza de la organización, aunque los más usuales son los que a ahora se indican [19]:

- Robo de información confidencial y su posible revelación a terceros no autorizados.
- Filtración de datos personales de usuarios registrados en el sistema: empleados, clientes, proveedores.
- Posible impacto en la imagen de la empresa ante terceros: pérdida de credibilidad, daño a la reputación de la empresa, pérdida de confianza.
- Pago de indemnizaciones por daños y perjuicios a terceros, teniendo que enfrentar posibles acciones legales y la imposición de sanciones administrativas.

La información dispersa, con el creciente uso de PC, la información tiende a almacenarse en los discos duros locales de cada estación de trabajo creando en ocasiones inconvenientes de redundancia e inconsistencia: estos consisten en que una misma información que debiera tener el mismo valor, está almacenada en dos o más sitios con diferentes valores. La dispersión es una amenaza solo cuando está asociada a otros inconvenientes como la inconsistencia o fallas de seguridad en las estaciones de trabajo. Robos y copias no autorizadas, adulteración, revelación de secretos, sabotaje, vandalismo, etc. Estas amenazas se enfrentan con dos clases de

política: restricción de acceso y asignación estricta de responsabilidades. Perdidas de información por efecto de virus o monitoreo remoto con troyanos. Fallas técnicas del disco, cortes de suministro eléctrico, operación indebida, recalentamiento, desastres naturales, incendios, inundaciones, etc. Para estas amenazas se usan las políticas usuales de seguridad industrial [19].

2.2.2 Seguridad de la información

La seguridad de la información se usa para asegurar los datos que tiene, maneja y dispone una determinada organización. Los términos seguridad de la información, seguridad informática y garantía de la información son usados con bastante frecuencia. El concepto de dichas palabras es diferente, pero todos persiguen la misma finalidad que es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización. Entre dichos términos existen pequeñas diferencias, estas diferencias proceden del enfoque que le dé, las metodologías usadas y las zonas de concentración. La definición de la norma ISO/IEC 27001 menciona la seguridad de la información como la preservación de su confidencialidad, su integridad y su disponibilidad, en relación del tipo de información manejada y de los procesos realizados por una organización [20] estos pueden ser:

- **Confidencialidad**: Cada dato transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario.
- **Integridad**: Los datos se mantienen intactos libre de modificaciones o alteraciones de terceros. Únicamente los usuarios autorizados deben ser capaces de alterar los datos cuando sea necesario.
- **Disponibilidad**: Pilar esencial de la seguridad de la información se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de modo que pueda estar constantemente a disposición de los usuarios que deseen acceder a sus servicios o información.

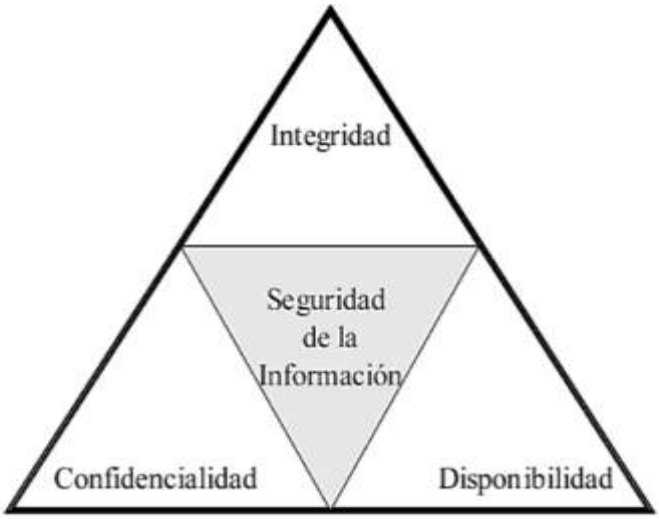


Figura 12: Seguridad de la Información según la norma ISO/IEC 27001

2.2.3 Aplicación web

En la Ingeniería de software se denomina aplicación web a aquellas aplicaciones que los usuarios pueden utilizar accediendo a un Servidor web a través de Internet o de una intranet mediante un navegador. En otras palabras, es una aplicación (Software) que se codifica en un lenguaje soportado por los navegadores web en la que se confía la ejecución al navegador.

Es esencial indicar que una Página Web puede contener elementos que permiten una comunicación activa entre el usuario y la información. Esto permite que el usuario acceda a los datos de modo interactivo, gracias a que la página responderá a cada una de sus acciones [21].

2.2.3.1 Consideraciones técnicas

Una ventaja significativa es que las aplicaciones web deberían trabajar igual independientemente de la versión del sistema operativo instalado en el cliente. En vez de elaborar clientes para Windows, Mac OS X, GNU/Linux y otros sistemas operativos, la aplicación web se escribe una vez y se ejecuta igual en todas partes. Sin embargo, hay aplicaciones inconsistentes escritas con HTML, CSS, DOM y otras especificaciones estándar para navegadores web que pueden ocasionar problemas en el desarrollo y soporte de estas aplicaciones, principalmente debido a la carencia de adicción de los navegadores a dichos estándares web (principalmente

versiones de Internet Explorer anteriores a la 7.0). Adicionalmente, la posibilidad de los usuarios de personalizar muchas de las características de la interfaz (tamaño y color de fuentes, tipos de fuentes, inhabilitar Javascript) puede interferir con la consistencia de la aplicación web [21].

2.2.3.2 Estructura de las aplicaciones web

Si bien existen muchas variaciones posibles, una aplicación web está normalmente estructurada como una aplicación de tres-capas. En su forma más frecuente, el navegador web ofrece la primera capa y un motor capaz de utilizar alguna tecnología web dinámica (ejemplos: PHP, Java Servlets o ASP, ASP.NET, CGI, ColdFusion, EmbPerl, Python (lenguaje de programación) o Ruby) constituye la capa de en medio. Por último, una base de datos constituye la tercera y última capa. El navegador web manda peticiones a la capa de en medio que ofrece servicios valiéndose de consultas y actualizaciones a la base de datos y a su vez proporciona una interfaz de usuario [21].

2.2.3.3 Lenguaje de programación

Existen numerosos lenguajes de programación utilizados para el desarrollo de aplicaciones web en el servidor, entre los que destacan:

- PHP
- Java, con sus tecnologías Java Servlets y JavaServer Pages (JSP)
- Javascript
- Perl
- Ruby
- Python
- HTML
- XML
- ASP/ASP.NET, aunque no es un lenguaje de programación en sí mismo, sino una arquitectura de desarrollo web en la que se pueden usar por debajo distintos lenguajes (por ejemplo VB.NET o C# para ASP.NET o VBScript/JScript para ASP).

Se utilizan para servir los datos adecuados a las necesidades del usuario, en función de cómo hayan sido definidos por el dueño de la aplicación. Los datos se almacenan en alguna base de datos estándar [21].

2.2.4 NIST SP 800-115

La NIST SP 800-115 concibe las pruebas de intrusión como un paquete de pruebas de seguridad que se realizan utilizando los mismos métodos y herramientas que emplean los atacantes reales. Se emplean para verificar las vulnerabilidades descubiertas en fases anteriores y sirven para demostrar como las vulnerabilidades pueden ser explotadas iterativamente para ganar privilegios de accesos al sistema [16].

Su concepción de la Evaluación de Seguridad de la Información gestionada mediante un proyecto estándar y la redacción de un documento conteniendo las Reglas de Interacción, lo convierten en referente para la construcción del proceso de gestión de las Prueba de Intrusión. Por otra parte, se evidencian limitantes que impiden que pueda ser tomado como base para la ejecución de pruebas de seguridad concretas en aplicaciones informáticas en sentido general y en aplicaciones web de manera específica [16].

2.2.5 Norma RFC 2350

Describe los de servicios de un CSIRT de acuerdo al RFC 2350 (Request for Comments desarrollados por la comunidad IETF: Internet Engineering Task Force, utilizados comúnmente como estándares de referencia en la industria) [22].

1. Información del Documento
   1.1.Fecha de la última actualización
   1.2.Listas de Distribución
   1.3.Ubicación del Documento
   1.4.Autenticación del Documento
2. Información de Contacto
   2.1.Nombre del Equipo
   2.2.Dirección
   2.3.Zona Horaria
   2.4.Número de Teléfono
   2.5.Número de Fax
   2.6.Otras Comunicaciones

2.7.Dirección de Correo Electrónico

2.8.Llaves Públicas y encriptación de información

2.9.Miembros del Equipo

2.10.Más Información

2.11.Horario de Atención

2.12.Puntos de contacto para clientes

3. Constitución

3.1. Misión

3.2. Comunidad a la que brinda Servicios

3.3. Patrocinio / Afiliación

3.4.Autoridad

4. Políticas

4.1. Tipo de Incidentes y nivel de Soporte

4.2. Cooperación, Interacción y divulgación de la Información

4.3. Comunicación y Autenticación

5. Servicios

5.1. Respuesta a Incidentes

5.1.1. Investigación de Incidentes

5.1.2. Coordinación del Incidente

5.1.3. Resolución del Incidente

5.2. Actividades Proactivas

5.3. Servicios de Gestión y Calidad de la Seguridad

6. Formas de notificación de incidentes

7. Disclaimer

(Ver Anexo 2) para información más detallada del CSIRT-UPSE

2.2.6 CSIRT

El CSIRT está conformado por un grupo de expertos causantes de evitar, rastrear y actuar ante un problema de seguridad informática. El equipo de respuesta proporciona los servicios fundamentales para realizar la mitigación ante incidencias asociados a los sistemas de información, actuar de manera rápida y eficaz cuando se presentan riesgos. En cierto sentido, aparte de fortalecer y proteger la seguridad de la organización, también realizan planes y búsquedas de técnicas para recuperase de incidencias o vulnerabilidades encontradas. [1].

Los principales objetivos de un CSIRT son [1]:

- Definir las políticas, procedimientos y servicios de respuesta a incidentes proporcionados.
- Manejar adecuadamente la capacidad de informar sobre los incidentes detectados.
- Manejar el incidente (Identificarlo, contenerlo y erradicarlo).
- Recuperarse del incidente (Determinar la causa, reparar el daño y restaurar el sistema). Investigar el incidente (Identificar la causa, recolectar evidencia y asignar la culpa).
- Ayudar en la prevención de una repetición del incidente.

2.2.7 Plan de respuesta a incidencias de seguridad informática IRP

Podríamos definir a un plan de contingencias como una estrategia planificada con una sucesión de métodos que facilitan u orienten a tener una solución alternativa que permitan restituir de una manera rápida los servicios de la organización frente a eventualidades que lo puedan paralizar, así sea de manera parcial o total. El plan de contingencia es una herramienta que ayudará a que los procesos críticos de una empresa u organización sigan funcionando a pesar de una posible falla en los sistemas computarizados. Es decir, un plan que facilita a su negocio u organización, continuar operando, aunque sea al mínimo [23].

2.2.8 Sistema web para registro de incidencias de seguridad informática

El mecanismo prioritario de esta clase de sistema informático es de controlar y gestionar los requerimientos e incidencias solicitados por los usuarios hasta que se dé la solución y dar el cierre del mismo. Las peticiones son almacenadas con sus datos personales y técnicos del requerimiento, cuando el usuario envía la solicitud de servicio y esto también crea un ticket de soporte (número de identificación de la solicitud) para que lo atiendo un profesional o el administrador encargado de dar la atención y dar la respuesta a éste hasta la solución del requerimiento solicitado [24].

A continuación, se detallan los beneficios de un sistema [24]:

- Panel Administración de solicitudes
- Verificar estado de tickets: abiertos, cerrados, pendiente.
- Configuración de accesos por roles o grupos.
- Envió de notificaciones a los usuarios de sus tickets.
- Reportes que ayuden al comprobar la cantidad de solicitudes atendidas al día o en un periodo de tiempo.

2.3 MARCO TEÓRICO

Para el avance de este proyecto se consultaron casos semejantes al objeto de estudio con la finalidad de contribuir a la comprensión del tema planteado. A continuación, se detallan los casos encontrados.

2.3.1 Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la universidad de las fuerzas armadas ESPE.

De La Torre Moscoso, Hubo Marcelo Parra Rosero, Mario Andrés en su trabajo de titulación escribieron acerca de la importancia de los CSIRT académicos concluyendo que, debido al desarrollo tecnológico constante en las actividades de la sociedad, resulta primordial asegurar el uso adecuado de los sistemas de información y garantizar su seguridad mediante la implementación de mecanismos adecuados.

La implementación de un CSIRT académico y robusto requiere de una alta inversión que resulta difícil debido a la infraestructura y equipamiento necesario para su operación. Sin embargo, plantear una solución inicial que reutilice componentes, herramientas y personal que ya posee la Universidad conjuntamente con una solución futura se obtendrían resultados positivos [1].

2.3.2 Diseño de un plan estratégico de continuidad de servicios universitarios en casos excepcionales para la PUCE sede Ambato.

Diego Fernando Caicedo Núñez menciona que toda entidad es susceptible de vivir un desastre sea este de alto, mediano o bajo impacto. Ya sea desastres naturales como: inundaciones, terremotos, entre otros y desastres producidos por los humanos (antrópicos) como ataques cibernéticos o sabotajes. Estos incidentes son impredecibles, pero una correcta prevención permitirá responder de mejor manera antes las diferentes amenazas existentes en el entorno [25].

La disminución del tiempo de respuesta, la reducción en la toma de decisiones, minimización de pérdidas económicas y la eliminación de la confusión son claros ejemplos de resultados que se obtendrían gracias a una planificación [25].

2.3.3 Implementación de un sistema Help Desk en Linux para gestionar incidentes informáticos para la nube interna de la carrera de ingeniería en sistemas computacionales

Luis Humberto Pilay Sánchez expresa que la herramienta de soporte administrativo ayuda a atender los requerimientos de servicios reportados por los usuarios, de manera que el sistema facilite a la organización la reducción de la carga operativa y mejorar significativamente la satisfacción del cliente, dando una solución inmediata y eficiente [24].

Un sistema Help Desk, permitiría a los estudiantes solicitar la resolución de un problema a través de la generación de un ticket, el cual será registrado y atendido por el personal asignado para dicha función, hasta el cierre del ticket [24].

El sistema Help Desk que utilizaremos será el Request Tracker que será la aplicación web para realizar las pruebas de registro de incidencias informáticas (Ver Anexo 3).

2.4 PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICAS

Se pretende establecer un plan de respuesta a incidentes informáticos que contribuya con los elementos necesarios para identificar, controlar y registrar de modo acertada los posibles incidentes, permitiendo su posterior estudio con el fin de prevenir posibles ataques que puedan complicar a la seguridad de los sistemas informáticos.

2.4.1 Constitución del equipo de respuesta a incidentes

El Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) deberá estar constituido por las personas que cuentan con la experiencia y la formación que se requiere para poder actuar frente las incidencias y desastres que tengan la posibilidad de perjudicar a la seguridad informática de la organización. Es muy importante que se considere al equipo de respuesta a incidentes como un integrante importante dentro del plan de respuesta, debe ejercer como parte del conocimiento profesional [26]:

- Definir los procedimientos para la atención de incidentes.
- Definir la categorización de incidentes.
- Atender incidencias de seguridad: Recibir y resolver incidencias de seguridad según métodos establecidos.
- Recopilar y analizar evidencia digital: guardar, registrar y analizar evidencias cuando sea necesario.
- Realizar notificaciones de seguridad: Deben estar informados sobre nuevas vulnerabilidades, actualizaciones de plataforma y recomendaciones de seguridad informática a través de
- determinados métodos de comunicación.

- Realizar auditorías de seguridad de TI y trazabilidad: el equipo debe verificar periódicamente el estado de las plataformas para analizar nuevas
- vulnerabilidades de seguridad.
- Validación del producto: El equipo verifica la implementación de la nueva aplicación en producción para cumplir con los requisitos de seguridad informática establecidos.
- Configurar y gestionar dispositivos de seguridad informática: serán los responsables de la correcta gestión de los elementos de seguridad informática.
- Clasifique y priorizar los servicios: identificar servicios sensibles y aplicaciones para prevenir o remediar ataques.
- Investigar o desarrollar nuevas herramientas: el equipo debe buscar frecuentemente nuevos productos en el mercado o desarrollar nuevas herramientas de protección para hacer frente a las vulnerabilidades de seguridad y proponer nuevos proyectos de seguridad de la información.

El (Anexo 4) muestra a los actores con su perfil y cuál es el proceso que realiza cada uno en el plan de respuesta a incidentes de seguridad de la información.

Usuario Sensibilizado: Usuario externo con acceso a la infraestructura que se debe de estar pendiente de las pautas de seguridad que se han implementado en la entidad, estos usuarios suelen informan de las incidencias informáticas que se presenten.

Agente primer punto de contacto: Encargado de tomar las peticiones de parte de los usuarios, también de escalarlos a la persona encargada de la atención de incidentes. Este agente debe contar adicionalmente con capacitación en seguridad de la información y debe comprender perfectamente la clasificación de incidentes y los procesos de escalamiento de incidentes. Complementariamente debe tener con una capacitación básica en técnicas forenses, especialmente en recolección y manejo de pruebas. La función principal del agente primer punto de contacto es dar un tratamiento inicial y escalar el incidente.

Administrador del Sistema: Usuario responsable de configurar y conservar los activos informáticos, este usuario recibe las notificaciones de las incidencias reportadas del primer punto de contacto para dar solución mediante la mitigación de datos. Al final debe documentar e informar la solución del mismo. Adicional los administradores deben contar con capacitaciones en seguridad de la información, conocer perfectamente la clasificación, los procesos de escalamiento de incidentes.

Administrador de los sistemas de Seguridad: Usuario similar al administrador del sistema, pero con la diferencia que sean profesionales en seguridad de la información (en redes, erradicación de vulnerabilidades, ética hacking y técnicas forenses). Se encarga de configurar y mantener un activo informático relacionado con la seguridad de la plataforma por ejemplo firewall, sistemas de prevención de intrusos, routers, sistemas de administración y monitoreo

Analista Forense: Debido que existen incidencias de seguridad informáticas de alto impacto es necesario contar con un analista forense disponible para tomar acciones legales (en caso de ser necesario) y para tener una exploración completa es necesario contar con los siguientes ítems:

- Que sucedió.
- Donde sucedió.
- Cuando sucedió.
- Quien fue el Responsable.
- Como sucedió.

Este actor debe ser un apoyo para los demás integrantes que conforman el grupo de solución de incidencias para aclaras inquietudes sobre los pasos y ejercer un liderazgo técnico en la resolución y atención de incidencias de seguridad de la información

Líder del grupo de atención de incidentes: Encargado de actuar inmediatamente a las peticiones de las incidencias informáticas que tengan un efecto rápido en los activos informáticos de la organización, también es el encargado de verificar y valorar los indicadores de gestión que corresponde a la solicitud de incidentes de

seguridad para presentar a los directivos. El líder grupo de atención de incidentes estará en la capacidad de reunir a los miembros de otras administraciones de la organización cuando el tema lo amerita. Además, debe estar enterado del cumplimiento de los usuarios nombrados anteriormente y de verificar que cada uno cumpla con el perfil asignado, así como evaluar los métodos y si es factible mejorar dichos métodos de mitigación. Finalmente, el líder del grupo de atención de Incidentes será responsable del modelo que se establecerá en la gestión y tener la capacidad de cerciorarse todas las incidencias de seguridad y los puntos estipulados que manejan el servicio de las herramientas Help Desk que utilicen [26].

2.4.2 Detección de incidentes de seguridad

La organización debería prestar especial atención a los probables indicios de una falla de seguridad o posibles ataques en los activos informáticos. A continuación, se muestra una relación de los primordiales indicadores de probables incidentes de seguridad:

- Precursores de un ataque: actividades anteriores de reconocimiento del sistema informático, como fallas de servidores, puertas traseras, escaneo de puertos.
- Notificación en los IDS (Sistemas de detección de intrusiones).
- Notificaciones en los cortafuegos o antivirus.
- Actividad rara en los logs (registros) de servidores y dispositivos de red o aumento sustancial del número de entradas en los logs.
- Aparición de nuevas carpetas o archivos con nombres raros en un servidor, o modificaciones llevadas a cabo en archivos del sistema.
- Mal desempeño de algún servidor: reinicios inesperados, errores en algunos servicios, aparición de alertas, crecimiento inusual del desempeño del procesador o excesivo consumo de memoria del sistema.
- Detección de procesos raros en ejecución dentro de un sistema, que se inician a horas poco comunes o que consumen más recursos de los normales (tiempo de procesador o memoria).
- Notable caída en el desempeño de la red o de algún servidor, gracias a un aumento inusual del tráfico de datos.

- Cambios en la configuración de determinados equipos de la red: modificación de las políticas de seguridad y auditoría, activación de nuevos servicios, puertos libres que no estaban autorizados, activación de las tarjetas de red en modo promiscuo (para poder atrapar todo el tráfico que circula por la red interna mediante sniffers).
- Existencia de herramientas no autorizadas en el sistema.
- Aparición de nuevas cuentas de usuario o registro de actividad inusual en varias cuentas: conexiones de usuarios en horarios raros, utilización de la misma cuenta desde diferentes equipos a la vez, bloqueo reiterado de cuentas por errores en la autenticación, ejecución inusual de determinados servicios desde algunas cuentas, etc.
- Informes de los propios usuarios del sistema alertando de algún comportamiento raro o de su imposibilidad de entrar a algunos servicios.
- Generación de tráfico extraño en la red.
- Notificación de un intento de ataque lanzado contra terceros desde equipos correspondientes a la propia organización.
- Desaparición de equipos de la red de la organización.
- Aparición de dispositivos extraños conectados de manera directa a la red o a algunos equipos de la organización.

2.4.3 Análisis de incidentes

El Plan de Respuesta a Incidentes debe determinar cómo el equipo debería seguir al análisis de un viable incidente de seguridad en cuanto éste fuese detectado por la organización, determinando en primer lugar la caracterización técnica del incidente y cuál es su alcance: ¿qué equipos, redes, servicios y/o aplicaciones se pudieron ver damnificados? ¿Se pudo poner en una situación comprometedora información confidencial de la organización o de sus usuarios? ¿Ha podido perjudicar a terceros?

Las actividades de análisis de eventos involucran una secuencia de otros elementos. Se recomienda considerar lo siguiente [26]:

- Comprender las funciones a nivel de red y de sistema.
- Los gestores de TI tienen que tener conocimiento total sobre los hábitos de la infraestructura que están administrando.

- Información que generan los servidores, redes, aplicaciones denominados Logs.
- Es conveniente llevar a cabo correlación de eventos, dado que a través de este desarrollo se tienen la posibilidad de conocer patrones de comportamiento anormal y poder detectar de forma más simple la causa del incidente.
- Crear y mantener una base de conocimientos con información relacionado a vulnerabilidades nuevas o anteriores.
- Determine la clase de incidencia informática en función de las intenciones del atacante y las amenazas existentes.
- Determinar la raíz del incidente, tomar las respectivas prevenciones y métodos de control para prever o mitigar la recurrencia futura.
- Identifique el origen del ataque y el atacante.

2.4.3.1 Evaluación

Se podría utilizar una "Matriz de Diagnóstico" para hacer más simple la actuación del equipo en momentos de máximo estrés, evadiendo que se logren tomar decisiones precipitadas que conduzcan a fallos. La gravedad de la incidencia podía ser [26]:

Alto impacto: las incidencias de seguridad informática tendrán un efecto negativo a gran escala a los activos de información llegando ocasionar pérdidas o daños a servicios físicos. Estas incidencias también podrían afectar la reputación o valoración de la organización.

Medio Impacto: las incidencias de seguridad informáticas afectan a activos de la información con resultados moderados influyendo a uno o varios procesos de la organización.

Bajo Impacto: las incidencias de seguridad informáticas afectan a activos de información con resultados menores e insignificante, que no influyen los procesos de la organización. Estos incidentes deben estar siendo monitoreado para evitar un cambio de impacto repentino.

2.4.3.2 Clasificación de incidentes de seguridad de la información

Esta clasificación depende de cada entidad, en función de su infraestructura y la importancia de los activos informáticos. Algunos ejemplos de clasificación de incidentes podrían ser [26]:

- **Acceso no autorizado:** es un incidente que implica a un individuo sistema o código malicioso que obtiene acceso lógico o físico al sistema, la aplicación, la información o el activo de información sin la debida autorización del propietario.
- **Modificación no autorizada de recursos**: incidentes que involucran a personas, sistemas o códigos malintencionados que destruyen la integridad de la información o los sistemas.
- **Uso inapropiado de recursos:** un incidente que involucra a un usuario que quebranta las políticas de la organización.
- **No disponibilidad de los recursos:** un incidente que involucra a un individuo, sistema o código malicioso que impide la utilización autorizado de un activo de información.
- **Multicomponente:** conformado por varios incidentes anteriormente mencionados.
- **Otros:** esta clase de incidentes debe monitorearse con el fin de detectar la necesidad de crear nuevas categorías, debido que estos incidentes no están clasificados.

2.4.3.3 Priorización de incidentes

Tener atención correcta a los incidentes (análisis, contención y erradicación) una vez que se obtiene la información de que tipo de incidencia es, hay que saber el nivel de prioridad del mismo, y así atenderlos como corresponde de acuerdo con la necesidad.

A manera de ejemplo se definen una serie de variables que podrán ser usadas para realizar la evaluación de los incidentes [26]:

- Prioridad
- Criticidad de impacto
- Impacto Actual

- Impacto Futuro

Nivel de Prioridad: Es dependiente del valor o consideración dentro de la entidad y del proceso que soporta el o los sistemas perjudicados.

Nivel criticidad	Valor	Definición
Bajo	0,25	Sistemas no críticos, trabajan individualmente.
Medio	0,50	Sistemas que contiene varias dependencia de otros sistemas en la entidad.
Alto	0,75	Sistemas correspondientes a estaciones de trabajo de usuarios con funciones críticas
Superior	1	Sistemas críticos para la entidad.

Tabla 8: Nivel de criticidad de impacto

Impacto Actual: Numero de impedimentos que resultaron afectados en el momento que se ha registrado la incidencia informática.

Impacto Futuro: Numero de impedimentos que resultaran afectados e si no es contenido, ni erradicado la incidencia informática.

Nivel criticidad	Valor	Definición
Bajo	0,25	Impacto bajo en uno de los sistema de información o estación de trabajo de la entidad.
Medio	0,50	Impacto medio en uno de los sistema de información o estación de trabajo de la entidad.
Alto	0,75	Impacto alto en los sistemas de información o estaciones de trabajo de la entidad.
Superior	1	Impacto en los sistema de información o estaciones de trabajo de la entidad.

Tabla 9: Impacto actual e impacto futuro

La prioridad se obtiene mediante la siguiente fórmula [26]:

Nivel de Prioridad = (Impacto actual*2,5) + (Impacto futuro *2,5) + (criticidad del sistema *5)

Y el resultado se compara con la siguiente tabla para determinar el nivel de prioridad de atención:

Nivel de prioridad		Valor
Bajo	4	02,50 – 03,74
Medio	3	03,75 – 05,00
Alto	2	05,25 – 07,99
Superior	1	08,00 – 10,00

Tabla 10: Nivel de prioridad

2.4.4 Contención, erradicación y recuperación

Dentro del Plan de Respuesta a Incidentes, el equipo de respuesta debe elegir una determinada estrategia de contención del incidente de seguridad. Las actividades de mitigación también deben ser continuas e irse adaptando a medida que se reúne y analiza más información durante la fase de detección y análisis. Los objetivos de la mitigación son: contener el incidente de seguridad física informática, erradicar todo software maligno de los sistemas afectados, y recuperar la función del sistema.

Contención: esta actividad está diseñada para detectar incidentes para que no se expandan y puedan causar más daño a la información o arquitecturas de una organización. Para facilitar esta tarea, las entidades deben tener una estrategia de contención predefinida para tomar decisiones de manera inmediata.

Una vez adoptada una estrategia de contención, se recogerán las evidencias, para lo cual se deben considerar los siguientes puntos:

- **Autenticidad:** La persona que recopile las evidencias debe poder probar que son auténticas.
- **Cadena de Custodia:** Registro detallado del procedimiento de la evidencia, para evitar cambios o modificaciones que afecten la evidencia.

- **Validación:** Asegurar que la evidencia recolectada es la misma que la evidencia proporcionada a las autoridades.

Durante el proceso de recolección de evidencias, se debe tomar las siguientes medidas:

- Registrar información sobre las evidencias.
- Marque todos los medios que se usarán como evidencia.
- Guarde todas las pruebas de forma segura.
- Haga una copia de respaldo de la evidencia original.
- Realizar revisiones periódicas para garantizar que la evidencia se conserve adecuadamente

Las estrategias de contención varían según el tipo de incidente y los estándares deben estar completamente documentados para facilitar una toma de decisiones rápida y eficaz. Algunos estándares que se pueden utilizar como base son:

- Estándares forenses
- Posible pérdida y robo de propiedad.
- Necesidad de preservar la evidencia.
- Servicio disponible.
- Tiempo y recursos necesarios para implementar la estrategia.
- La efectividad de la estrategia para controlar el evento (parcial o totalmente)
- Duración de la solución

Erradicación y Recuperación: Una vez contenido el incidente, los rastros de códigos maliciosos que dejó el incidente deben eliminarse, y luego restaurar los sistemas o servicios afectados. El administrador de TI debe restaurar las funciones del sistema afectado y realizar el fortalecimiento del sistema para evitar en el futuro incidentes similares.

En el anexo 5 se realizó un cuadro con diferentes tipos de incidentes de seguridad informática con sus respectivos conceptos y la mitigación a realizar (Ver Anexo 5).

2.4.5 Identificación de ataque y posibles actuaciones

Dentro del Plan de Respuesta a Incidentes, la identificación del atacante es que se requiere para poder emprender acciones legales para reclamar responsabilidades e indemnizaciones. Sin embargo, conviene tomar en cuenta que por lo general sólo se va a poder detectar la máquina o máquinas desde las que se ha realizado el ataque, pero no de manera directa al individuo responsable de su utilización. La identificación del atacante puede ser una labor gaste bastante tiempo y recursos, por lo cual no debería obstruir en la contención y erradicación del incidente. Algunas organizaciones optan por no perseguir legalmente a los atacantes por el esfuerzo necesario: gastos, trámites judiciales. Además, los ataques realizados desde otros países con ciertos marcos legales en el tratamiento de los delitos informáticos tienen la posibilidad de hacer más difícil las reclamaciones judiciales, puesto que se complica mayormente en el proceso de extradición de los causantes. Hay diferentes técnicas para saber la dirección IP del equipo o equipos desde el que se ha realizado el ataque contra el sistema informático: utilización de herramientas como ping, traceroute o whois, etc. Sin embargo, es requisito tomar en cuenta una secuencia de obstáculos que tienen la posibilidad de hacer más difícil esta tarea:

- Mediante técnicas de "IP Spoofing" se podría enmascarar la dirección en algunos tipos de ataque.
- El atacante podría estar utilizando equipos de terceros para realizar sus acciones, situación que se produce con bastante frecuente hoy en día.
- El atacante podría haber empleado una dirección IP dinámica, asignada a su equipo por un proveedor de acceso a Internet.
- El equipo del atacante podría estar situado detrás de un servidor proxy con el servicio NAT activo (traducción de direcciones internas a una dirección externa), compartiendo una dirección IP pública con otros equipos de la misma red.

Por esto, en varios casos va a ser primordial pedir la colaboración de los responsables de otras redes y de los proveedores de acceso a Internet que pudieron ser usados por los atacantes. Una labor que además podría ayudar a la identificación del atacante es el análisis de las actividades de exploración (escaneos de puertos y de vulnerabilidades en el sistema) que suelen anteceder a un ataque, sobre todo si

éstas han podido ser registradas por los "logs" de los equipos damnificados o por el Sistema de Detección de Intrusiones (IDS). En relación a la ejecución de acciones contra el atacante, se sugiere presentar una denuncia ante las unidades policiales especializadas en este tipo de incidentes o ataques informáticos, para poder emprender de este modo las correspondientes actuaciones policiales y judiciales.

2.4.6 Documentación de incidentes de seguridad

El Plan de Respuesta a Incidentes debería establecer cómo se tiene que documentar un incidente de seguridad, reflejando de forma clara y precisa aspectos como los que se presentan en la siguiente relación:

- Descripción del tipo de incidente.
- Hechos registrados (eventos en los "logs" de los equipos).
- Daños producidos en el sistema informático.
- Decisiones y actuaciones del equipo de respuesta.
- Comunicaciones que se han realizado con terceros y con los medios.
- Lista de evidencias obtenidas durante el análisis y la investigación.
- Comentarios e impresiones del personal involucrado.
- Posibles actuaciones y recomendaciones para reforzar la seguridad y evitar incidentes similares en el futuro.

2.5 DISEÑO DE PLATAFORMA WEB DE REGISTRO DE INCIDENCIAS

La arquitectura que se estará manejando será Cliente-Servidor, las peticiones o acciones que realice por parte del cliente será receptada por el servidor y a su vez devolverá una respuesta dependiendo de la solicitud que realice el cliente.

Cliente

En la plataforma web tendrá acceso a varios menús de carácter informativo relacionado a seguridad informática, información del CSIRT-UPSE y a la aplicación web para el registro de incidentes informáticos.

Servidor

En el servidor se encontrará activo el servicio web Request Tracker donde se estará gestionando los reportes o alertas de incidentes de seguridad informática que realicen los usuarios.

2.5.1 Diagrama de caso de uso

2.5.1.1 Caso de uso: Súper administrador

Aplicación Web	**Pág. 1/3**	
	Fecha creación 22/08/2020	**Fecha edición** 22/08/2020
Dirigido a: Súper administrador	**Autor:** Rosales Reyes Jesús Daniel	

Caso de uso: Súper administrador

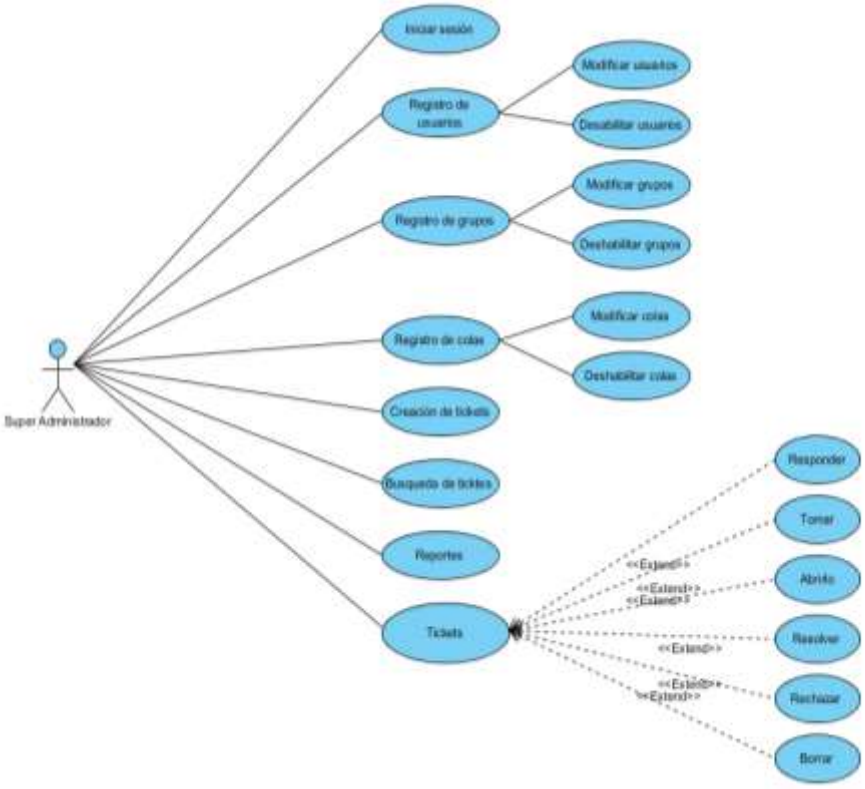


Figura 13: Caso de uso: Súper administrador

Descripción: El diagrama de caso de uso representa las actividades que pueden realizar el usuario con el perfil de súper administrador en la aplicación web Request tracker.

El Súper Administrador es el personal del CSIRT-UPSE y cuenta con las siguientes funciones:

Registrar, modificar y deshabilitar:

• Usuarios • Grupos • Colas

Tabla 11: Caso de uso: Súper administrador

2.5.1.2 Caso de uso: Administrador

Aplicación Web	**Pág. 2/3**	
	Fecha creación **22/08/2020**	**Fecha edición** **22/08/2020**
Dirigido a: Administrador	**Autor:** Rosales Reyes Jesús Daniel	
Caso de uso: Aplicación web		

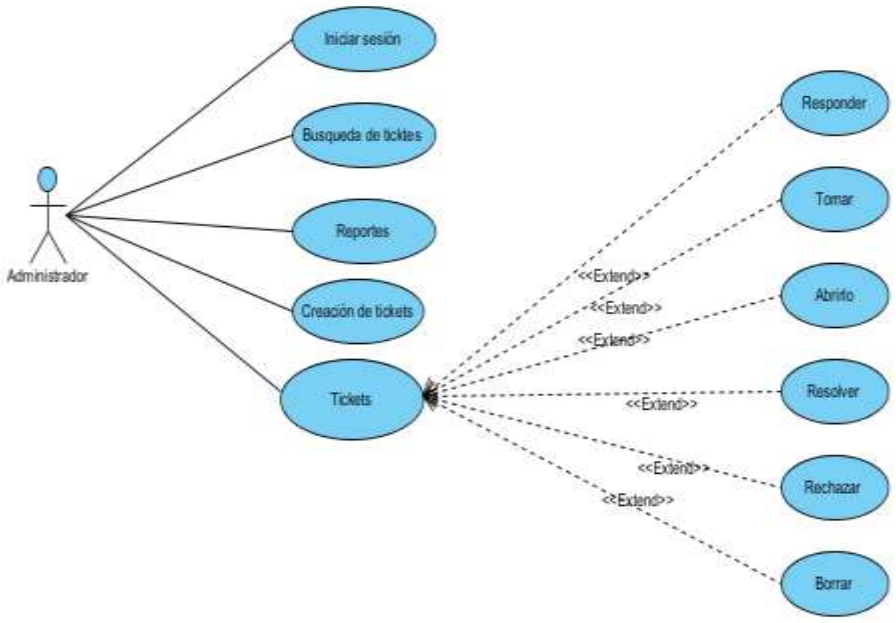


Figura 14: Caso de uso: Administrador

Descripción: El diagrama de caso de uso representa las actividades que pueden realizar el usuario con el perfil de administrador en la aplicación web Request tracker..

El Administrador son el personal del CSIRT-UPSE.

Cuando el actor publico haya creado un ticket, un administrador o el mismo súper administrador puede realizar las siguientes acciones con el ticket:

- Responder
- Tomar

- Abrirlo
- Resolver
- Rechazar
- Borrar

Cuentan con la función de buscar tickets que estén pendientes o resueltos y también pueden crear tickets cuando ocurre una incidencia informático a nivel interno que el actor público no puede presenciar, para mantener un registro y que se refleje en los reportes que se generan.

Tabla 12: Caso de uso: administrador

2.5.1.3 Caso de uso: Público en general

Aplicación Web	**Pág. 3/3**	
	Fecha creación **22/08/2020**	**Fecha edición** **22/08/2020**
Dirigido a: Público en general.	**Autor:** Rosales Reyes Jesús Daniel	
Caso de uso: Público en general		

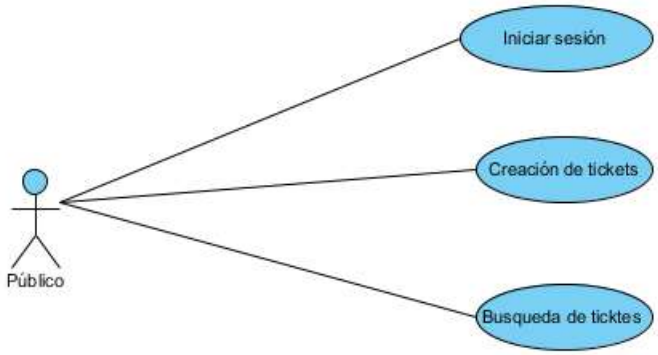


Figura 15: Caso de uso: Publico en general

Descripción: El diagrama de caso de uso representa las actividades que pueden realizar el usuario con el perfil de público en general en la aplicación web Request tracker.

El actor público puede ser estudiantes y profesores, pueden crear tickets y buscar los tickets que hayan creado ya sea:

- Tickets abiertos
- Tickets cerrados

Tabla 13: Caso de uso: Público en general

2.5.2 Diseño de interfaz grafica

2.5.2.1 Módulos del Request Tracker

Request tracker consta de varios módulos las cuales se detallarán los módulos por actor y afines al tema, los demás módulos no serán mencionados ya que no son parte del estudio, pero se podría tomar en cuenta en las recomendaciones ya que también aportan a mejorar el funcionamiento de la organización.

2.5.2.1.1 Actor Súper administrador

Para el actor súper administrador se mostrará esta interfaz gráfica cuando inicia sesión.

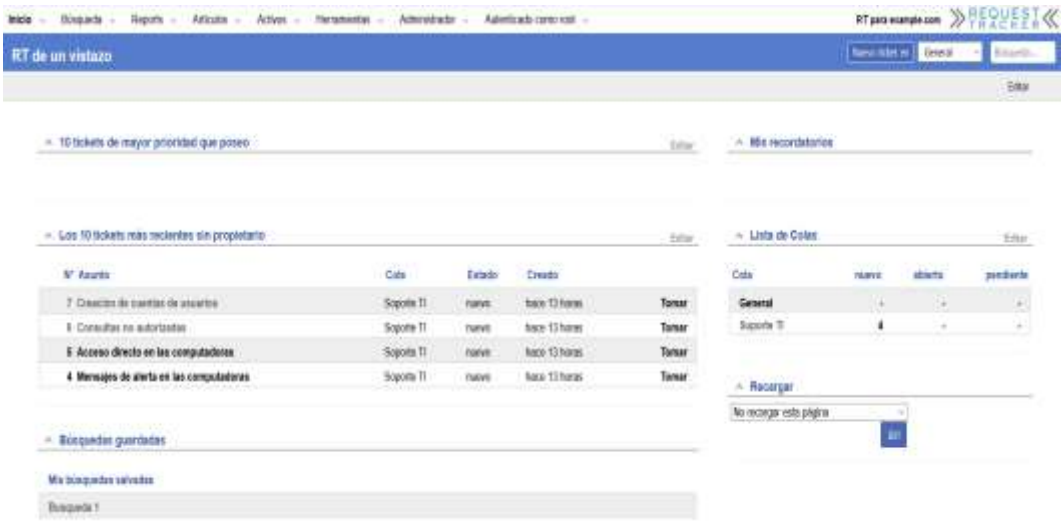


Figura 16: Interfaz para Actor Súper Administrador

2.5.2.1.1.1 Búsqueda

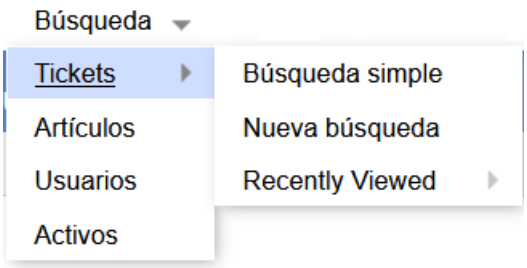


Figura 17: Módulo búsqueda para Actor Súper Administrador

El primer módulo permite realizar búsquedas de tickets, usuarios, artículos y activos. En Tickets existe tres tipos de búsqueda:

- Búsqueda simple
- Nueva búsqueda
- Recently Viewed (visto recientemente)

En donde se destaca Nueva búsqueda porque permite realizar búsquedas personalizadas dependiendo del caso o reglas del negocio, generar reportes (textual y gráfico) y exportarlo en Hoja de cálculo, RSS (formato XML para contenido web) y iCal.

En Usuarios se hace una búsqueda simple por su correo electrónico, nombre o nombre Real.

2.5.2.1.1.2 Reportes

Figura 18: Módulo reportes para Actor Súper Administrador

Este módulo está enfocado en visualizar únicamente reportes simples: el número total de tickets resueltos, los tickets resuelto en un rango de tiempo determinado y los tickets creados en un rango de tiempo determinado por ende el módulo anterior es más factible utilizarlo al momento de crear reportes.

2.5.2.1.1.3 Administrador

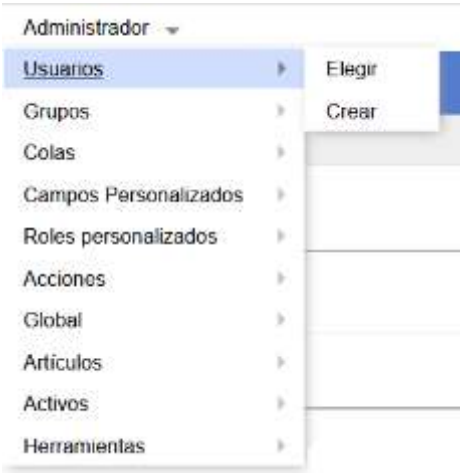


Figura 19: Módulo administrador para Actor Súper Administrador

Este módulo exclusivo del actor súper administrador y contiene las siguientes características:

- Crear, modificar, deshabilitar a usuarios, grupos y colas de acuerdo a las condiciones de la organización.
- Personalizar los permisos o privilegios de cada perfil dependiendo del cargo que ejercen en la organización.
- Visualizar las especificaciones técnicas del Request tracker: versión, módulos cargados, configuraciones.
- CSS personalizada.

2.5.2.1.1.4 Autenticado

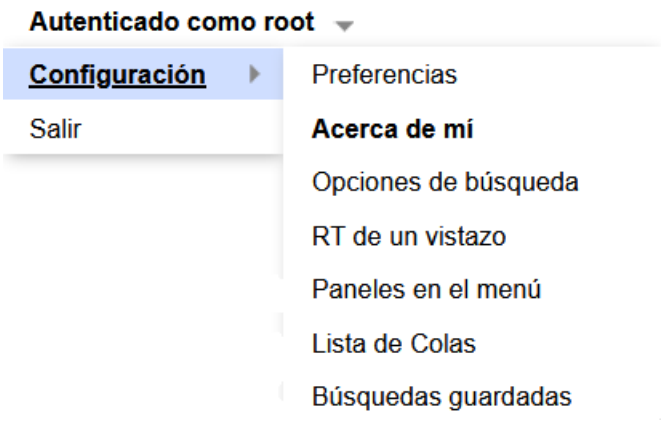


Figura 20: Módulo Autenticado para Actor Súper Administrador

En este último módulo muestra al usuario logueado (en este caso al súper usuario) donde podrá ver su información, cerrar sesión y haciendo redundancia en las opciones disponibles debido que también se puede acceder en sus módulos respectivos por ejemplo la opción de búsquedas guardadas que también puede ser encontrado en el módulo Búsqueda > Tickets > Nueva Búsqueda

2.5.2.1.2 Actor administrador

Para el actor Administrador se mostrará esta interfaz gráfica cuando inicia sesión el cual se destaca los paneles:

- 10 tickets de mayor prioridad que poseo: Tickets enviados que fueron tomados por el personal del CSIRT-UPSE.

- Los 10 tickets más recientes sin propietario: Tickets enviados que siguen sin ser tomados por el personal del CSIRT-UPSE.
- Mis recordatorios: En este apartado el usuario logueado podrá crear notas de recordatorios para los tickets que tiene en su bajo su supervisión.
- Lista de colas: Muestra todos los tickets tanto como nuevos y pendientes.

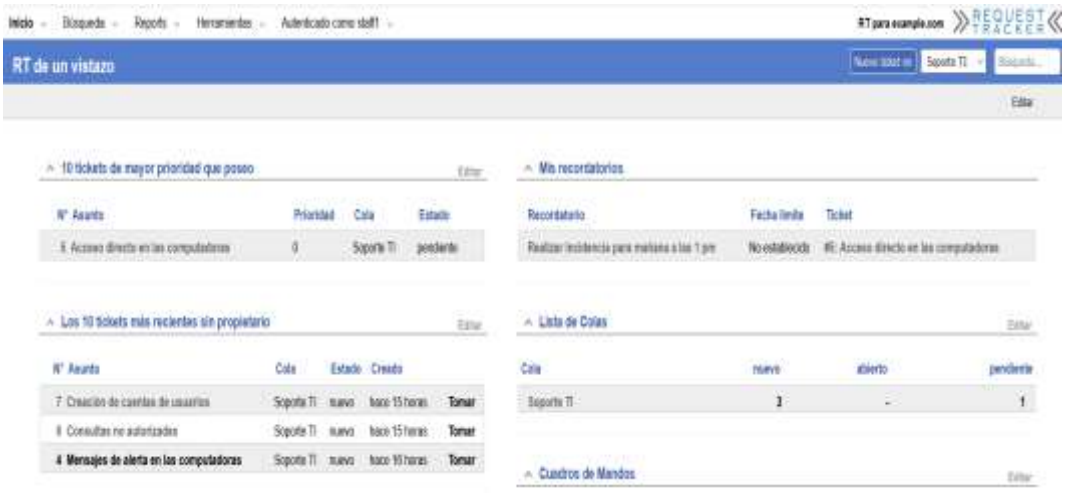


Figura 21: Interfaz para Actor Administrador

2.5.2.1.2.1 Búsqueda

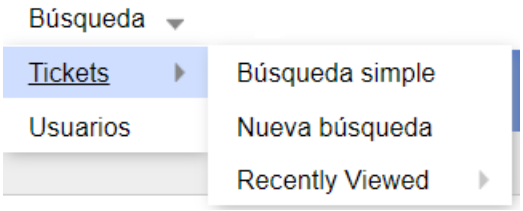


Figura 22: Módulo búsqueda para Actor Administrador

El primer módulo permite realizar búsquedas de tickets y usuarios. En Tickets existe tres tipos de búsqueda:

- Búsqueda simple
- Nueva búsqueda
- Recently Viewed (visto recientemente)

En donde se destaca Nueva búsqueda porque permite realizar búsquedas personalizadas dependiendo del caso o reglas del negocio, generar reportes (textual

y gráfico) y exportarlo en Hoja de cálculo, RSS (formato XML para contenido web) y iCal.

En Usuarios se hace una búsqueda simple por su correo electrónico, nombre o nombre Real.

2.5.2.1.2.2 Reportes

Figura 23: Módulo reportes para Actor Administrador

Este módulo está enfocado en visualizar únicamente reportes simples: el número total de tickets resueltos, los tickets resuelto en un rango de tiempo determinado y los tickets creados en un rango de tiempo determinado por ende el módulo anterior es más factible utilizarlo al momento de crear reportes.

2.5.2.1.2.3 Herramientas

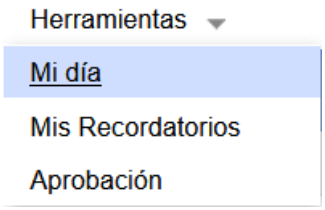


Figura 24: Módulo herramientas para Actor Administrador

En este módulo proporciona la información de todos los recordatorios creado de cada ticket que el usuario haya o esté realizando.

En el último modulo Autenticar solo muestra el nombre actual del usuario logueado y la opción de cerrar sesión.

2.5.2.1.3 Actor público

Para el Actor Publico se mostrará esta interfaz gráfica cuando inicia sesión

Figura 25: Interfaz para Actor Público

La cual contiene tres módulos:

- Nuevo ticket: En este módulo podrá informar mediante tickets al personal del CSIRT-UPSE las incidencias informáticas que ocurran.
- Tickets: Muestra sus tickets informados tanto los abiertos que significa que aún no han sido tomadas o están en proceso de solución por parte personal del CSIRT-UPSE y los tickets cerrados que son los tickets resueltos.
- Autenticado como: Muestra el nombre del usuario actual logueado y la opción de finalizar su sesión.

2.6 ESTUDIO DE FACTIBILIDAD

2.6.1 Factibilidad técnica

En la factibilidad técnica se estableció las categorías de hardware, software, equipos de oficina de una infraestructura para el CSIRT-UPSE además de otros recursos necesarios.

CATEGORÍAS	COMPONENTES/RUBROS	CANTIDADES
Recursos de Hardware	Computadoras de escritorio	5
	Impresora multifuncional	1
	Servidores HP Proliant	1
	Monitores	5
	Partes y accesorios computacionales	-
	CentOS 7	1

Recursos de Software	Windows 10	1
	Help Desk Request Tracker	1
	Programas de monitoreo de red	-
	Programas de análisis de malware	-
Equipos de oficina	Sillas	5
	Escritorios	5
	Archivadores de pared	2
	Suministros de oficina	-
Recursos Varios	Servicios básicos	-

Tabla 14: Factibilidad técnica

2.6.2 Factibilidad operativa

Se requiere de un personal capacitado en el área de seguridad informática, forense y de un analista de sistemas que se detalla a continuación:

CATEGORÍAS	COMPONENTES/RUBROS	CANTIDADES
Recursos Humanos	Analista de Seguridad Informática	1
	Analista forense	1
	Analista en Sistemas	1

Tabla 15: factibilidad operativa

2.6.3 Factibilidad económica

CATEGORÍAS	COMPONENTES/RUBROS	CANTIDADES	PRECIO UNITARIO	TOTAL
Recursos de Hardware	Computadoras de escritorio	5	$400.00	$2,000.00
	Impresora multifuncional	1	$350.00	$350.00
	Servidores HP Proliant	1	$7,000.00	$7,000.00
	Monitores	5	$105.00	$525.00
	Partes y accesorios computacionales	-	$400.00	$400.00
TOTAL RECURSOS DE HARDWARE				**$10,275.00**
	CentOS 7	1	$0.00	$0.00

Recursos de Software	Windows 10	5	$289.00	$1,445.00
	Help Desk Request Tracker	1	$0.00	$0.00
	Programas de monitoreo de red	-	$0.00	$0.00
	Programas de análisis de malware	-	$0.00	$0.00
TOTAL RECURSOS DE SOFTWARE				**$1,445.00**
Equipos de oficina	Sillas	5	$40.00	$200.00
	Escritorios	5	$150.00	$750.00
	Archivadores de pared	2	$75.00	$150.00
	Suministros de oficina	-	$100	$100
TOTAL EQUIPOS DE OFICINA				**$1,200.00**
Recursos Humanos	Analista de Seguridad Informática	4 meses	$600.00	$2,400.00
	Analista forense	4 meses	$900.00	$3,600.00
	Analista de Sistemas	2 meses	$500.00	$1,000.00
TOTAL RECURSOS HUMANOS				**$7,000.00**
Recursos Varios	Servicios básicos	-	$1,500.00	**$1,500.00**
TOTAL				**$21,420.00**

Tabla 16: Factibilidad económica

2.6.4 Costo implementación

El presupuesto de recursos de hardware, software, equipos de oficinas y recursos varios son el reflejo para la creación de una infraestructura para que opere el CSIRT-UPSE, este monto no es considerado para la realización del proyecto debido que la aplicación está alojada en un servidor local y se utiliza herramientas gratuitas

facilitando así el desarrollo de la propuesta, finalmente para la creación del IRP solo son pautas para saber qué acciones tomar mediante una incidencia informática.

La actividad por parte de recursos humanos es de $0.00 ya que el tesista asume dichas actividades.

CATEGORÍAS	Costos
Recursos de Hardware	**$ 0.00**
Recursos de Software	**$ 0.00**
Recursos Humanos	**$ 0.00**
Gastos Varios	**$ 0.00**
Total	**$ 0,00**

Tabla 17: Costo implementación

2.7 PRUEBAS DE FUNCIONAMIENTO

2.7.1 Ingreso y registro de una incidencia informática

En la actualidad con la herramienta Help Desk el proceso de ingresar una petición de servicios o incidentes informáticos se lleva a cabo de una forma regularizada y mucho más eficaz, el usuario solo debe entrar al sistema desde la página web del CSIRT-UPSE y registrar su petición en unos simples y pocos pasos y la herramienta Request Tracker se encarga de notificar a los encargados del área de soporte la presencia de una nueva petición.

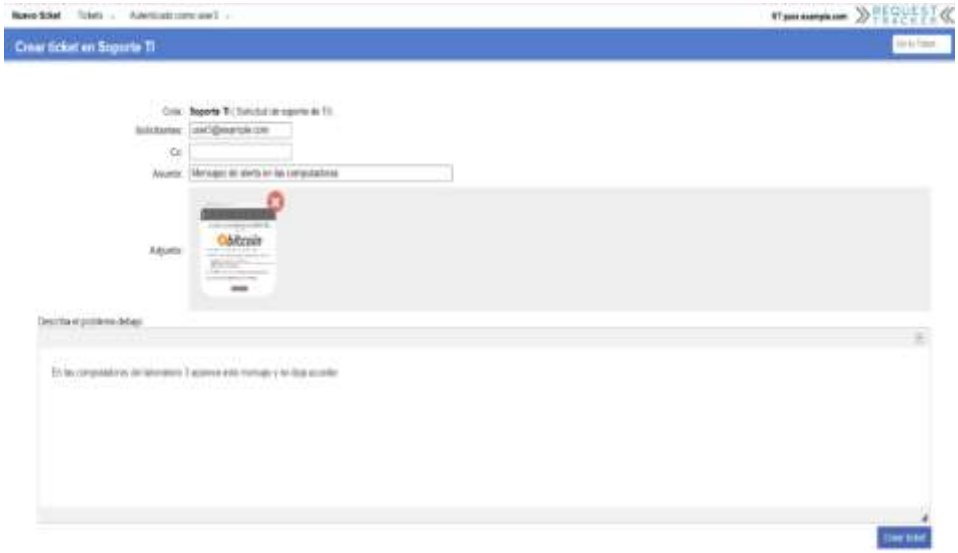


Figura 26: Ingreso y registro de una incidencia informática

2.7.2 Recepción y asignación del personal del CSIRT-UPSE a la petición del ticket ingresado

La herramienta facilita la administración de los incidentes informáticos , cuando estos son ingresados por los usuarios los muestra en un panel general (figura 25), para asignar el ticket respectivamente a la persona indicada es importante tomar en cuenta las pautas que se hicieron en el subapartado 2.4.1 CONSTITUCIÓN DEL EQUIPO DE RESPUESTA A INCIDENTES del apartado 2.4 PLAN DE RESPUESTA A INCIDENTES, una vez que la persona es asignado podrá realizar las acciones disponibles como se muestra en la (figura 26) dependiendo de las características del ticket podrá Tomarlo para las respectivas tareas para solucionarlo o rechazarlo debido a que no es una incidencia informática.

Figura 27: Panel general del Request tracker con tickets pendientes

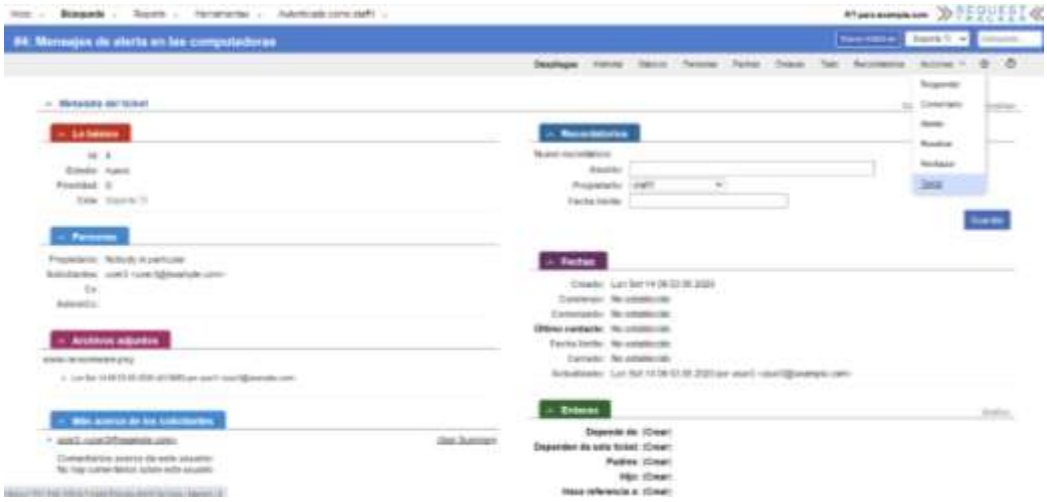


Figura 28: Acciones disponibles de un ticket

En la (figura 27) muestra las características de la incidencia informática alertada se define el tiempo que tomará en resolver el problema, es importante tomar en cuenta las pautas en los subapartados 2.4.3.2 CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN y 2.4.3.3 PRIORIZACIÓN DE INCIDENTES del apartado 2.4.3 ANÁLISIS DE INCIDENTES para llegar a una deducción verídica. Se tomó como un ejemplo la simulación de un incidente informático que ataco a las computadoras del laboratorio 3 como estaba descrito en la descripción del ticket ver (figura 28) con el análisis del personal experto del CSIRT-UPSE mas la evidencia adjuntada del ticket se concluyó que es un Ransomware que es un incidente informático de código malicioso y deberá hacer la mitigación respectiva (Ver Anexo 5)

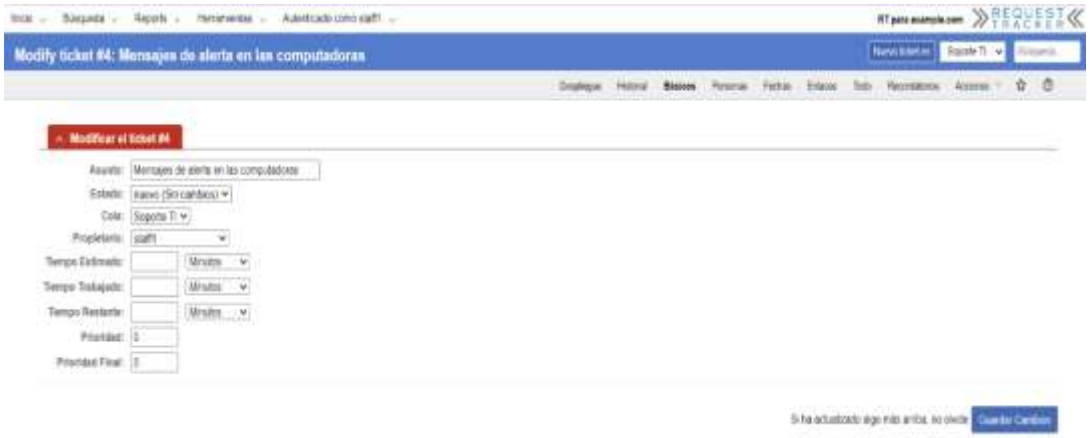


Figura 29: Detalles a agregar a una incidencia informática

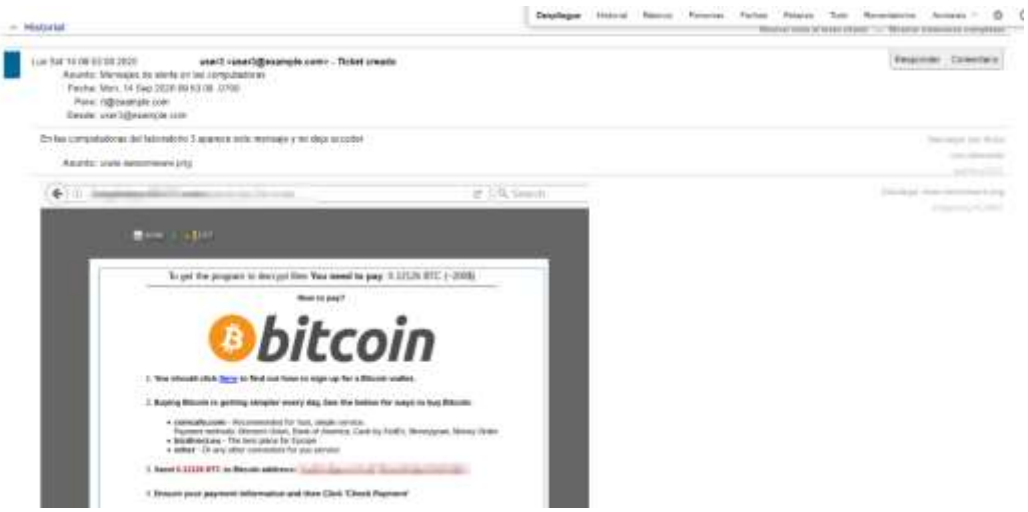


Figura 30: Incidencia informática Ransomware

Paralelamente con la mitigación respectiva se debe de guardas otros datos del ticket para tener un correcto historial de los incidentes informáticos, para calcular el nivel de prioridad se utilizará la siguiente fórmula:

Datos:

Nivel de Prioridad = ?

Impacto actual = 0,75

Impacto futuro = 0,75

Criticidad del Sistema = 0,75

$$Nivel\ Prioridad = (Impacto\ actual * 2{,}5) + (Impacto\ futuro * 2{,}5) + (Criticidad\ del\ Sistema * 5)$$

$$Nivel\ prioridad = (0{,}75 * 2{,}5) + (0{,}75 * 2{,}5) + (0{,}75 * 5)$$

$$Nivel\ Prioridad = 7{,}5$$

El resultado dio una prioridad de 7,5 comparando con el cuadro del subapartado 2.4.3.3 PRIORIZACIÓN DE INCIDENTES del apartado 2.4.3 ANÁLISIS DE INCIDENTES se establece que es una prioridad de nivel 2 (Alto), finalmente el tiempo estimado depende del personal cuanto tiempo tardaría.

Para saber el nivel de prioridad ya establecidos puede consultar el (Anexo 6) Prioridad de incidencias de seguridad en elementos informáticos, cabe señalar que cada entidad es libre de definir la prioridad de las incidencias informáticas, siempre que lo considere oportuno y dependa de la gravedad de los activos afectados.

2.7.3 Seguimiento del incidente informático

La herramienta permite llevar un rastreo completo del incidente informático, desde el momento de su ingreso hasta la solución y cierre del mismo. Cada modificación que se lleve a cabo sobre el incidente en algunas de sus etapas (tomar el incidente, poner en estado pendiente, etc.) es registrado de forma automática. Tanto el usuario que ingreso el ticket de la incidencia informático como el personal experto encargado de brindar el soporte pueden visualizar las modificaciones que este último puede ir realizando sobre el incidente hasta el momento de darle solución definitiva y llegar a su cierre. El personal del área con privilegios (súper administrador) también puede visualizar dicho historial de modificaciones de cada uno de los incidentes o requerimientos.

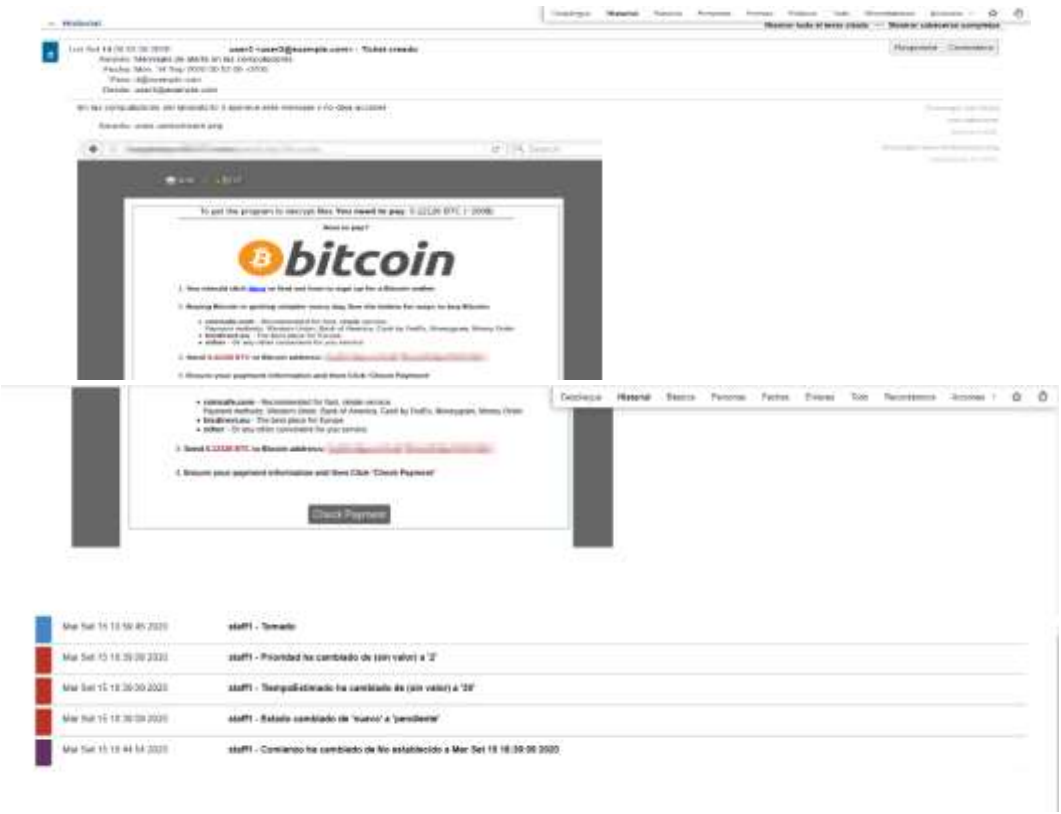


Figura 31: Historial de la incidencia informática

2.7.4 Solución y cierre del incidente informático

Una vez solventado el incidente informático, en la pestaña Acciones se procede a resolverlo para que pase a estado resuelto, adicional la redacción de las acciones que se realizaron, capturas de pantallas y toda la información recopilada para luego

en un futuro cuando ocurra un incidente similar se proceda a buscar dicho incidente y de esta manera la solución sea aún más rápida comparado de la última vez.

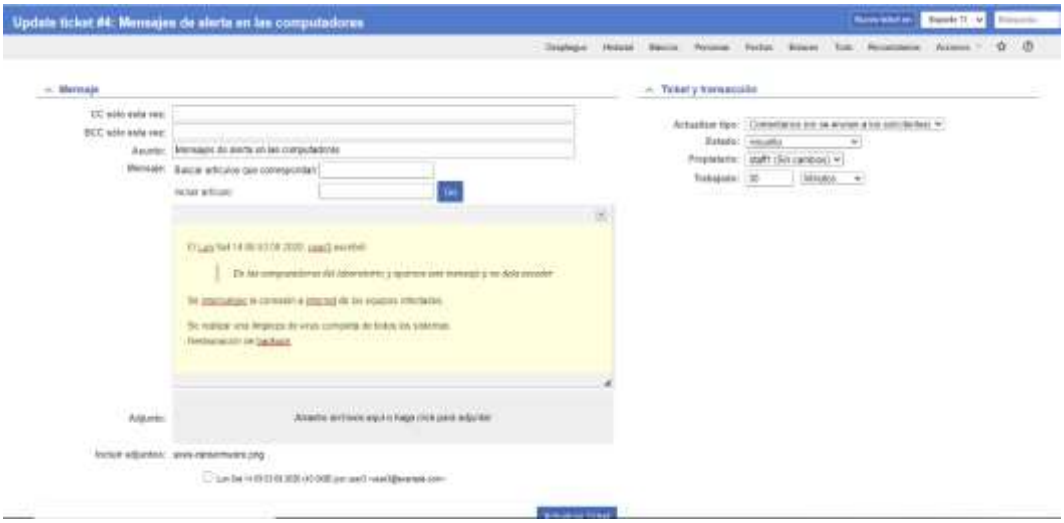


Figura 32: Solución de la incidencia informática

Figura 33: Cierre de la incidencia informática

2.8 REPORTES ESTADÍSTICOS

En la (figura 32) se muestra mediante una lista las incidencias informáticas reportadas ya sea resultas, rechazados, pendientes o nuevos mediante la aplicación web, también se puede mostrar con gráficos (figura 33)

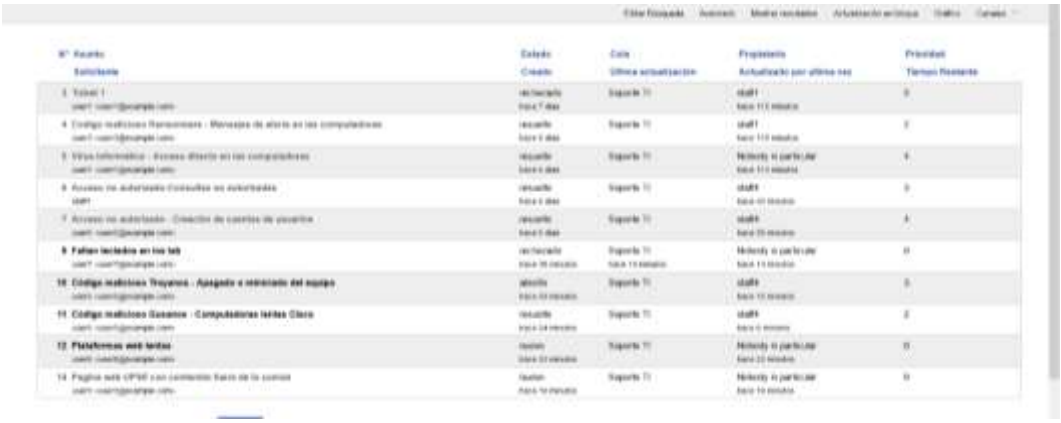


Figura 34: Lista de incidencias informáticas ingresadas

Estado	Total de tickets
abierto	1
nuevo	2
rechazado	2
resuelto	5
Total	10

Figura 35: Grafica de incidencias informáticas ingresados

Request Tracker tiene varios filtros de búsquedas en esta ocasión se buscó las incidencias informáticas que fueron resueltas y que estén agrupadas por el nivel de prioridad.

Figura 36: Lista de incidencias informáticas resultas

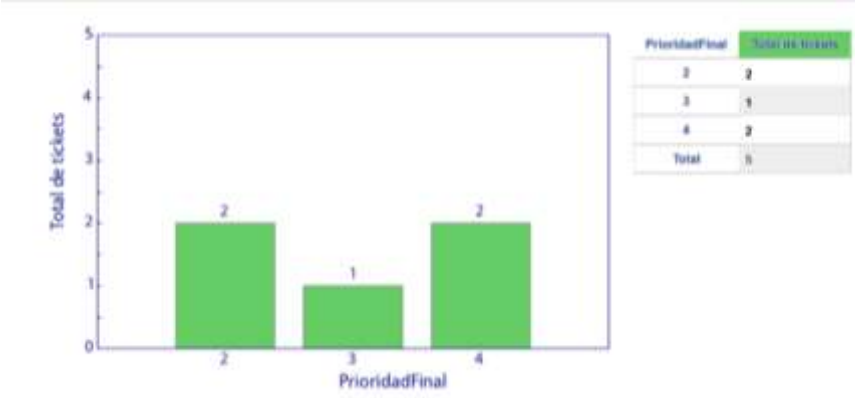


Figura 37: Gráfica de incidencias informáticas resueltas

CONCLUSIONES

- Se logró desarrollar una plataforma Web informativa donde los usuarios pueden enterarse lo que ocurre en el campo universitario en temas de seguridad informática, de las incidencias que suceden y además de instruirse con boletines de interés para concientizar en el ámbito en temas de seguridad informática.
- Gracias a la implementación de la aplicación web Request Tracker ubicado en la página web CSIRT-UPSE los usuarios podrán notificar las incidencias informáticas que se presenten y el personal encargado de solucionar estos incidentes lo desarrollarán de manera ordenada y más ágil teniendo como resultado un área eficiente y funcional.
- Al contar con un plan de incidencias accesible para el personal autorizado los problemas de seguridad informáticos reportados se podrán solucionar con más rapidez y eficacia debido que el plan de incidencia cuenta ya con pautas establecidos de que hacer o cómo actuar en diversas situaciones.
- Los reportes generados en el Request Tracker muestran de manera más especifica la incidencia informática: qué tipo de malware es, nivel de criticidad, acciones a realizar, estos datos permitirán actuar de manera más rápida y eficaz en un futuro donde vuelva a ocurrir una incidencia igual o similar
- La implementación de un CSIRT académico completo y robusto necesita de una alta inversión que resulta complicado de aprobar por una institución académica publica, debido a la infraestructura y equipamiento primordial

para su operación. Sin embargo, plantear una solución inicial que reutilice elementos, herramientas y personal que ya tiene la universidad resulta positivo para la aceptación de la comisión de proyectos.

RECOMENDACIONES

- Las pautas establecidas para el plan de respuesta a incidencias de seguridad informática es el resultado de diversas investigaciones por lo tanto esta propenso a sufrir cambios de parte de la organización para adaptarlo a las necesidades de la misma.
- Capacitar continuamente a todos los usuarios de la organización en la correcta y responsable utilización de la herramienta y la seguridad de la información.
- Utilizar los otros módulos del Request Tracker puesto que serían de gran ayuda en la gestión correcta de todos los recursos informáticos de la organización.
- Además de la utilizar todos los módulos de la herramienta, para conseguir un más alto beneficio se sugiere el análisis y la implementación de los diversos plugins existentes para de este modo tener una herramienta robusta y apta para cubrir las necesidades y expectativas de la organización.
- Un plugins sugerido es RT::Authen::ExternalAuth::DBI una implementación para poder utilizar una base de datos externa para la autenticación del Request tracker.
- Se sugiere hacer capacitaciones continuas al personal asignado para el CSIRT académico para la mejora de los procesos diseñados.

BIBLIOGRAFÍA

[1] M. A. De La Torre Moscoso, Hugo Marcelo; Parra Rosero, “Estrategia y diseño de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) académico para la universidad de las fuerzas armadas ESPE,” 2014.

[2] Universidad Internacional de Valencia, “Herramientas de seguridad informática más recomendadas en 2018 | VIU,” *2018*. [Online]. Available: https://www.universidadviu.com/herramientas-seguridad-informatica-mas-recomendadas-2018/. [Accessed: 15-Jul-2019].

[3] Generalitat Valenciana, “CSIRT-CV | CSIRT-CV.” [Online]. Available: https://www.csirtcv.gva.es/es/paginas/csirt-cv.html. [Accessed: 15-Jul-2019].

[4] Diario Norte, “El delito informático cada vez más peligroso | Norte Chaco,” 2013. [Online]. Available: http://www.diarionorte.com/article/87777/el-delito-informatico-cada-vez-mas-peligroso. [Accessed: 14-Jul-2019].

[5] M. Jezreel, M. Mirna, and U. Edgar, “Services establishment in the computer security incident response teams: A review of state of art,” in *2015 10th Iberian Conference on Information Systems and Technologies (CISTI)*, 2015, pp. 1–6.

[6] Diario El Universo, “Ecuador ha recibido 40 millones de ataques cibernéticos, revela viceministro de Telecomunicaciones | Política | Noticias | El Universo,” 2019. [Online]. Available: https://www.eluniverso.com/noticias/2019/04/15/nota/7287215/ecuador-ha-recibido-40-millones-ataques-ciberneticos-revela. [Accessed: 03-Jun-2019].

[7] J. M. Miranda and H. Ramirez, “Estableciendo controles y perimetro de seguridad para una pagina web de un CSIRT,” *RISTI - Rev. IbÃ\copyrightrica Sist. e Tecnol. InformaÃ§Ã\poundso*, pp. 1–15, 2016.

[8] CNCERT/CC, “About Us.” [Online]. Available: https://www.cert.org.cn/publish/english/index.html. [Accessed: 25-Jul-2019].

[9] Equipos de Ciberseguridad y Gestión de Incidentes españoles, “Miembros.” [Online]. Available: https://www.csirt.es/index.php/es/miembros. [Accessed: 25-Jul-2019].

[10] Centro de Respuesta a Incidentes Informáticos, “Nosotros.” [Online]. Available: https://www.ecucert.gob.ec/nosotros.html. [Accessed: 25-Jul-2019].

[11] GoAnywhere, “Planes de respuesta ante incidentes de seguridad informatica | Templates y recursos,” *14-11*, 2017. [Online]. Available:

https://www.goanywhere.com/es/blog/plan-de-respuesta-a-incidentes-de-seguridad-informatica. [Accessed: 30-Sep-2019].

[12] Universidad Estatal Peninsula De Santa Elena, “Soporte Informático UPSE.” [Online]. Available: http://www.upse.edu.ec/soporte/. [Accessed: 24-Jul-2019].

[13] M. Tim, “Complete Guide to CSIRT: How to Build an Incident Response Team,” *19-07*, 2018. [Online]. Available: https://www.exabeam.com/incident-response/csirt/. [Accessed: 30-Sep-2019].

[14] FACSISTEL-UPSE, “LÍNEAS DE INVESTIGACIÓN.” [Online]. Available: http://facsistel.upse.edu.ec/index.php?option=com_content&view=article&id=58&Itemid=463. [Accessed: 03-Jun-2019].

[15] G. Lebet, “Técnicas de recolección de datos. Preparación de la Entrevista,” p. 9, 2016.

[16] NIST 800-115, “Technical Guide to Information Security Testing and Assessment,” *Nist Spec. Publ.*, vol. 800, pp. 1–80, 2008.

[17] Kendall Kenneth and Kendall Julie, *Análisis y Diseño de Sisyemas*. 2005.

[18] F. Ruiz, *Ingeniería Del Software I*. 2012.

[19] B. Rodríguez, “Plan de Seguridad informática para la red de datos de la Cooperativa San José de Montalvo,” 2017.

[20] ISO/IEC 27000, “Information technology — Security techniques — Information security management systems — Overview and vocabulary,” *ACM Work. Form. Methods Secur. Eng. DC, USA*, vol. 34, no. 19, pp. 45–55, 2018.

[21] EcuRed, “Aplicación web.”

[22] N. Brownlee and E. Guttman, “Expectations for Computer Security Incident Response,” 1998.

[23] J. I. Verdú Fernández, “Plan de contingencia de tecnologías de la información en entornos distribuidos,” 2015.

[24] L. Pilay and B. Iñiguez, “Implementación De Un Sistema Help Desk En Linux Para Gestionar Incidentes Informáticos Para La Nube Interna De La Carrera De Ingeniería En Sistemas Computacionales,” 2013.

[25] D. F. Caicedo Nuñez, “Diseño de un plan estratégico de continuidad de servicios universitarios en casos excepcionales para la PUCE sede Ambato,” 2019.

[26] P. G. D. E. Incidentes, “Plan gestion de incidentes.”

ANEXOS

Anexo 1: Formato para el cuestionario

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE TECNOLOGÍA DE LA INFORMACIÓN

CUESTIONARIO PARA ESTUDIANTES Y DOCENTES DE FACSISTEL

1. **¿Tiene conocimiento básico de buenas prácticas de seguridad informática?**
   - Si
   - No
2. **Seleccione que equipos informáticos es el que más utiliza dentro de la facultad de sistemas y telecomunicaciones.**
   - Equipos informáticos de los laboratorios de la facultad
   - Equipos informáticos personales
3. **¿Has sufrido incidentes informáticos en los laboratorios de la facultad o en sus equipos informáticos?**
   - Si
   - No
4. **¿Qué medio usa actualmente para comunicarse con el área de servicios TIC cuando necesita ayuda ante una situación de incidencia informática?**
   - Correo electrónico
   - Teléfono
   - Herramienta especializada de gestión de incidencias
   - De manera personal

5. **A partir de que usted comunica su incidencia, ¿cuánto tiempo transcurre hasta que el servicio técnico lo contacta?**
    - De 0 a 10 minutos
    - De 11 a 20 minutos
    - De 21 a 30 minutos
    - Más de 30 minutos
6. **¿Cuánto tiempo toma al departamento de TIC en atender sus requerimientos?**
    - 30 minutos
    - 1 hora
    - 2 horas
    - Más de 2 horas
7. **¿Estaría de acuerdo en utilizar una plataforma web para solicitar ayuda ante un personal capacitado si esto implica una mejora en el tiempo de atención y satisfacción en una situación de incidencia informático?**
    - Si
    - No

Anexo 2: Formato para la creación del CSIRT-UPSE

NORMA RFC 2350 | CSIRT

1. Información del Documento

1.1. Fecha de la última actualización: lunes, 24 de junio de 2019

1.2. Listas de Distribución:

Actualmente del CSIRT-UPSE no usa ninguna lista de distribución acerca de los cambios de este documento.

1.3. Ubicación del Documento: La versión actual del documento está disponible en el sitio web del CSIRT-UPSE.

1.4. Autenticación del Documento: No disponible

2. Información de Contacto

2.1. Nombre del Equipo:

CSIRT-UPSE, **Equipo de Respuesta a Incidentes de Seguridad Informática de la Universidad Estatal Península de Santa Elena**.

2.2. Dirección:

Universidad Estatal Península de Santa Elena, Dirección de Tecnologías de Información y Facultad de Sistemas y Telecomunicaciones a través del Equipo de ciberseguridad, Riesgos y Auditoría forense, CSIRT-UPSE

Avenida Eleodoro Solorzano, vía La Libertad Santa Elena

La Libertad- Santa Elena

Ecuador

2.3. Zona Horaria:

América/Guayaquil (UTC-GMT -0500)

2.4. Número de Teléfono:

+593 (04) 2781732

+593 (04) 2781738

2.5. Número de Fax: No disponible

2.6. Otras Comunicaciones: No disponible

2.7. Dirección de Correo Electrónico:

Dirección oficial <csirt@upse.edu.ec> revisada y atendida por algunos de los miembros del equipo

2.8. Llaves Públicas y encriptación de información: No disponible

2.9. Miembros del Equipo:

MSIA. Daniel Quirumbay Yagual coordinador y contacto del CSIRT-UPSE, dquirumbay@upse.edu.ec
GPG: 0xA9CC038C
MGTI. Omar Orrala, apoyo CSIRT-UPSE y contacto del CSIRT-UPSE, omarorrala@upse.edu.ec
MSIA. Wellington Robys, apoyo CSIRT-UPSE, wrobys@upse.edu.ec
MSIA. Fabricio Ramos, apoyo CSIRT-UPSE, framos@upse.edu.ec
MSIA. Iván Coronel S., apoyo CSIRT-UPSE, icoronel@upse.edu.ec

2.10. Más Información:

Información general acerca del CSIRT-UPSE, recomendaciones de seguridad y más puede encontrarla en http://csirt.upse.edu.ec

2.11. Horario de Atención: de lunes a viernes de 8:30 – 12:30 y de 15:00 – 17:00.

2.12. Puntos de contacto para clientes: Para comunicarse con el CSIRT-UPSE acerca de información de vulnerabilidades o alertas de seguridad, puede utilizar medios como correo electrónico, teléfono o fax.

Correo electrónico: csirt@upse.edu.ec

Url: http://csirt.upse.edu.ec

3. Constitución

3.1. Misión

"Prevención de incidentes de ciberseguridad en la UPSE, así como promover concienciación sobre la seguridad de la información."

3.2. Comunidad a la que brinda Servicios

Todos los funcionarios de las diferentes áreas y estudiantes de la UPSE

3.3. Patrocinio / Afiliación

El Equipo CSIRT – UPSE, es patrocinado por la Universidad Estatal Península de Santa Elena – a través de la Facultad de Sistemas y Telecomunicaciones (FACSISTEL) y la Dirección de Tecnologías de la Información (TIC-UPSE)

Además de Mantener contacto con diferentes equipos nacionales e internacional CSIRT y CERT de acuerdo con sus necesidades y cultura de intercambio, como por ejemplo CSIRT CEDIA.

3.4. Autoridad

El CSIRT-UPSE opera bajo el auspicio y con autoridad compartida de la Facultad de Sistemas y Telecomunicaciones y la Dirección de Tecnologías de la Información (TIC) de la Universidad Estatal Península de Santa Elena.

CSIRT-UPSE coopera con los administradores y usuarios de sistemas, dentro de lo posible evita relaciones de autoridad o formación de cadenas de mando. Sin embargo, en caso de ameritar la situación, CSIRT-UPSE buscara que las autoridades de la Dirección de Tecnología de la Información y la Facultad de Sistemas y Telecomunicaciones ejerzan su autoridad de forma directa o indirecta.

4. Políticas

4.1. Tipo de Incidentes y nivel de Soporte

El Equipo CSIRT-UPSE se encarga de manejar y dar solución a los incidentes relacionados con ciberseguridad, riesgos informáticos que sean reportados por los administradores de los servicios críticos de la Universidad, y los reportes de usuarios que sean escalados desde el área de Mesa de Servicios de TIC.

El nivel de apoyo que brinde el CSIRT-UPSE y el tiempo de respuesta del mismo, dependerá de la gravedad del incidente de ciberseguridad reportado, la carga de trabajo del equipo y la integridad de la información disponible. La gravedad de los mismos se determinará haciendo uso de criterios establecidos por el CSIRT-UPSE, la respuesta se realizará en base a uso y manejo de una metodología para el manejo de incidentes relacionados con seguridad informática o información. Cuando sea necesario el CSIRT-UPSE proporcionará la información necesaria a los administradores de los sistemas acerca de las medidas de seguridad que deben tomar en cuenta en las actividades que realizan.

Es responsabilidad del CSIRT-UPSE mantener informada a la comunidad universitaria acerca posibles vulnerabilidades antes de que están sean explotadas, para esto están disponibles los reportes de vulnerabilidades emitidos por el CSIRT-UPSE, y los boletines de alertas y advertencias emitidos por otros CSIRT o proveedores de aplicaciones a través de su portal Web.

4.2. Cooperación, Interacción y divulgación de la Información

La información será manejada con absoluta confidencialidad de acuerdo con las políticas y procedimientos para la Gestión de Incidentes establecidos para el CSIRT

y de las políticas y normas de la UPSE, en el caso de que se proceda a publicar la información esta será previa autorización de los dueños de la misma, en el caso que esto se incumpla el caso será manejado de acuerdo a las políticas establecidas por la Universidad y en el Equipo para estos casos.

4.3. Comunicación y Autenticación

Los emails no encriptados no serán considerados suficientemente seguros, pero serán adecuados para la transmisión de información poco sensitiva.

5. Servicios

5.1. Respuesta a Incidentes

CSIRT UPSE apoyará a los administradores en el manejo de aspectos técnicos y organizacionales de los incidentes de ciberseguridad. En particular proveerá asistencia o aviso referente a los siguientes aspectos del manejo de incidentes:

Servicios **Reactivos**

- Alertas y avisos
- Manejo de Incidentes
    - Análisis de Incidentes
    - Respuesta a incidentes in-situ
    - Apoyo en respuesta a incidentes
    - Coordinación en respuesta a incidentes
- Manejo de vulnerabilidades

Los servicios **proactivos** que se brindarán en el Equipo CSIRT-UPSE son:

- Servicios de Detección de Intrusiones
- Definición de políticas de seguridad.
- Vigilancia Tecnológica
- Auditorías o evaluaciones de seguridad
- Configuración y mantenimiento de Herramientas de Seguridad, Aplicaciones e Infraestructuras
- Servicios de Detección de Intrusos
- Diseminación de Información relacionada con la Seguridad

5.2. Servicios de Gestión y Calidad de la Seguridad

- Concientización sobre seguridad digital
- Educación y entrenamiento en seguridad digital
- Consultoría de Seguridad informática

5.2.1. Investigación inicial de incidentes

- Investigar si en efecto un incidente ha ocurrido
- Determinar el alcance del incidente

- Signos indicadores y precursores, análisis de riesgo

5.2.2 Coordinación de incidentes

- Determinar la causa inicial del incidente (vulnerabilidad explotada).
- Facilitar contacto con otros sitios que pueden haber estado involucrados.
- Crear reportes para otros CSIRTs.
- Preparar anuncios a usuarios, si aplicara.

5.2.3 Resolución de incidentes

- Eliminar la vulnerabilidad
- Apoyo en el aseguramiento de sistemas derivados de lo aprendido en el incidente.
- Evaluar si ciertas acciones pueden arrojar resultados en proporción con su costo y riesgo, en particular acciones dirigidas a un eventual proceso judicial o acción disciplinaria: recolección de evidencias luego del hecho, observación de un incidente en progreso, plantando trampas al intruso, etc.

6. **Formas de notificación de incidentes**

Para realizar el reporte de incidentes debe utilizar los formatos elaborados por el Equipo CSIRT-UPSE, los mismos que se pueden obtener en el Equipo CSIRT-UPSE o en el portal web del equipo.

7. Disclaimer

El Equipo CSIRT-UPSE no se responsabiliza por el mal uso que se dé a la información aquí contenida.

Anexo 3: Cuadro comparativo de Herramientas Help Desk

HERRAMIENTAS			
CARACTERÍSTICAS	**REQUEST TRACKER**	**OTRS**	**OSTICKET**
Campos personalizables	√	√	√
Búsqueda de texto completa	√	√	√
Utilizado para grandes empresas	√	X	√
Software basado en web	√	X	√
Integración de correo electrónico	√	√	√
Gestión de incidentes / solicitudes	√	√	X
Base de datos de conocimiento	√	√	√

Anexo 4: Constitución del equipo de respuesta a incidencia

TAREA	QUIEN LO HACE	CUANDO LO HACE
Notificar los incidentes de seguridad informática o las actividades sospechosas.	Usuario sensibilizado, o Administrador de TI	Instantáneamente tiene conocimiento del incidente
Registro del incidente o acontecimiento	Primer punto de contacto	En el instante del reporte del incidente o evento
Detectar el tipo de incidente	Primer punto de contacto	Instantáneamente al reporte del incidente y de acuerdo con la tabla de tiempos de respuesta
Escalar el incidente	Primer punto de contacto	Instantáneamente al reporte del incidente de acuerdo con la tabla de tiempos de respuesta
Utilizar la estrategia de contención	Administrador de los sistemas de Seguridad, Administrador del Sistema	Inmediato al reporte del incidente
Recolectar la evidencia	Administrador del Sistema	Desde el conocimiento del incidente
Manejo de la evidencia	Administrador del Sistema	Al cierre del proceso
Evaluar el impacto	CSIRT	Según la tabla de tiempos de respuesta
Verificar existencia de recursos	Administrador de los sistemas de Seguridad, Administrador del Sistema	Instantáneamente luego de la delegación
Aplicar la estrategia de erradicación	Administrador de los sistemas de Seguridad, Administrador del Sistema	Según la tabla de tiempos de respuesta
Comunicar a los usuarios	Primer punto de contacto	Una vez de conozca la disponibilidad de recursos.
Aplicar la estrategia de recuperación	Administrador de los sistemas de Seguridad, Administrador del Sistema	De acuerdo con la tabla de tiempos de respuesta
Comunicar el restablecimiento del servicio	Primer punto de contacto	Instantáneamente a la terminación de las

		acciones de restauración
Pruebas	Administrador del Sistema	Instantáneamente a la terminación de las acciones de rehabilitación
Retroalimentación	Primer punto de contacto	Instantáneamente a la terminación de las pruebas
Cerrar el proceso	Primer punto de contacto	Posterior a las pruebas de satisfacción

Anexo 5: Clasificación y tratamiento de incidentes

CLASIFICACIÓN Y TRATAMIENTO DE INCIDENTES			
INCIDENTE	**CONCEPTO**	**TIPO DE INCIDENTE**	**MITIGACIÓN**
Denegación de servicios	La denegación de servicio o DoS (Denial of Service) se define como la imposibilidad de acceder temporal o permanentemente a un recurso o servicio por parte de un usuario legítimo. Existen dos tipos de incidentes: **DoS:** son aquellos causados por el número de peticiones realizada desde una misma máquina. **DDoS:** se realizan peticiones o conexiones empleando un gran número de ordenadores.	• Tiempo de respuesta fuera de lo normal. • Interrupción de servicios tecnológicos. • Ataques a través de equipos bots o zombis. • Consumo de recursos computacionales • Sobrecarga del servidor de correo y/o de las redes afectadas.	**Contención** • Bloquear los paquetes de ataque. • Cambiar URL de las páginas • Detener las IPs inválidas. • Detener los floods en los protocolos TCP/UDP. • Detener los procesos no deseados en los servidores y enrutadores. **Erradicación** • Solicitar ayuda al proveedor de servicios de internet (ISP) para bloquear el trafico más cercano a su origen **Recuperación** • Volver el servicio a su estado original
Código malicioso	El software malicioso puede modificar el funcionamiento de un	• Virus informáticos • Gusanos • Troyanos	**Contención** • Aislar el equipo de la red **Erradicación**

	equipo informático o alterar la información que procesa, ya sea borrándola, modificándola o enviándola sin conocimiento a terceras personas.	• Spyware • Adware • Hijacking • Ransonware	• Eliminar los códigos maliciosos detectados • Corregir los efectos que se produjo • Mejorar las defensas • Instalación de parches **Recuperación** Restauración de backups
Acceso no autorizado	Un ataque de acceso no autorizado es un incidente que permite el acceso a utilizar cuentas web, bases de datos confidenciales y demás información. Involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada a un sistema o aplicación.	• Obtención de cuentas de usuarios y contraseñas • Ataques de fuerza bruta • Consultas no autorizadas • Divulgaciones de información no autorizada • Creación de cuentas de usuarios	**Contención** • Bloquear las cuentas • Apagar el sistema **Erradicación** • Cambiar contraseñas • Implementar bloqueos de excesos de intento automáticamente • Usar contraseñas robustas • Control de acceso en el firewall **Recuperación** • Habilitar el sistema • Habilitar las cuentas del usuario
Reconocimiento	Es el proceso en el que se analiza los puertos de una máquina conectada a la red con la finalidad de verificar cuáles puertos están abiertos, cerrados o cuenta con algún protocolo de seguridad, el resultado de	• Escaneo de puertos	**Contención** • Identificar el puerto • Cerrar el puerto **Erradicación** • Agregar reglas al firewall **Recuperación** • Abrir el puerto

	este análisis permitirá que los intrusos puedan saber información como la composición de nuestra arquitectura, el sistema operativo de nuestros ordenadores y los posibles agujeros de seguridad que luego serán explotados por los atacantes.		
Modificación de recursos no autorizados	Incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.	• Borrado, modificación o eliminación de la información • Modificación, instalación o eliminación no autorizada de software	**Contención** • Bloquear la cuenta **Erradicación** • Corregir los efectos producidos en los sistemas • Sustituir los archivos comprometidos **Recuperación** • Restaurar copias de seguridad
Vandalismo	Cambio o daño de la información o los recursos informáticos, así mismo afectar los servicios de una institución de manera intencional	• Modificación del sitio web • Inyección de scripts	**Contención** • Deshabilitar los servicios afectados **Erradicación** • Reparar el servicio afectado • Aplicar parches de seguridad **Recuperación**

			• Restaurar los servicios • Restauración de backups
Daños físicos	Circunstancia del entorno que causan daños a los recursos informáticos ya sea de manera natural, por el hombre o averías del hardware	• Temblores, terremotos • Fuego • Inundaciones • Fallos en el suministro eléctrico	**Contención** • Cortar el suministro eléctrico • Usar extintores **Erradicación** • Reparación técnica de los equipos informáticos • Restaurar copias de seguridad **Recuperación** • Reinstalar los equipos informáticos y dejar en funcionamiento
Uso inapropiado de recursos	Involucra a una o varias personas que viola las políticas de la institución del uso de los recursos informáticos	• Fuga de información • Alteración de la información • Alteración de los servicios de la red • Abuso de privilegios • Robo de información • Robo de equipos informáticos	**Contención** • Identificar el atacante • Bloquear el usuario **Erradicación** • Reconfigurar la seguridad de la base de datos • Informar a recursos humanos **Recuperación** • Habilitar el sistema • Restauración de backups • Restauración de los componentes informáticos

Anexo 6: Prioridad de incidencias de seguridad en elementos informáticos

Elementos informáticos	Prioridad	
Acceso a sistemas	03,75 – 05,00	3
Servidores	08,00 – 10,00	1
Computadoras, laptops	05,25 – 07,99	2
Backups	08,00 – 10,00	1
Redes	08,00 – 10,00	1
Base de datos	08,00 – 10,00	1
Módems	08,00 – 10,00	1
Página web	05,25 – 07,99	2
Servicios web	05,25 – 07,99	2

Anexo 7: Reporte Urkund

La Libertad, 07 de octubre del 2020.

Ing. Freddy Villao S.
Director (E) de Carrera
En su despacho.

Por medio de la presente me es muy grato saludarle y poner a su disposición el resultado del análisis del software anti-plagio URKUND del documento con el tema de titulación “Plan de respuesta a incidencias de seguridad informática (IRP) para la Dirección de Tecnologías de la información de la UPSE”, correspondiente a la Sr. ROSALES REYES JESUS DANIEL, estudiante de la Carrera de Tecnología de la Información.

URKUND

Document Information

Analyzed document	PROPUESTA TECNOLOGICA JesusRosales.docx (D80782513)
Submitted	10/5/2020 10:26:00 PM
Submitted by	DANIEL IVAN QUIRUMBAY YAGUAL
Submitter email	dquirumbay@upse.edu.ec
Similarity	1%
Analysis address	dquirumbay.upse@analysis.urkund.com

LSI. Daniel Quirumbay Yagual, MSIA
Docente Tutor

C.C.: Dirección Carrera Informática, Archivo