UNIVERSIDAD TÉCNICA DEL NORTE FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"DISEÑO DE UN CENTRO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) ACADÉMICO EN LA UNIVERSIDAD TÉCNICA DEL NORTE"

AUTOR:

Jonathan Alejandro Mera Terán

DIRECTOR:

MsC. Edgar Alberto Maya Olalla

Ibarra – Ecuador

2021

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100367712-5		
APELLIDOS Y NOMBRES:	MERA TERÁN JONATHAN ALEJANDRO		
DIRECCIÓN:	Cdla. PILANQUÍ		
EMAIL:	jamerat@utn.edu.ec		
TELÉFONO FIJO:	062952895	**TELÉFONO MÓVIL:**	0997232142

DATOS DE LA OBRA	
TÍTULO:	DISEÑO DE UN CENTRO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) ACADÉMICO EN LA UNIVERSIDAD TÉCNICA DEL NORTE
AUTOR (ES):	MERA TERÁN JONATHAN ALEJANDRO
FECHA: DD/MM/AAAA	23/07/2021
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
ASESOR /DIRECTOR:	MAYA OLALLA EDGAR ALBERTO MSc.

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 23 días del mes de JULIO de 2021

EL AUTOR:

.....
Jonathan Alejandro Mera Terán

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Msc. EDGAR ALBERTO MAYA OLALLA, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN

CERTIFICA:

Que, el presente trabajo de Titulación "DISEÑO DE UN CENTRO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) ACADÉMICO EN LA UNIVERSIDAD TÉCNICA DEL NORTE", ha sido desarrollado por el señor Mera Terán Jonathan Alejandro bajo mi supervisión

Es todo en cuanto puedo certificar en honor de la verdad.

.....

Msc. Edgar Alberto Maya Olalla

cédula

DIRECTOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

El agradecimiento primero va dirigido a Dios, a la Virgen Dolorosa, a mis padres y esposa que jamás permitieron que bajara los brazos en el transcurso del presente trabajo, siempre estuvieron de cerca brindándome todo el apoyo.

También quiero reconocer la labor de mi tutor, el Ingeniero Edgar Maya, que, sin su apoyo, este trabajo no hubiese salido adelante, además es importante el reconocimiento a mis asesores de tesis, el Ingeniero Mauricio Domínguez y el Ingeniero Fabián Cuzme.

Y agradezco a todos y cada uno de mis profesores, que en el transcurso de la carrera aportaron con sus conocimientos y así poder ser un excelente profesional, lleno de conocimientos, ética, valores y sobre todo capaz para asumir cualquier reto que se me presente en la vida

Por otro lado, un especial agradecimiento a las personas que me brindaron las facilidades para obtener información y poderme guiar en el transcurso de esta etapa uno de ellos es el Ingeniero Vinicio Guerra, quién me brindo información importante, así como a la Ingeniera Mirian López del EcuCERT e Ingeniero Ernesto Pérez del CSIRT de CEDIA.

Finalmente, también quiero agradecer a mis dos amigos y compañeros, Israel Gudiño y Mario Guerra, que juntamente desarrollamos un sin número de trabajos y proyectos, siempre brindándonos un apoyo incondicional.

Jonathan A. Mera

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

El presente trabajo de titulación es dedicado primero a Dios y a la madre Dolorosa, como parte de una etapa de mi vida, que sin su bendición no podría haber sido realizado, además, con mucho amor, la dedicación va dirigida a mis padres Raúl Mera, Carlota Terán, Abuelita Norma Hernández y mi esposa Jennifer Flores, que me apoyaron durante todo el proceso, así como también a mis tías Aracely y Miriam que desde el cielo sé que siempre estuvieron intercediendo por mí.

Jonathan A. Mera

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

RESUMEN

En el presente trabajo se realiza el Diseño de un Centro de Respuesta de Incidentes de Seguridad Informática del tipo académico para la UTN, el mismo que se encargará de brindar apoyo y solución ante la presencia de incidentes de seguridad informática, en el diseño se define los servicios que el CSIRT-UTN podría brindar en etapas iniciales, entre los que destacan son la gestión de incidencias, comunicados y concientización en temas de seguridad informática.

Este diseño es realizado con la finalidad de que en un futuro se implemente el CSIRT-UTN, para lo cual se deja estableciendo el plan estratégico, con el cual se puede proceder a la segunda etapa que es la implementación. Dentro del plan estratégico se establece la razón de ser del CSIRT-UTN, los objetivos estratégicos que permitirán llevar con éxito la implementación del mismo, así como las políticas necesarias, topología de red para que el CSIRT-UTN pueda comenzar a operar una vez que sea implementado.

Como parte del desarrollo del presente trabajo se procedió a realizar una prueba de funcionamiento básico del CSIRT, en el cual se tiene la parte del análisis de vulnerabilidades con NMAP, monitorización de red con NAGIOS, y la notificación de incidentes mediante OTRS, como servicio de mesa de ayuda, permitiendo observar el funcionamiento básico del Centro de Respuesta de Incidentes de Seguridad Informática.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

ABSTRACT

In this research, the Design of an Academic Type of Information Security Incident Response Center for "Técnica del Norte" is carried out, which will be responsible for providing support and resolution in the presence of computer security incidents. The design defines the services that CSIRT-UTN could provide in the early stages, among which are incident management, communications, and awareness of computer security issues.

This design is carried out to implement the CSIRT-UTN in the future, for which the strategic plan is left establishing, which serves as the basis for its subsequent implementation. Within the strategic plan the reason to be of the CSIRT-UTN is established, the strategic objectives that will allow the successful implementation of the same, as well as the necessary policies based on norms, standards, and codes of good practices such as ISO/IEC 27002, ITIL V4, COBIT 2019, and the network topology so that the CSIRT-UTN can start to operate once be implemented.

As part of this work, a basic functioning test of the CSIRT was carried out, which includes the vulnerability analysis part with NMAP, network monitoring with NAGIOS, and the notification of incidents through OTRS, as a service of the help desk, allowing to observe the basic operation of the Computer Security Incident Response Center.

CAPÍTULO I ANTEPROYECTO

El presente proyecto de investigación, cuyo tema es el Diseño de un CSIRT Académico en la Universidad Técnica del Norte (UTN), contiene en el primer capítulo el anteproyecto, en el cual se informa acerca de la problemática del estudio, haciendo mención a la situación actual de la seguridad informática en la UTN, que en los últimos se ha visto amenazada de ciertas incidencias como Botnets y ataques de denegación de servicio en sus servidores afectando a la seguridad de la red.

Esta problemática abarca objetivos, alcance y justificación, donde sus objetivos específicos son cuatro siendo los más relevantes: el análisis de la seguridad informática y de incidencias en la UTN, requerimientos estratégicos y de diseño, requerimientos normativos y de estándares de diseño y funcionamiento, como también los requerimientos de infraestructura y equipos, para finalmente elaborar la propuesta de prueba piloto del CSIRT Académico para evaluar su eficiencia en el monitoreo y respuesta de incidencias que suceden en el sistema informático en tiempo real (Garrido, 2007).

El alcance es el dimensionamiento de cada objetivo explicado más profundamente, el contexto evalúa las investigaciones anteriores y actuales sobre el tema del proyecto, y finalmente, la justificación, que es un bosquejo de los aspectos que respaldan el desarrollo de este proyecto, donde se resalta el hecho de que el diseño de un CSIRT ayudará en la gestión y respuesta de incidencias en la UTN.

1.2 ANTECEDENTES

El Centro de Respuesta a Incidentes Informáticos, es un equipo que se encarga de proveer servicios y apoyo para prevenir, gestionar y responder incidentes de seguridad de la información, que se presentan en una organización, cuyo direccionamiento se basa en la aplicación de normas y estándares como la ISO/IEC 27002 “Código de buenas prácticas para

la gestión de seguridad de la información", ISO/IEC 27035 "Gestión de incidentes de seguridad de la información", la NIST 800-61 "Guía de Seguridad para la Gestión de Incidentes", ITIL V4 "Gestión de servicios de tecnologías de la información" y publicaciones del CERT/CC.

Existen varias denominaciones para este centro de respuesta, tales como Equipo de Respuesta a Incidentes (IRT), Equipo de Respuesta a Incidentes Informáticos (CIRT), Capacidad de Respuesta a Incidentes Informáticos (CIRC), Equipo de Respuesta a Incidentes de Seguridad (SIRT), Equipo de Respuesta a Incidentes de Seguridad informática (CSIRT): y Equipo de Respuesta a Emergencias Informáticas (CERT), siendo los más usados IRT y CSIRT (Radical Company, 2001).

Los tipos de CSIRT, más utilizados en el Ecuador son: CSIRT académico, CSIRT público y CSIRT nacional, con un total de 14 CSIRT para el año 2018, entre ellos, los más importantes son: CSIRT CEDIA, EcuCERT, CSIRT CELEC EP, CSIRT Telconet, CSIRT EPN y CSIRT UTPL; cuyos objetivos son la planificación, gestión, retroalimentación y comunicación de incidentes, siendo las organizaciones con las cuales mantienen relaciones de confianza el FIRST: Foro de Respuesta a Incidentes y Equipos de Seguridad, OAS: Organización de Estados Americanos, ITU-D: Sector de Desarrollo de las Telecomunicaciones, IMPACT: Servicios de Seguridad Impacto y AP-CERT: Equipo de Respuesta a Emergencias Informáticas de Asia y el Pacifico (Csirt Cedia, 2019).

1.3 PROBLEMÁTICA

En la Universidad Técnica del Norte, debido a que actualmente su infraestructura de red no posee un sistema de seguridad perimetral de última generación presenta una brecha de seguridad en la red, generando impactos negativos dentro de la red de la UTN, según la entrevista realizada al personal de la Dirección de Desarrollo Tecnológico e Informático

(DDTI), se han presentado periódicamente incidentes de seguridad informática, lo que ha causado que sus equipos y red sean cada vez más vulnerables de ataques, estos ataques aproximadamente se presentan en una frecuencia de dos veces por mes durante el año, donde los ataques de mayor impacto fueron causados por botnets, malware, spam y ataque de denegación de servicios que afectaron a equipos y servidores web, inclusive causando la saturación del CPU del Firewall provocando la perdida de conectividad.

Por otra parte, el DDTI de la UTN no cuenta con personal que se encargue específicamente de la gestión de estos incidentes de seguridad informática, ya que en la actualidad el personal del DDTI realiza muchas funciones dentro de la dirección, siendo su labor polifuncional, por tal motivo no se maneja de una manera rápida y eficaz en cuanto al manejo y gestión de incidencias y vulnerabilidades (Garrido, 2007).

La presente propuesta consiste en el diseño de un Centro de Respuesta a Incidentes Informáticos (CSIRT) Académico, sin fines de lucro, para la Universidad Técnica del Norte (UTN), el mismo que brindará servicios de detección y respuesta a incidentes de seguridad de la información, como es la búsqueda y mitigación de ataques informáticos a los servidores, sistemas operativos, cuya comunidad objetivo será el personal administrativo, de redes, docentes y estudiantes de las distintas facultades y escuelas que conforman el campus universitario de la UTN.

El CSIRT académico se lo ubicará en la UTN, por ser un punto de contacto desde el cual este equipo operará, beneficiando a su comunidad académica, con servicios especializados operados por personal experimentado con la finalidad de que este equipo esté capacitado para responder de forma inmediata cada incidencia presentada en los sistemas informáticos y equipos que afectan sus áreas de trabajo en cada facultad o área administrativa de la UTN.

1.4 OBJETIVOS

1.4.1 Objetivo General

Diseñar un Equipo de Respuesta de Incidentes de Seguridad Informática (CSIRT) Académico, utilizando normas, estándares y procedimientos de creación de un CSIRT para brindar servicios de prevención, detección, identificación, manejo y recuperación de incidentes de seguridad informática que se presenten en la Universidad Técnica del Norte.

1.4.2 Objetivos Específicos

1. Analizar el esquema teórico de un CSIRT y la situación actual de la seguridad informática en la Universidad Técnica del Norte.
2. Definir los requerimientos para el diseño del CSIRT Académico en la Universidad Técnica del Norte.
3. Elaborar las políticas y procedimientos para el diseño del CSIRT Académico en la UTN.
4. Elaborar la propuesta de diseño del CSIRT Académico en la UTN.

1.4.3 Alcance

El diseño de un Centro de Respuesta a Incidentes Informáticos (CSIRT) Académico, para la Universidad Técnica del Norte, se elaborará en base al documento publicado por el CERT/CC y el Instituto de Software de la Universidad de Carnegie Mellon, en el que se hace referencia a ocho pasos básicos para el diseño de un CISRT, con los cuales se define el alcance de esta investigación, que dimensiona el estudio bibliográfico de un CSIRT, el análisis de toda la información relevante sobre la gestión de incidencias de seguridad informática en la UTN, requerimientos y la presentación de la propuesta de diseño.

El primer objetivo, está enfocado al estudio teórico de un Equipo de respuesta a Incidentes de Seguridad y al análisis de la situación actual de la gestión de incidentes de seguridad informática realizado por el personal administrativo y docente en la UTN. Para el desarrollo de la fundamentación teórica, se realizará la investigación bibliográfica sobre los diferentes tipos, funciones, estructura, la forma en la que están constituidos los Equipos de Respuesta a Incidentes de Seguridad, en donde se analizará el Manual de diseño de un CSIRT publicado por el CERT/CC, *"además se definirán aquellas normas y estándares con los cuales se van a elaborar las políticas y procedimientos de gestión de incidentes de seguridad para el CSIRT Académico en la UTN, como es la norma ISO/IEC 27002, la norma RFC 2350, los estándares ITIL V4 y COBIT 2019"* (Muñoz y Rivas, 2015).

Como segundo objetivo se va a definir los requerimientos para el diseño de un CSIRT Académico, que comprende la metodología de dos fases que son la fase de Planeamiento estratégico y la fase de Diseño. La primera fase de Planeamiento estratégico comprende la elaboración del Plan estratégico y Plan Operativo Anual (POA) para el CSIRT Académico, en donde el Plan Estratégico, va a definir requisitos como: personal que conformará el CSIRT Académico, misión, objetivos estratégicos, relación con otros equipos, normas y estándares que darán cumplimiento a los objetivos y metas trazadas del proyecto.

En el POA se definirá aquellas actividades que van a realizar los responsables y personal del CSIRT Académico en base a los objetivos estratégicos determinados en el Plan Estratégico, el cual permitirá la mejora de procesos, tomando en cuenta las expectativas de desarrollo futuro que tendrá el CSIRT Académico, durante su proceso de creación en la UTN, y así poder optimizar su infraestructura, procesos y servicios, para la comunidad objetivo en esta institución.

El personal que conformará el CSIRT Académico, se definirá a través de procesos de selección y contratación, donde se crearán perfiles de cargo con requerimientos para los diferentes cargos, luego se aplicarán procesos de contratación, y se establecerán funciones y responsabilidades para cada cargo. La misión comprende definir lo que pretende realizar el CSIRT a corto plazo es decir al inicio de sus operaciones de seguridad en la UTN, para lo cual se consideran aspectos como servicios, políticas y procedimientos.

Como objetivos estratégicos se elaborarán aquellos que permitan la recuperación y mitigación de incidentes. Luego se agendarán reuniones con otros CSIRT, para establecer un diseño adecuado a las nuevas exigencias en lo que respecta a centros de incidencias de seguridad informática.

En lo que respecta a la selección de normas y estándares, se tomará en cuenta aquellos que permitan el desarrollo de procesos y procedimientos de respuestas a incidentes con los cuales los servicios que brindará el CSIRT cumplirán con su gestión, donde se analizarán normas como la ISO/IEC 27002 (gestión de incidentes de seguridad de la información) y la RFC 2350, con las cuales se podrán determinar los procedimientos y políticas de gestión de incidentes, y estándares como el ITIL V4 y COBIT 2019, con los cuales se definirán las políticas de respuesta de incidencias y políticas para la gestión de servicios CSIRT (Hinson, Deura, Marappan, Vergara, & Regalado, 2007).

La segunda fase de diseño, se definen requisitos para crear el CSIRT Académico tales como: tipos de servicios que se van a brindar, estructura organizacional del CSIRT Académico en la UTN, organigrama posicional, así como su infraestructura y equipamiento. En lo que se refiere a la definición de los tipos de servicios de gestión de incidentes que brindará el CSIRT Académico para la comunidad de la UTN, estos se realizará partiendo de las respuestas obtenidas de las encuestas aplicadas al administrador de red, personal

administrativo, docentes y estudiantes de la UTN, donde se conocerá la situación actual de la seguridad informática, con respecto a incidencias que atacan los sistemas informáticos y la forma como manejan los riesgos, herramientas utilizadas para su detección, y métodos para eliminar estas incidencias.

Luego se procederá a establecer la estructura organizacional que tendrá el CSIRT Académico, con su ubicación en el organigrama de la UTN, dentro de la Dirección de Desarrollo Tecnológico e Informático (DDTI), donde se diseñará un flujograma distribuido con un área específica para el CSIRT Académico, y con este esquema poder elaborar el organigrama posicional donde se definirán los cargos del personal para el CSIRT.

El diseño de la infraestructura de red y equipos, se lo realizará basándose en la guía CSIRT del proyecto AMPARO, la cual informa acerca de ciertas recomendaciones en cuanto al ambiente físico, infraestructura de red, hardware, software, infraestructura de telecomunicaciones y diagramas de topologías de red, necesarios para que las operaciones del CSIRT Académico cumplan con los servicios de respuesta a incidentes y procedimientos de mitigación y control.

La elaboración del tercer objetivo comprenderá la elaboración de las políticas y procedimientos de gestión de incidentes de seguridad informática, para el CSIRT Académico, cuyo desarrollo se realiza a partir de los tipos de servicios de gestión de incidencias identificados anteriormente, en donde las políticas a elaborarse, garantizarán la integridad, confidencialidad y la disponibilidad de los datos, las cuales parten de estándares y procedimientos direccionados en base a los lineamientos de la Norma ISO 27002:2005, en su sección No 9 “Gestión de incidentes de seguridad de la información” donde las políticas que se tomarán en cuenta para el CSIRT Académico son políticas de clasificación, diseminación y comunicación de la información, políticas de seguridad y manejo de

Incidentes de Seguridad Local, las cuales se elaborarán tomando como base la información del marco normativo y de los servicios que ofrecerá el CSIRT Académico a la comunidad de la UTN.

Así para la diseminación y comunicación de la información en servicios y estructura del CSIRT a la comunidad de la UTN, se utilizará la guía RFC 2350, para formular las políticas de respuesta a incidentes se tomará como base los direccionamientos del estándar COBIT 2019 y para crear las políticas y procedimientos de gestión de incidentes se utilizará el estándar ITIL V4.

Además, se diseñarán los formularios para el registro y seguimiento de incidencias del CSIRT, cuyo esquema está conformado por campos para el registro de nombres de la persona que informa el incidente, datos de contacto, fecha del incidente, departamento u organización proveniente, información del incidente, aviso de políticas de privacidad y números de contacto del CSIRT de la UTN.

Dentro de este objetivo se elaborará el cronograma de implementación del CSIRT Académico, el cual servirá de base para la implementación en un futuro del CSIRT Académico, este cronograma se elaborará bajo el método de diagramación de precedencia (PDM), cumpliendo los parámetros de la guía de ENNISA, en el cual se detallarán las actividades en medidas de tiempo y el área encargada de realizarlo como: servicios, políticas, procedimientos, formularios de reporte de incidentes, infraestructura y equipos.

Para la propuesta de diseño de un CSIRT Académico en la UTN, se planificará el desarrollo de un modelo de prueba piloto para comprobar la eficiencia del CSIRT en cuanto al monitoreo y gestión de incidencias, para lo cual, se determinará la necesidad de un equipo independiente que puede ser virtualizado o físico, en donde se hará uso de software

opensource para analizar la seguridad en las redes, tales como: Nmap para el escaneo de puertos, Nagios para el monitoreo de redes alertando cuando exista una amenaza, Simprocess, como simulador de procesos basado en eventos durante la gestión de incidencias, que permitirá evaluar la eficacia en la resolución de incidentes informáticos, además OTRS (Open Tickets request System), que es un Sistema de solicitud de tickets utilizado por el CSIRT, que se lo va a utilizar para la gestión de incidentes informáticos, generando tickets para la evaluación o resolución de las incidencias informáticas.

1.5 JUSTIFICACIÓN

El diseño del CSIRT académico en la UTN contribuye al plan de la sociedad de la Información y el Conocimiento 2018-2021 del Ministerio de Telecomunicaciones y de la Sociedad de la Información, en el que en uno de sus programas denominado "Seguridad de la información y uso responsable de las TIC" busca trabajar en coordinación con las diferentes entidades del sector público y privado entre ellos el sector de la educación, fortaleciendo al EcuCERT que funciona como CERT nacional.

Siendo el CSIRT central de cada industria garantizando el intercambio de información, de esta manera se estaría fortaleciendo mecanismos de seguridad de la información, mediante estrategias de ciberseguridad cómo, medidas técnicas, desarrollo de capacidades, marco regulatorio, educación, concienciación pública y cooperación interna y externa, para articular los distintos sectores de la sociedad del país (Guaygua, 2018).

La realización del diseño de un CSIRT académico para la Universidad Técnica del Norte, aportará en la solución de incidencias que afectan la seguridad de la información al interior de la comunidad universitaria, sus sistemas informáticos y redes, cuya importancia radica en que este CSIRT Académico responderá a todas las incidencias reportadas, siendo un punto de contacto multilateral que resguardará la información digital, en donde a través de la

coordinación y apoyo multidisciplinario del personal administrativo, docente y alumnos de la UTN con otros equipos CSIRT nacionales e internacionales como el EcuCERT, CSIRT CEDIA, OAS, CSIRT/CC, etc., podrá responder con todas las incidencias reportadas en el menor tiempo posible mitigando así sus impactos en las operaciones normales de esta institución entre clientes y usuarios.

Se justifica la localización del CSIRT Académico en la UTN, ya que sus servicios y asistencia técnica al usuario y clientes apoyara la labor de prevención y mitigación desarrollada por le EcuCERT, dentro del Cantón de Ibarra, debido a que en esta ciudad no existe una organización de tales características, que opere en función de la seguridad informática de una universidad, donde las relaciones de confianza permitirán el intercambio de reportes de incidencia sucedidas en el ámbito universitario, métodos de prevención y control y formas de establecer planes de contingencia ante tales amenazas, optimizando la seguridad informática no solo de este cantón sino de toda la provincia de Imbabura.

La propuesta del diseño de un CSIRT académico para la UTN, presenta su factibilidad tecnológica, con su infraestructura de servicios de respuesta a incidencias, donde mediante objetivos estratégicos determinados en un Plan Operativo Anual, el CSIRT Académico, demostrara su eficiencia y eficacia operativa a través de un modelo de pruebas piloto donde se simulara la presencia de incidencias con el usos de varias herramientas de escaneo de vulnerabilidades, monitoreando en tiempo real la seguridad informática tanto en servidores como en equipos dentro de la red de datos e internet de la UTN.

Como parte de sus servicios prestados a la comunidad académica, el CSIRT Académico, aportara con jornadas de concienciación sobre seguridad informática a todo el personal administrativo y docente de la UTN, mediante la transmisión de consejos y notificaciones que pueden ser compartidos en redes sociales o en la misma página web institucional, entre

los cuales esta información acerca de que procedimientos de seguridad informática, se deberán aplicar para mantener libre de incidencias sus sistemas, reduciendo así con los tiempo de respuesta a estos ataques.

Así también proporcionará servicios de capacitación y formación a usuarios donde se impartirán talleres, cursos, seminarios acerca de procedimientos de seguridad de información y gestión de incidencias y vulnerabilidades, con los cuales el usuario podrá responder independientemente a una urgencia causada por un incidente en su sistema y así evitar que se incremente el riesgo en la UTN.

El estudio teórico y conceptual, para el diseño de un CSIRT académico en la UTN, permitirá el conocimiento pleno de aquellas características, ventajas, servicios, normas, estándares y documentos que dimensionan a un CSIRT académico, con los cuales se podrá direccionar el plan estratégico, plan operativo y diseño del CSIRT, con sus políticas y procedimientos.

La presente propuesta utilizará diferentes metodologías, normas y estándares para el diseño y funcionamiento del CSIRT Académico en la UTN, como son la norma ISO/IEC 27002:2005, estándares ITIL V4, COBIT 2019 y la norma RFC 2350; por medio de las cuales se definirán procedimientos, políticas y actividades de gestión de incidencias, con sus servicios reactivos y de gestión de calidad, como también aquellos pasos para comunicar acerca del funcionamiento del CSIRT en la UTN a los miembros de la comunidad académica (Andrade R. O., 2013).

CAPÍTULO II MARCO TEÓRICO

El segundo capítulo consiste en la investigación bibliográfica necesaria para estructurar los fundamentos teóricos de un Equipo de Respuesta de Incidentes de Seguridad Informática CSIRT, y como parte de esta información, se menciona el CSIRT Académico; así como la metodología, normas y estándares internacionales que direccionarán el diseño y operatividad, aplicados en el ámbito nacional.

2.1 Definición de CSIRT

De acuerdo con (Lanfranco y Pérez, 2019) un CSIRT (Computer Security Incident Response Team), es un equipo de respuesta a incidentes de seguridad informática, el cual ha sido creado como una organización encargada de brindar respuesta a las incidencias de seguridad informática de una comunidad objetivo, a través de la prestación de servicios preventivos, reactivos y de calidad en gestión de incidencias, basados en estrategias, métodos y herramientas informáticas, para disminuir o mitigar los riesgos e impactos de ataques informáticos.

En este sentido, existen varias denominaciones para un centro de respuesta a incidentes de seguridad informática, tales como Equipo de Respuesta a Incidentes (IRT), Equipo de Respuesta a Incidentes Informáticos (CIRT), Capacidad de Respuesta a Incidentes Informáticos (CIRC), Equipo de Respuesta a Incidentes de Seguridad (SIRT), Equipo de Respuesta a Incidentes de Seguridad informática (CSIRT) y Equipo de Respuesta a Emergencias Informáticas (CERT), siendo los más usados IRT y CSIRT.

Ahora bien, partiendo de la definición de un CSIRT, el objetivo general de un CSIRT, es prevenir y responder ante los incidentes de seguridad informática que se presentan o pueden

presentarse dentro de su grupo de clientes atendidos (MINTEL, 2016), en la tabla 1 se menciona los siguientes objetivos específicos de un CSIRT.

Tabla 1 Objetivos específicos de un CSIRT

Objetivos específicos de un CSIRT

Objetivos específicos
Elaborar la planificación estratégica de respuesta a incidentes.
Establecer políticas y procedimientos de respuesta de incidentes.
Definir servicios de respuesta de incidentes
Identificar, contener y eliminar incidentes
Comunicar y coordinar los incidentes detectados con otros equipos de trabajo.
Gestionar la recuperación del incidente
Prevenir la repetición del incidente

Fuente: *(MINTEL, 2016)*

Por otra parte, como principales características de un CSIRT en general se tienen que, es una organización conformada por un equipo de especialistas profesionales en seguridad de las TI, auditoria forense de seguridad informática, derecho informático y de dirección informática, donde estos CSIRT cuentan con financiación a través de una entidad pública o privada o por autogestión de la propia entidad en donde se va a ubicar el CSIRT.

Otro aspecto importante, radica en que todos estos centros se regulan en base a la norma RFC 2350 con la cual se gestiona la información de datos importantes como misión, visión, objetivos, la comunidad objetivo y su autoridad, servicios preventivos y educativos y el uso de claves PGP (UTPL, 2019).

Por otra parte, los CSIRT mantienen el apoyo del FIRST (Forum of Incident Response and Security Teams) para su certificación a nivel mundial, y también, usan canales de comunicación como la web, email, teléfono, para dar aviso y alertas sobre las vulnerabilidades del software y el hardware en uso e informar a sus clientes sobre malware y virus que se aprovechan de estas vulnerabilidades.

2.2 Servicios de un CSIRT

Los servicios de un CSIRT, se definen comúnmente en base a la misión, visión y grupo de comunidad objetivo o clientes atendidos. En otros tipos de CSIRT, los servicios se relacionan con el tratamiento de incidentes como son el manejo de vulnerabilidades, alertas y advertencias, comunicados, sensibilización y concienciación a usuarios, auditoria forense y el análisis de riesgos (OEA, 2016).

Ahora bien, los servicios básicos con los que un CSIRT debe iniciar sus operaciones son: alertas y advertencias, emisión de comunicados y tratamiento de incidentes. A continuación, en la tabla 2, se presenta una lista de servicios CSIRT según el Manual CSIRT del CERT/CC (Computer Emergency Response Team / Cordination Center):

Tabla 2 Servicios básicos para inicio de operaciones de un CSIRT

Servicios básicos para inicio de operaciones de un CSIRT

Servicios reactivos	Servicios proactivos	Gestión de calidad de la seguridad
Alertas y advertencias	Comunicados	Análisis de riesgos
Tratamiento de incidentes	Observatorio de tecnología	Continuidad del negocio y recuperación tras un desastre
Análisis de incidentes	Evaluaciones o auditorías de la seguridad	
Apoyo a la respuesta a incidentes		Consultoría de seguridad

Coordinación de la respuesta a incidentes Respuesta a incidentes in situ Tratamiento de la vulnerabilidad Análisis de la vulnerabilidad Respuesta a la vulnerabilidad Coordinación de la respuesta a la vulnerabilidad	Configuración y mantenimiento de la seguridad Desarrollo de herramientas de seguridad Servicios de detección de intrusos Difusión de información relacionada con la seguridad	Sensibilización Educación/formación Evaluación o certificación de productos

Fuente: (CEDIA, 2020)

2.2.1 Servicios Reactivos

De acuerdo con la guía de la Agencia de la Unión Europea para la Ciberseguridad, ENISA (2006) los servicios reactivos se encargan del tratamiento de incidentes y la mitigación en caso de daños existentes, en la tabla 3 se presenta las actividades que se pueden realizar dentro de estos servicios.

Tabla 3 Resumen de actividades de los servicios reactivos

Resumen de actividades de los servicios reactivos

Tipo	**Definición**
Alertas y advertencias	Este servicio difunde información como reacción a un problema de seguridad detectado, por tanto, describe el ataque o la

	vulnerabilidad de seguridad encontrada, esta información es notificada a la comunidad objetivo a la cual se presta los servicios
Tratamiento de incidentes	Para el tratamiento de incidentes, se ofrece varias actividades como: protección de los sistemas de red de datos e Internet atacados por intrusos, se proporciona técnicas y estrategias como soluciones para mitigar las incidencias a partir de alertas o advertencias, filtrar el tráfico de red y diseñar métodos de respuesta a incidencias.
Análisis de incidentes	El análisis de incidentes consiste en analizar de forma profunda un incidente, verificando su origen, alcance, nivel de impacto, efectos en los sistemas informáticos; en el cual el equipo propondrá soluciones viables para dar respuesta a las incidencias.
Apoyo a la respuesta de incidentes	Este servicio se encarga de enviar documentación, o se comunica telefónicamente con los clientes o

	comunidad objetivo, con el fin de proporcionar información para que el personal del sistema afectado pueda solucionar las incidencias y recuperar el sistema, sin necesidad de que se realice una asistencia directa al cliente.
Coordinación de la respuesta a incidentes	La coordinación de respuesta a incidentes se realiza mediante la recolección de datos del cliente, investigar estadísticas sobre los sistemas afectados por las incidencias, para poder coordinar con otros CSIRT, en el intercambio de información.
Respuesta a incidentes in situ	Este proceso se realiza mediante la asistencia directa del equipo CSIRT al cliente, brindando el soporte para la recuperación del sistema ante la presencia de una incidencia, en el cual se pueden realizar varios trabajos como: análisis e identificación física de los sistemas afectados, así como la reparación y recuperación de los mismos.

Tratamiento de la vulnerabilidad	El tratamiento de la vulnerabilidad, es aquel proceso en el cual recepta información y alertas de monitoreo con sus respectivos reportes sobre todas las vulnerabilidades tanto en Software como Hardware de una organización, analizando causas y efectos de estas vulnerabilidades en los sistemas, aportando con soluciones estratégicas para reparar dichas vulnerabilidades (García, Arias, Buenaño, Merizalde, & Noriega, 2013).
Análisis de la vulnerabilidad	Consiste en la revisión e identificación de las vulnerabilidades y la forma en que pueden ser explotadas, utilizando mecanismos o herramientas de explotación de vulnerabilidades como software de escaneo de puertos, escaneo de código fuente, utilizando software de hacking ético o de auditoria, y de esta forma mitigar los ataques y el funcionamiento de este.

Respuesta de la vulnerabilidad	Este servicio se ejecuta mediante la investigación y desarrollo continuo de correcciones y soluciones momentáneas afín de determinar una respuesta válida a los clientes para mitigar y reparar las vulnerabilidades, donde el valor agregado es la comunicación de estrategias de mitigación a través de avisos o alertas.
Coordinación de la respuesta a la vulnerabilidad	En este servicio el CSIRT reporta las vulnerabilidades al cliente y coordina acciones para comunicar los datos principales de estas vulnerabilidades, cómo reparar o mitigar esta vulnerabilidad, así como también compartir información de estrategias de respuesta con otros CSIRT's nacionales e internacionales para reparar las vulnerabilidades y recuperar el sistema.

Fuente: *(LACNIC, 2012)*

2.2.2 Servicios Proactivos

Los servicios proactivos se encargan de mejorar la infraestructura de red, sistemas, y procesos de seguridad en la organización, de esta forma se trata de evitar amenazas como

ataques e intrusiones, mitigando su ocurrencia e impactos en la organización (Carazo, 2013). Las subcategorías que conforman los servicios proactivos según (Carazo, 2013) son presentadas en la tabla 4.

Tabla 4 Resumen de actividades de los servicios proactivos

Resumen de Actividades de los Servicios Proactivos

Tipo	**Definición**
Comunicados	Los anuncios o comunicados informan a la comunidad objetivo del CSIRT, acerca de nuevas invenciones e investigaciones con proyectos de mediano y alto impacto, a largo plazo, tales como vulnerabilidades recientemente encontradas o el uso de nuevas herramientas para detectar intrusos. Los anuncios permiten a los clientes proteger sus sistemas y redes contra problemas recientemente encontrados antes de que puedan ser explotados. Los anuncios incluyen subprocesos como alertas de intrusión, advertencia de vulnerabilidad y avisos de seguridad.
Observatorio de tecnología	El observatorio de tecnología, monitorea y observa nuevos desarrollos técnicos,

	actividades de intrusos y nuevas tendencias, para ayudar a identificar futuras amenazas, incluyendo notificaciones sobre reformas, leyes y normativas relacionadas con las incidencias y seguridad informática, así como las últimas tecnologías aplicadas por los grupos CSIRT. Este servicio incluye el monitoreo de correos, sitios web de seguridad y noticias, artículos de revistas actuales en los campos de la ciencia, tecnología, política y gobierno para extraer información relevante para la seguridad de los sistemas constituyentes y redes.
Evaluaciones o auditorias de la seguridad	Las auditorias de seguridad o auditorias forenses proporcionan una revisión y análisis detallados de la infraestructura de seguridad de una organización, basada en los requisitos definidos por la organización o por otros estándares que se apliquen. Entre sus servicios están: revisión de infraestructura de seguridad, revisión de

	mejores prácticas, escaneo y pruebas de penetración (PCI Council, 2018).
Configuración y mantenimientos de la seguridad	El servicio de configuración y mantenimiento de la seguridad se encarga de identificar o proporcionar orientación adecuada sobre cómo configurar y mantener de forma segura herramientas, aplicaciones y la infraestructura informática general utilizada por los clientes CSIRT o por el CSIRT mismo. Además de proporcionar orientación, el CSIRT puede realizar actualizaciones de configuración y mantenimiento de herramientas y servicios de seguridad, como IDS, escaneo de redes o sistemas de monitoreo, filtros, cortafuegos, redes privadas virtuales (VPN) o mecanismos de autenticación. El CSIRT puede incluso brindar estos servicios como parte de su función principal. El CSIRT también puede configurar y mantener servidores, computadoras de escritorio, computadoras portátiles,

	asistentes digitales personales (PDA) y otros dispositivos inalámbricos basados en pautas de seguridad. Este servicio incluye la coordinación con gerencia ante cualquier problema, ya sea de configuraciones o el uso de herramientas y aplicaciones que el CSIRT cree que podrían dejar un sistema vulnerable a un ataque.
Desarrollo de herramientas	En cuanto al desarrollo de herramientas de seguridad, este servicio incluye el desarrollo de nuevas herramientas creadas para cubrir las necesidades del CSIRT, como, por ejemplo, desarrollar parches de seguridad para software personalizado utilizado por las distribuidoras de software de seguridad. Se utiliza para reconstruir hosts comprometidos. También puede incluir el desarrollo de herramientas o scripts que extiendan la funcionalidad de las herramientas de seguridad existentes, como un nuevo complemento para una vulnerabilidad o escaneo de red, scripts que

	facilitan el uso de tecnología de encriptación o mecanismos de distribución de parches automatizados.
Servicios de detección de intrusos	Este servicio se encarga de revisar los registros de IDS (Sistema de Detección de Intrusos) existentes, analizan y brindan respuestas a incidentes, o reenvían alertas de acuerdo con un nivel de servicio predefinido. En muchos casos, se utilizan herramientas especializadas, para sintetizar e interpretar la información que provienen de falsas alarmas, ataques o eventos de red; permitiendo implementar estrategias para eliminar o minimizar tales eventos. Algunas organizaciones optan por externalizar esta actividad a otros equipos que tengan más experiencia en la realización de estos servicios, como por ejemplo proveedores de servicios de seguridad gestionados.
Difusión de información	En cuanto a la difusión de información sobre seguridad, este servicio proporciona a

	los clientes información útil que ayuda a mejorar la seguridad, la misma que incluye: informar pautas e información de contacto para el CSIRT, archivos de alertas, advertencias y otros anuncios, documentación sobre las mejores prácticas actuales, orientación general de seguridad informática, políticas, procedimientos y listas de verificación, desarrollo de parches e información de distribución, enlaces de proveedores, estadísticas y tendencias actuales en la notificación de incidentes, entre otras. Esta información puede ser desarrollada y publicada por el CSIRT o por otra parte de la organización (TI, recursos humanos o relaciones mediáticas), y puede incluir información de recursos externos como de otros CSIRT, proveedores y expertos en seguridad

Fuente: *(LACNIC, 2019)*

2.2.3 Gestión de la Calidad de la Seguridad

Como afirma (Bronk, 2006), la gestión de la calidad de la seguridad, son servicios diseñados para mejorar la seguridad de la información de una organización, aprovechando las experiencias obtenidas en la prestación de los servicios reactivos y proactivos descritos anteriormente. De tal forma que, un CSIRT puede aportar perspectivas únicas a estos servicios de gestión de calidad que de otro modo no podrían estar disponibles, Por ello, estos servicios están diseñados para incorporar comentarios y lecciones aprendidas basadas en el conocimiento obtenido al responder a incidentes, vulnerabilidades y ataques.

Igualmente, este proceso puede mejorar los esfuerzos de seguridad a largo plazo en una organización, dependiendo de la estructura organizacional y sus responsabilidades, y así, un CSIRT puede proporcionar estos servicios o participar como parte de un programa del equipo organizacional. Las subcategorías que explican cómo la experiencia de un CSIRT puede beneficiar a cada uno de estos servicios de gestión de calidad de seguridad se encuentran en la tabla 5.

Tabla 5 Actividades del servicio de Gestión de la calidad de la seguridad

Resumen de actividades del servicio de Gestión de la calidad de la seguridad

Tipo	Definición
Análisis de riesgos	Este servicio se encarga de proporcionar evaluaciones cualitativas y cuantitativas de riesgos para los activos de información y para evaluar estrategias de protección y respuesta. Los CSIRT que realizan este servicio apoyan con las actividades de

	análisis de riesgos de seguridad de la información para nuevos sistemas y procesos de negocios o para la evaluación de amenazas y ataques contra activos y sistemas constituyentes.
Continuidad del negocio y recuperación tras un incidente	Esta sub categoría está basada en sucesos pasados y predicciones futuras de incidentes emergentes o tendencias de seguridad, cada vez más y más incidentes tienen el potencial de causar una grave degradación de las operaciones comerciales de una empresa. Por lo tanto, el CSIRT emite ciertas recomendaciones, para determinar la mejor manera de responder a tales incidentes, garantizando así con la continuidad del negocio, por tanto, están involucrados en la continuidad del negocio y en la planificación de recuperación ante desastres relacionados con incidentes, amenazas y ataques de seguridad informática.

Consultoría de seguridad	Este servicio se encarga de brindar asesoría sobre las mejores prácticas de seguridad que se puede aplicar dentro de la comunidad a la cual se presta los servicios, incluyendo orientación y asistencia para el desarrollo de políticas de seguridad, además asiste en compras, instalaciones o en la protección de nuevos sistemas, dispositivos o software.
Sensibilización	Los CSIRT que realizan este servicio buscan oportunidades para aumentar la conciencia de seguridad informática a través del desarrollo de artículos, carteles, boletines, sitios web u otros recursos informativos que explican sobre la mejor práctica de consejos de seguridad, y proporcionan recomendaciones sobre las precauciones a tomar. Las actividades también pueden incluir la programación de reuniones y seminarios para mantener a los clientes actualizados con los procedimientos de seguridad en curso y las

	posibles amenazas para sus sistemas organizacionales.
Educación / formación	Este servicio implica proporcionar información a los clientes sobre problemas de seguridad informática a través de seminarios, talleres, cursos y tutoriales. Los temas pueden incluir pautas para la notificación de incidentes, métodos de respuesta adecuados, herramientas de respuesta a incidentes, métodos de prevención de incidentes y otra información necesaria para proteger, detectar, informar y responder ante incidentes de seguridad informática.
Evaluación o certificación de productos	Para este servicio, el CSIRT puede realizar evaluaciones de productos en herramientas, aplicaciones u otros servicios para garantizar la seguridad de los productos y su conformidad con el CSIRT o prácticas de seguridad organizacional. Las herramientas y aplicaciones revisadas pueden ser de

	código abierto o productos comerciales. Este servicio se puede proporcionar como una evaluación o mediante un programa de certificación, dependiendo de los estándares que aplique la organización o por el mismo CSIRT.

Fuente: *(Lacnic, 2012).*

2.3 Tipos de CSIRT

Los tipos de CSIRT, se refiere a los sectores en los cuales un CSIRT puede ofrecer sus servicios de respuesta a incidentes de seguridad de la información, es decir el tipo de CSIRT, el cual está definido en base al factor demanda y factor servicio que se ofrecerá a una comunidad objetivo. Ahora, para definir los tipos de CSIRT, se lo categoriza en los siguientes sectores: CSIRT Académico, CSIRT Nacional CSIRT Gubernamental, CSIRT Comercial, CSIRT de infraestructuras críticas (CIP/CIIP), CSIRT Interno, CSIRT Militar, CSIRT de la Pequeña y Mediana Empresa (PYME) (Uribe, 2014).

Ahora es necesario considerar que el CSIRT Académico, es una organización que trabaja en función de dar un beneficio a una comunidad académica, mediante la prestación de servicios de respuesta a incidentes de seguridad de la información generados en las áreas del personal y estudiantes de una universidad, instituto tecnológico o politécnico (Bronk, Thorbruegge, & Hakkaja, 2006).

Agregando a lo anterior, en el Ecuador, existen alrededor de 14 CSIRT, donde los tipos de mayor impacto son el CSIRT académico, CSIRT gubernamental y CSIRT nacional, entre ellos, los más importantes: CSIRT CEDIA, EcuCERT, CSIRT CELEC EP, CSIRT Telconet, CSIRT EPN y CSIRT UTPL (Uribe, 2014).

2.4 Beneficios de un CSIRT

Los beneficios de un CSIRT en forma general son, establecer un punto de contacto centralizado para la respuesta a incidentes de seguridad de la información de una forma rápida, coordinada y estandarizada, también provee a la organización o comunidad objetivo información acerca de cómo gestionar y solucionar las incidencias reportadas en el centro, en este sentido, también brinda una colaboración, apoyo y soporte a las entidades o instituciones de seguridad del sector de las telecomunicaciones, gubernamental y militar (PCI Council, 2018).

Así mismo, los beneficios de un CSIRT, se los puede agrupar en categorías cuantificables y cualificables, que determinan la existencia de un CSIRT en una empresa; siendo estos, beneficios económicos, sociales, empresariales y legales.

En este sentido, el beneficio económico que se obtiene al crear un CSIRT, es la participación del personal y agilidad para gestionar el incidente, de esta forma el beneficio económico resulta en menos gastos operativos y menor tiempo invertido por incidente. Estos beneficios económicos resultan en un mejor aprovechamiento de los recursos humanos para manejar los incidentes, reduciendo la pérdida en productividad de los empleados afectados por el incidente.

Además, el beneficio económico radica en la actualización de las TICs, mismas que permiten un rendimiento adecuado de los procesos, evitando gastos infructuosos o pérdida

de información relevante dentro de la institución; también garantiza la seguridad de la información interna y por tanto la rentabilidad y carta de presentación de la institución hacia el público externo que pretende trabajar en alianza con instituciones seguras y confiables.

Por otra parte, los beneficios sociales de un CSIRT, permiten proveer a la ciudadanía de conocimientos técnicos, indispensables en la prevención de riesgos, incentivando la concientización de los usuarios en el manejo adecuado de los sistemas informáticos para evitar la presencia de incidencias como por ejemplo ataques cibernéticos.

Pasando a otro aspecto, los beneficios legales de un CSIRT, prevalece en el aporte que brinda, en situaciones de conflicto legal, ante ataques cibernéticos a los sistemas informáticos de las organizaciones públicas y privadas, donde este equipo será sujeto de prueba, aportando con reportes e informes sobre su presencia ante tribunales o jueces.

Sobre todo, en el aspecto legal, el aporte de un CSIRT tiene un enfoque esencial en una organización ya que se gestiona de mejor forma los requerimientos legales relacionados con los incidentes, en caso de ser necesaria la protección de evidencias digitales como material de prueba.

2.5 Recursos Humanos de un CSIRT

Los recursos humanos de un CSIRT, son encargados de reclutar y seleccionar en base a un perfil específico de cargos, destacando la experiencia y conocimientos en el área informática, administrativa, financiera, legal y de asesoría técnica. Por lo tanto, el recurso humano seleccionado dependerá básicamente de la estructura organizacional, misión, servicios y comunidad a la que brinda servicios el CSIRT (Van Der Heide, 2017).

Las características del personal que se reclutará y seleccionará, junto con los diferentes roles y responsabilidades se mencionan en la tabla 6 y son los siguientes:

Tabla 6

Perfil de cargos en el CSIRT

Habilidades personales	Cargos
Técnicas de comunicación Relaciones humanas Espíritu de Equipo Innovadores, analíticos e íntegros, son un equipo que trabaja dando soluciones a problemas Capaces de tomar decisiones rápidas ante ataques y situaciones de emergencias de manera que nada quede sin dar respuesta Capacidad de seguir políticas y procedimientos. Experiencia laboral en temas de seguridad informática **Técnicas** Conocimiento en sistemas LINUX y Windows Conocimiento de protocolos y aplicaciones de Internet Conocimiento en seguridad informática Hacking Ético Conocimiento de equipos de infraestructura de redes	Líder CSIRT Administrador de Incidentes Administrador de Help Desk /Call Center Analista de incidentes de seguridad Jefe /Asistente de relaciones públicas, Abogado / Asistente Legal, Jefe / Asistente de Talento Humano

Por otro lado, en la tabla 7 se detalla los cargos y responsabilidades que se puede tener dentro de un CSIRT

Tabla 7 Cargos y responsabilidades del personal del CSIRT

Cargos y responsabilidades del personal del CSIRT

Cargo	Responsabilidades
Líder del equipo	Por lo general, es un miembro del personal ejecutivo. El papel clave del líder del equipo es comunicar los incidentes al personal ejecutivo y a la junta y garantizar que el CSIRT reciba la atención y el presupuesto adecuado.
Administrador de incidentes	El administrador de incidentes puede trabajar en toda la organización y es responsable de convocar reuniones y responsabilizar a los miembros del equipo por sus acciones, también resume los hallazgos y cualquier impacto en la comunicación en todo el CSIRT, antes de escalar los problemas a niveles más altos.
Administrador de Help Desk	Es aquel personal responsable de la mesa de ayuda del CSIRT, en donde se receptan los datos de reportes de incidentes de seguridad, así como también, atienden las llamadas a la línea de call center del CSIRT, para luego, clasificar los tipos de

	incidencias de acuerdo a su rango de relevancia o importancias establecidos en el CSIRT.
Analista de incidentes de seguridad	Este recurso técnico, como un analista de seguridad o un respondedor de incidentes dedicado en el SOC (Security Operation Center), es responsable de investigar los sucesos durante un incidente de seguridad. El investigador principal puede trabajar con un equipo extenso de analistas de seguridad e investigadores forenses.
Jefe / Asistente de relaciones públicas	Idealmente, se trata de una persona en el equipo de marketing responsable de las relaciones públicas, respondiendo cualquier consulta o declaración de prensa, según sea necesario, y redactando comunicaciones para enviar a los empleados, socios y clientes, además el monitoreo de las redes sociales también es una función que desempeña el jefe/asistente de relaciones públicas.

Abogado / Asistente Legal	Esta persona aconseja sobre la necesidad de revelar incidentes, como una violación, y se ocupa de cualquiera de las consecuencias resultantes del incidente de seguridad, como demandas de accionistas o empleados.
Jefe / Asistente de talento humano	Este puesto lo ocupa generalmente el jefe de recursos humanos, que puede gestionar cualquier problema relacionado con el personal que ocurra, especialmente si se trata de robo de información privilegiada. El representante de Recursos Humanos también ofrece sugerencias sobre cómo se comunican los incidentes a los empleados.

Fuente: *(OAS, 2016)*

2.6 Estructura Organizacional de un CSIRT

Según el Manual Básico del proyecto Amparo, la estructura organizacional de un CSIRT se puede establecer mediante los modelos mencionados en la tabla 8: Equipo de seguridad, CSIRT distribuido, CSIRT centralizado interno, y CSIRT de coordinación (LACNIC, 2010).

Dentro de estos modelos el personal encargado de la seguridad está conformado generalmente por administradores de sistemas, redes o seguridad, a nivel local o en forma

ad-hoc y, a veces, aislados como parte de sus responsabilidades generales o asignaciones de trabajo (Killcrece, 2003).

Tabla 8

Estructura organizacional para un CSIRT

Modelos organizacionales	Definición
Equipo de seguridad	Las actividades del equipo de seguridad son coordinadas con el personal y herramientas existentes dentro de la organización, por tanto, no existe un equipo dedicado exclusivamente para la respuesta de incidentes, por tanto, en caso de existir incidentes, quien se encarga de dar respuesta y seguimiento es el administrador de los equipos involucrados. Este modelo no permite un desarrollo óptimo en temas de seguridad informática ya que no cuenta con un equipo especializado.
Modelo distribuido	El CSIRT bajo el modelo distribuido, es adecuado para organizaciones grandes u organizaciones que están dispersas geográficamente, ya que tiene varios equipos de respuesta de incidentes de

	seguridad, que conforman uno sólo, los cuales se encargan de dar respuesta a cada división de la empresa o de acuerdo a segmentos lógicos o físicos, todos estos equipos están coordinados por una unidad central, garantizando los servicios y que dependiendo de los incidentes sea necesario el trabajo en conjunto.
Modelo centralizado interno	El CSIRT bajo el modelo centralizado interno, sirve como punto único de contacto con la organización, para la gestión de informes o alertas de monitoreo de vulnerabilidades o el manejo de incidentes, este modelo es adecuado para organizaciones que no tienen su infraestructura tecnológica geográficamente dispersa o lejana u organizaciones pequeñas.
CSIRT de coordinación	El CSIRT de coordinación sirve como punto único de contacto con la organización en relación con los informes o actividades

	de incidentes y vulnerabilidades para las áreas internas y externas de la organización a la cual pertenece. El CSIRT de Coordinación**,** como su nombre, coordina y facilita el manejo de incidentes en una variedad de organizaciones externas o internas, que podrían incluir otros CSIRTs. Este modelo de CSIRT puede ser una entidad coordinadora para las filiales individuales de una empresa, o para las múltiples ramas de una organización militar, instituciones en una red de investigación, o para varias organizaciones dentro de un país o estado en particular. Siendo su función principal proporcionar análisis de incidentes y vulnerabilidades, soporte y servicios de coordinación, distribuir pautas, consejos, advertencias, recomendaciones para mitigar incidencias y soluciones de recuperación.

Fuente: *(LACNIC, 2012)*

2.7 CSIRT Académico

De acuerdo con (Carozo, 2010), un CSIRT Académico es aquella organización, que está ubicada en un centro educativo o académico, el cual se encarga de gestionar acciones de prevención y respuesta de incidentes de seguridad de la información, que sean eficientes para mitigar los impactos causados en los sistemas informáticos de una universidad, centro de investigación o centro educativo.

Así mismo, las actividades principales de un CSIRT Académico son esencialmente preventivas tales como expresa (Rajnovic, 2011). capacitación, concienciación, sensibilización a usuarios, difusión de alertas generadas por otros CSIRT, elaboración de políticas de respuesta a incidentes, contestar reportes de incidencias generados en los departamentos de la universidad, además de identificar y solucionar los problemas de atención de incidentes"

Otro aspecto importante para el diseño de un CSIRT es el planeamiento estratégico, el cual comprende aquellos recursos administrativos que inicialmente deben realizarse para que el CSIRT académico pueda comenzar sus operaciones en la universidad y cumpla con los objetivos de seguridad de la información previamente definidos, en beneficio de la comunidad académica, siendo este, el elemento que viabilizará estas acciones estratégicas con la finalidad de que las operaciones a corto y largo plazo del CSIRT cumplan con las expectativas y proyectos del plan operativo anual POA, en la tabla 9 se presenta lo que debería contener el planeamiento estratégico.

Tabla 9 Planeamiento estratégico del CSIRT Académico

Planeamiento estratégico del CSIRT Académico

Contenido de un plan estratégico de un CSIRT
1. Requerimientos de personal que conformará el CSIRT

2. Definición de la misión y objetivos estratégicos del CSIRT
3. Localización del CSIRT en la estructura organizacional
4. Normas y estándares para apoyar la gestión de incidencias
5. Relaciones con otros equipos a nivel nacional e internacional
6. Comunicación del plan estratégico a la comunidad académica

---

Es necesario considerar que, para definir la visión del CSIRT Académico es necesario conocer la situación actual de la universidad, en el cual se localiza, por tanto, el planeamiento estratégico contendrá los siguientes aspectos como misión, visión y objetivos del equipo, la comunidad objetivo del CSIRT académico, el lugar que va a ocupar en la organización y la relación del CSIRT Académico, con otros CSIRT´s.

2.7.1 Objetivos del CSIRT Académico

Los Ingenieros Ernesto Pérez y Miriam López de CSIRT – CEDIA y EcuCERT respectivamente, en entrevista realizada en el año 2020, concuerdan en que los principales objetivos del CSIRT Académico son los siguientes:

- Cumplir los requerimientos para calificarse como parte del FIRST (Forum of Incident Response and Security Teams).

- Aplicar políticas de seguridad de la información propias de la universidad, para incrementar los niveles de seguridad.

- Mantener un punto de contacto centralizado para el reporte y respuesta de incidencias.

- Investigar y capacitar en temas de seguridad de la información.

2.7.2 Modelo Organizacional y Personal del CSIRT Académico

El CSIRT Académico, se ubica dentro de la estructura organizacional del centro universitario, educativo o centro de investigación al cual pertenece, donde el modelo organizacional es el interno centralizado, por tanto el CSIRT tiene completa responsabilidad en el manejo de incidentes y vulnerabilidades de seguridad de la información que se presenta en la universidad, además tiene la obligación de encontrar soluciones, estrategias y emitir informes de aquellos incidentes encontrados, mediante la cooperación directa con el equipo del CSIRT y administrador de red y sistemas de la universidad, quienes se encargarán de evaluar la seguridad informática de la universidad, brindando capacitaciones y asesoría en temas de gestión de incidencias y vulnerabilidades a la comunidad objetivo. (Carozo y Vidal, 2008)

Así mismo, la autoridad del CSIRT Académico, es compartida, siendo el departamento de TI o de Informática y Sistemas, con el cual se toman decisiones a través de la coordinación e intercambios de actividades e información con el equipo CSIRT académico, el cual al final gestionará las respuestas a estas incidencias proporcionando asesoría directa para esta toma de decisiones.

Igualmente, el CSIRT académico, se lo ubica como parte de la estructura organizacional de la universidad o centro educativo, situándolo como un nuevo departamento, unidad o sección, localizado cerca de la dirección TI de la universidad, con el fin de realizar labores conjuntas con el personal de administradores de red y de sistemas informáticos. (Rajnovic, 2011).

2.7.3 Relaciones de Confianza con Equipos CSIRT Nacionales e Internacionales

Las relaciones de confianza se establecen entre varias organizaciones, tanto nacionales como internacionales. En el caso del FIRST (Foro de Respuesta a Incidentes y equipos de Seguridad), los CSIRT miembros de esta organización son apoyados con asesorías para realizar las mejores prácticas, herramientas y comunicación confiable de forma que respondan a los incidentes de una forma más precisa (Andrade & Fuertes, 2013).

De esta forma los diferentes CSIRT alrededor del mundo establecen relaciones de confianza, mediante el intercambio de experiencias y conocimientos, la oferta de servicios para los colectivos CSIRT, y ayudar a la creación de nuevos CSIRT (ENISA, 2006). Entre los objetivos más destacados de estos grupos de trabajo son: crear servicios piloto para los grupos CSIRT, ofrecer un foro de intercambio de experiencias y conocimientos, fomentar normas y procedimientos comunes para responder a los incidentes de seguridad de la información y ayudar a la creación de nuevos CSIRT y a la formación del personal.

Por otra parte, otras organizaciones altamente especializadas en la seguridad para respuesta a incidentes, con las cuales los CSIRT a nivel mundial, mantienen relaciones de colaboración y apoyo son: La Agencia Europea de Seguridad de las Redes y de la Información (ENISA), OAS: Organización de Estados Americanos, ITU-D: Sector de Desarrollo de las Telecomunicaciones, IMPACT: Servicios de Seguridad Impacto y AP-CERT: Equipo de Respuesta a Emergencias Informáticas de Asia y el Pacifico.

Ahora, en el Ecuador, los CSIRT Académicos y de otros sectores, establecen relaciones de coordinación y comunicación a través del intercambio de reportes de alertas e incidentes, entre los principales son, EcuCERT, CSIRT-CEDIA, y a nivel internacional con el CERT/CC de la Universidad Carnegie Mellón, CERT de la Universidad Nacional de la Plata

en Uruguay, así como el CERT de la Universidad Autónoma de México UNAM y el CERT Red Iris (Csirt Cedia, 2019).

2.8 Normas y Estándares de Diseño e Implementación de un CSIRT

Las normas y estándares utilizados para el diseño e implementación de un CSIRT, son los siguientes: Norma ISO/IEC 27002, Norma RFC 2350, Estándar COBIT 2019. Estándar ITIL V4, las cuales en conjunto sirven para desarrollar las políticas y procedimientos para la gestión de incidentes de seguridad de la información del CSIRT.

2.8.1 Norma ISO / IEC 27002: 2013

De acuerdo con (Gavidia Mamani & Torres Torres, 2018), la ISO 27002, es una guía que brinda recomendaciones de mejores prácticas para gestionar la información de una organización, de forma que, presenta directrices de normas de seguridad de la información, teniendo en cuenta la selección, administración e implementación de los controles de seguridad informática.

Agregando a lo anterior, (Contero Ramos, 2019), menciona que la norma ISO 27002:2013, se divide en 14 dominios, 35 objetivos de control y 114 controles, cabe mencionar que en este apartado se destacan los dominios que ayudarán al CSIRT en la gestión de incidentes informáticos.

Por otra parte, el primer dominio importante es el A5, política de seguridad de la información, para lo cual según (Gavidia Mamani & Torres Torres, 2018), manifiesta, que la información es un activo que posee un valor importante para la organización, y por ende debe ser protegida, de esta manera se asegura la continuidad del negocio, es por eso que hay que tener presente los tres pilares de la seguridad de la información, disponibilidad, integridad y confidencialidad.

Ahora bien estos tres pilares de la seguridad de la información, según (Magdalena, 2015), los define de la siguiente manera, la disponibilidad de la información, garantiza a los usuarios el uso de la información cuando sea necesitada o requerida, la integridad define la exactitud con que la información responde a lo que dice representar y finalmente la confidencialidad define el ámbito en el que la información puede darse a conocer, identificando quién o quiénes tienen acceso.

Dicho esto, el dominio A5, tiene como objetivo orientar y apoyar con lineamientos para establecer políticas de seguridad de la información, las cuales deben ser definidas, aprobadas y publicadas, así como también deben ser revisadas y actualizadas periódicamente según las necesidades de la organización.

Por otra parte, el segundo dominio es el A13, seguridad en las comunicaciones, el cual se encarga de proporcionar recomendaciones para la protección de la información cuando ésta es transmitida por cualquier medio, en la tabla 10 se menciona el contenido de este dominio.

Tabla 10

Dominio A13, Seguridad de las comunicaciones

Objetivos de control	**Controles**	**Contenido**
Gestión de la seguridad de red	Controles de Red	Monitoreo y registro, control de acceso, control de privilegios.
	Seguridad de los servicios de red	Definición de acuerdos de calidad de servicios

Intercambio de información	Separación en redes	Accesos restringidos, separación de redes de forma lógica y/o física
	Políticas y procedimientos de intercambio de información	Definir políticas y procedimientos para proteger la información contra copias, intercepción, modificación, destrucción, encriptación, manejo de archivos.
	Acuerdos de intercambio de información	Establecimiento de acuerdos como cumplimiento de cifrado de datos, responsabilidades en cadena de custodios, controles de acceso a información, responsabilidades en el usp y protección de la información.
	Mensajería electrónica	Aplicación de controles que permitan proteger la información ante accesos

		que no estén autorizados, disponibilidad y confiabilidad de los servicios, asegurar el correo mediante llaves.
	Acuerdos de confidencialidad y de no divulgación	Dentro de los acuerdos se debe considerar la duración, establecer responsabilidades, naturaleza de la información, clausular que conlleven al cumplimiento de la confidencialidad y sobre todo registrar y firmar estos acuerdos.

Fuente: *(Gavidia Mamani & Torres Torres, 2018)*

Y finalmente, el tercer dominio es el A16, que corresponde a la gestión de incidentes de seguridad de la información, este dominio se encuentra encaminado a una atención eficaz frente a incidentes de seguridad de la información que sean reportados.

Por esta razón, este dominio recomienda la implementación de herramientas que permitan gestionar los incidentes de seguridad de la información, el cual debe contemplar el siguiente proceso: detección, y evaluación de incidentes de seguridad de la información, respuesta

ante incidentes, reporte de vulnerabilidades y el aprendizaje de los incidentes de seguridad de la información.

Agregando a lo anterior, el proceso para gestionar los incidentes de seguridad de la información comienza cuando un evento es detectado por una persona, por lo cual es notificado mediante correo, llamada o herramienta de gestión de tickets, seguidamente al recibir la notificación, el incidente es clasificado según parámetros establecidos, entonces se procede a tomar medidas que permitan brindar una solución al incidente de seguridad de la información, a continuación antes de cerrar el incidente se procede a registrar el incidente, y finalmente se notifica el cierre del incidente reportado, es importante registrar toda la información acerca del incidente, ya que en caso de que ocurra algo similar se puede brindar una solución rápida y oportuna.

La norma ISO 27002, dentro del dominio A16, gestión de incidentes de seguridad de la información, menciona 7 controles, los cuales son responsabilidades y procedimientos, reporte de eventos, debilidades, evaluación y decisión, respuesta, aprendizaje de los incidentes de seguridad de la información y recolección de evidencia.

Para mejor comprensión se define cuatro términos fundamentales, que son amenaza, vulnerabilidad, evento e incidente de seguridad de la información, en consecuencia una amenaza es cualquier factor que puede producir daños a la organización, en cambio una vulnerabilidad es una debilidad en la cual deja expuesto la seguridad de la información, por otro lado, un evento, es la ocurrencia de algún cambio en las operaciones normales de la organización y finalmente un incidente de seguridad de la información puede ser uno o algunos eventos inesperados que pueden comprometer las operaciones de la organización.

Ahora bien, es importante la clasificación de los incidentes para lo cual es necesario tener presente los siguientes parámetros: impacto y urgencia, el impacto es un daño que causa a la institución y la urgencia es la necesidad de corregir con rapidez un incidente.

De esta manera se puede dar una prioridad a los incidentes que se presenten, signando valores a los mismos, en la tabla 11 se menciona la categorización a los mismos.

Tabla 11

Categorización de incidentes

Urgencia | Impacto	Alto 3	Medio 2	Bajo 1
Alta 3	Critico	Critico	Grave
Media 2	Critico	Grave	Leve
Baja 1	Grave	Leve	Leve

Fuente: *(ISO 27002:2013)*

2.8.2 Estándar ITIL V4

Según (Padilla Martinez & Uria Santos, 2019), ITIL es un marco de referencia en el cual se describe un conjunto de conceptos, mejores prácticas y recomendaciones para una mejor administración de los servicios de tecnologías de la información, y este, a su vez aporta con prácticas de gestión de servicios, el cual permite brindar valor a los servicios prestados.

Hay que tener en cuenta que AXELOS es la empresa dueña de ITIL, la cual publicó en el 2019 su última versión, y según (KNOWLEDGEHUT, 2020), una empresa líder en capacitaciones en el campo de la tecnología y gestión, brinda información completa acerca de ITIL4, en esta publicación describe las prácticas de gestión, las cuales se dividen en tres partes, prácticas de gestión general, gestión de servicios y gestión técnica.

Las prácticas de gestión general están enfocadas a toda la organización, para el éxito de sus negocios y servicios brindados, las prácticas de gestión de servicios, son aplicables a ciertos servicios específicos de la organización, y las prácticas de gestión técnica, las cuales, su enfoque está relacionado con el desarrollo e implementación de infraestructura y software.

Dentro de estas prácticas, las que son de importancia para los servicios que un CSIRT presta, son las prácticas de gestión de servicios, y que se subdividen en 17 prácticas, las cuales en la tabla 12 se describen de manera resumida, haciendo hincapié en las prácticas que se ajustan al CSIRT, ya que este equipo está encargado de brindar servicios para la solución de cualquier interrupción que se pueda presentar y que pueda afectar el normal funcionamiento de la organización.

Tabla 12

Prácticas de Gestión de Servicios

Práctica	**Descripción**
Gestión de la disponibilidad	Esta práctica se encarga de que exista una satisfacción por parte de la empresa, garantizando la disponibilidad de los servicios requeridos.
Análisis del negocio	Este aspecto pretende asegurar un análisis de cada elemento comercial que compone a la empresa, garantizando brindar las mejores soluciones para el negocio.
Gestión de la capacidad y el rendimiento	Esta práctica permite asegurar disponibilidad de los servicios en términos

	de capacidad para que los mismos funcionen en niveles esperados y que satisfaga la demanda de los usuarios.
Control de cambios	El control de cambios, hace referencia, a que cualquier cambio en Hardware, Software, productos, documentos, deben contar con autorización, garantizando así la integridad en los sistemas de manera controlada
Gestión de incidentes	Este control orienta a la restauración de los servicios a las condiciones normales en el menor tiempo posible.
Gestión de activo TI	Un activo es cualquier componente de carácter valioso en la organización, por tanto, la gestión de activos se centra en llevar un registro con todos los detalles de los activos, siendo estos actualizados periódicamente.
Monitoreo y gestión de eventos	Esta práctica permite dar seguimiento a cualquier evento que se produzca en la empresa, garantizando la prevención o eliminación de un posible impacto negativo en la organización.

Gestión de problemas	Se encarga de la identificación de las causas que generaron un incidente, proporcionando una solución temporal o permanente.
Gestión de versiones	La gestión de versiones ayuda a la comprensión de las características y funcionalidades del nuevo servicio.
Gestión de catálogo de servicios	Este control tiene como propósito brindar información como única fuente de información para los servicios ofertados.
Gestión de la configuración de servicios	Esta gestión permite tener información sobre todos los elementos de configuración utilizados para determinado servicio, incluyendo Software, Hardware, personas, documentos, etc.
Gestión de la continuidad de servicios	Permite asegurar la disponibilidad de los servicios, en caso de presentarse algún incidente.
Diseño del servicio	El propósito de esta práctica consiste en presentar un diseño de los servicios y productos, de tal manera que sean útiles, logrando el resultado requerido.

Servicio de atención al cliente	Este propósito, hace referencia al helpdesk, siendo este, un punto único de contacto ante la presencia de una interrupción en los servicios.
Gestión del nivel de servicio	Esta gestión, define y establece objetivos claros para los servicios prestados.
Gestión de peticiones del servicio	Brinda a los usuarios, un proceso adecuado para la solicitud de un determinado servicio.
Validación y prueba del servicio	La validación y prueba de servicio, consiste en establecer criterios que aseguren que los servicios o productos ya sean nuevos o modificados cumplan con los requisitos definidos y acordados.

Fuente: *(AXELOS, 2019)*

Una vez mencionadas las prácticas de gestión de servicios, a continuación, se detallan las que son necesarias para un CSIRT, las cuales son, gestión de incidentes, monitoreo y gestión de eventos, gestión de problemas y gestión de atención al cliente o mesa de ayuda (helpdesk). Estos controles permiten agregar valor a la seguridad de los activos más críticos, orientando en el diseño, desarrollo y práctica para la gestión de los servicios ofertados por un CSIRT.

En primer lugar, el propósito de la gestión de incidentes, radica en asegurar la restauración de los servicios a sus condiciones normales, a través de la restauración y resolución de los servicios durante el incidente, tratando de minimizar en el menor tiempo posible, el impacto que éste pueda generar a la organización.

ITIL define a un incidente, como una interrupción o degradación de los servicios de TI, resultando en un impacto negativo para la empresa. Para evitar este impacto, y poder gestionar las incidencias, ITIL proporciona los siguientes pasos mencionados en la tabla 13, los cuales permiten gestionarlos.

Tabla 13

Pasos para gestionar incidentes

Pasos para la gestión de incidencias	**Descripción**
1. Detectar la incidencia	La detección del incidente puede ser detectada por parte de los usuarios, o a su vez por software de monitorización, lo cual permite reaccionar y minimizar el incidente. Por ello es importante brindar herramientas que permitan reportar los incidentes.
2. Registro del incidente	Es necesario, una vez reportado un incidente, que el mismo sea registrado, incluyendo información sobre el incidente, datos importantes son, fecha, hora, persona que reportó, descripción del problema.
3. Análisis y Clasificación	El análisis consiste en examinar el incidente, permitiendo categorizar, según

	su impacto en las operaciones normales de la organización, esta categorización está basado en el impacto que puede producir el incidente al negocio y la urgencia que conlleva la resolución del mismo.
4. Priorización	El paso anterior, permite dar una prioridad de resolución al incidente, siendo los niveles, crítico, alto, medio y bajo, esta priorización tendrá en cuenta el tiempo de interrupción, usuarios afectados, y las consecuencias que pueda generar el incidente.
5. Resolución del incidente	Para poder brindar una solución al incidente es necesario, realizar un diagnóstico inicial, con base a la información proporcionada por quien lo reportó, en caso de ser necesario el incidente puede ser escalado a un nivel superior, además puede realizarse un diagnostico e investigación del incidente, y una vez que se tenga la solución debe ser aplicada de manera inmediata, asegurándose que el incidente este resuelto de manera correcta, finalmente se cierra el

incidente, registrando la solución adoptada, en caso de que vuelva a ocurrir el incidente.

El segundo control corresponde al seguimiento y gestión de eventos, para lo cual un evento según ITIL, es un acontecimiento detectable o discernible, el cual tiene un impacto significativo en la gestión de los servicios, los eventos son notificaciones que pueden ser informativos, de advertencia o de excepción, los informativos no presentan ningún impacto en los servicios, los eventos de advertencia, pueden, en caso de no ser tratados, provocar fallas en los servicios, y los eventos excepcionales, hacen referencia a fallos de los servicios, generando impactos a la organización, por tanto esta práctica, permite la supervisión y seguimiento a los posibles cambios que puedan producirse en los servicios.

Por lo tanto, la gestión de eventos se puede aplicar a cualquier aspecto de la gestión de servicios que necesita ser controlado, y que puede ser automatizado. Estos incluyen: elementos de configuración, condiciones ambientales (por ejemplo, detección de incendios y humo), software de supervisión de licencias de uso para garantizar una óptima y legal utilización de licencias, seguridad (por ejemplo, detección de intrusos), la actividad normal (por ejemplo, el seguimiento del uso de una aplicación o el rendimiento de un servidor). El valor para el negocio de la Gestión de Eventos es generalmente indirecto, pero hay que tener en cuenta que:

- Proporciona mecanismos para la detección anticipada de incidentes. En muchos casos es posible que el incidente se detecte y asigne al grupo apropiado antes de que se produzca cualquier interrupción real de servicio.

- Permite que algunos tipos de actividades automatizadas se monitoreen por excepción, lo que elimina la necesidad de costosos sistemas de monitoreo en tiempo real, reduciendo el tiempo de inactividad.
- Proporciona una base para automatizar operaciones, lo que reduce costos innecesarios en capital humano que se podrán utilizar para trabajo más innovador, como diseño de nuevas funcionalidades o definición de nuevas formas en las que la empresa puede aprovechar la tecnología para aumentar la competitividad.

Ahora bien, otro de los controles importantes que hay que tomar en cuenta es la gestión de problemas, para ello, es importante definir que para ITIL, un problema es una causa desconocida que puede provocar uno o más incidentes de seguridad de la información, para lo cual el propósito de este control es identificar las causas reales de los incidentes y reducir la probabilidad de impacto, brindando soluciones permanentes o alternativas hasta identificar la causa que lo originó. Esta práctica implica la identificación de problemas, control de problemas y errores.

Por último, se tiene la gestión del nivel de servicio, este control, permite proporcionar la existencia de un único punto de contacto denominado mesa de ayuda (Helpdesk), el cual permite que los usuarios de los servicios informen de la interrupción de los mismos. Esta mesa de ayuda es la encargada del registro, clasificación, priorización y el cierre de los incidentes que puedan ocurrir en la organización, la mesa de ayuda o Helpdesk utiliza herramientas como, teléfono, correo, chatbots, o herramientas de generación de tickets para la recepción de solicitudes.

2.8.3 Marco de Referencia COBIT 2019

COBIT (Control Objectives for Information Systems and Related Technology) es un marco de trabajo para el gobierno y gestión de las tecnologías de la información de una empresa, en la cual evalúa sus necesidades, condiciones u opciones, permitiendo determinar objetivos y tomar decisiones para mejorar el desempeño y cumplimiento de los objetivos trazados, mediante la planificación, ejecución y monitoreo de las actividades (ISACA, 2020).

COBIT 2019, está conformado por 40 objetivos de control, divididos en cinco objetivos de gobierno y treinta y cinco objetivos de gestión. Los objetivos de gobierno según (ISACA, 2020), se enfoca en tres escenarios, el primero es asegurarse de que las condiciones, necesidades y opciones sean evaluadas para poder trazar objetivos, segundo, es importante la priorización y toma de decisiones y el tercer escenario está relacionado con la evaluación del rendimiento y cumplimiento de los objetivos. Ahora los objetivos de gestión son los encargados de planificar, construir, ejecutar y monitorear las actividades que permitan alcanzar los objetivos.

Por consiguiente, COBIT, define los componentes para crear y sostener el sistema de gobierno. Un sistema de gobierno se encarga de alinear las tecnologías de la información y comunicación, con las estrategias del negocio, integrando las mejores prácticas de organización, planificación, entrega de servicios, implementación, de tal manera que monitoriza el rendimiento de TI, asegurándose que tanto la información de la organización y sus tecnologías soporten los objetivos empresariales.

Por esta razón, este marco de referencia brinda los componentes para crear y sostener el sistema de gobierno, brindando información de procesos, estructuras organizativas, y sobre

todo políticas y procedimientos, por lo cual, es una base que permite crear procedimientos de gestión de incidencias y de servicios de respuesta a incidentes, donde este marco de trabajo, delimita buenas prácticas para la realización de las políticas de respuesta a incidentes de seguridad informática que se utilizan en el CSIRT, el cual se complementa y trabaja conjuntamente con ITILV4, permitiendo establecer directrices para la gestión de servicios de incidencias del CSIRT, basadas en factores como: estrategia, diseño y transición del servicio.

Igualmente, COBIT, permite conocer el nivel de madurez y realizar el análisis situacional en cuanto a gestión de incidentes de seguridad de la información mediante la aplicación de la matriz RACI y matriz PAM. Para ello, con el apoyo del dominio Entregar, dar Servicio y soporte, se tiene el objetivo de gestión DSSO2 – Gestionar las peticiones y los incidentes de servicio, este objetivo tiene como propósito, conseguir mayor productividad y minimizar las interrupciones de los servicios mediante una respuesta rápida y oportuna, en la resolución de incidentes, por tanto, brinda las mejores prácticas que se deberían poner en marcha para la gestión de incidentes de la seguridad de la información, las cuales se detallan en la tabla 14.

Tabla 14

Prácticas de gestión DSS02

Práctica de gestión	**Descripción**
DSS02.01 Definir esquemas de clasificación para incidentes y solicitudes de servicio.	Definir esquemas de clasificación, modelos de incidentes y peticiones de servicio.

DSS02.02 Registrar, clasificar y priorizar solicitudes e incidencias.	Identificar, registrar y clasificar las peticiones de servicio y los incidentes y asignarles una prioridad de acuerdo con la criticidad para el negocio y los acuerdos de servicio.
DSS02.03 Verificar, aprobar y cumplir con las solicitudes de servicio.	Seleccionar los procedimientos apropiados para peticiones y verificar que las solicitudes de servicio cumplan con los criterios de solicitud definidos. Obtener aprobación, si se requiere, y satisfacer las solicitudes.
DSS02.04 Investigar, diagnosticar y asignar incidencias.	Identificar y registrar los síntomas de los incidentes, determinar las causas posibles y asignarlos para su resolución.
DSS02.05 Resolver y recuperarse de incidentes.	Documentar, aplicar y probar las soluciones definitivas o temporales identificados. Realizar acciones de recuperación para restaurar el servicio relacionado con I&T.
DSS02.06 Cerrar solicitudes de servicio e incidentes.	Verificar la solución satisfactoria del incidente y/o cumplimiento de la petición y su cierre.
DSS02.07 Seguimiento del estado y generación de informes.	Hacer seguimiento, analizar e informar regularmente sobre incidentes y el

	cumplimiento de las solicitudes. Examinar tendencias para proporcionar información para la mejora continua.

Fuente: *(COBIT, 2019)*

En base a estas prácticas de gestión se puede aplicar la matriz RACI y matriz PAM, lo cual permite conocer la situación actual de la gestión de incidencias en el DDTI de la UTN.

2.8.3.1 Matriz RACI. Como expresa (Garzón Cruz & Morea Vergara, 2020), la matriz RACI es un herramienta que asigna responsabilidades y roles a cada empleado de la organización en un proyecto, las responsabilidades se presentan a continuación en la tabla 15:

Tabla 15 Descripción de roles de la matriz RACI

Descripción de roles de la matriz RACI

	Rol	Descripción
R	Responsable	Este rol corresponde a quien efectivamente realiza la tarea. Lo más habitual es que exista sólo un encargado (R) por cada tarea.
A	Aprobador	Este rol se responsabiliza de que la tarea se realice y es el que debe rendir cuentas sobre su ejecución. Sólo puede existir una persona que deba rendir cuentas (A).
C	Consultado	Este rol posee alguna información o capacidad necesaria para realizar la tarea.
I	Informado	Este rol debe ser informado sobre el avance y los resultados de la ejecución de la tarea. A diferencia del consultado (C), la comunicación es unidireccional.

Fuente: *(COBIT, 2015).*

2.8.3.2 Matriz PAM. Process Assessment Model (PAM), es un modelo de Evaluación de Procesos de COBIT; es compatible con la norma ISO/IEC 15504 (Determinación de la Capacidad de Mejora del Proceso de Software), y se puede utilizar como base para la realización de una evaluación de la capacidad de cada uno de los procesos

de COBIT. El proceso de evaluación está basado en evidencia para permitir una evaluación confiable, coherente y repetible en el ámbito de la Gestión de las TI de la institución.

El PAM de COBIT apoya la realización de una evaluación y proporciona indicadores para orientar la interpretación del propósito del proceso y los resultados esperados. “Se compone de un conjunto de indicadores de desempeño y capacidad del proceso; los indicadores se utilizan como base para recopilar pruebas objetivas que permitan a un evaluador asignar calificaciones” (UTPL, 2020). Además, proporciona una vista en dos dimensiones: una dimensión del proceso y la otra dimensión de la capacidad.

2.8.4 Norma RFC 2350

La Norma RFC 2350, denominada “Expectativas en el ámbito de la respuesta a incidentes de seguridad informática”, es un documento publicado en 1998 por la universidad de Auckland. Y según (Chuquiguanca, 2020), menciona que este estándar proporciona un marco de trabajo para presentar información relevante en cuanto a incidentes cibernéticos y que son de interés para el público en Internet, en este sentido este estándar presenta una plantilla cuyo objetivo es el de informar de manera detallada a los clientes y público en general dicha información, la cual corresponde a: políticas, constitución, procedimientos que un CSIRT debe cumplir.

Por lo tanto, se complementa con los procedimientos para los servicios de respuesta de incidentes de seguridad de la información en donde esta norma formaliza aquellos requerimientos que debe poseer el CSIRT, para comunicar acera del funcionamiento y servicios que proporcionará el CSIRT en la organización, a todos sus usuarios, mediante el uso de distintas herramientas como email, página web, comunicaciones, etc.

Con base en (RFC2350, s/f), menciona que el propósito de esta norma, es expresar las expectativas que el CSIRT posee, de manera general, siendo esta información la carta de presentación hacia el público y la o las organizaciones a las cuales preste sus servicios, en este sentido, se presenta la siguiente plantilla en la tabla 16, proporcionada por la RFC 2350, la cual consta de 7 secciones, que son: información del documento, información de contacto, estatuto, políticas, servicios, formularios de notificación de incidentes y el descargo de responsabilidad, con una breve explicación de cada sección.

Tabla 16 Plantilla de información del CSIRT en base al RFC 2350

Plantilla de información del CSIRT en base al RFC 2350

1. Información del documento	
Este apartado precisa información de la última modificación del documento, listas de correo como mecanismo para distribuir información haciendo uso de firmas digitales y la ubicación en la cual se puede acceder al documento.	1.1 Fecha de la última actualización 1.2 Lista de distribución para notificaciones 1.3 Ubicaciones donde se puede encontrar este documento
2. Información de contacto	
En esta sección, se detalla información que sirva para ponerse en contacto con el CSIRT.	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 telecomunicaciones
	2.7 Direcciones de correo electrónico
	2.8 Claves públicas e información de cifrado
	2.9 Miembros del equipo
	2.10 Otra información
	2.11 Puntos de contacto con el cliente
3. Estatuto	
La subsección estatuto, especifica lo que el equipo CSIRT va a realizar, a quién va dirigido la prestación de los servicios, la organización que patrocina el CSIRT y la autoridad que posee en la organización a la cual brinda sus servicios.	3.1 Declaración de la misión
	3.2 Unidad constitutiva
	3.3 Patrocinio y/o afiliación
	3.4 Autoridad
4. Políticas	
El epígrafe de las políticas brida información sobre los lineamientos que se van a seguir para gestionar incidentes, se especifica con que otros CSIRT se interactúa, y los métodos que permita brindar una comunicación segura y verificable.	4.1 Tipos de incidentes y nivel de apoyo
	4.2 Cooperación, interacción y divulgación de información
	4.3 comunicación y autenticación

5. Servicios	
La sección de servicios, permite especificar los servicios que brinda el CSIRT	5.1 Respuesta a incidentes 5.2 Actividades proactivas
6. Formularios de notificación de incidentes	
Es importante, presentar un formulario simple, que puedan hacer uso los usuarios para notificar incidentes.	
7.Descargo de responsabilidad	
Finalmente, precisa informar la exención de cualquier responsabilidad y advertir de limitaciones de la información presentada.	

Nota: *Adaptado de (RFC2350, s/f).*

2.9 Metodologías de Proceso de Diseño de un CSIRT

Las metodologías utilizadas para el proceso de diseño de un CSIRT, están contenidas en la documentación guía, en este sentido se tiene el Manual del CSIRT publicado por el CERT/CC y la Universidad de Carnegie Mellon, la Guía de creación de un CSIRT publicada por ENISA, y, el Manual de Gestión de Incidentes de Seguridad informática, publicado por el proyecto AMPARO. A continuación, su detalle:

2.9.1 Manual del CSIRT Publicado por el CERT/CC

El Manual del CSIRT, publicado por el CERT/CC y el Instituto de Software de la Universidad de Carnegie Mellon, informa sobre los pasos para crear un CSIRT, haciendo mención de ocho pasos básicos, como se presentan en la tabla 17, que son:

Tabla 17 Pasos Básicos para Crear un CSIRT

Pasos Básicos para Crear un CSIRT

Pasos para crear un CSIRT
1. Obtener el apoyo de la organización para la planificación e implantación del CSIRT
2. Determinar el plan estratégico del CSIRT
3. Obtener información relevante
4. Diseñar la visión del CSIRT
5. Comunicar la visión y el plan operativo del CSIRT
6. Comenzar con la implementación del CSIRT
7. Anunciar que el CSIRT está en funcionamiento
8. Evaluar la efectividad del CSIRT

Fuente: *(Manual CSIRT del CERT/CC, 2017)*

Aunque los CSIRT son diferentes en su funcionamiento, debido al personal disponible, la experiencia, los recursos presupuestarios y las circunstancias únicas de cada organización, existen algunas prácticas básicas que se utilizan para su diseño, en las que el CERT/CC hace referencia y que son los ocho pasos anteriormente descritos, cuyos procesos no son secuenciales, ya que muchos pasos pueden gestionarse en paralelo.

Paso 1: Obtener soporte de administración y aceptación

La aprobación y el apoyo de la gerencia, permite que exista la provisión de recursos, financiación y tiempo, a la persona o grupo de personas, para que actúen como parte del equipo del proyecto para implementar el CSIRT. Esto también incluye ejecutivos de negocios o departamentos, gerentes de división y su personal, dedicando tiempo a participar en este proceso de planificación. Es importante obtener las expectativas y percepciones de la gerencia sobre la función y la respuesta del CSIRT.

Sin esta información, se puede formar un equipo cuyos servicios y autoridad no se entiendan, junto con la obtención de apoyo de gestión, para el proceso de planificación e implementación, es igualmente importante obtener el compromiso de la gerencia para mantener las operaciones y la autoridad del CSIRT a largo plazo.

Paso 2: Determinar el Plan Estratégico del CSIRT

El Plan estratégico del CSIRT consiste en definir asuntos administrativos que deben ser tratados, y qué problemas de gestión de proyectos deben abordarse, como son plazos específicos que cumplir, el grupo de proyecto, su ubicación, además se tendrá que dejar que la organización conozca el plan a seguir para la creación del CSIRT en las primeras etapas de desarrollo, esto ayudará el personal a que se sienta parte del proceso de diseño.

Paso 3: Recopilar información relevante

Se necesitará recopilar información para determinar la respuesta a incidentes y las necesidades de servicio que tiene la organización, es decir revisar los tipos de actividad de incidentes que actualmente se informan dentro de la organización, identificar qué información es necesaria para planificar e implementar el CSIRT, en este sentido es importante definir quién tiene esa información y la mejor manera de obtener esa información es a través de encuestas, foros de discusión, entrevistas, reunirse con las partes interesadas clave para analizar no solo sus necesidades de respuesta a incidentes, sino también para lograr un consenso sobre las expectativas, dirección estratégica, definiciones y responsabilidades del CSIRT.

Las partes interesadas podrían incluir a las siguientes áreas*:* "gerentes de negocios, representantes de TICs, del departamento legal, de recursos humanos, de relaciones públicas, cualquier grupo de seguridad existente, incluida la seguridad física, especialistas en auditoría

y gestión de riesgos, representantes generales de la organización*" (Manual CSIRT del CERT/CC, 2017).*

Ahora bien, otro aspecto importante es saber qué necesitará hacer el CSIRT, con el objetivo de identificar a las personas adecuadas que participen en el desarrollo de los procedimientos. También puede haber algunos recursos disponibles para su revisión que ayudarán en la recopilación de información, los cuales incluyen en la tabla 18:

Tabla 18 Herramientas de recopilación de información para CSIRT

Herramientas de recopilación de información para CSIRT

Recursos útiles de recopilación de la información
Organigramas para la empresa y funciones comerciales específicas
Topologías para sistemas y redes organizacionales o de organización
Sistema crítico e inventarios de activos
Planes existentes de recuperación ante desastres o de continuidad del negocio.
Pautas existentes para notificar a la organización de una violación de seguridad física
Cualquier plan de gestión de incidentes existente
Cualquier regulación parental o institucional
Cualquier política y procedimiento de seguridad existente

Fuente: *(Manual CSIRT del CERT/CC, 2017)*

La revisión de estos documentos tiene un doble propósito: primero, identificar las partes interesadas existentes, los recursos y propietarios del sistema; y segundo, proporcionar una visión general de las políticas existentes a las que el CSIRT deberá sujetarse.

Paso 4: Diseño de la visión CSIRT

A medida que la información reunida pone en primer plano las necesidades de respuesta a incidentes de la organización y a medida que construye su comprensión de las expectativas de la gerencia, se comienza a identificar los componentes clave del CSIRT. Esto le permite definir la visión del CSIRT, sus objetivos y funciones, agregando a lo anterior, la visión para el CSIRT debe incluir una explicación clara de dónde funcionan estos equipos, su ubicación en la estructura organizacional actual y cómo el CSIRT interactúa con la organización.

La visión, explica qué beneficios proporciona el CSIRT, qué procesos se lleva a cabo, con quién se coordina y cómo realiza sus actividades de respuesta. Al crear la visión, se puede seguir el proceso detallado en la tabla 19:

Tabla 19 Proceso para crear la visión del CSIRT

Proceso para crear la visión del CSIRT

Procedimiento para crear la visión del CSIRT
1. Identificar la organización a quien presta servicios el CSIRT
2. Definir la misión, metas y objetivos CSIRT
3. Seleccionar los servicios CSIRT que brindará a la organización (u otros)
4. Determinar el modelo organizacional
5. Identificar los recursos requeridos
6. Determinar la financiación CSIRT

Fuente: (*Manual CSIRT del CERT/CC, 2017)*

Paso 5: Comunicación de la visión del CSIRT

Se comunicará la visión y el plan operativo del CSIRT a la gerencia, su organización y otros departamentos, quienes necesiten conocer y comprender sus operaciones, esta es una

forma de comenzar a comercializar el CSIRT a la organización y de esta manera obtener la aceptación de cada uno de los miembros.

Paso 6: Evaluación de la efectividad del CSIRT

Una vez que el CSIRT ha estado en funcionamiento por un tiempo, es necesario, determinar la efectividad del equipo y utilizar los resultados de la evaluación para mejorar los procesos del CSIRT y garantizar que el equipo reúna las necesidades de la organización.

El CSIRT, en conjunto con la gerencia y la organización, desarrollarán un mecanismo para realizar dicha evaluación. Ahora, la información sobre la efectividad, puede recopilarse a través de una variedad de mecanismos de retroalimentación, que incluyen: evaluación comparativa contra otros CSIRT, discusiones generales con representantes de la organización, encuestas de evaluación distribuidas periódicamente a los miembros de la organización y creación de un conjunto de criterios o parámetros de calidad que luego es utilizado por una auditoria o por un tercero para evaluar el equipo.

También puede ser útil revisar información recopilada previamente sobre el estado de la organización u organizaciones, antes de la implementación del equipo. Esta información se puede utilizar como línea de base para determinar el efecto del CSIRT en la organización. Además, la información recopilada para la comparación, puede incluir: número de incidentes reportados, tiempo de respuesta o tiempo de vida de un incidente, número de incidentes resueltos con éxito, información presentada a la organización sobre problemas de seguridad informática o actividad continua, atención a los problemas de seguridad dentro de la organización, técnicas preventivas y prácticas de seguridad establecidas (UTPL, 2020).

2.9.2 Guía de Creación de un CSIRT Publicada por ENISA

El presente documento describe el proceso de creación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) desde todas las perspectivas pertinentes, como la gestión empresarial, la gestión de procesos y el punto de vista técnico. Los principales grupos destinatarios de este informe son las instituciones públicas o no, que decidan crear un CSIRT para proteger su propia infraestructura de TI o la de sus grupos de interés. (ENISA, 2006).

Este documento explica qué es un CSIRT, qué servicios puede prestar y qué pasos hay que dar para ponerlo en marcha. De este modo se presenta una visión general adecuada y práctica del enfoque, la estructura y el contenido de la creación de un CSIRT. Esta guía consta de los siguientes capítulos descritos en la tabla 20:

Tabla 20 Capítulos que contempla la creación del CSIRT - ENISA

Capítulos que contempla la creación del CSIRT - ENISA

Estructura de creación de un CSIRT
1. Introducción
2. Estrategia general de planificación y creación de un CSIRT
3. Desarrollar un plan comercial
4. Promover el plan comercial
5. Ejemplos de procedimientos operativos y técnicos
6. Formación del personal del CSIRT
7. Ejercicio: producción de un aviso
8. Descripción del plan de proyecto

Fuente: *(ENISA)*

2.9.3 Manual de Gestión de Incidentes de Seguridad Informática, Publicado por el Proyecto AMPARO

Este documento, permite comprender que es un CSIRT, sus características, beneficios, tipos de servicios, se detalla lineamientos y recomendaciones que será utilizada para la creación de un CSIRT como recomendaciones para los medios de comunicación los cuales deberán garantizar una comunicación segura, los tipos de estructura organizacional, recomendaciones de políticas de seguridad informática, recomendaciones en cuanto a la infraestructura física para un CSIRT, infraestructura de red y los procesos de gestión de incidentes de seguridad (Lacnic, 2012).

Las recomendaciones más relevantes de este manual se presentan en la tabla 21 que corresponde a recomendaciones de seguridad física y ambiental y en la tabla 22, se menciona las recomendaciones de la arquitectura de redes, cabe recalcar que no todas las recomendaciones deben implementarse desde un inicio, si no deberán ir adaptándose a su realidad y conforme el tiempo y los servicios avancen podrá ir adoptando las recomendaciones.

Tabla 21

Recomendaciones de Seguridad Física y Ambiental

SEGURIDAD FÍSICA Y AMBIENTAL	
PARÁMETROS	**RECOMENDACIONES**
1. Local Físico	Espacio disponible, acceso a equipos y personal, instalaciones eléctricas, acondicionamiento térmico y elementos de seguridad,
2. Espacio y Movilidad	Características de espacio, posición de columnas, movilidad de equipos, suelo falso o móvil,
3. Tratamiento Acústico	Equipos ruidosos o sujetos a vibración deben encontrarse en zonas de amortiguación,
4. Ambiente Climático	Temperatura de oficinas con computadoras debe estar entre 18 y 21°C y la humedad relativa del aire de estar entre 45% y 65%, debe contar con sistemas que renueven el aire periódicamente, y el ambiente sonoro no debe superar a los 55 decibeles,
5. Instalación Eléctrica	Independencia de suministro eléctrico para el centro de cómputo y los equipos para evitar interferencias con elementos de protección,
6. Picos y Ruidos Electromagnéticos	Evitar subidas y caídas de tensión, interferencias de ruido con los componentes electrónicos, datos.
7. Cableado	Selección del cableado indicado y certificación, los riesgo más comunes son la interferencia, corte del cable y tiempo del cableado.
8. Iluminación	El sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas y falta de luz.

9.	**Seguridad Física del Local**	Deberá contar con sistema contra incendios, protección contra inundaciones y otros peligros que afecten a las instalaciones y condiciones del lugar.
10.	**Recomendaciones en futuro**	Debido al crecimiento que se puede tener es importante reforzar otros elementos que permitan la escalabilidad y robustecer la seguridad, como por ejemplo aseguramiento contra situaciones hostiles (robo de equipos, información, fraude, sabotajes), el establecimiento de control de accesos (acceso biométrico, circuitos cerrados, protección electrónica).

Tabla 22

Recomendaciones Arquitectura de Redes

ARQUITECTURA DE REDES		
PARÁMETROS		**RECOMENDACIONES**
1. Ambiente Físico	1.1. Áreas Administrativas	Salas de reuniones pueden ser compartidas con el resto de la organización.
	1.2.Áreas Operativas	Salas de trabajo del equipo técnico, sala de servidores, laboratorio, son considerados ambientes críticos por tanto debe considerarse un ambiente aislado, segmentación del circuito de servicios (separación física, las redes de computadoras, así como el accesos a internet), acceso restringido, políticas de seguridad de la información.
Las áreas físicas mínimas recomendables son: recepción, oficina del director, sala de reuniones, sala de archivos, sala de operaciones, laboratorio, sala de servidores.		

2. Infraestructura de Red	La red de computadores del CSIRT deberá estar separada de la infraestructura de la organización.	
3. Hardware	3.1. Equipos y medios de conectividad	Routers, Switches, Cableado Estructurado, Internet, Dispositivos de Seguridad (Antivirus, IDS, IPS), Firewall, Detección de Intrusos, Correo electrónico, WEB, NTP, DNS, Bitácoras, Intranet, Acceso Remoto (RVP), Backup.
	3.2. Estaciones de trabajo y equipos portátiles	Estaciones de trabajo, computadores portátiles, Discos Duros Externos, pen drive, herramientas.
	3.3. Equipos para la seguridad en ambiente físico	Sistema de protección contra incendios, sistema de refrigeración, infraestructura de protección contra interrupciones de energía eléctrica.
	3.4. Otros	Proyectores, impresora, cintas magnéticas, trituradora de papel, material de oficina
4. Software	Uso de software libre para sistemas operativos de servidores, estaciones de trabajo y equipos portátiles, siempre que sea posible	
	4.1. Aseguramiento de sistemas	Configuración en modo seguro, instalar últimas actualizaciones y correcciones de seguridad, sistema de registro de eventos, sistema de control de flujo de trabajo para el registro y seguimiento de incidentes, sistemas de información en la web para recolectar información de incidentes y divulgación de alertas, recomendaciones estadísticas, aplicativos de criptografía y firma digital, aplicativos para análisis forense, programas de virtualización

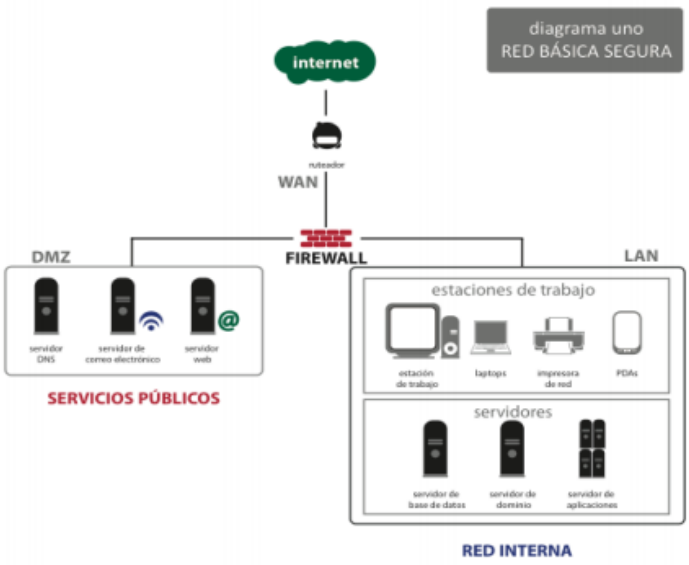
Otra de las recomendaciones que presenta el manual del proyecto AMPARO tiene que ver con las políticas de seguridad de la información, las cuales sirven como medio de comunicación con los usuarios, ya que se establece un comportamiento formal de parte del personal de la organización con los recursos y servicios de la empresa. En este sentido la recomendación del manual sugiere que para la formulación de políticas de seguridad informática es importante considerar los siguientes elementos: alcance, objetivo (s), identificación de roles, responsabilidad y procedimientos.

Por otra parte, el manual básico de gestión de incidentes de seguridad informática del proyecto AMPARO presenta cuatro esquemas de red los cuales se detalla a continuación:

En la figura 1 el esquema corresponde a la red básica segura, el cual está conformado por un equipo Firewall, una DMZ y la red interna, siendo una red para organizaciones medianas y recursos humanos compartidos.

Figura 1

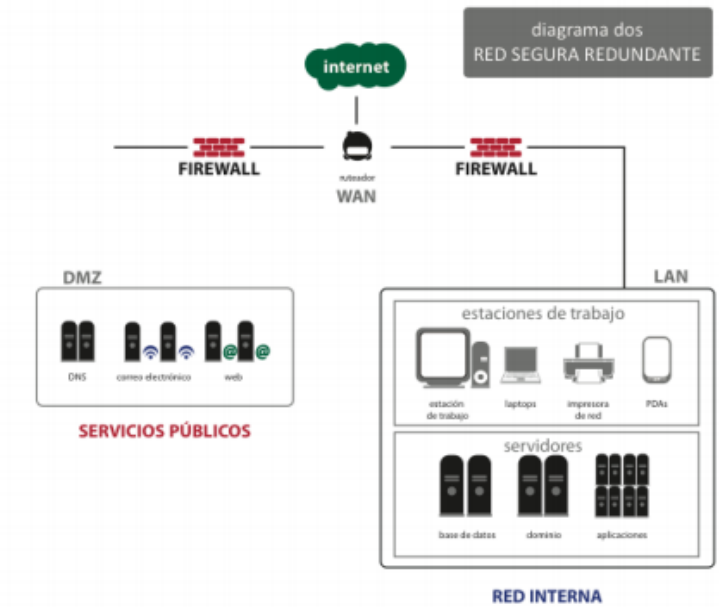
Red básica segura



Por otra parte, en la figura 2 se presenta el esquema de red segura redundante, este esquema está conformado por dos Firewall, una DMZ y la red interna, esta red permite brindar servicios reactivos.

Figura 2

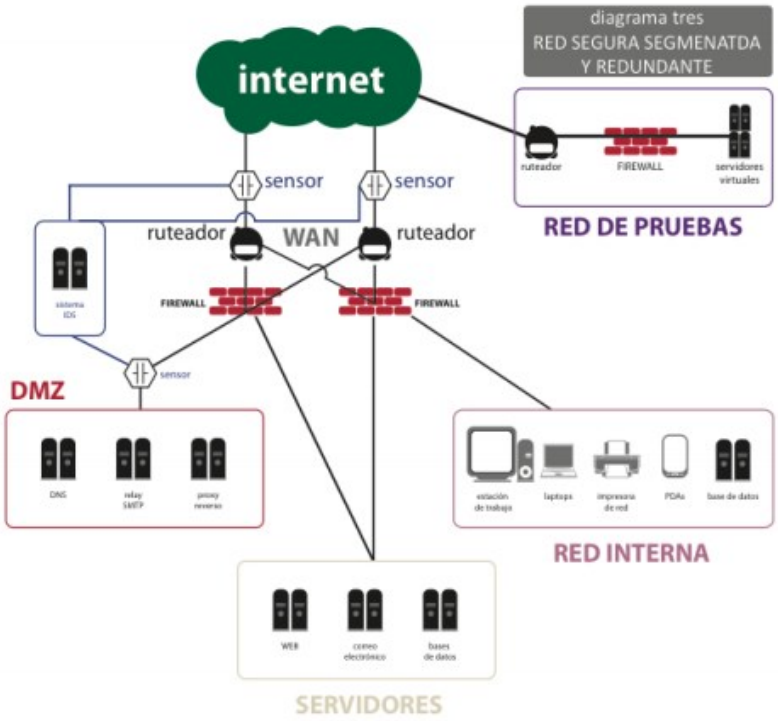
Red Segura Redundante



En este sentido en la figura 3 se tiene el esquema de red segura segmentada y redundante, la red está conformada por dos Firewall que trabajan en forma redundante, una DMZ, una red de pruebas, la cual tiene sensores y sistema de detección de intrusos (IDS), enlaces de internet redundantes, alta disponibilidad en sus servicios y la red interna, este esquema permite brindar servicios reactivos y proactivos.

Figura 3

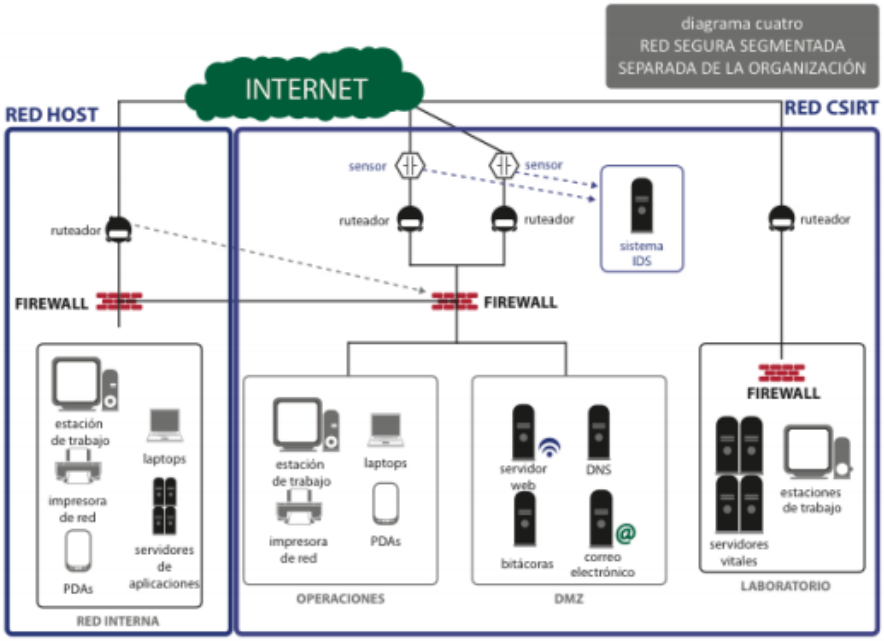
Red Segmentada y Redundante



Finalmente, en la figura 4 se presenta la red segura segmentada separada y redundante, este esquema presenta separación física entre la red del CSIRT y de la organización, tres redes diferentes, enlaces de internet redundantes, sensores e IDS, una red aislada para pruebas, es ideal para prestar servicios reactivos y proactivos (Lacnic, 2012).

Figura 4

Red Segura Segmentada Separada y Redundante



De modo que todos estos esquemas de red, deben adaptarse según los servicios que se vayan a brindar, así como la infraestructura que se posee, inicialmente se puede comenzar con una red básica segura, y conforme los servicios se vayan incrementando y el CSIRT vaya madurando puede ir escalando a otro esquema de red.

2.10 Herramientas de Monitoreo de Redes

Según (Velasco Briones & Cagua Ordoñez, 2017), una herramienta de monitoreo, es un sistema que permite la monitorización constante, así como la búsqueda de fallas en los servicios de una red, los cuales son notificados al administrador de red, permitiendo detectar a tiempo algún evento y minimizando cualquier impacto que se presente en la organización. En este sentido, (Sánchez, 2016), menciona que una herramienta de monitoreo de redes deberá presentar características como: administración remota vía WEB, notificaciones en caso de la presencia de fallos y ser capaz de mostrar el comportamiento de los dispositivos de la red.

Ahora bien, dentro de las opciones, se puede encontrar múltiples herramientas que permiten el monitoreo de las redes, de esta manera existen herramientas que son de pago como por ejemplo Solarwinds, PRTG Network, OpManager, y herramientas de código libre como Zabbix, Cacti y Nagios. En consecuencia, para el presente trabajo se analizan exclusivamente estas tres últimas herramientas por ser de código libre, ya que según (MINTEL, 2020), menciona el decreto 1073 emitido el 12 de junio del 2020 denominado "Reglamento para la adquisición de software por parte de las entidades contratantes del sector público", en el cual establece el uso de software de código libre en instituciones públicas, por tanto a continuación se menciona las características de estas herramientas.

En este sentido, según (Sánchez, 2016), Zabbix permite la monitorización y el registro del estado de los servicios y equipos de la red, como por ejemplo SMTP (Protocolo para Transferencia Simple de Correo) o HTTP (Protocolo de Transferencia de Hipertexto), carga del CPU, espacio en disco, haciendo uso de SNMP (Simple Network Manager Protocol), los cuales se pueden visualizar mediante una interfaz web.

Por otro lado, se tiene la herramienta Cacti, esta herramienta monitoriza y presenta estadísticas de redes y servidores, haciendo uso de RRDtool (Round-Robin database tool) como herramienta para el almacenamiento y representación de datos, puede monitorizar la carga del CPU, capacidad de memoria, número de paquetes perdidos, tráfico de la red. (Velasco Briones & Cagua Ordoñez, 2017).

Así mismo (Velasco Briones & Cagua Ordoñez, 2017), mencionan que Nagios es una herramienta muy utilizada para la comprobación de conectividad de los dispositivos de la red, de esta manera se garantiza que se brinde los servicios a la organización, para ello Nagios permite la supervisión de los recursos de los dispositivos y servicios de la red, tanto

en hardware como en software, mediante el envío de notificaciones, posee una interfaz web para su administración, y presenta gráficas de estados de los diferentes componentes de los dispositivos de la red.

2.11 Sistemas Operativos de Seguridad de la Información

Existen múltiples sistemas operativos (S.O) de código libre los cuales tiene herramientas para realizar auditorías de seguridad, alguno de los sistemas operativos que se encuentran son Kali Linux, Back Box, Black Buntu, entre otros, estos sistemas operativos comparten características relacionadas con la seguridad informática, en la tabla 23 se menciona características como su sistema operativo base, y características necesarias para realizar análisis de seguridad de la información, como por ejemplo: recopilación de información, mapeo de red, evaluaciones de seguridad y vulnerabilidades así como la detección y prevención de intrusos.

Tabla 23 Características y Requerimientos de los S.O de Seguridad Informática

Características y Requerimientos de los S.O de Seguridad Informática

	Kali Linux	**BackBox**	**BlackBuntu**
S.O basado en	Debian	Ubuntu	Ubuntu
Recopilación de la Información	Si	Si	Si
Mapeo de Red	Si	No	Si
Evaluación de Vulnerabilidades	Si	Si	Si

Detección y Prevención de Intrusos	Si	No	No
Evaluaciones de seguridad	Si	Si	Si

Ahora bien, en referencia a la tabla 23, según (Ericka, 2015) la recopilación de la información de la red permite la obtención de datos de la red, como las direcciones IP, tecnología utilizada tanto en hardware como en software, así mismo el mapeo de red, que permite reconocer los host que están activos, y con esto conocer los puertos y aplicaciones que están haciendo uso, así como sistemas operativos y servicios.

Por otro lado, para (Romero Castro, Figueroa Moràn, & Vera Navarrete, 2018) el análisis de vulnerabilidades permite conocer un fallo en los sistemas y redes, el cual puede ser explotado por atacantes convirtiéndose en un riesgo para la organización, de esta manera es necesario realizar una evaluación de seguridad de la información, cuyo objetivo es evaluar la eficiencia de la red, mediante la detección de fallas para su posterior solución. Con base en (Tinoco, 2020), brinda un dato importante que permite aclarar la diferencia entre un análisis de vulnerabilidades y un pentesting, siendo así, el primero se limita a identificar, analizar y reportar vulnerabilidades, mientras que el pentesting por lo general consta de fases como: recolección de información, escaneo de vulnerabilidades, ataque y reporte de las vulnerabilidades encontradas.

De esta manera, como lo hace notar (Hertzog, O'Gorman, Aharoni, & O'Gorman, 2021), Kali Linux, es una distribución de Linux basado en Debian, además, es una herramienta

desarrollada por Offensive Security, la cual es una empresa que trabaja con pentesting, seguridad de la información y análisis forense digital, esta distribución posee herramientas para la recolección de la información, análisis de vulnerabilidades, ataques, intrusión, explotación y herramientas forenses, haciendo de esta herramienta la más popular para usos de hacking ético, entre las herramientas para la recolección de información, y análisis de vulnerabilidades se tiene Nmap, Zenmap y OpenVas, así como también permite la configuración de Snort para la detección y prevención de intrusos, haciendo de este sistema operativo el más adecuado para el presente trabajo.

2.11 Herramientas de Gestión de Incidentes

El objetivo de gestionar incidentes, es la restauración del servicio lo antes posible, evitando causar daños en la organización, o a su vez minimizar los daños que se puedan ocasionar, de esta manera se garantiza mantener la disponibilidad y calidad en los servicios brindados, teniendo en cuenta para la gestión de incidentes, características como límite de tiempo, modelos de incidencias, escalado funcional y escalado jerárquico.

Ahora bien, una herramienta de gestión de incidentes es un sistema que tiene tres objetivos, restablecer el servicio y minimizar los incidentes, registro de información relevante sobre las incidencias y la incorporación de las mejores prácticas.

En este sentido, existen herramientas de código libre y de versión pagada que permiten la gestión de incidentes, para el caso del presente trabajo se menciona herramientas open source, por lo tanto, se tiene OTRS (Open-Source Ticket Request System), Mantis y Request Tracker, en la tabla 24 se menciona las características de cada una de ellas.

Tabla 24

Características de las herramientas de Tickets

Característica	OTRS	MANTIS	REQUEST TRACKER
Gestión de servicios compatibles con ITIL	Sí	No	Sí
Base de datos del Conocimiento	Sí	No	Sí
Respuestas automáticas	Sí	Sí	Sí
Encuestas	Sí	No	Sí
Reportes	Sí	No	Sí
Asignación de prioridades a los incidentes	Sí	Sí	No
Notificaciones por correo	Sí	Sí	Sí

Nota: Tomado de varios estudios (Robayo Carvajal & Castro Bayas, 2015; Arrogante, 2010)

En referencia a la tabla 24, se describe las características que se debe tener en cuenta para la elección de una herramienta de gestión de incidentes de seguridad de la información, como primer punto se menciona la gestión de servicios que sean compatibles con ITIL, en este sentido los servicios de importancia para un CSIRT, y, en base a ITIL, son la gestión de incidentes, eventos, problemas y atención al cliente, como segundo punto, se menciona como característica, que posea una base de datos del conocimiento, este aspecto corresponde a información detallada sobre incidentes, permitiendo brindar respuesta de una manera más ágil ante la presencia de un evento que haya ocurrido, otra característica de una herramienta de gestión de incidentes es brindar respuestas automáticas, ante el reporte de cualquier incidente, ayudando al usuario dar seguimiento a su reporte, seguidamente, para poder mejorar el servicio, es necesario contar con el envío automático de encuestas a los usuarios del servicio, permitiendo conocer su opinión en cuanto al servicio brindado, otro aspecto fundamental es la generación de reportes, facilitando la evaluación del servicio entregado, luego, un elemento indiscutible para la gestión de incidentes es la posibilidad de priorizar incidentes, según una evaluación previa, y finalmente permitir la notificación por correo la presencia de un incidente, así como el cierre del mismo al usuario.

CAPÍTULO III ANÁLISIS DE REQUERIMIENTOS

El tercer capítulo permite conocer a la Universidad Técnica del Norte como institución, y al Departamento de Desarrollo Tecnológico e Informático, en aspectos como la misión, visión, infraestructura tecnológica, y servicios tecnológicos que presta la universidad.

Además, en este capítulo se presenta una visión más clara sobre las vulnerabilidades del sistema informático en la Universidad Técnica del Norte, con una introspección a sus controles y herramientas de prevención, detección y mitigación, conociendo sus debilidades y fortalezas, mediante una metodología de investigación de campo con el desarrollo de encuestas aplicadas al administrador de red, personal administrativo, docentes y alumnos de la UTN en sus principales facultades.

Posteriormente, los resultados de estas encuestas son evaluadas, permitiendo obtener un diagnóstico final, que conjuntamente con el desarrollo, evaluación, análisis e interpretación de la matriz de riesgos de seguridad informática, el análisis FODA del DDTI en la UTN, el análisis de la matriz RACI y de la matriz PAM se podrán establecer y definir los servicios de gestión de incidentes de seguridad informática, que brindará el CSIRT Académico en la UTN.

3.1 Situación Actual de la UTN y la Dirección de Desarrollo Tecnológico e Informático (DDTI)

Uno de los requerimientos importantes para el desarrollo del diseño del CSIRT académico de la UTN, es conocer la institución, en aspectos tales como su razón de ser, perspectiva, servicios ofrecidos a su comunidad, que serán útiles para determinar la misión, visión y servicios del CSIRT.

Por lo tanto, la situación actual de la UTN y el DDTI, permite tener una idea más clara del entorno en el cual el CSIRT operará en un futuro, por tanto, se realiza un análisis interno y externo, para lo cual en el análisis interno permite identificar factores como la misión, visión, factor organizacional, servicios, y por parte del análisis externo el factor social y las fuerzas competitivas.

Por otro lado, el análisis externo permite identificar los factores que no pueden ser controlados en su totalidad por la institución, pero que se puede tomar acciones para tal efecto, para el caso de estudio se mencionan dos factores, el factor social y las fuerzas competitivas, el primero hace referencia a las características de la sociedad que le rodea a la universidad, con las cuales se puede trabajar conjuntamente para el beneficio de ambas partes, y en cuanto a las fuerzas competitivas, se menciona la existencia de otras instituciones de educación, en las cuales el CSIRT puede brindar sus servicios, permitiendo el crecimiento del mismo, y obteniendo ventajas competitivas sobre éstas.

3.1.1 Análisis Interno de la UTN

Ahora bien, el análisis interno de la UTN y el DDTI, implica identificar los aspectos más relevantes de la institución, los cuales permitan analizar la razón de ser y hacia dónde se dirige en un futuro, tanto de la UTN como del DDTI lo cual viene a ser su misión y visión.

Por otro lado, se tiene las áreas funcionales, que comprende el factor organizacional, en el cual se presenta su estructura y forma en la cual se coordina cada una de sus acciones, además se menciona su infraestructura tecnológica, y los servicios tecnológicos que presta la institución. Por lo tanto, en conformidad a lo presentado en el Plan institucional Anual de la UTN en el 2020 se obtuvo la siguiente información

Misión UTN

> La Universidad Técnica del Norte es una institución de educación superior, pública y acreditada, forma profesionales de excelencia, críticos, humanistas, líderes y emprendedores con responsabilidad social; genera, fomenta y ejecuta procesos de investigación, de transferencia de saberes, de conocimientos científicos, tecnológicos y de innovación; se vincula con la comunidad, con criterios de sustentabilidad para contribuir al desarrollo social, económico, cultural y ecológico de la región y del país (UTN, 2020).

Visión UTN

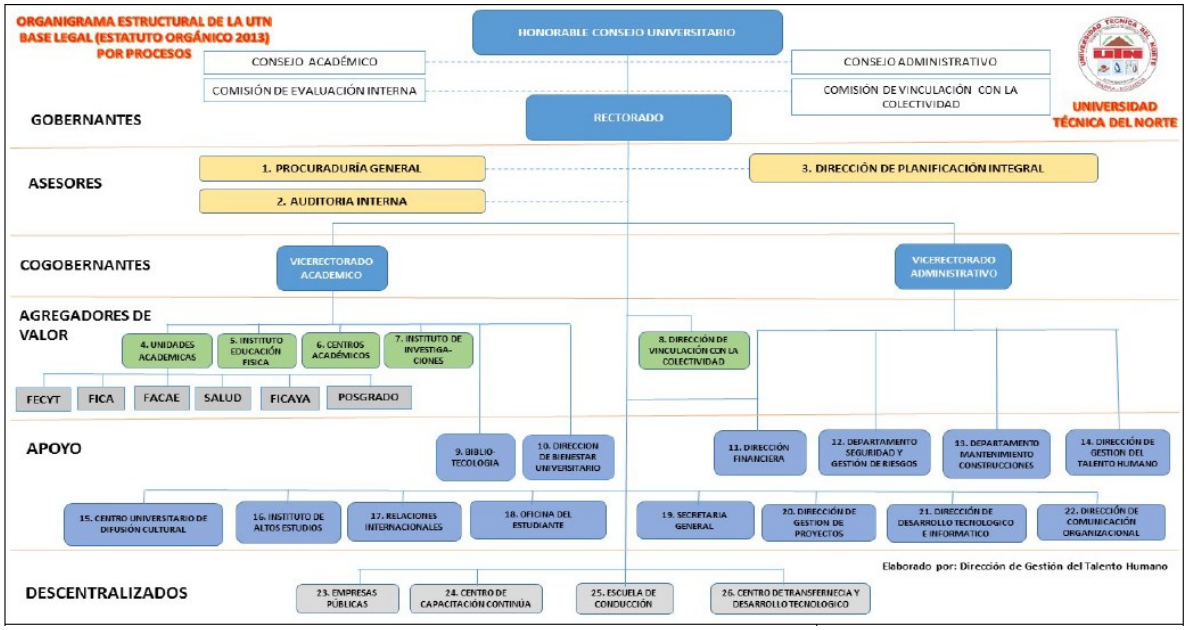
> La Universidad Técnica del Norte, en el año 2020, será un referente regional y nacional en la formación de profesionales, en el desarrollo de pensamiento, ciencia, tecnología, innovación y vinculación, con estos estándares de calidad internacional en todos sus procesos; será la respuesta académica a la demanda social y productiva que aporta para la transformación y la sustentabilidad (UTN, 2020).

Factor Organizacional

La UTN cuenta con la red organizacional presentada en la Figura 5, según lo dispuesto por la Dirección de Gestión del Talento Humano, con orden del Honorable Consejo Universitario (HCU):

Figura 5

Organigrama Estructural de la UTN

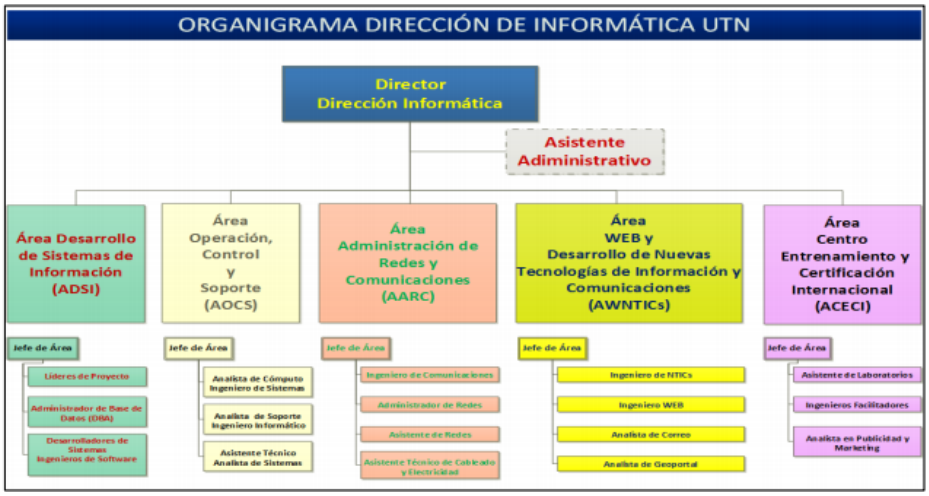


Fuente: *Tomado del portal web de la* ***UTN****, 2020*

Adicionalmente, la figura 6 presenta la estructura organizacional de la Dirección de Desarrollo Tecnológico e Informático (DDTI) de la UTN, la cual consta de cinco áreas importantes y enfocadas al aspecto tecnológico. En este sentido, el CSIRT propuesto deberá ser considerado como una nueva área dentro del organigrama del DDTI bajo los lineamientos de la misión y visión de dicha Dirección, mismos que se describen a continuación.

Figura 6

Organigrama del DDTI



Fuente: *Plan de Desarrollo Informático UTN 2013 - 2017, 2020*

Misión DDTI-UTN

La Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte, le corresponde administrar los servicios de informática, computación y comunicaciones, sin perjuicio de las demás funciones que se le recomiende. Ser el ente regulador de las políticas y normativas de carácter institucional; que deben ser llevadas a cabo con rigor, manteniendo el alto espíritu de calidad en todos los funcionarios, con el fin de lograr las expectativas encomendadas al departamento (UTN, 2020).

Visión DDTI-UTN

La dirección de informática en el año 2017 será quien ejerza el liderazgo a nivel institucional, regional y nacional en el campo de la informática, computación

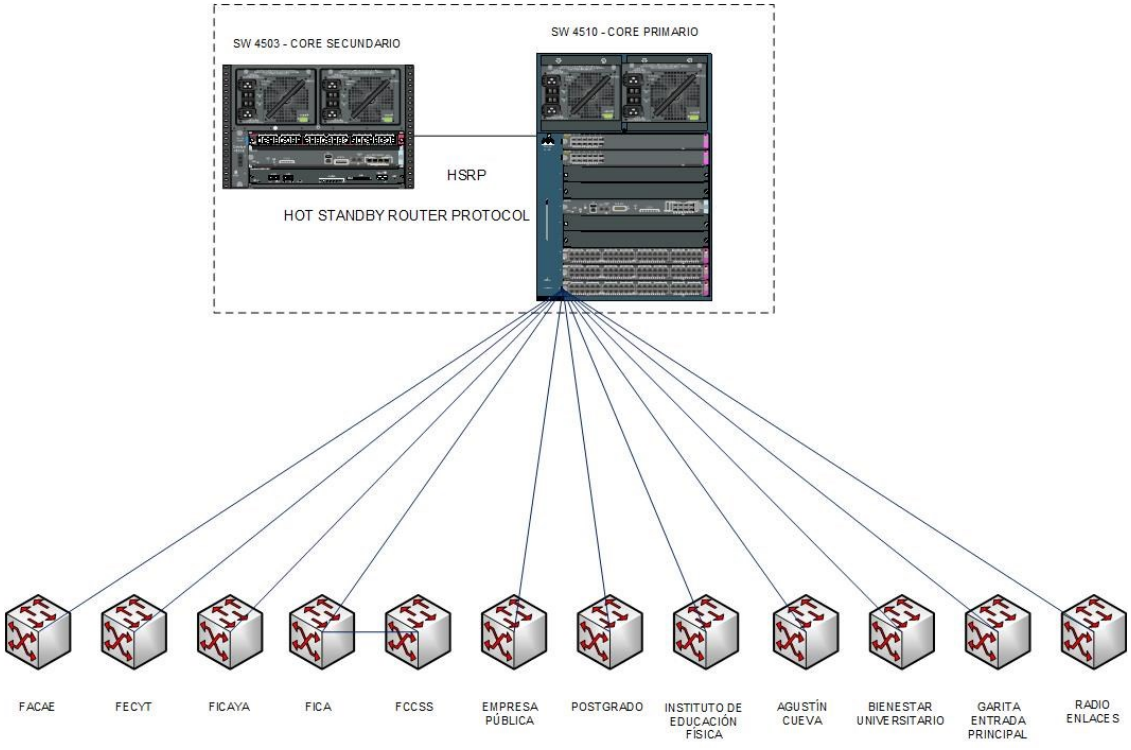
y telecomunicaciones con tecnología de punta, investigaciones de avanzada e innovación que aportará para la transformación de la UTN (UTN, 2020).

Factor Infraestructura

En este sentido, la UTN cuenta con una infraestructura tecnológica moderna, cuya red está segmentada por vlan´s distribuidas indistintamente por las facultades y las dependencias de la UTN. Como se muestra en el esquema de red interno de la UTN en la Figura 7, las diferentes facultades están interconectadas mediante enlaces de fibra óptica sin redundancia con una capacidad de canal de 1 Gbps.

Figura 7

Infraestructura de red de la UTN



Fuente: *Tomado del DDTI de la* ***UTN****, 2020*

En cuanto al esquema de red de datos y comunicaciones de la UTN se muestra en la Figura 8, en la cual el proveedor de internet (CEDIA) llega mediante 2 enlaces de fibra óptica con tecnología WDM, redundantes y con una capacidad de canal de 10 Gbps cada uno, los cuales se conectan a un router marca NOKIA, cumpliendo la función de router de frontera de la red de datos CEDIA-UTN.

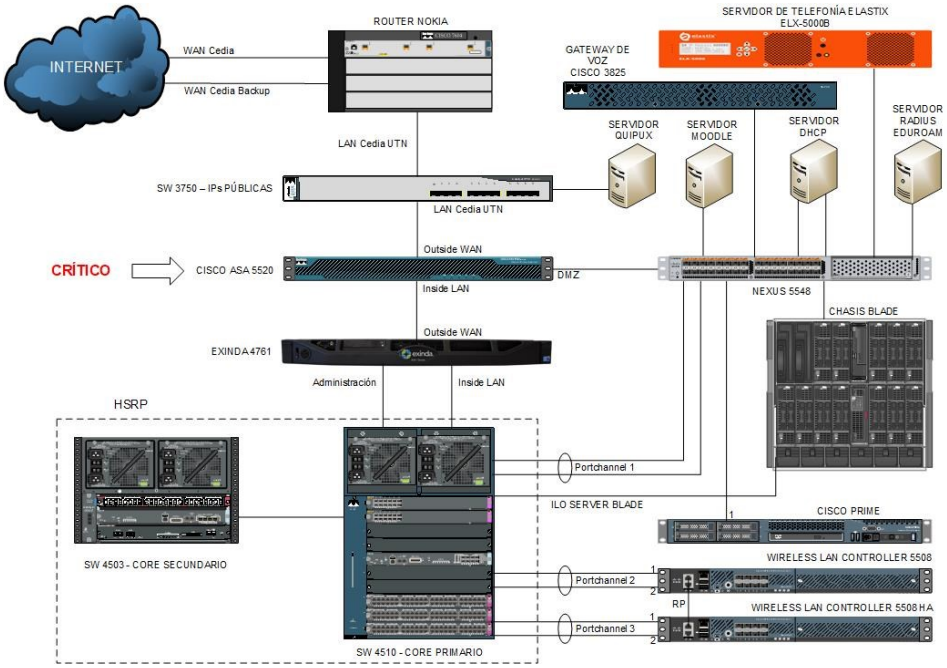
Por otra parte, el router NOKIA, a su vez se conecta a un switch CISCO 3750 que brinda IPs públicas, permitiendo la interconexión del router de frontera con un Firewall CISCO ASA 5520, el cual está encargado de brindar seguridad a la red interna de la UTN y brindar conectividad a los servidores de la DMZ mediante la conexión a un switch NEXUS; adicionalmente, el Firewall se encuentra conectado a un equipo marca EXINDA, el cual permite distribuir la capacidad de canal (comercialmente conocido como controlador de Ancho de Banda).

Asimismo, la red de datos interna está conformada por 2 switches de Core, uno de ellos es el CISCO 4510-E, que está conectado al controlador de ancho de banda EXINDA, mismo que se utiliza para la propagación de Vlans a las diferentes dependencias de la universidad, y este, a su vez está conectado a un switch CISCO 4503-E que proporciona conectividad a las cámaras de seguridad y a los diferentes access point.

Finalmente, en cuanto a servidores, en la universidad, los servicios que son administrados son el DHCP, Moodle, Eduroam y de telefonía IP. Ahora bien, la UTN cuenta con Software e infraestructura como servicio (SaaS e IaaS respectivamente) contratados, en este sentido se tiene a office 365 con su principal servicio el correo institucional y la nube de Oracle en el cual está alojado el sitio web y el sistema integrado de la universidad.

Figura 8

Esquema de red de la UTN



Nota: *Tomado del Departamento de Desarrollo Tecnológico e Informático UTN, 2020*

Factor Servicios

Otro aspecto importante, que permite conocer a la universidad de manera interna, son los servicios tecnológicos que presta actualmente la universidad a su comunidad, estos servicios se detallan a continuación:

Portal Web. – es el sitio web universitario, en el cual se ofrece información a la comunidad universitaria y acceso a todos los recursos y servicios de la universidad.

Portafolio estudiantil y Aula Virtual. – es la plataforma en la cual consta el registro académico, consulta de notas, horarios, pagos realizados y calendario de actividades.

Correo institucional y Suite Office 365. – este servicio permite el uso de las diferentes herramientas ofimáticas, la cual permite estar conectado a todos los documentos, notas y presentaciones, además con la suscripción con la que cuenta la universidad se obtiene

beneficios como almacenamiento, últimas versiones de office tanto para escritorio como aplicaciones para el móvil.

Eduroam. **–** Es un servicio que permite la conexión mediante la creación de un túnel hasta la institución donde el usuario posee una cuenta, mediante la utilización de medios proporcionados por la institución en la cual se ha conectado.

3.1.2 Análisis externo de la UTN

Como se mencionó anteriormente, dentro de la situación actual tanto de la UTN, como del DDTI, es preciso analizar dos factores externos, en este sentido se menciona el factor social y las fuerzas competitivas, que son importantes para el desarrollo del presente trabajo; cabe mencionar, que este análisis va enfocado en encontrar beneficios para el crecimiento del CSIRT académico de la UTN.

Factor Social

En relación a este factor se puntualiza la necesidad de vincular a la academia con la sociedad, articular acciones y fortalecer el tejido social con la participación de las organizaciones, en este aspecto se ejecuta las practicas preprofesionales, vinculación con la sociedad y trabajo rural de los estudiantes antes de titularse. Además, existen ejes que a través de convenios se puede influenciar en los aspectos productivos y culturales de la zona con una contraparte financiera y talento humano capacitado a su servicio y desde luego los espacios físicos que dispone la institución que se encuentran con un acceso libre para toda la colectividad.

Fuerzas Competitivas

Por otro lado, las fuerzas competitivas, sirven de ayuda para analizar los factores externos que se tiene para el ingreso de una nueva organización, pudiendo ser vistos estos factores

como oportunidades o amenazas, por lo tanto, viendo al CSIRT académico de la UTN, como una nueva organización, que en un futuro pueda brindar servicios externos, se hace mención de una manera positiva, en la cual el CSIRT pueda aprovechar la presencia de ciertas instituciones con las cuales puedan trabajar en conjunto.

Por ello alrededor de la UTN, se tiene instituciones de educación superior cercanas en el cantón Ibarra, de modalidad de estudios presenciales como la PUCESI, UNIANDES y YACHAY TECH, además institutos de formación profesional tecnológicos, que se desenvuelven en diversas ramas, e instituciones con ofertas académicas en línea. Sin embargo, estas fuerzas competitivas pueden traducirse en respaldos a la hora de trabajar en conjunto en proyectos de interés social.

3.2 Situación Actual de la Seguridad Informática en la UTN

Ahora bien, para el diseño del CSIRT, es necesario conocer la situación actual de la seguridad informática, para ello se procedió a realizar una encuesta a la comunidad universitaria, lo cual permitió realizar un diagnóstico de incidencias de seguridad informática en la universidad, realizar un análisis FODA, identificar los posibles riesgos y así determinar los servicios que el CSIRT académico puede brindar a la UTN.

3.2.1 Herramienta de Investigación, Metodología y Muestra

Cabe señalar que la herramienta de investigación utilizada para conocer la situación actual de la seguridad informática en la UTN es la encuesta, la cual se aplicó al administrador del DDTI, personal docente, administrativo y estudiantes de la UTN, es preciso detallar aspectos como la población y el respectivo cálculo de la muestra.

Población

En este aspecto, la población de la comunidad académica en la UTN, está conformada por: 10764 estudiantes, 646 docentes y 305 servidores públicos, para un total de 11715 personas. Cabe aclarar que esta información fue tomada a finales del año 2019.

Cálculo de la muestra

Por otro lado, es necesario recalcar que para el presente trabajo la población del objeto de estudio es finita, para lo cual es necesario conocer la muestra poblacional a ser estudiada, en la Ec. 1 se realiza el cálculo de la muestra.

$$n = \frac{N * {Z_\alpha}^2 * p * q}{d^2 * (N-1) + (Z^2 * p * q)} \qquad \textbf{Ec. 1}$$

Donde:

- n= Corresponde al total de la población.
- Zα= Nivel de confianza. En esta caso toma el valor de1.96 al cuadrado (siendo la probabilidad de confianza del 95%).
- p= Probabilidad de éxito, respecto a la veracidad de la información que brinda la muestra, también conocida como proporción esperada (en este caso 50% = 0.5)
- q= Es la probabilidad de error (1- p), siendo el valor de 0.5
- d= Es el porcentaje de error máximo, para este caso es del 7,52%

Ahora bien, reemplazando los valores en la Ec.1 se obtiene la muestra de población objetivo de la presente investigación, es decir ***n*=166 encuestas.**

$$n = \frac{11715 * (1.962 * 0.5 * 0.5)}{0.07552\ ^2(11715-1) + (1.96^2 * 0.5 * 0.5)} = 166$$

Finalmente, en la tabla 25 se detalla la distribución del personal y miembros de la comunidad académica que fueron encuestados.:

Tabla 25

Muestra de la población investigada

PERSONAL	CANTIDAD	PORCENTAJE
ADMINISTRATIVOS	10	6%
DOCENTES	4	2%
ADMINISTRADORES DE RED	1	1%
ESTUDIANTES	151	91%
TOTALES	166	100%

Como resultado, se presenta los porcentajes que se consideran para la aplicación de la encuesta, el 91% corresponde a los estudiantes por ser la población mayoritaria, el 6% al personal administrativo, el 2% a los docentes y el 1% al administrador de red, considerando la importancia y representatividad numérica de cada sector.

3.2.2 Diagnóstico de Gestión de Incidencias en la UTN

Sintetizando los resultados obtenidos de las encuestas, se presenta lo siguiente, en primer lugar, la gestión de incidencias en la Universidad Técnica del Norte está actualmente realizada por la Dirección de Desarrollo Tecnológico e Informático, donde el administrador es el encargado de atender todas las peticiones de servicio para contrarrestar las incidencias informáticas en los equipos y sistemas de la comunidad académica.

Por otra parte, el administrador de red, actualmente no posee suficientes herramientas para poder realizar un tratamiento de incidentes adecuado, ya que se necesitan procesos, equipos y sistemas que permitan mitigar los impactos negativos que pudiesen generar estas incidencias, así como también no se aplica políticas de gestión de incidentes informáticos, pudiendo generar un alto grado de impacto en la UTN, interrumpiendo varios servicios académicos, por tal motivo es necesario crear un equipo de respuesta de incidentes

informáticos que sirva de apoyo a la Dirección de Desarrollo Tecnológico e Informático en estos procesos.

Finalmente, el personal administrativo y docente, al igual que los estudiantes desconocen sobre incidentes informáticos y las consecuencias que estos pueden causar a los sistemas de red y equipos de la UTN, por consiguiente, la mayoría de ellos utiliza antivirus como medio de mitigación ante amenazas de seguridad informática, pero desconocen la necesidad de contrarrestar estas vulnerabilidades, con varios procesos de prevención y respuesta a incidentes, para que estos no vuelvan a repetirse.

3.2.3 Análisis FODA

Para conocer el estado en el que se encuentra la seguridad informática en la UTN, se procede a realizar el análisis FODA, el cual se obtuvo de las encuestas realizadas dentro de la comunidad universitaria, y la situación actual, lo cual permite realizar el análisis presentado en la tabla 26 donde se detallan las fortalezas, oportunidades, debilidades y amenazas detectadas en el DDTI de la UTN:

Tabla 26 Análisis FODA de seguridad informática en el DDTI de la UTN

Análisis FODA de seguridad informática en el DDTI de la UTN

Fortalezas	Oportunidades	Debilidades	Amenazas
Infraestructura tecnológica	Calificarse por la Norma ISO	Falta de capacitaciones, formación y programas de educación al personal de esta unidad	Amenazas de virus en la red
Presupuesto para TICs	Acceso a capacitación técnica	Falta de una infraestructura que satisfaga las necesidades del DDTI (gestión de	Exigencia de una atención adecuada y segura de los servicios

		incidencias y vulnerabilidades)	
Sistema integrado de información universitaria realizado en una arquitectura tecnológica robusta	Convenios entre instituciones	Falta de soportes backup para la información del módulo de gestión académica	Escaso presupuesto para la adquisición de equipos
Personal con alta experiencia en el manejo de redes y sistemas	Creciente demanda por servicios informáticos debido a consultas masivas	Falta de implementación de procesos de seguridad informática	Cobertura insuficiente de la infraestructura de telecomunicaciones del país
Uniportal UTN	Disponibilidad de encontrar en el mercado tecnologías de punta		Procesos lentos de contratación que comprometen el presupuesto de los próximos años
Planificación y participación en la toma de decisiones del presupuesto anual, presentación de proyectos	La academia como insumo para la firma de convenios de cooperación		Déficit de cobertura de programas de capacitación y personal calificado

Cabe señalar, que el análisis FODA permite delimitar los aspectos internos y externos de la seguridad informática en el DDTI de la UTN y como estos influyen en el desarrollo del CSIRT de forma positiva o negativa, para lo cual se delimita las fortalezas y debilidades como aspectos internos y las oportunidades y amenazas como aspectos externos. Una vez detectados estos parámetros se procede a realizar un cruce de variables que permite determinar las estrategias de acción para superar los conflictos, como se detalla en la tabla 27 a continuación:

Tabla 27 Cruce de variables de la matriz FODA

Cruce de variables de la matriz FODA

FACTORES INTERNOS / FACTORES EXTERNOS	Lista de fortalezas	Lista de debilidades
	Infraestructura tecnológica Presupuesto TIC Sistema integrado de información universitaria realizado en una arquitectura tecnológica robusta Personal con alta experiencia en el manejo de redes y sistemas Uniportal UTN Planificación y participación en la toma de decisiones del presupuesto anual, presentación de proyectos	Falta de capacitaciones, formación y programas de educación al personal de esta unidad Falta de una infraestructura que satisfaga las necesidades del DDTI (gestión de incidencias y vulnerabilidades) Falta de soportes backup para la información del módulo de gestión académica Falta de implementación de procesos de seguridad informática
Lista de oportunidades	**Cruce de FO**	**Cruce de DO**
Calificarse por la Norma ISO Acceso a capacitación técnica Convenios entre instituciones	Infraestructura tecnológica disponible para calificarse por la norma ISO Presupuesto TIC para capacitación técnica Creciente demanda por servicios informáticos relacionados con en el manejo de redes y sistemas	La falta de capacitaciones, formación y programas de educación al personal de esta unidad, superada por el Acceso a capacitación técnica La falta de una infraestructura que satisfaga las necesidades del DDTI (gestión de incidencias y

Creciente demanda de servicios informáticos debido a consultas masivas Disponibilidad de encontrar en el mercado tecnologías de punta La academia como insumo para la firma de convenios de cooperación.	Planificación y participación en la toma de decisiones del presupuesto anual, presentación de proyectos hacia la firma de convenios.	vulnerabilidades), superada por la academia como insumo para la firma de convenios de cooperación. Falta de implementación de procesos de seguridad informática, impulsado por la academia como insumo para la firma de convenios de cooperación.
Lista de amenazas		
Amenazas de virus en la red Exigencia de los usuarios de una atención oportuna y segura de los servicios Escaso presupuesto para la adquisición de equipos Cobertura insuficiente de la infraestructura de telecomunicaciones del país Procesos lentos de contratación que comprometen el presupuesto de los próximos años	**Cruce de FA** Sistema integrado de información universitaria realizado en una arquitectura tecnológica robusta para protegerse de las constantes amenazas de virus en la red Personal con alta experiencia en el manejo de redes y sistemas para satisfacer las exigencias de los usuarios de una atención oportuna y segura de los servicios Planificación y participación en la toma de decisiones del presupuesto anual, presentación de	**Cruce de DA** Falta de capacitaciones, formación y programas de educación al personal de esta unidad para atender las exigencias de los usuarios de una atención oportuna y segura de los servicios Falta de una infraestructura que satisfaga las necesidades del DDTI (gestión de incidencias y vulnerabilidades), por la cobertura insuficiente de la de telecomunicaciones del país Falta de implementación de procesos de seguridad informática por el déficit de cobertura de programas de capacitación y personal calificado.

Déficit de cobertura de programas de capacitación y personal calificado.	proyectos para administrar adecuadamente el escaso presupuesto para la adquisición de equipos.	

Ahora bien, analizando el cruce de variables entre fortalezas y oportunidades se obtiene como resultado, una infraestructura tecnológica disponible para calificarse por la norma ISO, el presupuesto TIC para capacitación técnica, la creciente demanda de servicios informáticos debido a consultas masivas a través del personal con alta experiencia en el manejo de redes y sistemas y finalmente la planificación y participación en la toma de decisiones del presupuesto anual con presentación de proyectos hacia la firma de convenios.

En cambio, entre las debilidades y oportunidades se sintetiza, la falta de capacitaciones, formación y programas de educación al personal de esta unidad, superada por el acceso a capacitación técnica, la falta de una infraestructura que satisfaga las necesidades del DDTI (gestión de incidencias y vulnerabilidades), superada por la academia como insumo para la firma de convenios de cooperación y la falta de implementación de procesos de seguridad informática, impulsado por la institución como insumo para la firma de convenios de cooperación.

Contrastando con estos resultados se hace hincapié entre el cruce de variables de debilidades y amenazas con los siguiente, la falta de capacitaciones, formación y programas de educación al personal de esta unidad para atender las exigencias de los usuarios de una atención oportuna y segura de los servicios, falta de una infraestructura que satisfaga las necesidades del DDTI (gestión de incidencias y vulnerabilidades), y la falta de implementación de procesos de seguridad informática por el déficit de cobertura de programas de capacitación y personal calificado.

3.2.4 Elaboración de la Matriz de Riesgos Informáticos en el DDTI.

Con la ayuda del análisis FODA se procede a sintetizar los riesgos informáticos en el DDTI, para lo cual se estandariza ciertos parámetros que permiten una medición adecuada del riesgo detallándolo de manera conceptual y cuantificando la probabilidad, gravedad, valor de riesgo y nivel. Además, se detalla la gravedad de impacto en base a la probabilidad con los parámetros: muy alta, alta, media, baja y muy baja; cada cual conceptualizado y descrito en la tabla 28:

Tabla 28 Matriz de Riesgos Informáticos en el DDTI

Matriz de Riesgos Informáticos en el DDTI

MATRIZ DE RIESGOS

RIESGO	Probabilidad (Ocurrencia)	Gravedad (Impacto)	Valor del Riesgo	Nivel de Riesgo
Falta de capacitaciones, formacion y programas de educacion al personal de esta unidad	4	2	8	Apreciable
Mala distribucion de las areas de trabajo	2	2	4	Apreciable
Infraestructura tecnologica con poco desarrollo	3	4	12	Importante
Poca innovacion y desarrollo en TIC´s	3	4	12	Importante
Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas)	3	4	12	Importante
Falta de implementación de procesos de seguridad informática	2	3	6	Apreciable

LEYENDA

GRAVEDAD (IMPACTO)			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
PROBABILIDAD	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	12
	MUY BAJA	1	1	2	3	4	5

Riesgo muy grave. Requiere medidas preventivas urgentes.
No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.

Riesgo importante. Medidas preventivas obligatorias.
Se deben controlar fuertemente las variables de riesgo durante el proyecto.

Riesgo apreciable. Estudiar económicamente ai es posible introducir medidas preventivas para reducir el nivel de riesgo.
Si no fuera posible, mantener las variables controladas.

Riesgo marginal. Se vigilará aunque no requiere medidas preventivas de partida.

3.3 Definición de Servicios del CSIRT Académico

De modo que, los tipos de servicios de gestión de incidentes que brindará el CSIRT Académico UTN, son realizados en base a las respuestas obtenidas de las encuestas aplicadas a la comunidad académica de la UTN, resultados de la matriz de riesgos del DDTI, matriz RACI (ver APÉNDICE H) y matriz de madurez de procesos PAM (ver APÉNDICE I) según COBIT.

De ahí que, con el diagnóstico de estas herramientas de evaluación, se obtuvo información sobre la situación actual de la seguridad informática en la UTN, con respecto a las incidencias que atacan a los sistemas informáticos, la gestión de los incidentes, y las herramientas utilizadas para la detección, y métodos que permiten eliminar estas incidencias.

3.3.1 Definición de Servicios según Resultados de Encuestas al Personal Administrativo

Mediante las encuestas realizadas al personal administrativo, se presenta los resultados más relevantes en la tabla 29, en cuanto a los incidentes informáticos que se han suscitado en los últimos 3 años.

Tabla 29 Resultados de encuesta al personal administrativo

Resultados de encuesta al personal administrativo

Incidencias Encontradas	Efectos de las Incidencias
Virus	Falla de computadores y equipos
Troyanos	Robo de información
Hackers	Pérdida de confidencialidad
	Fuga información
	Robo de identidad
	Saturación

Por otra parte, el personal administrativo manifestó que desconoce acerca de la gestión de un CSIRT, le hace falta jornadas de formación, educación y sensibilización en cuanto a temas de seguridad informática, desconocen de incidentes suscitados en la UTN, y están de acuerdo con la creación de un CSIRT en la UTN.

Con estos antecedentes se determinan los siguientes servicios según el personal administrativo: formación, educación, sensibilización, información sobre un CSIRT, comunicación y monitoreo de vulnerabilidades.

3.3.2 Definición de Servicios según Resultados de Encuesta al Administrador de Red

Con la encuesta realizada al administrador de red, en relación con las incidencias encontradas en los últimos 3 años se tiene: Virus, Botnets, Spam, Phishing y Ataques de ingeniería social.

Por otra parte, en base a la Gestión de incidencias en el DDTI se obtiene que:

1. El DDTI no utiliza normas y estándares para el manejo de incidencias
2. No se tiene procedimientos para el manejo de incidentes
3. No se maneja reportes de incidentes
4. No se utiliza políticas de gestión de incidentes de seguridad informática
5. No se realiza procedimientos de respaldo de información
6. No existe un área encargada de la seguridad informática
7. Está de acuerdo en crear un CSIRT para la UTN

Concluyendo, los servicios necesarios según el administrador de red, son los siguientes: Formación, educación, sensibilización, información sobre el CSIRT, comunicación, herramientas de monitoreo de incidencias, pentesting o Hacking Ético.

3.3.3 Definición de Servicios según Resultados de Encuestas a Docentes

La encuesta realizada a los docentes de la UTN permitió obtener información en cuanto a incidencias y los efectos producidos los cuales se muestran en la Tabla 30.

Tabla 30

Resultados de encuesta a docentes

Incidencias Encontradas	Efectos de Incidencias
Virus	Falla de computadores y equipos
Spam	Robo de información
Hackers	Bloqueo contraseña
	Alteración información
	Robo de identidad
	Saturación en la Red

Por otra parte, los docentes manifestaron no conocer sobre que es un CSIRT, les hace falta jornadas de formación, educación y sensibilización en temas de seguridad de la información, no conocen sobre las incidencias presentadas en la UTN y están de acuerdo en la creación de un CSIRT en la UTN.

Por tal motivo, los docentes demandan los siguientes servicios: Formación, educación, sensibilización, información sobre CSIRT, comunicación, herramientas de monitoreo de incidentes de seguridad informática y pentesting o Hacking Ético.

3.3.4 Definición de Servicios según Resultados de Encuestas a Estudiantes

Los resultados de las encuestas realizadas a los estudiantes de la UTN se presentan en la tabla 31, en cuanto a las incidencias encontradas y sus efectos:

Tabla 31

Resultados de encuesta a estudiantes

Incidencias Encontradas	Efectos de Incidencias
Virus	Falla de computadores y equipos
Malware	Robo de información
Ataque denegación de servicios	Bloqueo contraseña
Troyanos	Alteración información
Crackers	Robo de identidad
	Saturación
	Bloqueo de internet
	Pérdida de confidencialidad

De igual manera los estudiantes no conocen acerca de Equipos de Respuesta ante Incidentes de Seguridad Informática, les hace falta jornadas de formación, educación y sensibilización en temas de seguridad de la información, desconocen los incidentes informáticos que se han presentado en la UTN y están de acuerdo con la creación de un CSIRT en la UTN. Por ello los siguientes servicios son necesarios según los resultados de la encuesta a los estudiantes: formación, educación, sensibilización, información sobre el CSIRT, y comunicados en temas de seguridad informática.

3.3.5 Definición de Servicios Según Análisis de la Matriz de Riesgos

Los riesgos de impacto critico en el DDTI, pueden ocasionar que el sistema de seguridad informática sea vulnerable a la presencia de incidencias y vulnerabilidades, ya que, al poseer una infraestructura tecnológica con poco desarrollo y falta de innovación en las TICs, las amenazas externas e internas pueden atacar los servidores del DDTI, suspendiendo los servicios brindados a los usuarios de la comunidad universitaria.

Agregando a lo anterior, tales efectos de estos riesgos, demuestra la necesidad de crear servicios, que brinden respuesta a estas incidencias y vulnerabilidades, para que las contraseñas y datos estén seguros y no exista pérdida de información, robo de identidades, o ataques de virus. Por tanto, los servicios que se podría brindar según la matriz de riesgos, se mencionan a continuación:

- Manejo de incidencias
- Manejo de vulnerabilidades
- Análisis de incidencias
- Análisis de vulnerabilidades
- Formación y educación al usuario
- Capacitación al usuario
- Servicio de monitoreo de incidencias.
- Servicio de Alertas y Advertencias.
- Comunicados a los usuarios
- Difusión de información sobre seguridad informática a los usuarios
- Capacitación y educación al usuario

3.3.6 Definición de Servicios Según Análisis de la Matriz de Asignación de Responsabilidades RACI de COBIT

Según la matriz RACI de COBIT, (ver Apéndice H), las responsabilidades asignadas al personal DDTI, para realizar las prácticas relacionadas a la gestión de incidencias es deficiente, tales como registrar, investigar y solucionar incidentes, por lo que no han sido adecuadas, ya que todas estas responsabilidades lo deben hacer un equipo especializado en respuesta de incidentes, que tenga experiencia en riesgos cibernéticos, redes y sistemas internos.

Así, se determina como primer punto, que el personal no tiene experiencia en el manejo de incidentes por procesos, así como el análisis de vulnerabilidades, y, además la falta de equipos y sistemas tecnológicos de comunicación e información modernos, como Software y Hardware para pentesting, escaneo de vulnerabilidades monitoreo de incidentes, detección de intrusos, por tanto es necesario que los servicios CSIRT sean realizados por personal especializado, o que el personal del Help Desk y administrador de red del DDTI, sean capacitados para tales funciones.

La matriz RACI de COBIT, confirma que el personal del DDTI si realiza la gestión de incidencias, pero no en forma completa, siendo las actividades que faltan por implementarse y que servirían para que los servicios del CSIRT se realicen con eficiencia, sean los siguientes:

- Definir esquemas de clasificación de incidentes y peticiones de servicio
- Verificar, aprobar y resolver peticiones de servicio
- Cerrar incidentes y peticiones de servicio
- Dar seguimiento del estado de la gestión de incidentes y emitir informes
- Monitoreo de incidencias
- Manejo de vulnerabilidades
- Análisis de vulnerabilidades
- Registros o alertas de monitoreo o IDS (Sistema de detección de intrusos)

3.3.7 Definición de Servicios según Análisis de la Matriz PAM de COBIT 2019

De acuerdo con las prácticas base (BP) de COBIT, la matriz PAM (ver Apéndice I), demuestra que de las prácticas clave de gestión de incidencias, tienen un nivel de madurez deficiente, ya que cuatro de los siete indicadores no son conseguidas (definir esquemas de clasificación de incidentes, verificar, aprobar y resolver, cierre y seguimiento de incidentes

y dar seguimiento a la gestión de incidentes y emitir informes), y tres de las siete son conseguidas parcialmente (registrar e investigar incidentes, solución y recuperación de incidentes), lo que califica al DDTI entre el 0 y 30% de madurez en prácticas de gestión de incidentes.

De este análisis de la matriz PAM, se puede definir los siguientes tipos de servicios de gestión de incidencias que el CSIRT puede brindar en la UTN, los cuales son:

- Detectar y registrar los incidentes y las peticiones de servicios
- Informar a los usuarios finales (administradores, docentes y alumnos)
- Crear procedimientos de clasificación, escalamiento y priorización de incidentes
- Resolver, recuperar y cerrar incidentes
- Hacer reportes para el director de TI
- Reportes de incidencias
- Reportes de satisfacción de usuarios
- Alertas y advertencias
- Comunicados
- Difusión de información relacionada con la seguridad

De esta manera, en la tabla 32 se resume los servicios según el análisis de las prácticas clave de gestión de incidencias de COBIT

Tabla 32 Resumen de Servicios Según Factores de Riesgo de la Seg. Informática

Resumen de Servicios Según Matriz PAM

Servicios reactivos	Servicios proactivos	Gestión de calidad de la seguridad
Alertas y advertencias	Comunicados	Análisis de riesgos
Tratamiento e incidentes		Sensibilización

Análisis de incidentes Apoyo a la respuesta a incidentes Coordinación de la respuesta a incidentes Respuesta a incidentes in situ	Configuración y mantenimiento de la seguridad Desarrollo de herramientas de seguridad Servicios de detección de intrusos Difusión de información relacionada con la seguridad	Educación/formación Evaluación o certificación de productos

Ahora bien, se considera que los servicios generales y emergentes en cuanto a servicios reactivos en el CSIRT-UTN son: alertas y advertencias, tratamiento e incidentes, análisis de incidentes, apoyo a la respuesta a incidentes, coordinación de la respuesta a incidentes, respuesta a incidentes in situ y coordinación de la respuesta a la vulnerabilidad. Además, estos se complementan con los servicios proactivos: comunicados, configuración y mantenimiento de la seguridad, desarrollo de herramientas de seguridad, servicios de detección de intrusos y difusión de información relacionada con la seguridad.

A esto se añade la gestión de calidad para la seguridad informática con los siguientes servicios detectados: Análisis de riesgos, sensibilización, educación/formación y por último la evaluación o certificación de productos. Donde toda la comunidad universitaria es participe y de involucrarse en corresponsabilidad para el buen funcionamiento del CSIRT-UTN.

3.4 Tipos de Servicios

En conclusión, los tipos de servicios, han sido definidos en base a los resultados de las herramientas aplicadas (encuestas, matriz de riesgos DDTI y matrices COBIT) para el

análisis de la situación actual de la seguridad informática en la UTN y DDTI es importante mencionar que lo recomendable en etapas iniciales del CSIRT, debería brindar servicios básicos de gestión de incidentes, y conforme el CSIRT vaya obteniendo madurez con el tiempo, estos servicios sean ampliados. Por lo tanto, cuando el CSIRT sea implementado en un futuro, los servicios que el CSIRT académico de la UTN puede ofrecer son reactivos, proactivos y gestión de la calidad y seguridad como se detalla en la tabla 33.

Tabla 33

Tipo de Servicios DDTI-UTN

Servicios reactivos	**Servicios proactivos**	**Servicios de gestión de calidad y de la seguridad**
Monitoreo de sistemas informáticos y redes	Comunicados	Concienciación
Alertas y advertencias	Difusión de información sobre seguridad informática	Investigación y asesorías en seguridad informática
Manejo y análisis de incidentes y vulnerabilidades		Actividades de formación y capacitación a la comunidad académica
Respuesta a incidentes en el sitio		

3.4.1 Servicios Reactivos

Los servicios reactivos se encargan de brindar tratamiento a los incidentes o de mitigar las secuelas que pueda provocar los mismos, por ello a continuación se detalla cada servicio de la tabla 26. Dentro de los servicios reactivos, primeramente, se tiene el servicio de monitoreo de sistemas informáticos, el cual se encargará del monitoreo y vigilancia del estado de los equipos y servicios informáticos conectados a la red de la UTN, enviando alertas al administrador de red del DDTI cuando se detecte un comportamiento inadecuado.

Para este servicio se puede considerar, la herramienta llamada Nagios, la cual es utilizada para el monitoreo de sistemas informáticos y redes, siendo de código abierto, con el cual es posible la monitorización de los servicios de la red de la UTN, así como la vigilancia de los recursos de Hardware como procesadores, terminales, discos duros, memoria RAM, estados de los puertos, así como la monitorización de los sistemas operativos instalados en los computadores y servidores.

Así mismo, se tiene el servicio de alertas y advertencias, este servicio permite emitir avisos acerca de la presencia de posibles incidentes informáticos, la herramienta que puede ser utilizada para este fin, es Nagios, la cual genera alertas cuando existe comportamientos inusuales dentro de los equipos de la red, o por parte del reporte de los usuarios , a través de un sistema de tickets, el cual puede ser OTRS, ya que este Software es de código abierto y permite reportar incidentes informáticos..

En este sentido, las alertas y advertencias deberán ser analizadas y registradas, , las cuales serán informadas al administrador de red del CSIRT, para tomar medidas de precaución y así evitar incidentes y vulnerabilidades , que puedan afectar a los sistemas y equipos críticos, procediendo a registrar y clasificar estos incidentes para brindar una solución.

Por otro lado, está el servicio de manejo de incidentes, el cual consiste en la ejecución de las siguientes prácticas: análisis, clasificación y respuesta a los reportes de incidencias de seguridad informática.

Las respuestas a los reportes recibidos por parte de los usuarios, comprende las siguientes actividades: definición de soluciones y técnicas para disminuir el impacto de las incidencias reportadas, proporcionando informes de alertas y advertencias sobre la presencia de incidentes o vulnerabilidades, dirigidos a toda la comunidad académica, monitoreo del tráfico de información en la red y la aplicación de medidas de protección para los sistemas y redes afectados.

También se menciona el servicio de análisis de incidentes este servicio permite determinar el alcance de los incidentes informáticos, es decir hasta qué punto el personal encargado de este servicio realizará sus funciones. Con este servicio la comunidad académica se beneficiará con información sobre los efectos que pueda causar el incidente en los equipos y sistemas, así como el origen, y las estrategias de respuesta que se podrían brindar para la solución o mitigación.

Por lo tanto, el CSIRT UTN, puede utilizar los siguientes recursos: listado de los puertos conocidos y de los puertos utilizados para realizar un ataque, información actualizada de los Servidores de la UTN (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios), análisis de los procesos en la red: puertos de red utilizados, horarios de usos de los puertos, direcciones IP de mayor flujo de información, dirección IP de mayor número de peticiones.

Por consiguiente, las herramientas que el CSIRT UTN, necesitaría para proporcionar el servicio de análisis de incidentes son: computadores portátiles, software para recolección y análisis de incidencias y software de escaneo de puertos, como Nmap, el cual es open source.

Además, dentro de los servicios reactivos se encuentra el manejo de vulnerabilidades, este es un servicio que lo realizaría el CSIRT UTN, siendo este equipo el encargado de reportar mediante informes sobre las vulnerabilidades detectadas en el sistema de red y datos de la UTN, tanto en Hardware como en Software, estos reportes ayudarán con información sobre el origen, modos de acción y las consecuencias de las vulnerabilidades, donde el CSIRT proporcionará soluciones para detectar y reparar estas vulnerabilidades.

De igual manera, para el manejo de vulnerabilidades, es necesario contar con herramientas de gestión de vulnerabilidades, con la finalidad de que el administrador de red pueda identificar la presencia de las mismas, permitiendo una pronta respuesta y disminuir

la presencia de incidentes de seguridad informática las herramientas que pueden ser utilizadas para este propósito puede ser Metasploit, OpenVas o Nessus, la primera y segunda opción es de código abierto y en cuanto a la tercera opción existe la versión gratuita pero tiene ciertas restricciones, y su versión de pago que es mucho más completa pero el valor de adquisición está por sobre los $2900 USD.

Por último, para el servicio de análisis de vulnerabilidades, el CSIRT, estaría encargado de gestionar las vulnerabilidades que puedan presentarse dentro de la red de la UTN, localizando, y realizando ataques controlados, mediante procedimientos de evaluación tanto en Hardware como en el Software, utilizando para ello herramientas de explotación de vulnerabilidades. Para detectar estas vulnerabilidades, se puede hacer uso del sistema operativo Kali Linux, el cual es de código abierto y posee diversidad de herramientas que permiten realizar análisis de vulnerabilidades como por ejemplo Nmap u OpenVas.

3.4.2 Servicios proactivos

Los servicios proactivos establecen acciones y controles preventivos afín de disminuir el impacto de los incidentes sobre los activos informáticos más vulnerables, garantizando la seguridad informática de la red de datos y comunicaciones de la UTN. Estos servicios proactivos serían proporcionados por el CSIRT UTN, entre estos servicios están: comunicados y difusión de información sobre seguridad informática.

El servicio de comunicados, son alertas que se envían a los usuarios sobre nuevos incidentes, ataques, vulnerabilidades, que están afectando a los usuarios, la presencia de alguna incidencia o intrusión en los equipos o redes, así como de nuevos Hackers o Crackers que se están infiltrando en las redes universitarias, con la finalidad de evitar que estas amenazas ingresen a los sistemas de red de la UTN, dando tiempo al administrador de red del DDTI, para que pueda tomar las debidas precauciones.

Por otro lado, en cuanto a servicios proactivos, se tiene el servicio de difusión de información sobre seguridad informática, este servicio consistiría en informar a la comunidad académica sobre la seguridad informática y gestión de incidencias, con la finalidad de que los usuarios estén informados acerca de las mejores prácticas en temas de seguridad informática y gestión de incidentes. Esta información puede ser documentada y elaborada por el personal del CSIRT UTN. Entre esta información están: documentos digitales sobre nuevas incidencias en servidores y equipos en una red académica, mejores prácticas según COBIT, modelo de gestión de incidencias según ITIL, políticas de seguridad informática, informes estadísticos de incidencias y tendencias actuales.

3.4.3 Servicios de Gestión de Calidad de la Seguridad

Finalmente, se tiene los servicios de gestión de calidad de seguridad, los cuales comprende labores de concienciación, investigación y asesorías en seguridad informática, actividades de formación y capacitación, las cuales estarían dirigidas a los usuarios de la comunidad académica, y ejecutados por el CSIRT, cuya finalidad sería la de mejorar la seguridad informática.

El servicio de concienciación, se las puede realizar mediante reuniones, seminarios, boletines web, así como también, este servicio puede ir acompañado de capacitaciones, realizadas por personal interno o externo, que colabore con el CSIRT UTN, para instruir en técnicas de seguridad informática, con la ayuda de talleres, seminarios, cursos y tutoriales online.

Para terminar, se menciona el servicio de investigación y asesorías, este servicio tendría como finalidad brindar una guía al usuario sobre la aplicación de procedimientos en cuanto a la gestión de incidencias para la seguridad informática de la UTN, esta actividad servirá para el desarrollo de políticas de seguridad informática del DDTI.

CAPÍTULO IV DISEÑO DEL CSIRT ACADÉMICO UTN

El cuarto capítulo, trata sobre la definición de requerimientos de diseño del CSIRT Académico en la UTN, donde se hace mención a dos tipos de requerimientos: Estratégicos y requerimientos de Diseño y funcionamiento. Los requerimientos estratégicos, se dividen en dos subcapítulos que son planeamiento estratégico y plan operativo anual (POA).

Primeramente se tiene el plan estratégico, en el cual se definen los requisitos que debe cumplir el CSIRT académico, , que son: estructurar el personal operativo, administrativo y técnico, definir la misión y los objetivos estratégicos, localizar la estructura organizacional, políticas y procedimientos de gestión de incidencias con los cuales se respaldan los servicios creados, capacitación y entrenamiento del personal seleccionado y el organigrama posicional del CSIRT, aplicar normas y estándares de respuesta ante incidentes de seguridad de la información, establecer las relaciones con otros equipos a nivel nacional e internacional, y finalmente definir los medios de comunicación del equipo.

Luego se presenta el plan operativo anual (POA), el mismo que consiste en la planificación de objetivos, basado en estrategias, los cuales han sido delimitadas en el plan estratégico y cuyos proyectos optimizarán el desempeño del CSIRT académico de la UTN y su infraestructura tecnológica, en servicio de la comunidad académica.

Así mismo, en cuanto a los requerimientos de diseño y funcionamiento, que pertenecen al segundo subcapítulo, son; diseño de infraestructura tecnológica y equipos y finalmente el diseño de mecanismos de reporte de incidencias. Con este diseño, el CSIRT académico, podrá lograr la detección, prevención y mitigación de las diferentes incidencias que amenazan al sistema de red y datos de la UTN.

4.1 Plan Estratégico

En esta sección se propone y elabora el plan estratégico basado en el análisis de la situación actual de la UTN, el DDTI y de la seguridad informática en la institución. A continuación, se presenta la misión y visión para el CSIRT-UTN propuesto:

Misión

El CSIRT académico de la UTN brinda servicios de seguridad informática a la comunidad universitaria, permitiendo evitar y disminuir incidentes informáticos mediante servicios reactivos, proactivos y de gestión de la calidad de seguridad.

Visión

El CSIRT académico de la UTN, será un equipo de respuesta a incidentes de seguridad informática consolidado, cumpliendo normas y estándares internacionales, consiguiendo ser un referente en la zona 1 del Ecuador en cuanto a centros de respuesta de incidentes de seguridad informática, alcanzando reconocimientos y certificaciones por organismos internacionales.

Objetivos Estratégicos

Los siguientes objetivos estratégicos, servirán en pro de crecimiento del CSIRT académico de la UTN, con los cuales, se establecerán proyectos a mediano y largo plazo, hasta que el CSIRT se posicione como un referente, primeramente, de la comunidad en la cual prestará sus servicios, así como en el país, permitiendo certificarse internacionalmente, para lo cual se menciona los siguientes objetivos estratégicos:

Objetivo 1. Ser un punto único de contacto para el reporte de incidentes de seguridad informática dentro de la UTN.

Objetivo 2. Establecer alianzas estratégicas con otros CSIRT para la coordinación y cruce de información en temas de seguridad de la información.

Objetivo 3. Desarrollar estrategias de concientización a los usuarios en cuanto a seguridad informática para prevenir incidentes

Objetivo 4. Fortalecer los conocimientos del personal del CSIRT para la prevención y atención de incidentes de seguridad de la información.

Objetivo 5. Mejorar la gestión y servicios de respuesta de incidentes para obtener una certificación internacional del FIRST.

Políticas de Gestión de Incidentes de Seguridad Informática

La elaboración de las políticas de gestión de incidentes de seguridad informática, para el CSIRT Académico, se realiza a partir de los tipos de servicios de gestión de incidencias identificados anteriormente, en donde las políticas a elaborarse, garantizarán la integridad, confidencialidad y la disponibilidad de los datos, las cuales se basan en la Norma ISO/IEC 27002, y divulgadas en los estándares internacionales como son el estándar ITIL V4 y COBIT 2019.

Las políticas que se tomarán en cuenta para el CSIRT Académico, basados en los diferentes tipos de servicios de respuesta de incidencias previamente definidos, son las siguientes (ver Apéndice N):

- Política de clasificación de la información.
- Política de protección de la información.
- Política de destrucción de información.
- Política de divulgación de información.
- Política de gestión de incidentes de seguridad de la información.
- Política de seguridad de la información.

Estructura Organizacional del CSIRT-UTN

El CSIRT académico de la UTN, estará localizado al interior de la Universidad Técnica del Norte, en un departamento dentro de la estructura organizacional del DDTI, con el cual se coordinará actividades y procesos de apoyo para la eficiencia de la gestión de incidentes en la comunidad académica de esta institución.

Por consiguiente, el diseño de la estructura organizacional del CSIRT académico de la UTN, es de tipo académico, siendo su modelo organizacional, interno centralizado, donde el CSIRT, es el punto de contacto de respuesta de incidentes de toda la universidad, siendo responsable de la administración y control de los incidentes y ataques que puedan suscitarse en las diferentes facultades y áreas del campus universitario, inclusive de aquellos campus externos o extensiones que en un futuro la UTN implemente en el país.

Es importante mencionar que este modelo, proporciona ventajas como: inmediata atención a las vulnerabilidades e incidentes reportados, controlando y disminuyendo su impacto en la universidad, evitando que vuelvan a presentarse en los equipos y sistemas informáticos, proporcionando soluciones prácticas, asesoramiento y capacitaciones a la comunidad universitaria, para lograr la prevención y máximo control de estas incidencias, además, emitirá informes a través de reportes de incidentes y vulnerabilidades encontradas facilitando el trabajo del DDTI en temas de seguridad de la información en la UTN.

Capacidades y experiencia del personal:

De igual manera, para que el CSIRT consiga los objetivos planteados, requiere de personal que esté acorde a las funciones que va a realizar, es por ello que debe cumplir con un conjunto de capacidades, las cuales involucran las características y cualidades del personal, así como la experiencia, que le permita realizar las diferentes tareas, por consiguiente, el personal que trabajará en el CSIRT-UTN, debe cumplir con las siguientes

capacidades y experiencia: administración de redes, Firewall, IDS, escaneo, eliminación y recuperación ante incidentes informáticos, criptografía, almacenamiento y recuperación de datos, creación de documentación y mantenimiento de redes, creación y seguimiento de políticas.

Así, en la tabla 34, se presenta el personal que conformará el CSIRT académico en la UTN, el cual está compuesto de los siguientes cargos y responsabilidades: Director, Administrador de red, Equipo de respuesta, Técnicos y Abogado. Mientras que en la figura 9 se plantea la estructura organizacional del mismo.

Tabla 34 Cargos y Responsabilidades del Personal del CSIRT-UTN

Cargos y Responsabilidades del Personal del CSIRT-UTN

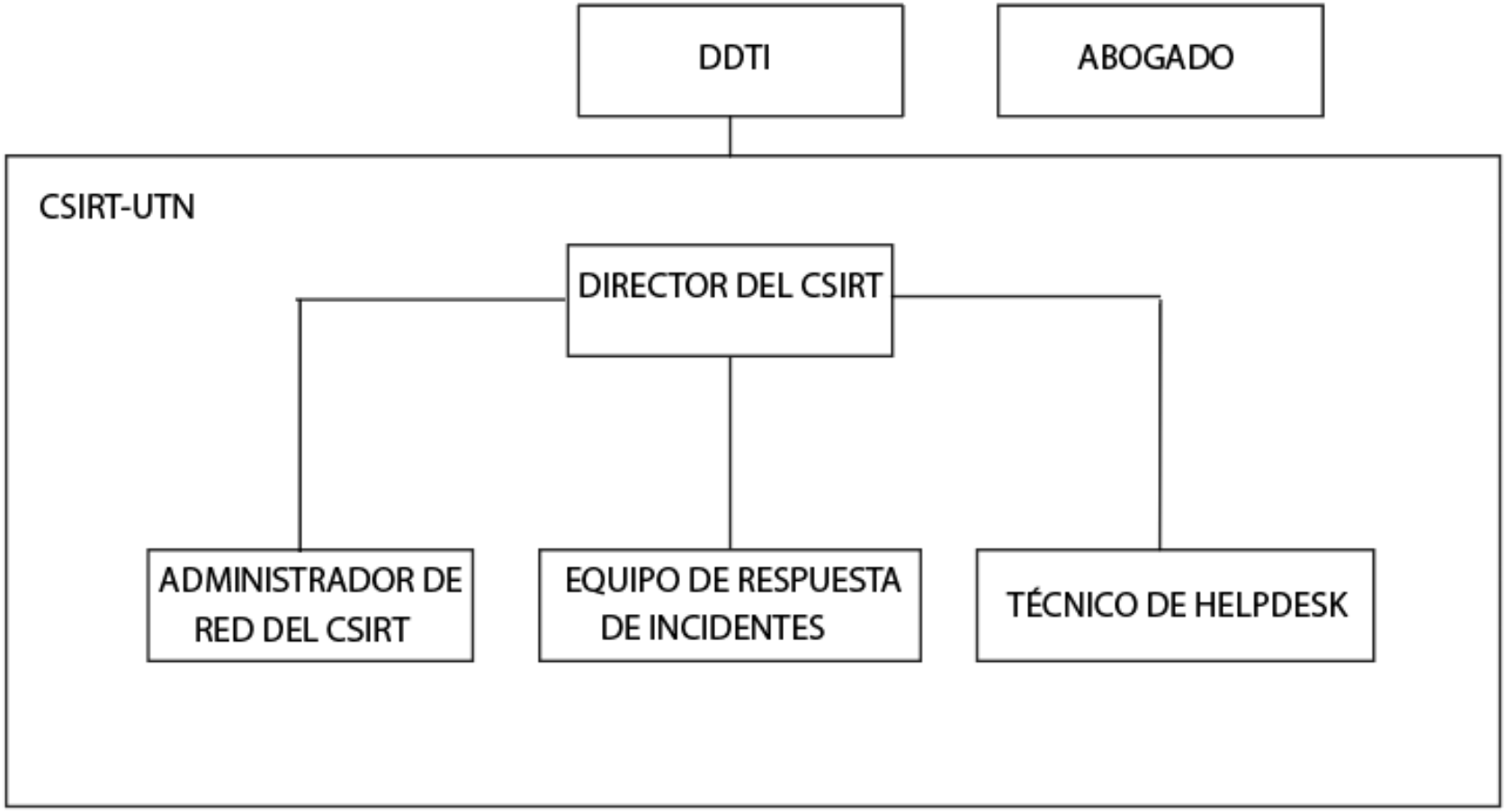
CARGO	RESPONSABILIDADES
Director del CSIRT	Planificar, organizar, ejecutar y supervisar procesos y actividades del CSIRT, y de administrar y contratar su personal.
Administrador de red	Administrar la red del CSIRT, atendiendo sus necesidades y requerimientos. Mantener en buen estado los sistemas de red. Supervisar los elementos del sistema de red
Equipo de respuesta a incidentes de seguridad informática	Responder ante incidentes y ataques a los sistemas informáticos y equipos, reportados y clasificados por el Helpdesk. Controlar las incidencias y ataques reportados brindando soluciones prácticas. Difundir información sobre incidentes y vulnerabilidades a toda la comunidad universitaria de la UTN.

	Monitorear los sistemas informáticos, realizar pruebas de penetración y controlar los equipos de detección de intrusos.
Técnicos de Helpdesk	Atender las llamadas y correos electrónicos universitarios, que reporten incidentes en los equipos y sistemas informáticos de la UTN, asesorar estas incidencias y clasificar esta información. Coordinar acciones con el equipo de respuesta a incidentes mediante el envío de reportes de incidentes.
Abogado	Asesorar y dar soporte legal en la elaboración de las políticas y procedimientos del CSIRT en cuanto a la gestión de incidencias, normas y estándares utilizados, controlar el cumplimiento de las leyes ecuatorianas aplicadas al CSIRT.

De esta manera, cabe señalar que el abogado de la institución debe tener conocimientos en derecho digital o informático, relacionados con delitos y amenazas informáticas, por esta razón, es importante en caso de ser necesario, que el departamento jurídico lleve a cabo cursos de actualización en temas de ciberseguridad que se acoplen a la legislación ecuatoriana.

Figura 9

Estructura Organizacional del CSIRT Académico UTN dentro del DDTI



Servicios CSIRT Académico UTN

Finalmente, en la tabla 35 se presenta los servicios que el CSIRT académico de la UTN brindará en sus operaciones iniciales los cuales están conformados por servicios reactivos, proactivos y de gestión de la calidad de la seguridad.

Tabla 35

Servicios CSIRT UTN

Servicios reactivos	**Servicios proactivos**	**Servicios de gestión de la calidad de la seguridad**
Monitoreo de sistemas informáticos y redes	Comunicados	Concienciación
Alertas y Advertencias	Difusión de información sobre seguridad informática	Actividades de formación y capacitación dirigida a la comunidad académica.
Manejo y análisis de incidentes y vulnerabilidades		
Respuesta a incidentes en el sitio		

4.2 Plan Operativo Anual (POA) CSIRT-UTN.

En la tabla 36 se presenta el plan operativo anual (POA), el cual consiste en la planificación de objetivos, basado en estrategias, las mismas que han sido delimitadas en el plan estratégico, y cuyos proyectos optimizarán el desempeño del equipo CSIRT Académico de la UTN y de su infraestructura tecnológica, en servicio de la comunidad académica.

Tabla 36

Plan Operativo Anual POA CSIRT UTN

Objetivos Estratégicos	Proyectos de Crecimiento CSIRT UTN	Responsables
1. Ser un punto único de contacto para el reporte de incidentes de seguridad informática	1. Innovar las prácticas de registro de incidencias mediante la utilización de herramientas automatizadas. 2. Uso de herramientas, para clasificar y evaluar los tiempos de escalamiento de las incidencias reportadas. 3. Aplicar indicadores de eficiencia para la gestión de respuesta de incidentes de seguridad.	Director del CSIRT-UTN
2. Establecer alianzas estratégicas con otros CSIRT para la coordinación y cruce de información en temas de seguridad de la información	1. Establecer contacto con otros CSIRT nacionales 2. Cooperar con el cruce de información cuando se detecte incidentes de seguridad informática	Administrador de red
3. Desarrollar estrategias de concientización a los usuarios en cuanto a seguridad informática para prevenir incidentes	1. Organizar charlas, eventos, programas relacionados con la seguridad informática	Técnicos helpdesk Equipo de respuesta de incidentes
4. Fortalecer los conocimientos del personal del CSIRT para la prevención y	1. Actualizar de manera constante los conocimientos del personal del CSIRT en	Director del CSIRT-UTN

atención de incidentes de seguridad de la información	temas de seguridad mediante cursos, foros, webbinars	
5. Mejorar la gestión y servicios de respuesta de incidentes para obtener una certificación internacional del FIRST	1. Crear políticas y procedimientos de gestión de incidentes aplicando estándares internacionales. 2. Participar en seminarios internacionales organizados por CSIRT miembros del FIRST, para conocer sobre nuevos procedimientos y servicios en la gestión de incidencias. 3. Conseguir un sponsor CSIRT internacional que promueva el ingreso del CSIRT UTN al FIRST.	Director del CSIRT-UTN Equipo de respuesta de incidentes

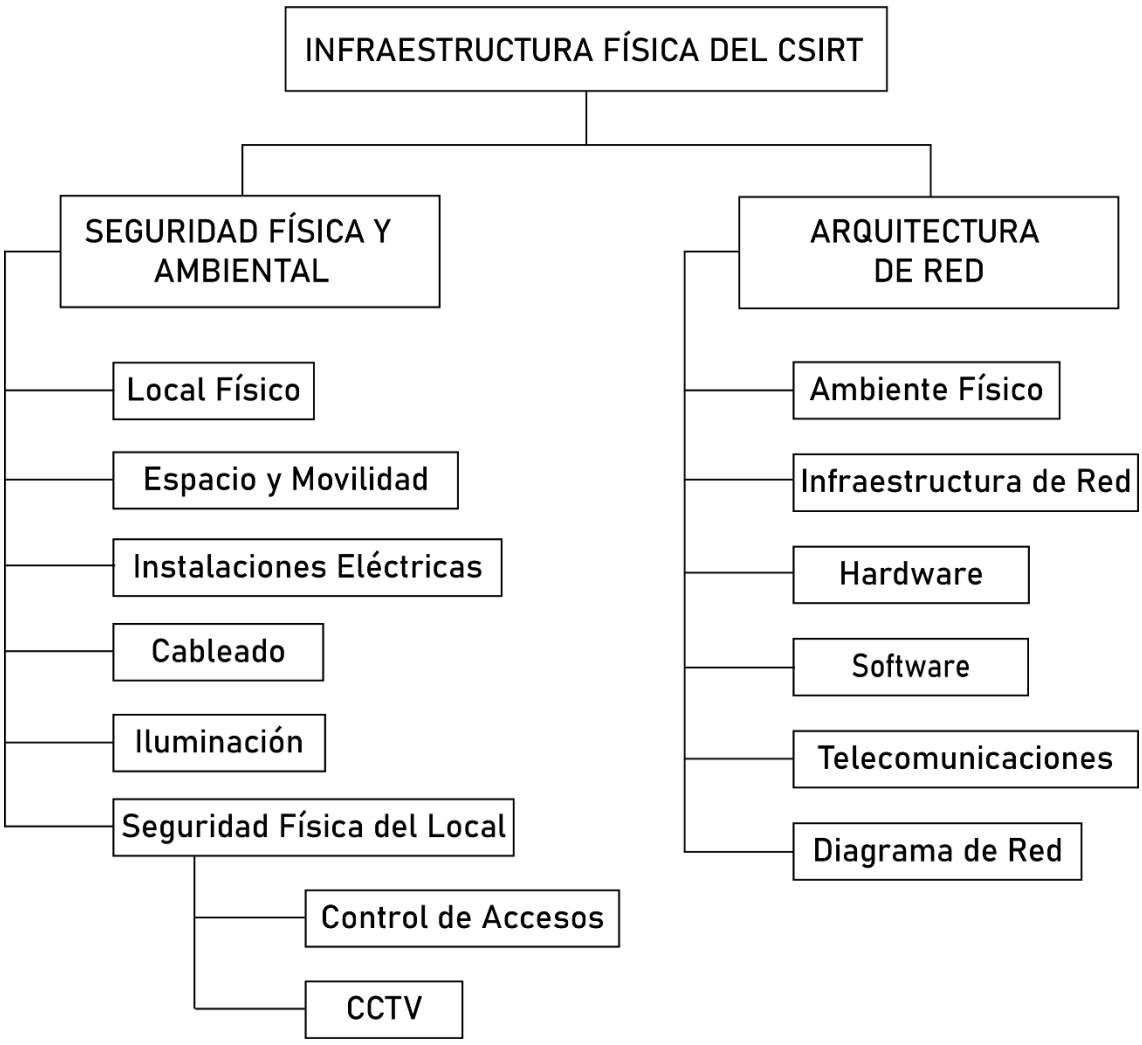
4.3 Infraestructura y Equipamiento

En base al manual básico de Gestión de Incidentes de Seguridad Informática del proyecto AMPARO, se destacan los parámetros a tener en cuenta sobre la infraestructura física de un CSIRT, los cuales se presentan en la figura 10, permitiendo comprender de una mejor manera los aspectos que se deben considerar al momento de implementar en un futuro el CSIRT académico de la UTN; los cuales, una vez que el CSIRT adquiera experiencia y amplíe sus servicios, pueda ir evolucionando y adaptando cada una de estas sugerencias.

En este sentido, se contempla parámetros como la seguridad física y ambiental, así como la arquitectura de red, por consiguiente, el primer parámetro hace referencia al espacio físico, instalaciones eléctricas, cableado, iluminación y seguridad física, y, por otra parte, el segundo punto contiene aspectos sobre el ambiente físico, infraestructura de red, hardware, software, infraestructura de telecomunicaciones y topología de red.

Figura 10

Parámetros de la Infraestructura Física del CSIRT



Nota: *Adaptado de (Lacnic, 2012)*

Ahora bien, en base a los parámetros señalados en la figura 10, el CSIRT académico de la UTN, estará ubicado dentro del DDTI, el cual dispone de un local físico, brindando espacio para los equipos como: computadores, estaciones de trabajo, impresoras, y movilidad para el personal del CSIRT, un lugar para reuniones, suministro eléctrico, cableado estructurado, con acceso a redes de telefonía y datos, iluminación, control de accesos para personal autorizado y monitoreo mediante cámaras de seguridad, cumpliendo con las recomendaciones del manual del proyecto AMPARO.

Por otra parte, la infraestructura de red y datos del DDTI, inicialmente servirá, para uso del CSIRT académico de la UTN, en la cual es necesario la implementación de herramientas que permitan el reporte y gestión de incidentes, y la monitorización de la red, siendo el acceso a estas herramientas exclusivas del personal del CSIRT de la UTN, con el fin de que estas herramientas faciliten los servicios que el CSIRT va a brindar, como son: monitoreo de la red, alertas y advertencias, manejo y análisis de incidentes y vulnerabilidades, respuesta a incidentes, comunicados, formación, concienciación y difusión de información sobre seguridad de la información.

Como consecuencia, para la arquitectura de red del CSIRT es necesario contar con un ambiente físico separado por dos áreas, la primera corresponde al área administrativa, siendo esta compartida con el DDTI y otra área operativa, para la cual es importante que sea en un ambiente aislado de los demás departamentos, para no interferir en las operaciones del CSIRT.

Por ende, es preciso mencionar que según el manual del proyecto AMPARO, la infraestructura de red del CSIRT debe estar separada de la infraestructura de red de la UTN, pero para el comienzo de sus operaciones y por los tipos de servicios que va a

brindar, la infraestructura de red del CSIRT hará uso de la DMZ de la red universitaria, para alojar los servidores de monitoreo de red y reporte de incidentes, debido a que estos servicios no comprometen la seguridad de la información de la red universitaria.

De modo que para las operaciones del CSIRT académico, en cuanto a hardware, son necesarios equipos como: computadores, dispositivos de almacenamiento (pendrive, discos externos), materiales y suministros de oficina, cableado estructurado, routers, switches, correo electrónico y servidor WEB.

Por lo tanto, y en base a las recomendaciones antes mencionadas, en primer lugar, se procede a la selección de la herramienta de monitoreo de redes, para lo cual, en la tabla 37, se compara parámetros funcionales entre Zabbix, Cacti y Nagios, ajustándose a las recomendaciones de ITIL.

Pues bien, estas recomendaciones corresponden a los objetivos de diseño de servicios según ITIL, entre ellas están: contribuir con los objetivos del negocio, en cuanto sea posible ahorrar dinero y tiempo, minimizar o prevenir riesgos, evaluar y mejorar los servicios de TI y desarrollar políticas.

En consecuencia, la elección de la herramienta de monitoreo de redes, debe apoyar para que la UTN brinde a los usuarios, los servicios necesarios para el desarrollo normal de sus operaciones, asimismo, hay que considerar el ahorro de costos de licencias, y permitir la optimización de tiempo para el personal, en otras palabras es importante mencionar que los recursos humanos del CSIRT puedan dedicarse a otras actividades, y que en caso de ocurrir algún problema dentro de la red, esta genere alertas, de igual forma la monitorización de la red permita la evaluación y mejora de los servicios de la red de la UTN, y con ello poder desarrollar políticas en los dispositivos de la red, y finalmente

permitir la prevención y mitigación de los riesgos de seguridad de la información en la red de datos de la UTN.

Tabla 37

Comparación de Herramientas de Monitoreo

Características	Herramientas		
	ZABBIX	CACTI	NAGIOS
Licencia de código libre	✓	✓	✓
Monitorización de Servicios	✓	✓	✓
Monitorización de Hardware	✓	X	✓
Gráficas	✓	✓	✓
Informes en tiempo real	X	X	✓
Estadísticas	✓	✓	✓
Alertas	✓	✓	✓
SNMP	✓	✓	✓
Mapeo de la Red	✓	X	✓
Autodescubrimiento de la Red	✓	X	✓
Monitoreo de QoS	✓	X	✓

Del análisis de la tabla 37, la herramienta CACTI, no permite la monitorización de hardware, no realiza un mapeo de dispositivos, no es posible el autodescubrimiento de los equipos pertenecientes a la red, no soporta SNMP, lo cual imposibilita la monitorización de múltiples dispositivos como routers, switches, servidores entre otros, además, CACTI y Zabbix no generan informes en tiempo real, así pues, las dos

herramientas antes mencionadas no permiten el cumplimiento de las recomendaciones de ITIL en cuanto al diseño del servicio mencionados en párrafos anteriores.

En definitiva, nagios reúne mejores características para la monitorización de la red, comenzando por la licencia que es de código libre, lo cual permite el ahorro de dinero, facilita la monitorización de recursos de hardware como el estado de los puertos, memoria, uso de discos, carga del procesador, soporta la supervisión de servicios como SMTP (Protocolo para Transferencia Simple de Correo), POP3 (Protocolo de Oficina de Correo), HTTP (Protocolo de Transferencia de Hipertexto), SNMP (Protocolo Simple de Administración de Red), generando alertas ante la presencia de alguna anomalía dentro de los equipos monitoreados, permitiendo la notificación en tiempo real al responsable de la monitorización de la red. De esta manera ayuda a evaluar y mejorar los servicios, implementar políticas, minimizar y prevenir posibles riesgos de seguridad de la información.

Por otro lado, en la tabla 38 se describen los recursos mínimos necesarios tanto en hardware como en software para la instalación de nagios, por ello los requerimientos de hardware dependen del número de hosts y servicios que se desea monitorear, es decir a mayor número de host, demandan un mayor requerimiento de hardware como RAM, núcleos de CPU y disco duro.

Tabla 38

Requerimientos para la Instalación de NAGIOS

HARDWARE				
# Hosts	# Servicios a monitorear	Disco Duro	# Núcleos CPU	RAM

50	250	40 GB	1 y 2	1 y 4 GB
100	500	80 GB	2 y 4	4 y 8 GB
+500	+2500	120 GB	+ 4	+ 8 GB
SOFTWARE				
Sistema operativo Linux (Debian, CentOS, Ubuntu, Fedora)				
Apache				
PHP				
Plugins de Nagios				

Fuente: (Velasco Briones & Cagua Ordoñez, 2017)

En segundo lugar, es necesario elegir la herramienta que permita el análisis y manejo de vulnerabilidades, de tal manera, esta elección, se basa en el uso del sistema operativo Kali Linux, ya que dentro de esta distribución se encuentran herramientas como NMAP y OpenVAS, que sirven para gestionar vulnerabilidades, sin embargo en la tabla 39 se realiza una comparación entre Open VAS y Nessus, siendo la primera opción de código abierto y la segunda una herramienta pagada, considerando que las dos opciones, son herramientas que sirven para el análisis y manejo de vulnerabilidades.

Por consiguiente, la comparación entre las dos herramientas se realiza con base en el estudio realizado por (Sowmyashree & Guruprasad, 2020), las características evaluadas en la investigación contienen detalles como: el tipo de licencia, si la herramienta posee interfaz web para su administración, formato en el que brinda los reportes de

vulnerabilidades, la cantidad de vulnerabilidades conocidas en su base de datos (CVEs) y si permite la evaluación de falsos positivos[1].

Tabla 39

Comparación entre Nessus y OpenVAS

Característica	OpenVAS	Nessus
Licencia	Código libre	$2990
Interfaz Web	Sí	Sí
Formato de reportes	HTML, PDF, CSV	HTML, CSV, XML
Common Vulnerabilities and Exposures (CVEs)	Sobre los 26000	Sobre los 50000
Prevención de falsos positivos	Sí	No

Fuente: *Adaptado de* (Sowmyashree & Guruprasad, 2020)

De manera que, en base a la tabla 39, se puede afirmar que OpenVAS y Nessus presentan características similares, en cuanto a los formatos de reporte de vulnerabilidades y la administración mediante una interfaz web; por otro lado, presenta diferencias en el tipo de licencia, la cantidad de CVEs, y la prevención de falsos positivos.

De modo que, considerando el valor de la licencia de Nessus, que se encuentra alrededor de 2900 dólares al año, y la limitación al momento de prevenir falsos positivos, la elección de la herramienta es de OpenVAS, debido a que esta herramienta es gratuita

[1] Un falso positivo, corresponde a la identificación de una actividad como un supuesto evento anormal, pero el evento corresponde a un comportamiento aceptable, en otras palabras, es una falsa alarma.

y presenta como principal beneficio, la evaluación de falsos positivos, permitiendo al encargado de la gestión de vulnerabilidades, determinar la razón de la presencia de los mismos. Como conclusión, se puede afirmar que OpenVAS brinda un equilibrio entre la seguridad de la información y el aspecto económico.

En consecuencia, en la tabla 40, se menciona los requerimientos mínimos necesarios para la instalación de Kali Linux, que es el sistema operativo que alberga la herramienta OpenVAS, para ello se presenta dos opciones de instalación, la primera es en modo consola y que su administración es totalmente por medio de comandos, y la segunda opción es en modo gráfico, en la que su administración es por medio de una interfaz web, en este sentido la última opción requiere la necesidad de mayores recursos tanto en memoria RAM como en disco duro.

Tabla 40

Requerimientos de Instalación de Kali Linux

Instalación en modo consola	Instalación en modo gráfico
Procesador con arquitecturas ARM, i386 y x64	Procesador con arquitecturas ARM, i386 y x64
1 GB RAM	2 GB RAM
8 GB Disco Duro	20 GB Disco Duro

Fuente: *(Kali.org, 2021)*

Finalmente, la elección de la herramienta de reporte de incidentes de seguridad de la información se apoya en la tabla 21 “Características de las herramientas de Tickets” en la que se analizan características como: la compatibilidad de la gestión de servicios con

ITIL, incorporación de una base de datos del conocimiento, generación de respuestas automáticas, posibilidad de realizar encuestas, generación de reportes, permitir la priorización de incidentes y notificaciones por correo.

Así pues, OTRS, es una solución que permite el manejo de incidentes, eventos y problemas de seguridad de la información que se susciten en la UTN, ajustándose al marco de referencia ITIL, además presenta múltiples opciones para la creación de tickets, ya sea por correo electrónico, portal de auto servicio o llamadas, permitiendo la recopilación de información mediante un formulario personalizado, facilitando la clasificación y priorización de los incidentes reportados según su nivel de criticidad, lo que posibilita dar cumplimiento a los niveles de servicio (SLAs) ofrecidos, adicionalmente permite brindar respuestas automáticas, así como poseer una base de datos de conocimientos para solucionar los incidentes de manera rápida y eficaz, aparte ofrece la posibilidad de evaluar el servicio brindado mediante encuestas, y para finalizar la administración de OTRS se la realiza mediante una interfaz web.

En este sentido en la tabla 41 se menciona los requerimientos mínimos para la instalación de OTRS, tanto en hardware, como el tipo de procesador, cantidad de memoria RAM, disco duro, y software como el sistema operativo, tipo y versión de base de datos y servidor web.

Tabla 41

Requerimientos para la Instalación de OTRS

Característica	**Requerimiento**
Procesador	Xeon o similar 2 GHz
RAM	2 GB

Disco Duro	160 GB
Sistema Operativo	Linux
Base de Datos	MySQL 4.1+ / Oracle 10g+ / DB2 8+ / PostgreSQL 8.0+
Servidor Web	Apache2 + PERL 5.8+

Fuente: Adaptado de (Calderón Morocho & Cargua Cargua, 2016)

De esta manera, una vez definido Nagios como la herramienta para el monitoreo de la red, OpenVAS, para el análisis y manejo de vulnerabilidades y OTRS para el reporte de incidentes de seguridad de la información, así como el hardware necesario para la instalación de cada herramienta, en la tabla 42 se presenta en síntesis la cantidad de equipos necesarios con el detalle de la herramienta, sistema operativo, y su correspondiente segmentación de red (IP) y Vlan.

Tabla 42

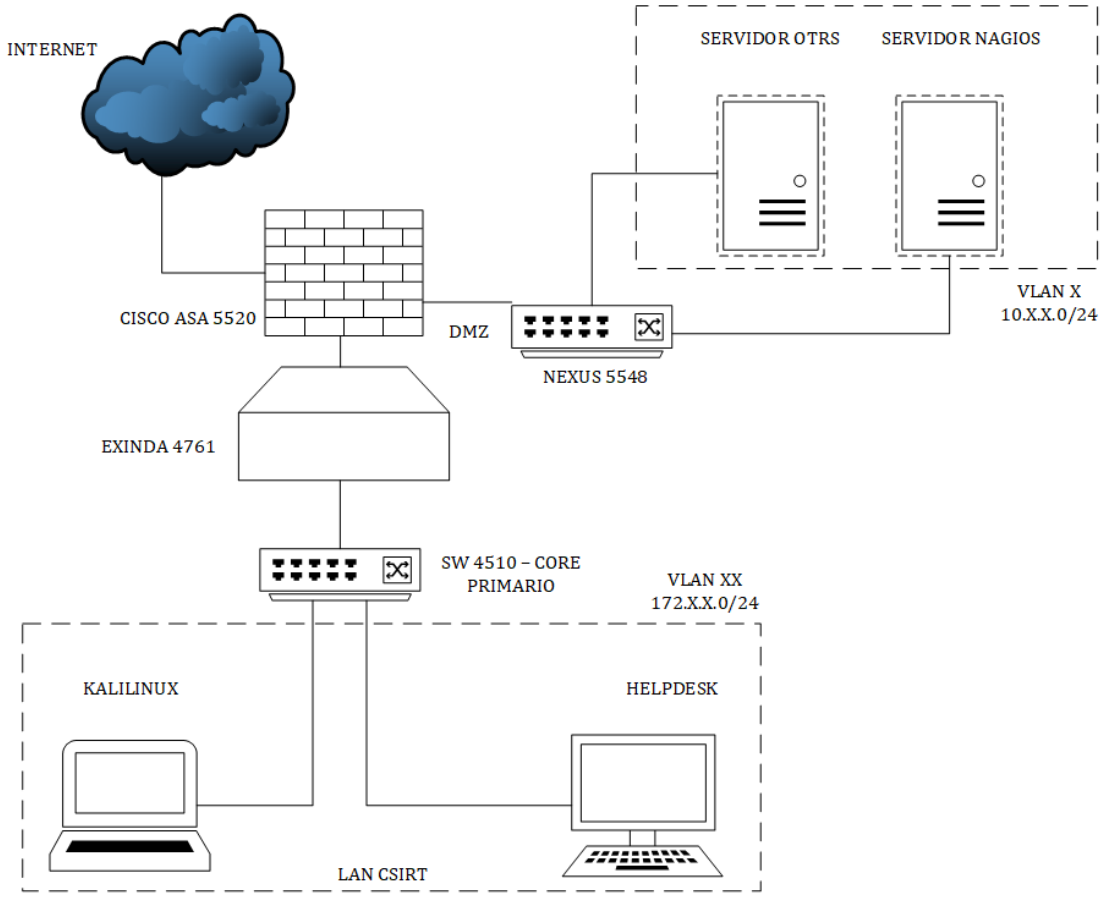
Síntesis de Equipos con su Respectiva IP y Vlan

Cantidad	**Detalle**	**IP**	**VLAN**
1	Servidor Nagios	10.x.x.0/24	VLAN DMZ
1	Servidor OTRS	10.x.x.0/24	
1	Computador con Kali Linux	172.x.x.0/24	VLAN CSIRT
1	Computador con Windows	172.x.x.0/24	

Para concluir, en la figura 11 se procede a representar de manera gráfica la infraestructura de red del CSIRT académico de la UTN, incluyendo los servidores de monitoreo nagios y sistema de gestión de tickets OTRS a la topología de red de la UTN, recalcando que en etapas iniciales, el CSIRT académico de la UTN hará uso de la DMZ de la universidad, para alojar estos servidores, por cuanto los servicios a brindar no comprometen la seguridad informática de la red de la UTN, así mismo el departamento del CSIRT, trabajará en una vlan independiente para atender los incidentes reportados (OTRS) y monitorizar la red (Open Vas – Kali Linux). En este sentido, la separación de la red del CSIRT mediante una vlan brinda seguridad de la información y se da cumplimiento con las recomendaciones de las guías para la creación de CSIRTs.

Figura 11

Infraestructura de Red del CSIRT



4.4 Aplicación de Normas y Estándares de Gestión de Incidentes

En este apartado se menciona la aplicación de normas y estándares que sirven de apoyo para que el CSIRT gestione los incidentes de seguridad de la información que sean reportados, y la presentación del CSIRT, a la comunidad objetivo y en general.

4.4.1 Aplicación del ITIL V4

El marco de referencia ITIL V4, conjuntamente con la norma ISO/IEC 27002, sirven para regular y mejorar la gestión de servicios de respuesta a incidentes de seguridad de la información, aplicando las prácticas de gestión de servicios, donde los aspectos que se toma en cuenta para el CSIRT Académico, son: seguimiento y gestión de eventos, gestión de incidentes, problemas y gestión del nivel del servicio.

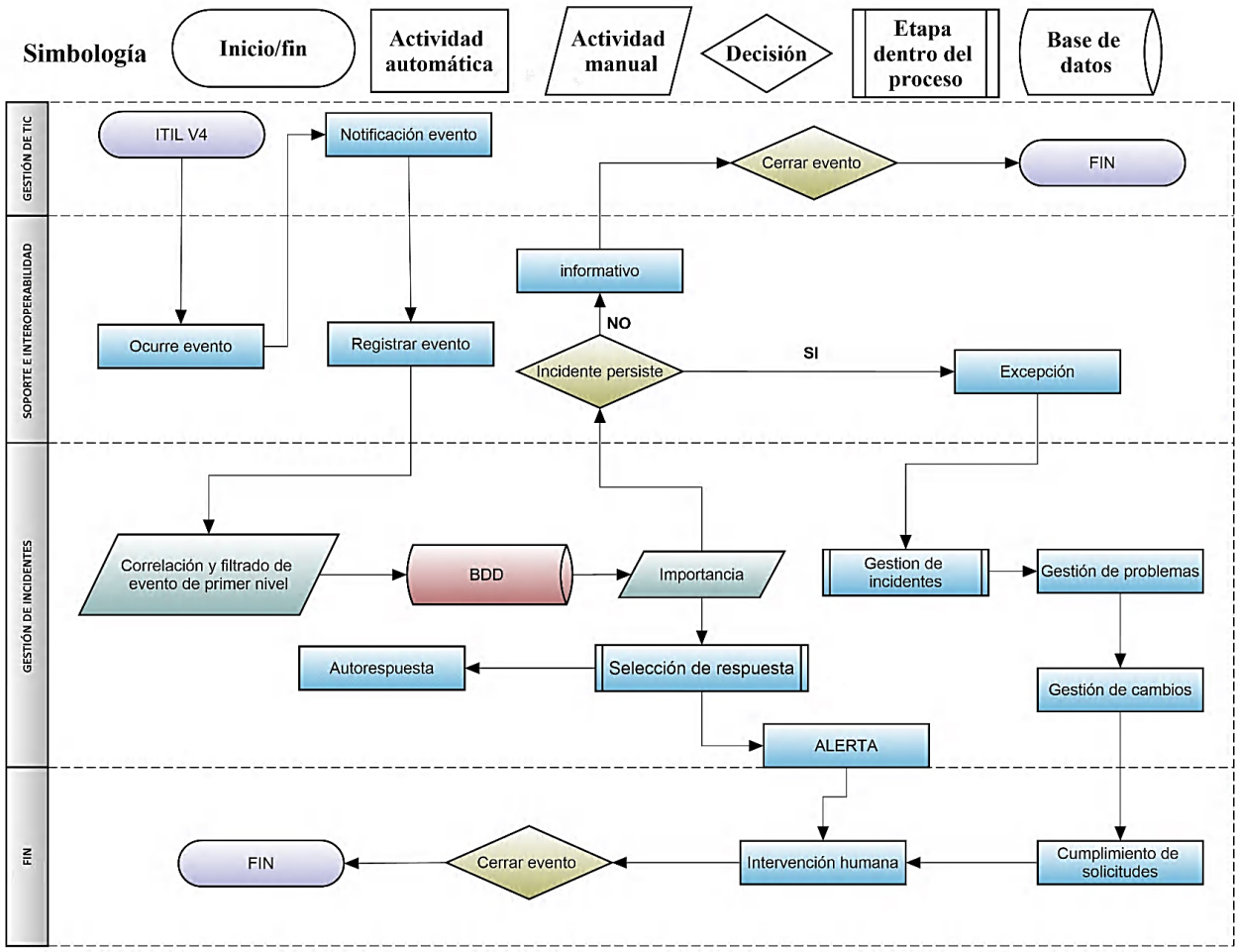
Primeramente, se hace mención a las prácticas de seguimiento y gestión de eventos. En efecto, antes de proceder con la aplicación de esta práctica, es necesario señalar que para ITIL, un evento es un suceso que afecta de forma directa a la infraestructura o la provisión de un servicio de TI (Tecnologías de Información).

Ciertamente, este proceso busca poder registrar, detectar, notificar, categorizar, correlacionar y cerrar cada evento que se presente durante la prestación de un servicio de TI, además de monitorear el servicio y detectar cuando el desempeño de estos servicios monitoreados presente algún comportamiento inadecuado.

Por lo tanto, las actividades claves de este proceso son: notificación, detección, registro del evento, primer nivel de filtrado y correlación de eventos, establecimiento de la importancia del evento, segundo nivel de correlación de evento, seleccionar una respuesta, revisar acciones y cierre del evento. Estas actividades se presentan en la figura 12 de la siguiente manera:

Figura 12

Proceso Para la Gestión de Eventos



De este modo, en base a la figura 12, el proceso para la gestión de eventos inicia en el momento en el que ocurre un evento, llevando a cabo su registro, lo que permite realizar la correlación de primer nivel o de segundo nivel, en otras palabras, se procede a buscar eventos suscitados anteriormente, seguido de esto, se hace una medición de la importancia del evento, es decir, si el evento es de tipo informativo se cierra, debido a que este, no afecta la provisión del servicio, por otro lado si es de tipo excepción, y puede afectar la red o sistemas de la UTN, se analiza si el evento se puede convertir en un incidente, de ser el caso se activa el proceso para gestión de incidentes, si es un problema se ejecuta el

proceso de gestión de problemas o si el evento genera un cambio se pone en marcha el proceso de gestión de cambios.

Agregando a lo anterior, luego de asignar el nivel de importancia que tiene el evento e identificar si se produce un incidente, un problema o un cambio se prosigue a determinar si se obtuvo una solución efectiva y se cierra el mismo.

Cabe mencionar, que dependiendo del impacto que tiene el evento puede existir eventos de segundo nivel, de ser así, es necesario analizar si es preciso realizar alguna acción adicional antes de cerrar el mismo, de lo contrario, se revisa si el evento genera un incidente, problema o cambio y continuar como en los pasos anteriores hasta cerrar el evento.

En segundo lugar, se presenta la práctica de gestión de incidentes, en el cual se incluye todo evento que interrumpa o que pueda interrumpir la prestación de un servicio de TI en la UTN, siendo comunicado al CSIRT académico de la UTN por cualquiera de las herramientas de notificación que este maneje, es relevante comentar que para ITIL la herramienta recomendada es el Service Desk o mesa de ayuda.

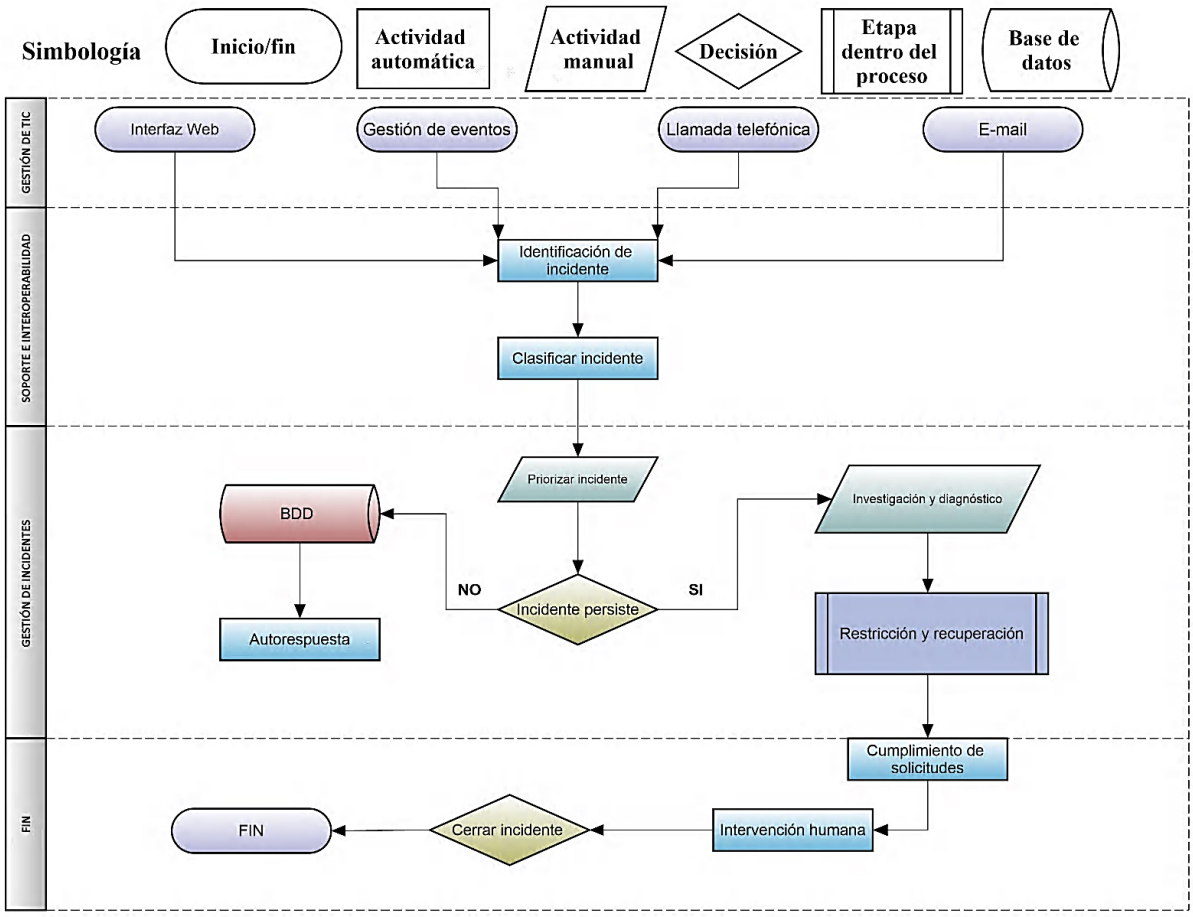
Más aún, para una buena gestión de incidentes es necesario la utilización de una herramienta que facilite seguir un flujo de trabajo estándar durante toda la operación, es decir, al registrar cada incidente, el agente debe obtener toda la información relativa del mismo, los pasos a seguir en orden cronológico para brindar una solución del incidente, así como responsabilidades, escalas de tiempos con sus umbrales y procedimiento para el escalamiento.

En consecuencia, este proceso consta de los siguientes pasos: identificación, registro, categorización, priorización, diagnóstico inicial, escalado, investigación y diagnóstico, resolución y restauración, y finalmente el cierre del incidente.

Cabe resaltar que durante todo el desarrollo de estas actividades se lleva el control sistemático de tiempo utilizado, hasta llegar al cierre del incidente y la recuperación del servicio interrumpido. En la figura 13 se presenta el manejo de la gestión de incidentes:

Figura 13

Manejo de Gestión de Incidentes



En relación con el proceso detallado en la figura 13, precisa mencionar que posee diferentes entradas por las cuales el cliente puede comunicar un incidente. Por ende, a medida que llega un incidente, es necesario registrar con fecha y hora, permitiendo conocer la trazabilidad que tiene el incidente desde la notificación hasta el cierre, continuando con la identificación del impacto que tiene sobre la organización, y de esta manera establecer el nivel de urgencia que requiere para determinar su prioridad.

Ahora, conociendo la prioridad y el impacto que el incidente tiene sobre la organización es posible determinar si es crítico, y de ser así, se procede a ejecutar el proceso adecuado para incidentes de este tipo.

Por otra parte, si el incidente no es crítico se lleva a cabo un diagnóstico inicial, apoyado en una Base de Datos de Errores Conocidos (KEDB), que permite brindar una solución, por ello es importante que el Service Desk se fije como objetivo, solucionar un porcentaje alto de incidentes en la primera notificación, de no ser posible se procederá a hacer el escalamiento hasta brindar una solución.

Para finalizar los últimos pasos corresponden a la documentación del incidente, y evaluar la satisfacción de los usuarios mediante una encuesta, lo que permite mejorar el servicio y finalmente se procede a cerrar el incidente.

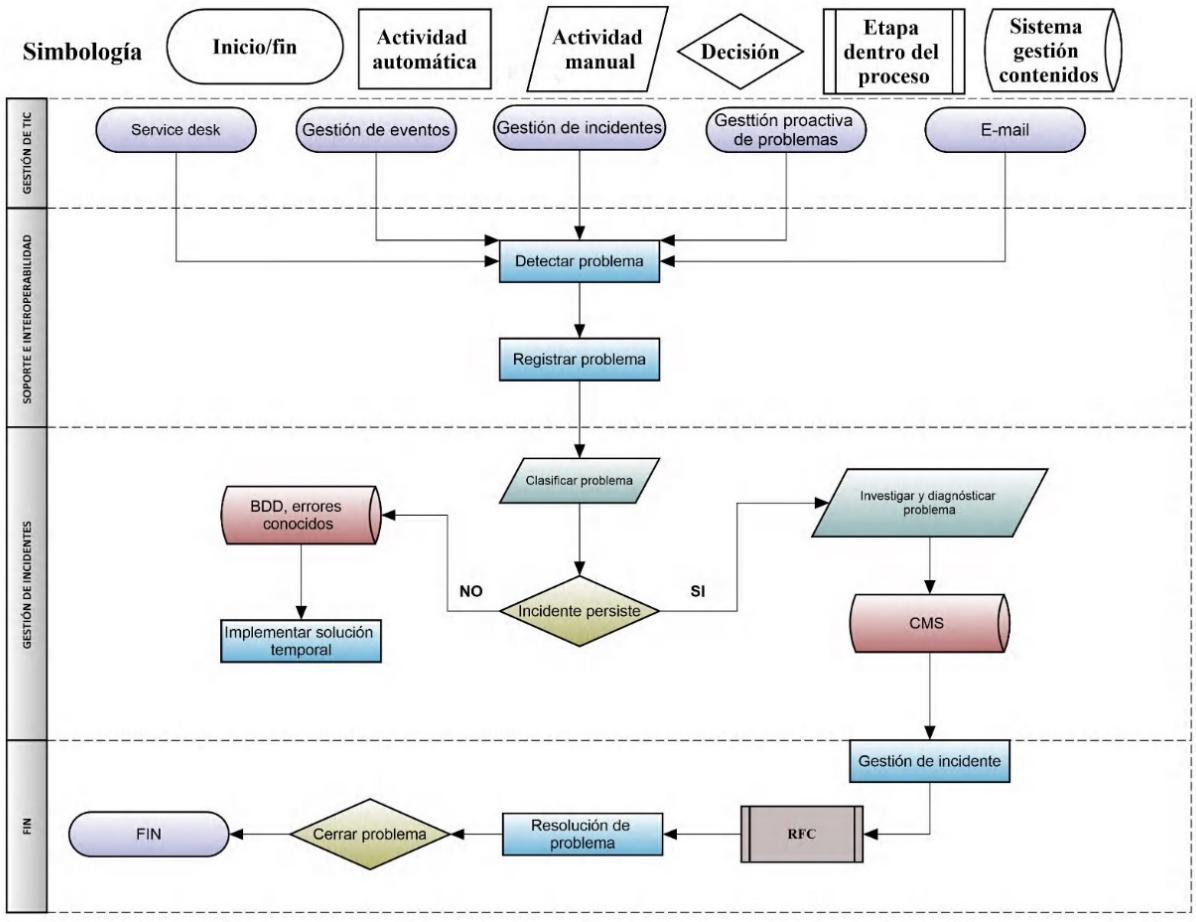
Para terminar, la última práctica corresponde a la gestión de problemas, la misma que se encarga de analizar y resolver las causas de los incidentes de seguridad de la información, así como desarrollar actividades proactivas para evitar incidencias futuras; para ello, utiliza el llamado “subproceso de errores conocidos”, permitiendo obtener diagnósticos rápidos ante la presencia de nuevas incidencias.

Por consiguiente, los objetivos principales de este proceso son: la administración del ciclo de vida de todos los problemas, prevenir la ocurrencia de problemas e incidentes, eliminar incidentes recurrentes y minimizar el impacto de los incidentes que no pueden ser prevenidos.

En efecto, las actividades de esta práctica son: detectar, registrar, clasificar, priorizar, investigar y diagnosticar el problema, encontrar una solución temporal, registrar el error conocido, resolver, cerrar el problema y revisar algún problema mayor, en este sentido, en la figura 14 se presenta el proceso a seguir para la gestión de problemas:

Figura 14

Proceso para la Gestión de Problemas



Consecuentemente, según la figura 14, la gestión de problemas se activa desde el Service Desk, mediante el envío de un correo electrónico, y como se detalla en la gestión de incidentes y eventos. el primero paso que se realiza, es la detección del problema, continuando con la clasificación y priorización del mismo, seguido de esto, se procede a investigar y diagnosticar los incidentes con la ayuda del CMS (Sistema de gestión de contenidos) en donde existe información de incidentes, problemas y errores conocidos.

De esta manera, una vez identificado y diagnosticado el problema, se procede a evaluar, en caso de ser necesario se brinda una solución temporal, permitiendo solucionar el problema en tiempo real, teniendo presente que más adelante deberá ser modificada, incluso puede activar el proceso de gestión de incidentes, caso contrario se registra el problema en la base de datos de errores conocidos.

Finalmente, si después de realizar este proceso, existe la necesidad de aplicar un cambio, se debe realizar un RFC (Request for Change) y pasar por el proceso de gestión de cambios para finalmente brindar una solución al problema, si el problema verdaderamente se solucionó se procede a cerrar el problema, caso contrario se procede a priorizar el problema y a realizar todo el proceso nuevamente hasta brindar una solución.

4.4.2 Aplicación de la Norma RFC 2350

La RFC 2350 permite informar de la creación del CSIRT académico a la UTN y al público en general, presentando de manera resumida información relevante como la versión del documento elaborado, información de contacto, la misión, políticas, servicios que brinda el CSIRT y formularios de notificación de incidentes.

De manera que, esta información se detalla en la tabla 43, cabe aclarar que se presenta información con la cual se posee en el momento de realizar el presente trabajo de

titulación, sin embargo, cuando el CSIRT académico de la UTN sea implementando, la información deberá ser cubierta en su totalidad.

Tabla 43

Descripción del CSIRT-UTN

1. Información del documento	
1.1 Fecha de la última actualización	01 de marzo de 2020
1.2 Lista de distribución para notificaciones	No disponible
1.3 Ubicaciones donde se puede encontrar este documento	La versión actual del documento no está disponible
2. Información de contacto	
2.1 Nombre del equipo	CSIRT-UTN, Equipo de Respuesta a Incidentes de Seguridad Informática de la Universidad Técnica del Norte.
2.2 Dirección	Universidad Técnica del Norte, Dirección de Desarrollo Tecnológico e Informático, CSIRT-UTN, Av. 17 de Julio, Ibarra-Ecuador
2.3 Zona horaria	UTC-GMT -5
2.4 Número de teléfono	No disponible
2.5 Número de fax	No disponible
2.6 Otras telecomunicaciones	No disponible

2.7 Direcciones de correo electrónico	No disponible
2.8 Claves públicas e información de cifrado	No disponible
2.9 Miembros del equipo	No disponible
2.10 Otra información	No disponible
2.11 Puntos de contacto con el cliente	No disponible
3. Estatuto	
3.1 Declaración de la misión	El CSIRT académico de la UTN se encarga de brindar servicios de seguridad informática a la comunidad universitaria, permitiendo evitar incidentes informáticos mediante servicios reactivos, proactivos y de gestión de la calidad de seguridad. Comunidad a la que brinda servicios: Todos los funcionarios de las diferentes áreas, Docentes y estudiantes de la UTN.
3.2 Unidad constitutiva	El CSIRT UTN brinda sus servicios a todos los funcionarios de las diferentes áreas, Docentes y estudiantes de la UTN.

3.3 Patrocinio y/o afiliación	El Equipo CSIRT – UTN es patrocinado por la Universidad Técnica del Norte y la– Dirección de Desarrollo Tecnológico e Informático.
3.4 Autoridad	El CSIRT-UTN opera bajo el auspicio y con autoridad compartida con el Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte.
4. Políticas	
4.1 Tipos de incidentes y nivel de apoyo	El Equipo CSIRT-UTN se encarga de manejar y dar solución a todos los incidentes 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. El nivel de apoyo que brinde el CSIRT-UTN y el tiempo de respuesta del mismo, dependerá de la gravedad del incidente

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-UTN, y la respuesta se realizará en base a uso y manejo de una metodología para el manejo de incidentes. Cuando sea necesario el CSIRT-UTN 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-UTN mantener informada a la comunidad universitaria acerca de posibles vulnerabilidades antes de que estas sean explotadas, para ello se encuentran disponibles los reportes de vulnerabilidades emitidos por el CSIRT-UTN, y boletines de alertas y advertencias emitidos por otros CSIRT o proveedores de aplicaciones.

4.2 Cooperación, interacción y divulgación de información	La información será manejada con absoluta confidencialidad de acuerdo a las políticas y procedimientos para la Gestión de Incidentes establecidos por el CSIRT y de las políticas y normas de la UTN, 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 el CSIRT-UTN.
4.3 comunicación y autenticación	No disponible

5. Servicios
Monitoreo de sistemas informáticos y redes
Alertas y advertencias
Manejo y análisis de incidentes y vulnerabilidades
Respuesta a incidentes en el sitio
Comunicados
Difusión de información sobre seguridad informática

Concienciación Actividades de formación y capacitación a la comunidad de la UTN
6. Formularios de notificación de incidentes
Para realizar el reporte de incidentes debe utilizar los formatos elaborados por el Equipo CSIRT-UTN, los mismos que se pueden obtener en el Equipo CSIRT-UTN o en el portal web del CSIRT-UTN.
7. Descargo de responsabilidad
El Equipo CSIRT-UTN no se responsabiliza por el mal uso que se dé a la información aquí contenida.

4.3 Relaciones con otros Equipos

Las relaciones con otros equipos del CSIRT Académico UTN, serán exclusivamente de comunicación, asesoramiento e intercambio de información relativa a la seguridad de la información y la gestión de incidencias y vulnerabilidades, a través de contactos con los siguientes equipos: CSIRT CEDIA y EcuCERT. En este sentido se obtuvo un primer acercamiento con los dos equipos, en el cual se obtuvo información relevante sobre los beneficios que se tendría al crear un CSIRT en la UTN, recomendaciones para llevar a cabo la creación y requerimientos para establecer colaboración con otros CSIRT.

De modo que, la comunicación con estos equipos, se la realizará mediante él envió de reportes de incidentes y vulnerabilidades, para buscar asesoramiento para la solución de tales eventos, cuando estos sean críticos y no existan métodos o herramientas para solucionarlos. Por tanto, es necesario crear un sitio en la web de la UTN, para el CSIRT

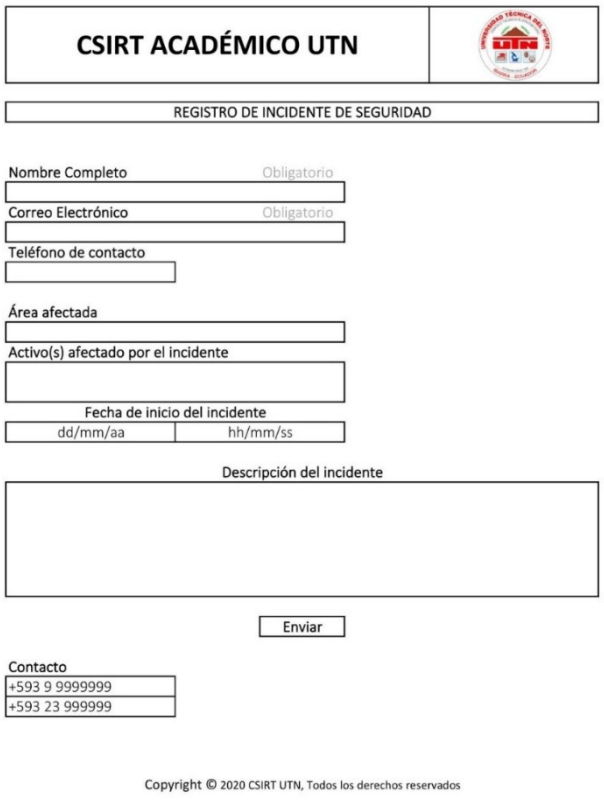
académico en donde se publique toda la información relacionada con incidencias y vulnerabilidades reportadas y clasificadas en la UTN.

4.4 Desarrollo de Formulario para el Registro de Incidentes

En la figura 15 se presenta el formulario para el registro de un incidente de seguridad de la información que sea reportado a través de la página web del CSIRT-UTN, o a su vez puede ser reportado mediante correo electrónico, en el cual deberá contener la misma información que se presenta en el formulario, la información solicitada corresponde a lo siguiente: nombre completo de la persona que notifica de la presencia del incidente de seguridad de la información, correo electrónico, teléfono de contacto, área y activo tecnológico al cual puede afectar el incidente, fecha y hora de la detección del incidente y una breve descripción del mismo.

Figura 15

Formulario para el Registro de Incidentes



4.5 Cronograma de Implementación del CSIRT Académico en la UTN

Para la implementación del CSIRT académico de la UTN en un futuro, se presenta el diagrama de precedencia en la tabla 44, en el que se detalla el contenido de las actividades, tiempo estimado y descripción para cada actividad, permitiendo hacer énfasis en las actividades que hay que realizar para poder continuar con la siguiente tarea, por tanto, ayuda a llevar a cabo un orden para la implementación del CSIRT.

Tabla 44

Diagrama de Precedencia

Clave de Actividad	Descripción	Duración	Actividad Precedente
A	Obtener aprobaciones necesarias e instalaciones donde operará el CSIRT.	(20 días)	Ninguna
B	Contratar y capacitar al personal inicial de CSIRT.	(20 días)	A
C	Definir servicios, desarrollar el conjunto inicial de políticas y procedimientos del CSIRT para respaldar los servicios.	(15 días)	B
D	Definir especificaciones de equipos, comprar e implementar la infraestructura de red necesaria para apoyar el CSIRT.	(10 días)	B
E	Desarrollar pautas y formularios de notificación de incidentes para la organización.	(10 días)	D

F	Implementar un sistema de seguimiento de incidentes.	(15 días)	C, E
G	Definir plan de comunicación y dispersión del CSIRT.	(5 días)	F
H	Ejecutar plan de comunicación y dispersión de CSIRT y comienzo de las operaciones del CSIRT	(5 días)	G
I	Evaluación de la efectividad del CSIRT	(5 días)	H

En consecuencia, en base a la tabla 44, cada actividad tiene una clave, la cual va en orden alfabético desde la letra A, hasta la I, permitiendo desarrollar el diagrama de precedencia, que posibilita la identificación y ejecución de cada actividad, en este sentido la primera actividad a realizar es la aprobación por parte de las autoridades, de ejecutar la implementación del CSIRT académico en la UTN, de esta manera se obtiene las instalaciones en donde puede operar el CSIRT.

Seguidamente se procede a la contratación del personal y capacitación en caso de ser necesario, y, una vez definido estas dos actividades, se procede a ejecutar la definición de servicios, políticas y procedimientos del CSIRT, asimismo, a la par se puede definir las especificaciones y compra de los equipos tecnológicos necesarios para el desarrollo de las actividades del CSIRT.

Por ende, una vez que se complete estas actividades se procede a desarrollar los formularios de notificación de incidentes de seguridad de la información y la implementación del sistema de seguimiento de incidentes, con esto, se lleva a cabo la

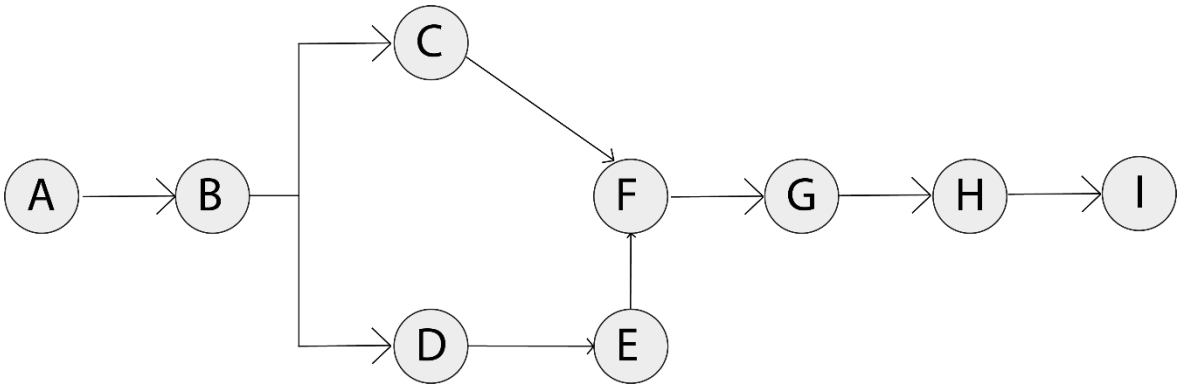
definición del plan de comunicación del CSIRT a la comunidad objetivo, continuando con la ejecución del mismo.

Finalmente, con la puesta en marcha del CSIRT se procede a ejecutar una evaluación en los procesos de gestión de incidentes para comprobar su efectividad y poder mejorar los mismos.

Por consiguiente, en la figura 16 se presenta de manera gráfica el diagrama de precedencia, que muestra la consecución de las actividades antes mencionadas, permitiendo estandarizar los procesos, y proporcionar un indicador de cumplimiento de los objetivos que se detallan en la investigación.

Figura 16

Diagrama de Precedencia con Recorrido Detallado



CAPÍTULO V FASE DE PRUEBA DEL CSIRT UTN

En este capítulo se realiza el desarrollo de la prueba piloto, para demostrar el funcionamiento del CSIRT académico en la UTN, las pruebas a realizar son, análisis de vulnerabilidades en el Data Center de la Facultad de Ciencias Aplicadas (FICA), es importante mencionar, que estaba previsto realizar las pruebas dentro del DDTI, pero por circunstancias que se atraviesa dentro del país debido a la pandemia del COVID, no se permitió el acceso a dicha área, sin embargo se pudo realizar las pruebas de manera exitosa, la segunda prueba corresponde al monitoreo de un servidor con Nagios, seguido de esto se realiza una simulación del reporte de incidentes y por último se lleva a cabo la evaluación de los procesos de gestión de incidentes de seguridad de la información.

Por lo tanto, dentro de las pruebas de análisis de vulnerabilidades, se utilizó software de código libre, como NMAP (Network Mapper), permitiendo conocer las vulnerabilidades que se presentan en la red, mediante el escaneo de puertos de los diferentes equipos, así como la búsqueda de vulnerabilidades presentes en los dispositivos del Data Center de la FICA.

En cuanto a la monitorización de un servidor, se realiza la prueba con Nagios, que permite realizar el monitoreo de servidores y equipos presentes dentro de una red, este servidor de monitorización permite conocer la existencia de algún comportamiento inadecuado, alertando la presencia de alguna vulnerabilidad en la red.

Por otra parte, se realiza una simulación de notificación de un incidente de seguridad de la información el mismo que es reportado mediante la herramienta OTRS, generando un ticket, al cual se brinda una solución mediante los procedimientos para la gestión de eventos, incidentes o problemas. Y finalmente se utiliza la herramienta SIMPROCESS,

que permite evaluar los procesos de gestión de incidentes del CSIRT académico en la UTN.

5.1 Escaneo de Puertos con NMAP y Análisis de Vulnerabilidades

El análisis de vulnerabilidades busca, mediante herramientas de escaneo o detección, enumerar las debilidades existentes dentro de una red, detectando aplicaciones y sistemas que puedan comprometer la seguridad de la red de la organización, ahora bien, para la presente prueba se sigue la metodología según (Romero Castro et al., 2018), en la cual detalla los siguientes pasos para el análisis de vulnerabilidades: acuerdo de confidencialidad, debido a que la información obtenida como proceso del análisis debe ser tratada con sigilo, además, como segundo punto es importante establecer las directrices a ser realizadas dentro del análisis, en las cuales se establecen los límites a seguir, el siguiente paso es la recolección de la información del objetivo a ser analizado y una vez que se obtiene la información se procede a realizar el respectivo análisis de vulnerabilidades, concluyendo con un informe de las vulnerabilidades encontradas. De esta manera, en el **Apéndice P,** se proporciona un ejemplo de cómo presentar una propuesta para el análisis de vulnerabilidades, siguiendo los pasos antes mencionados.

Ahora bien, en esta etapa de pruebas es preciso aclarar que se realiza un análisis de vulnerabilidades y no un pentesting o hacking ético, debido a que en esta sección se realiza un demo del funcionamiento del CSIRT académico de la UTN con los servicios de monitoreo de redes, y análisis de vulnerabilidades propuestos en el capítulo 4.

En efecto, en la tabla 45 en base a (Josue, 2020), se menciona las diferencias que contiene cada una de las pruebas mencionados en el párrafo anterior, presentado diferencias en parámetros como: el objetivo de la prueba, la metodología que se utiliza,

el tipo de personal que realiza la prueba, cuál es su valor principal y que contiene el informe final de la prueba.

Tabla 45 Diferencias Análisis de Vulnerabilidades, Pentesting, Hacking Ético

Diferencias entre Análisis de Vulnerabilidades, Pentesting y Hacking Ético

	Análisis de Vulnerabilidades	Pentesting	Hacking Ético
Objetivo	Enumeración de vulnerabilidades	Enumeración y descubrimiento de vulnerabilidades	Tomar control de la organización bajo cualquier circunstancia
Metodología	No tiene una metodología	OSSTMM, OWASP	Combinación de algunas metodologías
Quién lo realiza	Lo realiza personal interno, que posee credenciales y accesos privilegiados, no es necesario que posea altos conocimientos	Personal especializado, con alto nivel de conocimientos técnicos	Expertos en temas de seguridad ofensiva, casi parecido a una organización cibercriminal
Valor principal	Detección de vulnerabilidades en los sistemas, aplicaciones, servidores que puedan ser comprometidas	Identificar las vulnerabilidades que pueden poner en peligro la seguridad informática de la empresa para reducir y mitigar los posibles riesgos	Evaluar e identificar las vulnerabilidades
Informe	Se entrega un informe técnico, en el cual se enumera las vulnerabilidades que se identifiquen y procesos de remediación	Se entrega un informe ejecutivo y técnico de las vulnerabilidades halladas, en la cual se incluye posibles ataques y los ataques que se pudieron realizar, además los procesos de remediación	Se presenta un informe detallado técnico y ejecutivo de los vectores de ataque que se usaron, pruebas de ingeniería social, un informe de las posibles debilidades que presentan en la infraestructura de seguridad, el impacto que puede ocasionar, niveles de acceso y tareas que permitan

	remediar las debilidades

Fuente: (Auditech, 2020)

En este sentido, para el análisis de vulnerabilidades, se hace uso de NMAP, la cual es una herramienta que permite escanear los dispositivos conectados a la red, identificar puertos abiertos y conocer las vulnerabilidades en los servicios, siendo esta herramienta instalada dentro del sistema operativo Kali Linux, que es utilizado para realizar auditorías de seguridad informática.

En efecto, para el escaneo de puertos con NMAP, en primera instancia se obtiene toda la información acerca de los equipos de la red, luego con esta información se procede a realizar un escaneo de los puertos y por último se realiza la búsqueda de vulnerabilidades que puedan existir en los servicios y dispositivos de la red.

5.1.1 Recolección de Información de la Red

Existen tres metodologías para la obtención de información de la red y poder proceder con el análisis de vulnerabilidades, estos métodos son: de caja blanca, gris y negra, en tal sentido, en el primer método se tiene acceso total a la información de la red, la segunda se dispone de información parcial, y la última no se posee información de la red a ser auditada.

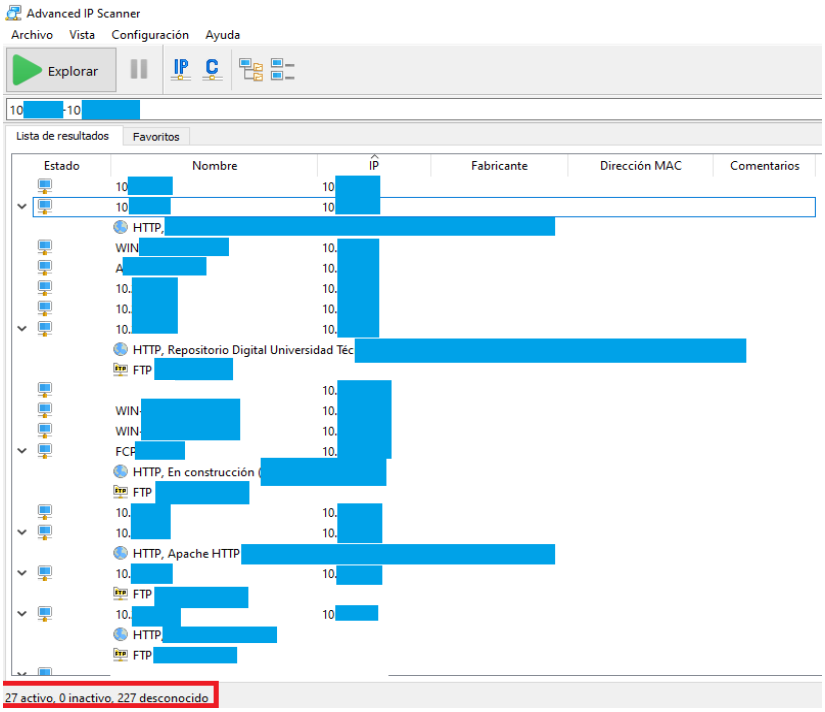
Precisamente, la metodología utilizada para el análisis de vulnerabilidades es de caja gris, por lo tanto la información que se obtuvo es la subred en la que se encuentran los servidores del Data Center de la FICA siendo objetivo de análisis, en este sentido primeramente se hace uso de la herramienta denominada Advance IP Scanner para la recolección de la información, la misma que es una herramienta gratuita que permite

descubrir los dispositivos activos en una red, para ello se realiza el escaneo a la red en la que se encuentran los servidores de interés para las pruebas.

Luego, en la figura 17 se presenta el resultado por parte de esta herramienta, brindando información sobre su estado, el nombre del servicio y la IP, y que por motivos de seguridad de la información las direcciones IP se presentan ocultas con una franja de color celeste, por lo tanto, se detecta la presencia de 27 IPs en el rango de la subred 10.X.X.X.

Figura 17

Escaneo de Host Activos Dentro de la Red

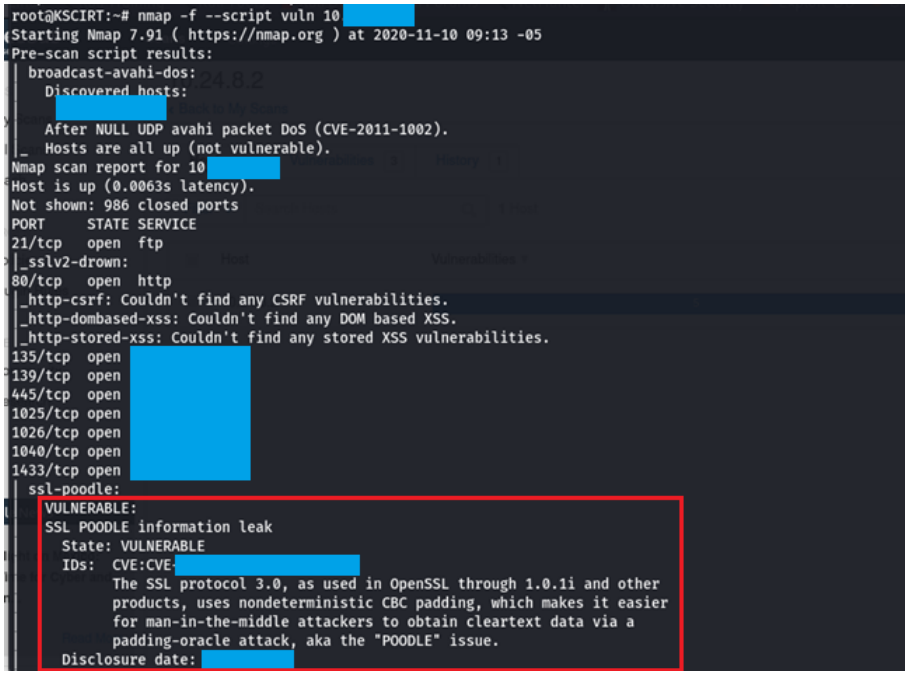


Seguido de esto, y en base a estas direcciones IP detectadas, se realiza la búsqueda de vulnerabilidades con el comando nmap -f –script vuln <IP a escanear>, este comando hace uso de un script propio de nmap, permitiendo encontrar vulnerabilidades existentes. En consecuencia, la figura 18 presenta un ejemplo de las vulnerabilidades encontradas en una dirección IP específica, y que por seguridad de la información se presenta la demostración de uno de los resultados del escaneo, el informe con las vulnerabilidades

encontradas se entregará de manera confidencial al administrador de la red del Data Center de la FICA.

Figura 18

Resultado de Escaneo de Vulnerabilidades



En base a la figura 18, se presenta el resultado del análisis de vulnerabilidades con nmap, descubriendo la presencia de una vulnerabilidad, la cual es detectada mediante un CVE (Common Vulnerabilities and Exposures), en otras palabras, el CVE hace referencia a un listado de vulnerabilidades conocidas, llevando un identificador que permite realizar la búsqueda de información de las vulnerabilidades encontradas en la página web https://www.cvedetails.com/.

En este sentido, luego de ingresar el CVE-ID, esta página proporciona información de la vulnerabilidad, la versión del software afectado, en caso de existir, brinda información de la solución que permita la mitigación de la misma y, además da a conocer cómo se puede realizar la explotación a esta vulnerabilidad.

Igualmente, al realizar el escaneo de las vulnerabilidades, muestra el estado de los puertos, si están en estado abierto o cerrado, así como también el servicio del puerto, siendo importante mencionar que el estado de puertos abiertos puede ser una vulnerabilidad, ya que es recomendable, en caso de no usar algún puerto, cerrarlo o a su vez asegurar los puertos abiertos.

5.1.2 Resultados del Escaneo de Vulnerabilidades con NMAP

A continuación, en la figura 19 se presenta un ejemplo de cómo se presenta el informe de vulnerabilidades encontradas, el mismo que consta de una matriz, en la que se especifica la IP a la cual se le realizó el escaneo de vulnerabilidades, los puertos abiertos, protocolos y servicios correspondientes a los puertos, detalle de las vulnerabilidades encontradas y los respectivos correctivos que se pueden realizar.

Figura 19

Registro de Vulnerabilidades Encontradas

REGISTRO DE ANÁLISIS DE VULNERABILIDADES		
SERVIDOR		
IP	**10.**	
S. O	**Linux Kernel 2.6**	
PUERTOS ABIERTOS	**PROTOCOLO**	**SERVICIO**
2	tcp	ftp
2	tcp	ssh
1	tcp	rpcbind
4	tcp	https
8	tcp	accessbuilder
3	tcp	mysql
5	Tcp	nrpe
5	tcp	vnc-http
5	tcp	vnc
5	tcp	ncd-conf
VULNERABILIDADES ENCONTRADAS		
1. Inyección de comandos en GNU Bash conocida como Shellshock 2. Servicio remoto acepta conexiones cifradas mediante SSL X.X, estas versiones son afectadas por fallas criptográficas 3. SSH hace uso de cifrado de flujo Arcfour 4. Servidor web remoto admite métodos TRACE y/o TRACK 5. Servidor web remoto contiene el script de prueba "test-cgi" 6. Detección mDNs		
CORRECTIVOS		
1. Aplicar parche que hace referencia al CVE- la misma que puede ser encontrada en https://access. 2. Desactivar SSL X.X, en su lugar hacer uso de TLS 1.2 o superior 3. Eliminación de cifrados débiles 4. Deshabilitar los métodos HTTP 5. Eliminar printerv de /cgi-bin 6. Filtrar el tráfico entrante al puerto UDP		

5.2 Monitoreo de Equipos con Nagios

Nagios es una herramienta de código abierto, que permite la supervisión de equipos y servicios en una red, generando alertas ante la presencia de comportamientos inadecuados, además brinda reportes del estado de los equipos monitoreados, permitiendo conocer el rendimiento de los mismos. Para este demo, la herramienta nagios, fue instalada en la distribución de LINUX denominada DEBIAN en su versión 10.

De modo que en esta etapa de prueba piloto se presenta algunas de las funcionalidades y configuraciones importantes tanto para el servidor monitorizado (equipo cliente), como el servidor de monitorización (ver Apéndice Q).

La monitorización con nagios, se la realiza mediante la instalación de un plugin denominado NRPE (Nagios Remote Plugin Executor), el cual es un agente que se instala en el dispositivo cliente, permitiendo la comunicación con el servidor de monitorización, en este sentido, es importante mencionar que NRPE es un módulo que permite ejecutar plugins locales de los dispositivos y así realizar peticiones para monitorear los equipos de manera activa.

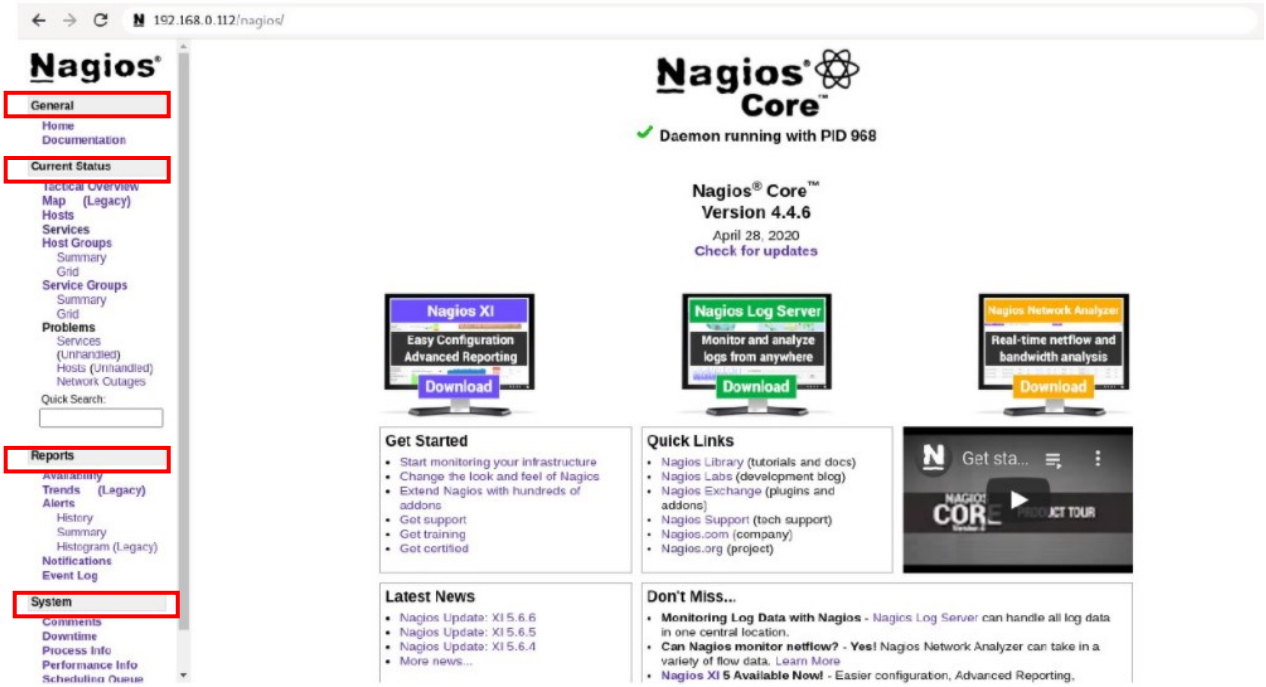
5.2.3 Resultados de la Monitorización con Nagios

Primeramente se presenta en la figura 20, la interfaz web de nagios, incorporando cuatro secciones denominadas de la siguiente manera: general, estado actual, reportes y sistema, ahora bien, la primera sección (General), permite dirigirse a la página principal (Home) y revisar la documentación acerca de nagios (Documentation), seguidamente se tiene la sección correspondiente al estado actual (Current Status), presentando información de los servicios y dispositivos de la red, a continuación presenta la sección de reportes (Reports), que permite conocer de manera gráfica el estado de cada equipo o

servicio monitoreado, y finalmente la sección del sistema (System), la misma que contiene alternativas que permiten conocer si existen dispositivos para mantenimiento, información del servidor, notificaciones, opciones de reiniciar o detener la monitorización e información del rendimiento de nagios.

Figura 20

Interfaz Web del Servidor Nagios

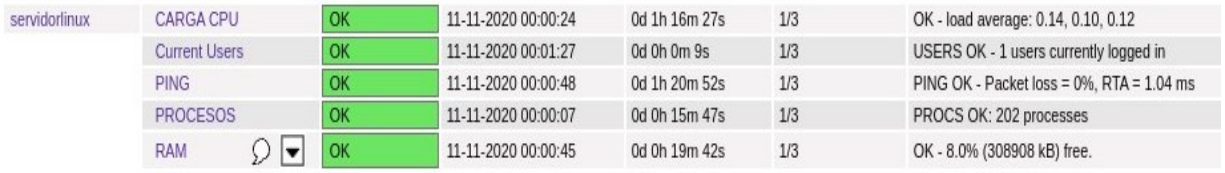


Por consiguiente, la sección principal de la interfaz web de nagios se encuentra dentro de la sub sección de servicios, la misma que se encuentra dentro del estado actual o current status, permitiendo observar el estado de los recursos y servicios de los equipos monitoreados, correspondientes a la carga del CPU, el número de usuarios conectados al servidor, estado de la comunicación o ping, los procesos que se están ejecutando y la ocupación de la memoria RAM, en este sentido se presenta el estado de los servicios en la figura 21, presentando el estado de todos los servicios como OK.

En este caso, es importante conocer los siguientes estados de notificación que la herramienta Nagios presenta: el estado de OK, muestra cuando los puertos o servicios que no presentan novedades, WARNING, es una alerta cuando ha superado el límite de advertencia, pero no alcanza el estado crítico, CRITICAL, es generado cuando excede el tiempo de espera, y UNKNOW, es una alerta generada cuando existe la presencia de algún error dentro de algún plugin.

Figura 21

Estado de los Servicios Monitoreados

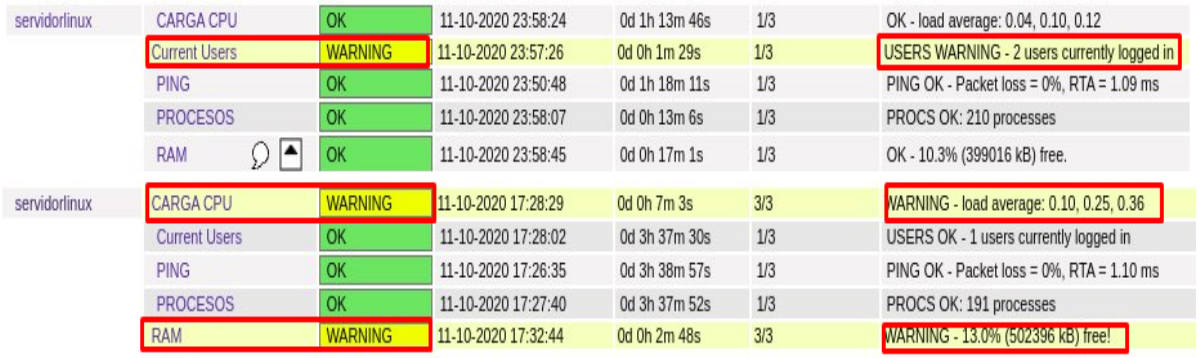


servidorlinux	CARGA CPU	OK	11-11-2020 00:00:24	0d 1h 16m 27s	1/3	OK - load average: 0.14, 0.10, 0.12
	Current Users	OK	11-11-2020 00:01:27	0d 0h 0m 9s	1/3	USERS OK - 1 users currently logged in
	PING	OK	11-11-2020 00:00:48	0d 1h 20m 52s	1/3	PING OK - Packet loss = 0%, RTA = 1.04 ms
	PROCESOS	OK	11-11-2020 00:00:07	0d 0h 15m 47s	1/3	PROCS OK: 202 processes
	RAM	OK	11-11-2020 00:00:45	0d 0h 19m 42s	1/3	OK - 8.0% (308908 kB) free.

De ahí que, para efectos de demostración y generar alertas, se realiza el cambio de los valores, referente a tres servicios, el primero corresponde al número de usuarios conectados al mismo tiempo en el servidor, el segundo servicio se ajusta los valores para la carga del procesador, y finalmente la ocupación de la memoria RAM. Los cambios realizados corresponden, por ejemplo, si existe la presencia de más de 1 usuario en el servidor, se establece parámetros de uso de memoria RAM, en el cual para que notifique una advertencia se fija el porcentaje de uso mayor al 5%, y de la carga de CPU, informe cuando su carga sea mayor al 5%, los resultados de las alertas generadas se presentan en la figura 22.

Figura 22

Alertas de los Servicios Monitoreados



servidorlinux	CARGA CPU	OK	11-10-2020 23:58:24	0d 1h 13m 46s	1/3	OK - load average: 0.04, 0.10, 0.12
	Current Users	WARNING	11-10-2020 23:57:26	0d 0h 1m 29s	1/3	USERS WARNING - 2 users currently logged in
	PING	OK	11-10-2020 23:50:48	0d 1h 18m 11s	1/3	PING OK - Packet loss = 0%, RTA = 1.09 ms
	PROCESOS	OK	11-10-2020 23:58:07	0d 0h 13m 6s	1/3	PROCS OK: 210 processes
	RAM	OK	11-10-2020 23:58:45	0d 0h 17m 1s	1/3	OK - 10.3% (399016 kB) free.
servidorlinux	CARGA CPU	WARNING	11-10-2020 17:28:29	0d 0h 7m 3s	3/3	WARNING - load average: 0.10, 0.25, 0.36
	Current Users	OK	11-10-2020 17:28:02	0d 3h 37m 30s	1/3	USERS OK - 1 users currently logged in
	PING	OK	11-10-2020 17:26:35	0d 3h 38m 57s	1/3	PING OK - Packet loss = 0%, RTA = 1.10 ms
	PROCESOS	OK	11-10-2020 17:27:40	0d 3h 37m 52s	1/3	PROCS OK: 191 processes
	RAM	WARNING	11-10-2020 17:32:44	0d 0h 2m 48s	3/3	WARNING - 13.0% (502396 kB) free!

En consecuencia, otra funcionalidad importante de Nagios es la generación de reportes mediante gráficas de barras y gráficos históricos denominados histogramas, brindando información del estado de los servicios monitoreados, en los cuales se puede observar la variación de los estados de los servicios por días y horas, en la figura 23 y 24, se presenta los reportes de variación de los servicios, con detalle de los estados y tiempos, estos reportes permiten tener información más exacta del momento en el que se ha generado alguna alerta.

Los histogramas y gráficas presentan 4 colores, el primer color es verde oscuro y representa el estado del servicio OK, seguido del color verde claro, el cual hace referencia al estado de WARNING, el tercer color correspondiente al estado UNKNOW es anaranjado, y finalmente el color rojo pertenece al estado de CRITICAL, Por ejemplo, el histograma correspondiente a la carga del CPU de la figura 23, presenta una advertencia en su pico más alto en el lapso de las 6:00 y 8:00 de la mañana llegando a presentar 7 eventos en este lapso de tiempo y un total de 4 eventos de estado crítico, por otro lado en la gráfica de Current User en la figura 24, presenta alertas los días martes, miércoles y jueves en los cuales ha estado conectado más de un usuario a la vez en el servidor Para

concluir, con estos resultados se demuestra el funcionamiento de nagios y la importancia de la monitorización de servidores y equipos en la red, ya que con este tipo de alertas se puede observar comportamientos inadecuados, los cuales pueden generar algún tipo de incidente.

Figura 23

Histograma de Estados de los Servicios Monitoreados

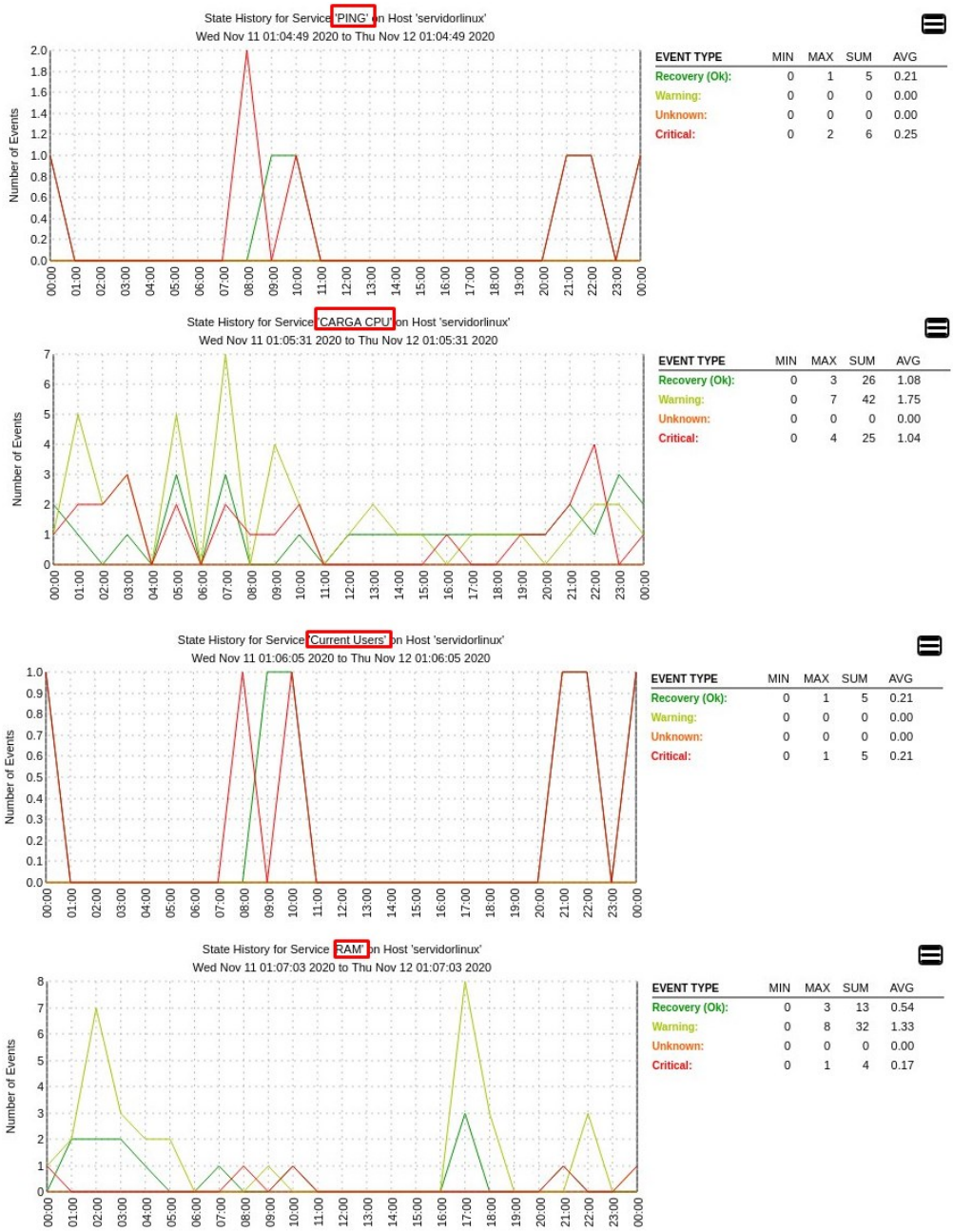
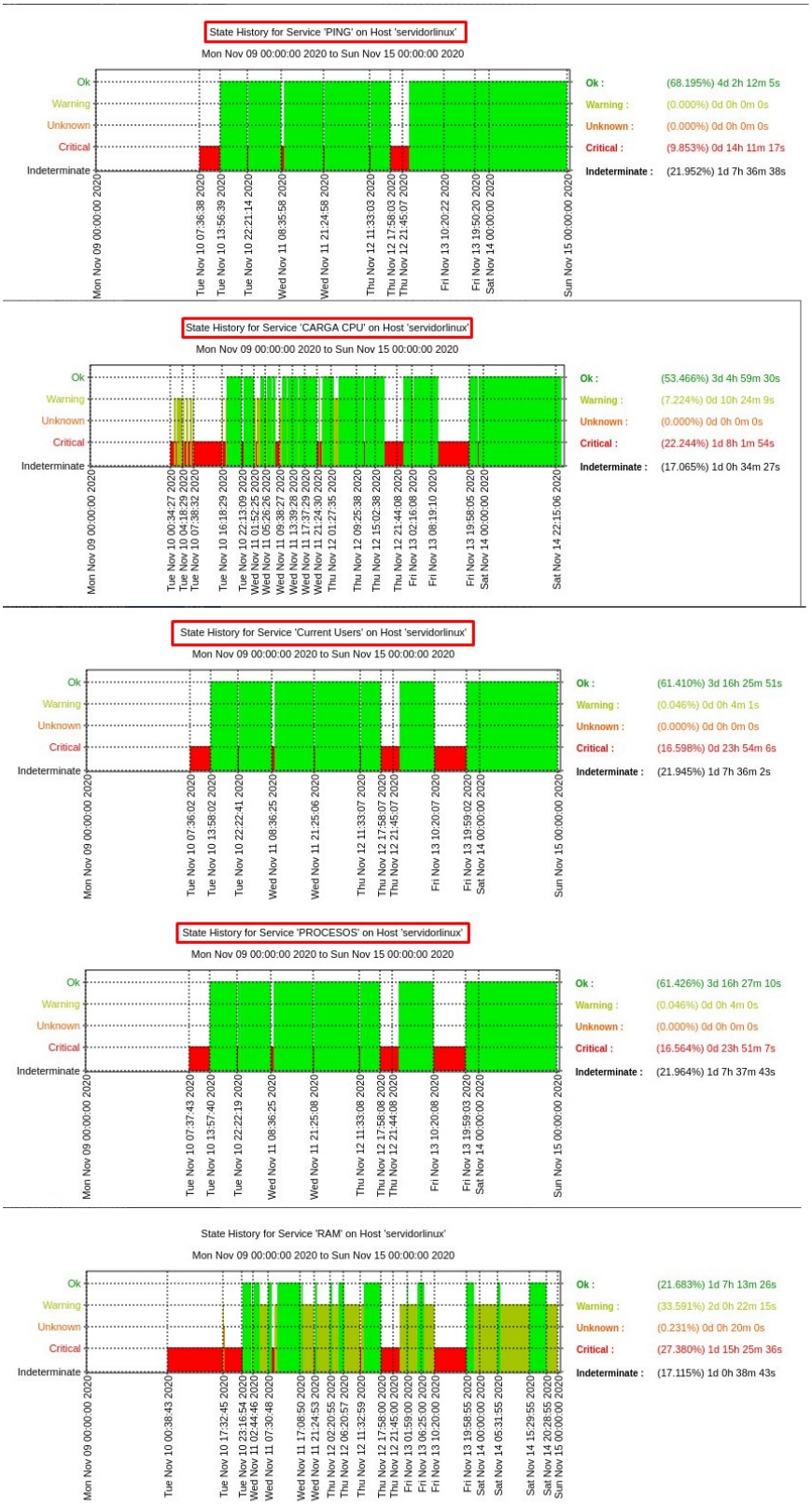


Figura 24

Reporte de Estados de los Servicios del Servidor Monitoreado



5.3 Simulación de Reporte de Incidentes Mediante OTRS

OTRS (Open-source Ticket Request System), es una herramienta de código abierto, que permite la gestión de problemas de manera ágil y eficiente, a través de tickets, ya que facilita el reporte de incidentes de seguridad de la información mediante el envío de correos electrónicos, asignando un identificador único a las solicitudes que llegan a OTRS, posibilitando el manejo y seguimiento de las solicitudes de los usuarios.

En este apartado se realiza una simulación de reporte de incidentes de seguridad de la información, por medio del envío de un correo electrónico por parte de un usuario, llegando este a la mesa de ayuda de OTRS.

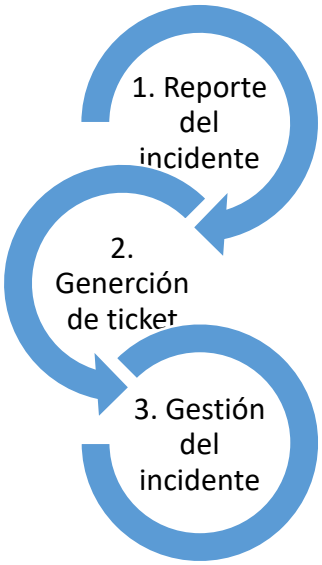
Seguidamente se genera un número de ticket a cada incidente reportado, atribuyendo una identificación a cada solicitud, con el fin de brindar una solución. En este sentido, se presenta dos casos, el primero corresponde al reporte de un incidente de seguridad de la información con un nivel bajo, pudiendo ser resuelto por el técnico de soporte de nivel 1, y en el segundo caso se realiza el reporte de un incidente con nivel de criticidad medio – alto, provocando un escalamiento del incidente desde el técnico de nivel 2 hasta el técnico de nivel 3 y finalmente se procede a cerrar el incidente de manera exitosa.

Ahora, como requerimientos básicos necesarios para que OTRS comience a gestionar las solicitudes entrantes son: la creación de un correo electrónico, el mismo que es vinculado a OTRS, y que permite reportar incidentes de seguridad de la información, seguido de esto, se procede a la creación y configuración de las colas, las cuales son el destino de los incidentes reportados al correo, las mismas que permiten clasificar los tickets; en otras palabras, las colas son casi similares a una bandeja de entrada del correo electrónico, permitiendo administrar los tickets y asignar a los agentes, quienes son los

encargados de gestionar los incidentes reportados a la mesa de ayuda, y finalmente, se procede a la configuración de las respuestas automáticas, las cuales se generan cuando un incidente es reportado a la mesa de ayuda del CSIRT, con estas configuraciones, (ver Apéndice R) la mesa de ayuda ya puede comenzar sus operaciones para brindar solución de manera rápida y ordenada a los incidentes de seguridad informática que se generen dentro de la universidad. El proceso a seguir para la gestión de incidentes mediante OTRS se presenta en la figura 25, el cual se ajusta a los procesos de gestión de incidencias.

Figura 25

Proceso de Gestión de Incidentes Informáticos con OTRS



Agregando a lo anterior, en base a la figura 25, el primer paso para la gestión de los incidentes informáticos es la detección del mismo por parte del usuario, seguidamente, el usuario lleva a cabo el reporte del incidente mediante el envío de un correo electrónico a la mesa de ayuda del CSIRT académico de la UTN, como consecuencia, OTRS genera

un ticket con un identificador único, el mismo que es enviado de manera automática al usuario que realiza el reporte.

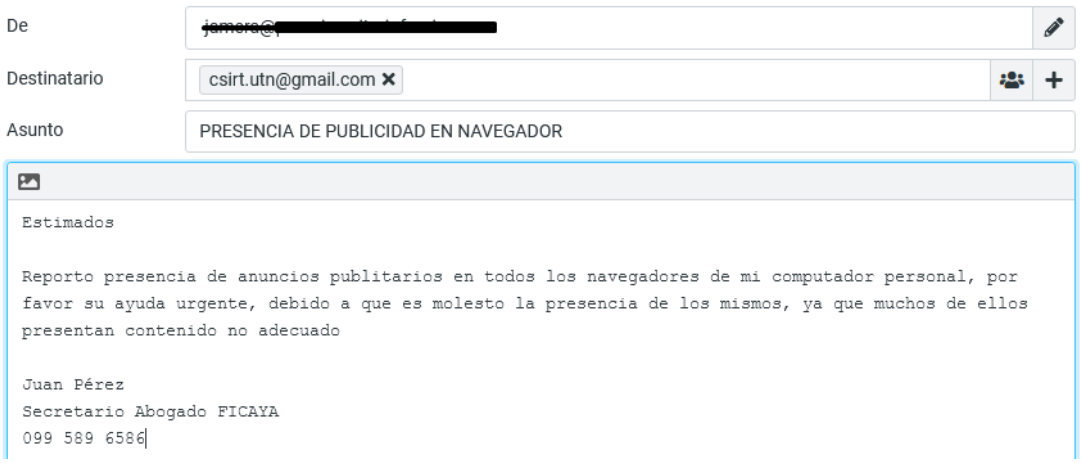
Con la generación del ticket, el técnico de soporte de nivel 1 de la mesa de ayuda, realiza la evaluación del incidente, y con el apoyo de los procesos para la gestión de incidentes, procede a analizar, y si se encuentra dentro de sus competencias brinda una solución, o caso contrario el caso es derivado o escalado a un técnico de nivel superior, según el nivel de criticidad, hasta cerrar con éxito el incidente.

5.3.1 Resultados de la Simulación (Caso 1)

En la figura 26, se presenta el reporte de un incidente por parte de un usuario del área administrativa de la UTN, procediendo a notificar mediante el envío de un correo electrónico a la mesa de ayuda, informando de la presencia de anuncios publicitarios en los navegadores.

Figura 26

Reporte de Incidente por Parte de Usuario a la Mesa de Ayuda

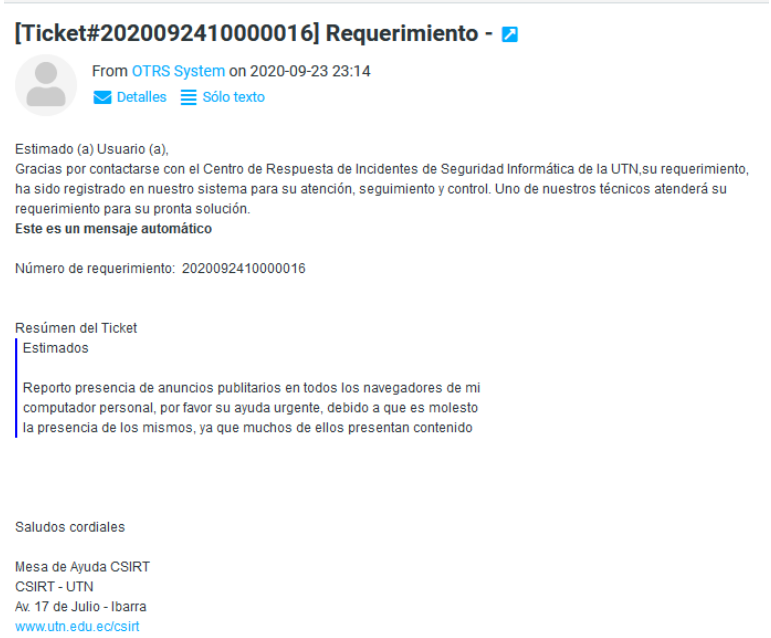


Una vez enviado el correo a la mesa de ayuda, OTRS, genera una respuesta automática, que es enviada al correo electrónico del usuario que reporta el incidente, tal como se precisa en la figura 27, el usuario recibe como respuesta un número de ticket, que sirve

para realizar seguimiento a su solicitud y un mensaje de agradecimiento y aviso de que el problema reportado será atendido.

Figura 27

Respuesta Automática con Identificador de Ticket



En consecuencia, en la figura 28 se presenta la visualización del ticket generado en OTRS, el mismo que llega a la cola del técnico de nivel 1 de la mesa de ayuda, siendo este analizado para su solución o para su respectivo escalamiento.

Figura 28

Tickets Generados en la Cola del Adminsitrador de la Mesa de Ayuda del CSIRT

Por consiguiente, en la figura 29 se observa información del incidente, como nombre de quien reporta, correo electrónico, teléfono de contacto, área afectada, fecha y descripción del incidente, de esta manera permite brindar una solución o a su vez el escalamiento al técnico de nivel superior, para este caso, el incidente reportado no presenta una amenaza crítica para el funcionamiento normal de los servicios que brinda la universidad, por lo tanto, el técnico de nivel 1 procede a brindar una solución, y finalmente procede a responder y cerrar el ticket, tal cual se exhibe en la figura 30.

Figura 29

Información del Ticket

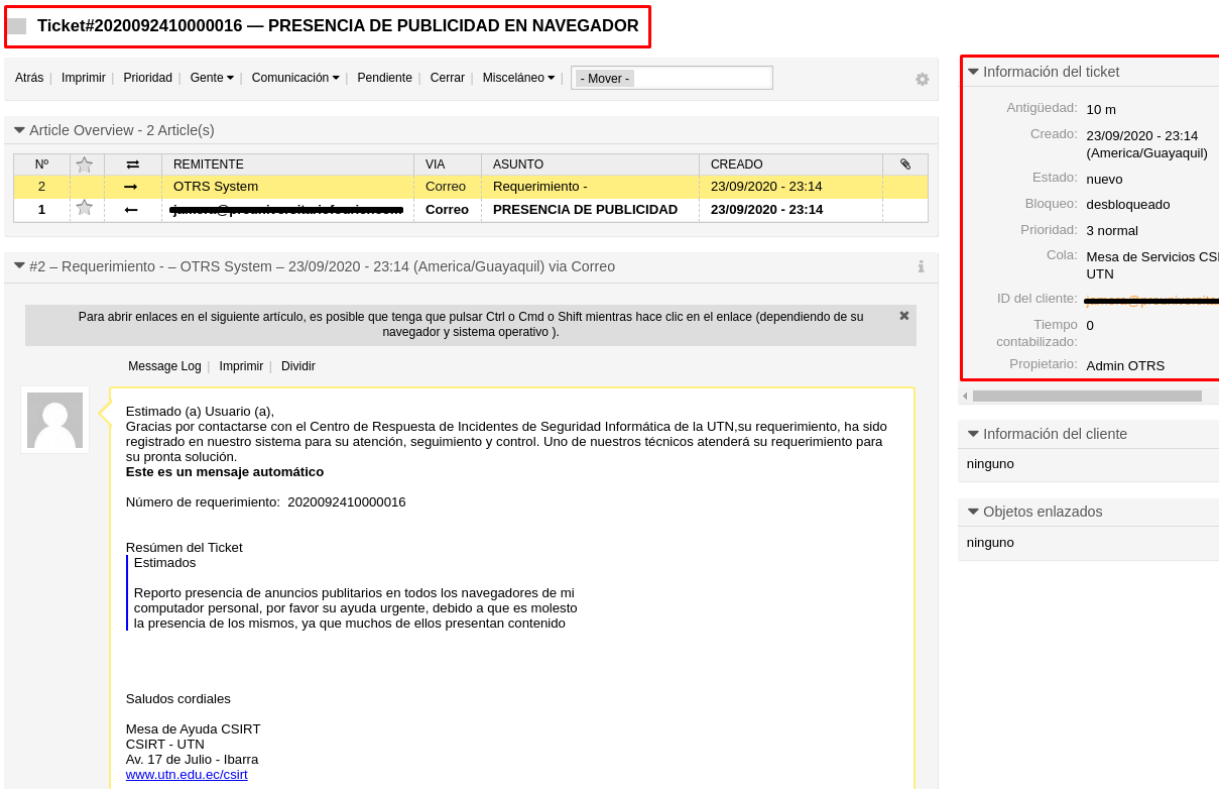
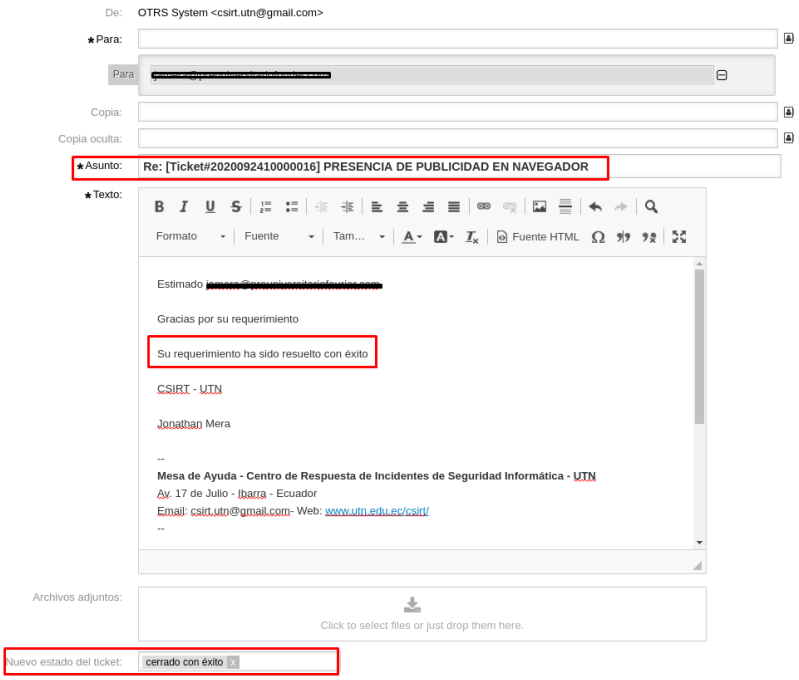


Figura 30

Respuesta y Cierre del Incidente



5.3.3 Resultados de la Simulación (Caso 2)

Ahora bien, para el segundo caso, en primer lugar, se muestra en la figura 31, el reporte del incidente mediante el envío de un correo electrónico a la mesa de ayuda por parte de un miembro del DDTI, el incidente corresponde a la saturación de la red de datos, como consecuencia presenta problemas en el servicio de correo y página web.

Figura 31

Reporte de Incidente por Parte de Usuario del DDTI

Una vez que ingresa el correo a OTRS, se genera el ticket, permitiendo al técnico de soporte de nivel 1 de la mesa de ayuda, realizar el respectivo análisis, y debido al impacto que este puede generar, procede al escalamiento del incidente a un técnico de soporte de nivel superior. En la figura 32 se indica el escalamiento del incidente al técnico de nivel 2.

Figura 32

Escalamiento de Ticket

Por consiguiente, el técnico de soporte de nivel 2 puede visualizar en la cola de su cuenta de OTRS, la asignación del ticket, por lo tanto, en la figura 33 se observa el ticket asignado en su cuenta.

Figura 33

Vista de Cola del Técnico de Soporte de Nivel 2

Sin embargo, debido a que el técnico de soporte de nivel 2 no puede brindar una solución para este incidente, el ticket es escalado al técnico de nivel 3 para su pronta

solución, en la figura 34, se presenta el escalamiento del ticket y en la figura 35 se observa la cola del técnico de nivel 3.

Figura 34

Escalamiento de Nivel para Solución de Ticket

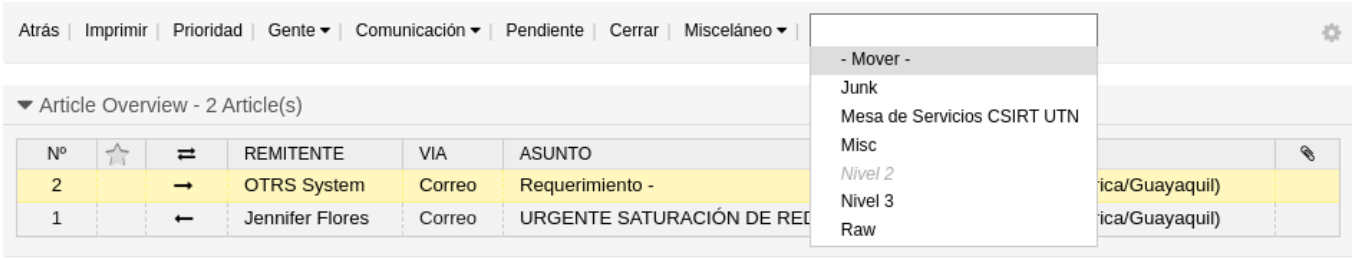
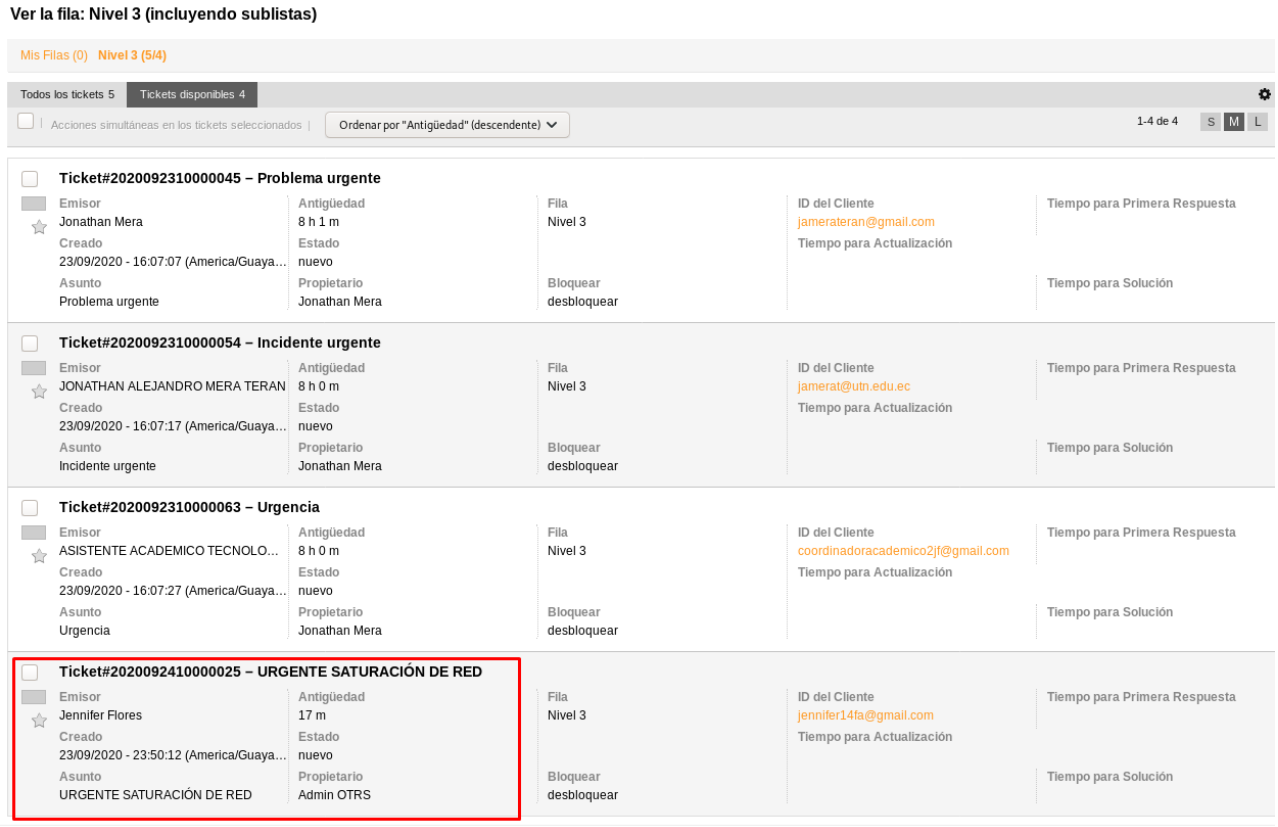


Figura 35

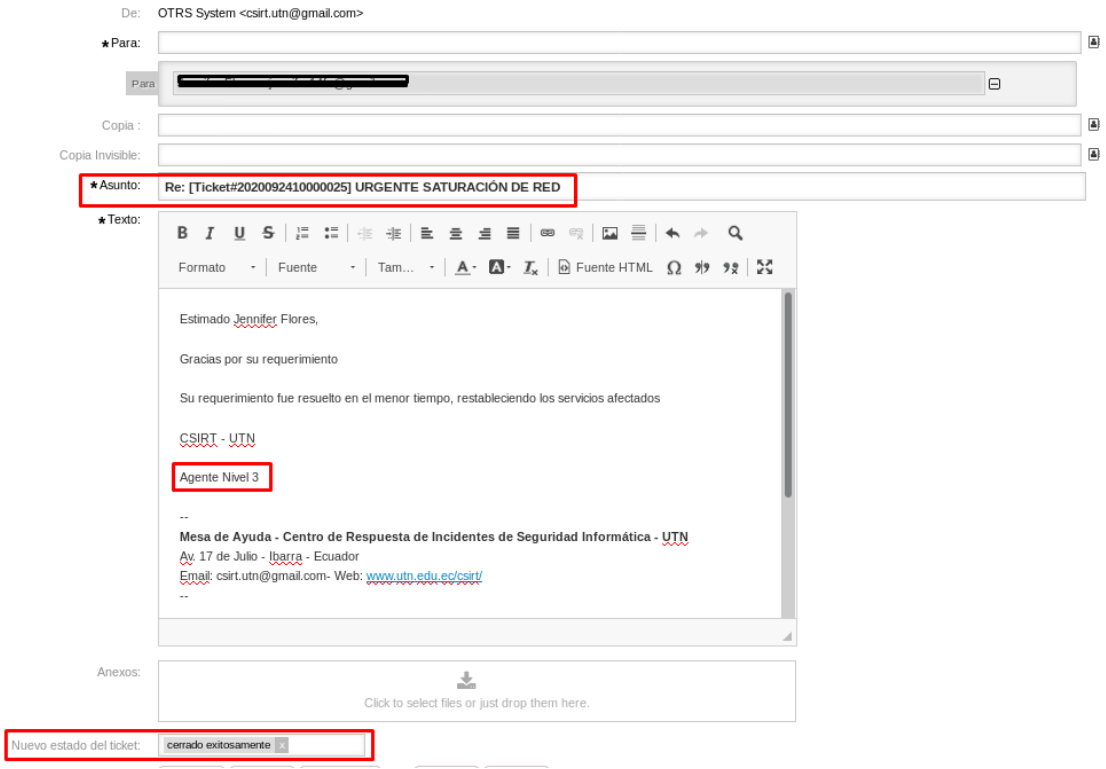
Cola del Técnico de Nivel 3



Finalmente, una vez escalado el incidente al nivel más alto, se brinda una solución al mismo, cerrando el ticket con éxito, y en la figura 36, se presenta la respuesta del ticket al usuario del DDTI.

Figura 36

Cierre de Ticket



5.4 Evaluación de Procesos de Gestión de Incidencias Informáticas con SIMPROCESS

Para la evaluación de procesos de gestión de incidentes de seguridad de la información se utiliza la herramienta denominada SIMPROCESS, que pertenece a la empresa CACI (Consolidated Analysis Center, Incorporated), y que se encarga de brindar servicios profesionales de TI (Tecnologías de Información), este software sirve para modelar, analizar y simular procesos, permitiendo mejorar los mismos.

Cabe considerar, que SIMPROCESS es una herramienta comercial, pero para efecto de las pruebas, se envió un correo solicitando una licencia de prueba gratuita, la cual fue otorgada por un lapso de 10 días, permitiendo simular y evaluar los procesos de gestión de incidentes. Es importante mencionar que los parámetros, configuraciones y simulaciones realizadas se encuentran detallados en el Apéndice S.

En este sentido, para la presente evaluación de procesos de gestión de incidentes se plantea dos escenarios, el primer escenario se evalúa los procesos de gestión de incidentes de seguridad de la información sin la presencia del CSIRT, sin software de generación de tickets, ni documentación que sirva de soporte para la gestión de los incidentes, y con dos personas que están en capacidad de solventar los incidentes reportados.

Por otra parte, el segundo escenario simulado, es evaluado con la presencia del CSIRT, la implementación de OTRS como herramienta de ayuda para la notificación de eventos, con documentación de apoyo para la resolución de incidentes informáticos y se dispone de dos técnicos del DDTI, y un experto en seguridad de la información perteneciente al CSIRT académico de la UTN.

De manera que, la simulación presenta los procesos necesarios para la resolución de gestión de incidentes de seguridad de la información, siendo el primer paso la notificación del incidente, a continuación, el técnico del helpdesk recibe la notificación y clasifica el incidente de manera adecuada, luego de clasificar el incidente, se procede a dar tratamiento según su gravedad, y una vez resuelto el incidente, se procede a cerrar el mismo, registrando la información y notificando el cierre del incidente.

Por lo cual, para los dos escenarios se tiene un total de 104 incidentes reportados en las 8 horas de la jornada laboral, dando un promedio de 13 incidentes por hora, siendo

estos incidentes distribuidos de la siguiente manera: 2 incidentes de prioridad alta, 4 de prioridad media y 7 de prioridad baja, , cabe recalcar que este número de incidentes y que se presenta en la tabla 46, son valores referenciales, ya que el DDTI no posee un registro de la cantidad de incidentes que se suscitan en la universidad.

Tabla 46

Distribución de Incidentes

Prioridad del incidente	**Número de incidentes por hora**
Prioridad alta	2
Prioridad media	4
Prioridad baja	7

De igual manera para los dos escenarios se establece tiempos en los que un incidente reportado debe ser solucionado, siendo referenciales, debido a que pueden variar dependiendo de la dificultad del incidente, estos tiempos se presentan en la tabla 47.

Tabla 47

Tiempo máximo de resolución de incidentes

Prioridad	**Tiempo de solución**
Bajo	2 horas
Medio	1 hora
Alto	30 min

5.4.1 Resultados de la Evaluación de Procesos para la Gestión de Incidentes

Una vez realizada las simulaciones respectivas, se presenta en la tabla 48, los resultados más relevantes. Para ello se realiza una comparación de los dos escenarios, en base a su prioridad (alta, media y baja) y a los incidentes que fueron atendidos satisfactoriamente e incidentes que no se brindaron solución alguna. En este sentido, de los 104 incidentes que son reportados en una jornada laboral de 8 horas, sin la presencia de un CSIRT, solo 18 incidentes son solucionados, representando el 17.3%, y con la presencia de un Centro de Respuesta de Incidentes de Seguridad Informática se brinda solución a 68 incidentes representando el 65.38%, por ende, sin la presencia del CSIRT se dejan 86 incidentes sin solución, mientras que con la presencia del CSIRT tan solo 36 incidentes quedan por resolver.

En definitiva, la presencia del CSIRT, permite brindar soluciones más eficaces a los incidentes de seguridad de la información que se presentan, debido a que la gestión de incidencias se la realiza bajo normas y estándares que permiten una mejor organización en cuanto a la gestión de incidencias, así como la presencia de la herramienta OTRS, que permite el registro de incidencias en menor tiempo.

Tabla 48 Comparación de Incidentes Solucionados vs Incidentes sin Solución

Comparación de Incidentes Solucionados vs Incidentes sin Solución

Prioridad de incidentes	**Número de incidentes reportados**	**Número de incidentes solucionados**		**Número de incidentes sin solución**	
		Escenario 1	**Escenario 2**	**Escenario 1**	**Escenario 2**
Prioridad alta	16	10	12	6	4

Prioridad media	32	8	24	24	8
Prioridad baja	56	0	32	56	24
Total	104	18	68	86	36

Por otro lado, en la tabla 49, se expone una comparativa en cuanto al porcentaje de ocupación del personal, que brinda la solución a los incidentes reportados, estos resultados obtenidos a través de los reportes de la herramienta SIMPROCESS, permiten observar que en los dos escenarios el personal pasa ocupado brindando solución a los incidentes de seguridad de la información, pero cabe destacar que sin la presencia del CSIRT y a pesar que el personal de soporte permanece casi siempre ocupado, es necesaria la optimización de los procesos de gestión de incidentes de manera urgente, ya que, no se aprovecha al máximo la utilización del personal.

Tabla 49 Porcentaje de Utilización del Personal de Soporte Técnico

Porcentaje de Utilización del Personal de Soporte Técnico

Personal de soporte	**Escenario 1**	**Escenario 2**
Help Desk (Técnico nivel 1)	100%	100%
Soporte nivel 2	94.79%	100%
Soporte nivel 3 (CSIRT)	NA	100%

CONCLUSIONES

El presente trabajo de investigación permitió cumplir con los objetivos planteados, el cual está apoyado con las mejores prácticas en cuanto a diseño de CSIRTs, normas y estándares que sirven de directrices para el planteamiento de procedimientos y políticas de gestión de incidentes y seguridad de la información, además que, con este diseño del Centro de Respuesta de Incidentes de Seguridad Informática de tipo académico en la UTN, se deja estableciendo parámetros importantes como el plan estratégico y todos los componentes del mismo, los cuales permitirán en un futuro la implementación del CSIRT-UTN. Por tanto, como conclusiones de la presente tesis se tiene las siguientes:

En primer lugar, el análisis teórico permitió conocer que un CSIRT es una organización que gestiona incidentes de seguridad de la información a una comunidad objetivo, a través de diversos servicios, preventivos, reactivos y de gestión de la calidad, apegados a métodos y herramientas que permiten mitigar los mismos. En este sentido si bien es cierto existe un gran abanico de servicios, como punto de partida es necesario la elección de servicios básicos, como por ejemplo la gestión de incidentes, concienciación, alertas y avisos de seguridad informática.

De ahí que, la gestión de incidentes, se encuentra apegada a normas, estándares y marcos de referencia existentes, y que brindan recomendaciones de buenas prácticas para la gestión de incidentes de seguridad de la información, tales como la norma ISO/IEC 27002, estándar ITIL V4, marco de referencia COBIT 2019 y la norma RFC 2350.

En consecuencia, se analizó básicamente manuales y guías de creación de CSIRTs, los cuales fueron, el manual publicado por el CERT/CC de la universidad de Carnegie Mellon, la guía publicada por ENISA y el manual de gestión de incidente de seguridad

informática del proyecto AMPARO, si bien es cierto, estos documentos permitieron una mejor comprensión para el diseño del CSIRT académico de la UTN, específicamente el documento publicado por el CERT/CC y la Universidad de Carnegie Mellon y el del proyecto AMPARO, permitieron obtener las directrices y pasos a seguir para el presente diseño.

De modo que, este último documento, es una guía que presenta información de manera completa y comprensible en aspectos como la razón de ser de un CSIRT, los tipos de CSIRT que existen, tipos de servicios, estructura organizacional, políticas del CSIRT, recomendaciones en cuanto a la infraestructura física, diferentes topologías de red y procesos para la gestión de incidentes.

Seguidamente, se realizó el análisis de la situación actual de la seguridad informática en la UTN, mediante la aplicación de encuestas, análisis de riesgos, matriz RACI y PAM, específicamente estas dos últimas apegadas a las recomendaciones de COBIT, en función del objetivo DSS02, encargado de gestionar las peticiones y los incidentes del servicio, enfocado a la solución de incidentes de seguridad de la información, de forma que en la UTN, existe la presencia de virus, Botnets, spam, phishing y realizan ataques de ingeniería social, por otro lado, en el DDTI hace falta capacitar al personal en temas de seguridad de la información, implementar políticas y procedimientos para gestionar incidentes informáticos, así como la implementación de herramientas que permitan gestionar y tratar los incidentes que se suscitan dentro de la universidad.

Por lo tanto, estos resultados dejan en evidencia la importancia de contar con un CSIRT, siendo este centro un punto único de contacto para la gestión de incidentes de seguridad de la información, apoyando al DDTI con la implementación de políticas que

permitan la gestión de incidentes informáticos, apegados a normas, estándares y marcos de referencia como ISO/IEC 27002, ITIL y COBIT, aportando con un valor agregado para la mejora de la seguridad informática dentro de la institución, permitiendo disminuir posibles incidentes que se susciten, así como la resolución de los mismos de manera ordenada y planificada.

De modo que, en base a los resultados obtenidos del análisis teórico y la situación actual de la seguridad informática de la UTN, se procedió a la definición de los requerimientos para el diseño del CSIRT académico en la UTN, definiendo primeramente la razón principal de este centro y que va enfocado a la disminución de los incidentes de seguridad de la información dentro de la UTN, mediante la prestación de servicios básicos como la gestión de incidentes, concienciación en temas de seguridad informática, alertas y advertencias, como punto de partida, y teniendo en cuenta que el principal servicio es la gestión de incidentes. Cabe resaltar que conforme el CSIRT vaya alcanzando un nivel de madurez, o en otras palabras vaya obteniendo experiencia, este puede ir incorporando más servicios.

Ahora bien, en otro aspecto, la norma ISO/IEC 27002, el estándar ITIL V4 y el marco de referencia COBIT, se encuentran estrechamente relacionados, ya que estos documentos presentan información relevante para la gestión de incidentes de seguridad de la información, permitiendo establecer procedimientos y políticas para gestionar incidentes informáticos. Por ende, la norma ISO/IEC 27002 e ITIL, permitieron establecer procesos para la gestión de eventos, problemas e incidentes.

En este sentido, específicamente la norma ISO/IEC 27002 e ITIL presentan información en cuanto a la gestión de incidentes y procedimientos a seguir para brindar

una solución, cumpliendo con los tres pilares de la seguridad de la información, disponibilidad, integridad y confidencialidad.

Así pues, COBIT, por otro lado, a más de presentar recomendaciones en cuanto a procedimientos para gestionar incidentes, sugiere buenas prácticas para la elaboración de políticas, sugiriendo el contenido que una política debe contener como el alcance, validez, consecuencias por incumplimiento, asimismo sugiere que las mismas tengan un ciclo de vida para su posterior actualización, además que toda política debe ser efectiva, eficiente y no intrusiva, desde el punto de vista que deben alcanzar el objetivo planteado, garantizar que los principios implementados sean eficientes y para quienes tengan que seguir las políticas las puedan seguir sin confusiones.

Ahora, en cuanto a las pruebas realizadas en tema de vulnerabilidades de seguridad de la información, se concluye, que la importancia de realizar este tipo de análisis permite mejorar la seguridad informática, puesto que cada día aparecen nuevas vulnerabilidades, y al realizar una auditoría, permite la corrección de las brechas que pueden aparecer con el transcurso del tiempo, sobre todo ir actualizando los sistemas operativos y cerrando puertos que no estén en uso, o a su vez brindar mayor seguridad a los puertos que están abiertos.

Igualmente es importante la presencia de herramientas que permitan reportar incidentes, de una manera centralizada, ya que ayuda a la optimización del tiempo para poder tomar decisiones acertadas, permitiendo brindar soluciones más eficientes.

Finalmente, el uso del software SIMPROCESS, como herramienta de evaluación de los procesos de gestión de incidentes, permitió observar la diferencia que existe en cuanto a la gestión que se brinda al solucionar incidentes, ya que, con la existencia de procesos,

herramientas y personal adecuados se puede brindar tratamiento de una manera más rápida y oportuna a los incidentes, disminuyendo el impacto cuando se trata de incidentes críticos, y una mejor organización al solucionar los incidentes de menor impacto, pudiendo distribuir de una manera más eficaz al personal adecuado.

RECOMENDACIONES

Para la gestión de incidencias, es recomendable poseer documentación en la que conste procedimientos para el correcto manejo de los incidentes, ya que esto permite disminuir el tiempo para la resolución de los incidentes, con esto se puede dar respuesta a un número más alto de incidentes generados en la universidad.

De modo que, se recomienda realizar una evaluación de riesgos de seguridad de la información para establecer los niveles de gravedad de los mismos y que pueden generarse dentro de la UTN, así como el establecimiento de servicios críticos dentro de la red de la institución.

Ahora bien, para el análisis de vulnerabilidades es recomendable, no solo hacer uso de la herramienta NMAP, si no utilizar otra herramienta que pueda generar reportes mucho más completos, tal es el caso de OpenVAS, esta herramienta brinda un reporte más completo de las vulnerabilidades encontradas, así como su posible solución.

Por otro lado, en cuanto a la monitorización de red con Nagios, es importante definir la parametrización de los valores de los servicios que se van a monitorizar, ya que de estos parámetros dependerá las alertas que se generen.

De manera que, se recomienda al DDTI, llevar un registro de incidentes reportados dentro de la UTN, ya que esta información será valiosa para la implementación del CSIRT-UTN, para poder contar con estadísticas sobre incidentes y poder establecer directrices que generen la disminución de incidentes recurrentes dentro de la universidad.

Finalmente, es importante que se realice un análisis de vulnerabilidades completo a los equipos de red y servidores del Data Center del DDTI y de la FICA, debido a que puede existir la presencia de vulnerabilidades, pudiendo afectar en la prestación de los servicios.

BIBLIOGRAFÍA

Ana, T. L. (Octubre de 2020). Análisis y clasificación de los ataques y sus exploits:. Málaga, España.

Andrade, & Fuertes. (2013). *Diseño y dimensionamiento de un equipo de respuesta ante incidentes de seguridad informática (CSIRT).* Sangolquí: Escuela Politécnica del Ejército.

Andrade, R. O. (2013). *Diseño y dimensionamiento de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) para la Escuela Politécnica del Ejército.* Sangolquí: ESPE. Obtenido de https://repositorio.espe.edu.ec/

Andrea Dufkiva. (05 de 2020). *FIRST.* Obtenido de https://www.first.org/membership/site-visit-v3.1.pdf

Arrogante, A. G. (s.f.). Análisis, Diseño e Implementación de una Herramienta de Gestión de Niveles de Servicio en .NET integrada con Gestión de Incidencias (OTRS): Servicios, Auditorías, SQP, SLR y OLA. Madrird, España.

atlantixlab, K. B. (09 de junio de 2015). *AtlantixLab.com*. Obtenido de http://kb.atlantixlab.com/archives/188

AXELOS. (2019). *ITIL 4 EDITION.* Obtenido de https://fliphtml5.com/ensds/cphj/basic

CACI. (2017). *SIMPROCESS.* Obtenido de SIMPROCESS: http://simprocess.com/Documentation/SPUserA.pdf

Calderón Morocho, R. E., & Cargua Cargua, L. M. (2016). ANÁLISIS DE LA HERRAMIENTA OTRS PARA LA GESTIÓN DE SOLICITUDES. Riobamba, Chimborazo, Ecuador.

Carazo, O. (2013). *Elaboración de un Plan de Seguridad de la información.* Barcelona, España: Interuniversitari en Seguretat de les TIC (MISTIC).

Carozo, E. (2010). *Manual de Gestión de Incidentes de Seguridad Informática.* Canadá: Proyecto AMPARO. Obtenido de https://docplayer.es/

Chuquiguanca, L. R. (Agosto de 2020). IMPLEMENTACIÓN DE UN EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) EN LA FISCALÍA GENERAL DEL ESTADO. Quito, Pichincha, Ecuador.

Contero Ramos, W. M. (03 de 2019). DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27002:2013, PARA EL SISTEMA DE BOTONES DE SEGURIDAD DEL MINISTERIO DEL INTERIOR. Quito, Pichincha, Ecuador.

Csirt Cedia. (15 de Noviembre de 2019). *Csirt Cedia*. Obtenido de FIRST Ecuador TC 2019: https://csirt.cedia.org.ec/

Elizabeth, T. F. (2015). IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE. Guayaquil, Guayas, Ecuador.

Ericka, Y. C. (2015). ANÁLISIS DE LAS HERRAMIENTAS PARA EL. Madrid, España.

García, Arias, Buenaño, Merizalde, & Noriega. (2013). *Análisis y solución de las vulnerabilidades de la seguridad informática y seguridad de la información de un medio de comunicación audio-visual.* Guayaquil: Universidad Politécnica Salesiana. Obtenido de https://dspace.ups.edu.ec/

Garrido, J. F. (2007). *Plan de desarrollo informático 2007-2012.* Ibarra: Departamento de informática UTN. Obtenido de http://www.utn.edu.ec/

Garzón Cruz, G. F., & Morea Vergara, K. J. (2020). IMPLEMENTACIÓN DE BUENAS PRÁCTICAS BASADAS EN ITIL 4 E ISO. Bogotá, Colombia.

Gavidia Mamani, S., & Torres Torres, L. (Abril de 2018). Implementación de los controles de la ISO/IEC 27002:2013 para la. Lima, Perú.

Gonzáles, H. V. (01 de 2016). Desarrollo de un modelo de Gestión de Servicios TI para aplicaciones de Telemedicina en el Ecuador. Quito, Pichincha, Ecuador.

Guaygua, D. E. (2018). *Importancia de los Equipos de Respuesta a Incidentes de Seguridad Informática –CSIRT, en el Ecuador.* Quito: Agencia de regulación y control de las telecomunicaciones. Obtenido de http://portal.uasb.edu.ec/

Hertzog, R., O'Gorman, J., Aharoni, M., & O'Gorman, J. (2021). Kali Linux Revealed Mastering the Penetration Testing. New York, EEUU.

Hinson, Deura, Marappan, Vergara, & Regalado. (2007). *Consejos de implantación y métricas de ISO/IEC 27001 y 27002.* Washington: Comunidad internacional de implantadores de ISO-27000. Obtenido de http://www.iso27000.es/

INGERTEC. (s.f.). *http://www.ingertec.com*. Obtenido de ISO 27001: https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/

ISACA. (3 de 01 de 2020). *COBIT 2019 Introducción y metodología*. Obtenido de Issuu: https://issuu.com/koshertechnology/docs/cobit-2019-framework-introduction-and-methodology_

Josue. (08 de 10 de 2020). *Auditech*. Obtenido de https://auditech.es/principales-diferencias-entre-analisis-de-vulnerabilidades-pentesting-y-ethical-hacking/

KNOWLEDGEHUT. (06 de 09 de 2020). *Tutorial de ITIL4.* Obtenido de https://www.knowledgehut.com/tutorials/itil4-tutorial

Lacnic. (2012). *Gestión de incidentes de seguridad informática* . México : Proyecto AMPARO.

Lanfranco y Pérez. (15 de diciembre de 2019). *CSIRTs.* Obtenido de Equipo de respuesta a incidentes de seguridad: https://www.itu.int/

Magdalena, T. N. (07 de 2015). Políticas de Seguridad de la información basado en la Norma ISO/ICE27002:2013para la Dirección de Tecnologíasde Información y Comunicación de la Universidad Técnica de Ambato. Ambato, Tungurahua, Ecuador.

Ministerio de Defensa. (2011). *Guía de Creación de un CERT/CSIRT.* Madrid: Centro Criptológico Nacional. Obtenido de https://www.ccn-cert.cni.es/

MINTEL. (2016). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. *Guía N°21*, 17-24. Obtenido de https://www.telecomunicaciones.gob.ec/

MINTEL. (12 de Junio de 2020). *Ministerio de Telecomunicaciones y de la Sociedad de la infomación*. Obtenido de MINTEL: https://www.telecomunicaciones.gob.ec/el-gobierno-nacional-emite-un-reglamento-para-la-adquisicion-de-software-en-el-sector-publico/

Muñoz y Rivas. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. *Revista lbérica de Sistemas y Tecnologías de Información*, 1-15. Obtenido de http://www.scielo.mec.pt/

OEA. (2016). *Buenas prácticas para establecer un CSIRT nacional.* Washington, D.C.: Secretaría General de la Organización de los Estados Americanos.

Padilla Martinez, E. P., & Uria Santos, R. (11 de 2019). Implementación del servicio de gestión de incidentes, empleando ITIL para mejorar el proceso de atención de servicios en una entidad financiera. Lima, Perú, Perú.

Palacios, P. (2018). *Equipo de respuesta ante incidentes de seguridad.* Ambato: UNIANDES. Obtenido de http://dspace.uniandes.edu.ec/

PCI Council. (2018). *Normas de seguridad de datos.* Washington: PCI Security Standards Council.

Radical Company. (2001). *Cybersecurity/Infrastructure.* Quito: Security Center. Obtenido de https://www.gruporadical.com/

Robayo Carvajal, K., & Castro Bayas, A. (Marzo de 2015). ESTUDIO DE FATIBILIDAD, ANÁLISI COMPARATIVO E IMPLEMENTACIÓN DE UN SISTEMA DE INCIDENCIAS (HELPDESK) PARA LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL. Guayaquil, Guayas, Ecuador.

Romero Castro, M. I., Figueroa Moràn, G. L., & Vera Navarrete, D. S. (Octubre de 2018). INTRODUCCIÓN A LA SEGURIDAD. Manta, Manabi.

Sánchez, O. L. (2016). IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA. Quito, Pichincha, Ecuador.

Sowmyashree, A., & Guruprasad, H. (2020). Evaluation and Analysis of Vulnerability Scanners: Nessus and. *International Research Journal of Engineering and Technology (IRJET)*, 6.

Tarazona, C. H. (2016). *Amenazas informáticas y seguridad de la información.* Bogotá: Seguridad de la Información, Etek Internacional. Obtenido de https://www.google.com/

Torres Núñez, E. M. (Julio de 2015). Políticas de Seguridad de la información basado en la Norma ISO/ICE27002:2013para la Dirección de Tecnologíasde Información y Comunicación de la Universidad Técnica de Ambato. Ambato, Ambato, Ecuador.

Uribe, E. F. (2014). *Proceso para la Definición de Servicios Iniciales en un Equipo de Respuesta ante Incidencias de Seguridad Informática (CSIRT).* Zacatecas: CIMAT. Obtenido de https://www.google.com/

UTPL. (17 de diciembre de 2019). *Descripción de Servicios de acuerdo a la Norma RFC 2350*. Obtenido de Norma RFC 2350: https://csirt.utpl.edu.ec/

UTPL. (24 de Enero de 2020). *CSIRT-Seguridad de la información*. Obtenido de Descripción de Servicios de acuerdo a la Norma RFC 2350: https://csirt.utpl.edu.ec/

Velasco Briones, C., & Cagua Ordoñez, G. (Enero de 2017). IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA. Guayaquil, Guayas, Ecuador.

APÉNDICE

Apéndice A Modelo de encuesta aplicada al administrador de red de la Dirección de Desarrollo Tecnológico e Informático

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CIERCOM

ENCUESTA AL ADMINISTRADOR DEL DDTI

Objetivo: Obtener información acerca de los incidentes de seguridad informática que se han presentado en el sistema de red y datos de la UTN, así como los mecanismos utilizados para prevenir y mitigar las incidencias

DATOS INFORMATIVOS

NOMBRE: _____

CUESTIONARIO

1. **Describa cuatro causas para que exista la presencia de incidencias en la red de la UTN**

   _____
   _____
   _____
   _____

2. **¿Cuáles son los procedimientos realizados para el análisis de incidencias en la red de la UTN? Describa tres procesos**

   _____
   _____
   _____

3. **Enumere los parámetros, normas y estándares utilizados por el DDTI, para realizar el manejo de incidencias de seguridad informática en la UTN**

   _____
   _____
   _____

4. **¿Cuáles son los procedimientos de seguridad ejecutados durante un ataque al sistema de red? Describa los más importantes**

   _____
   _____
   _____

5. **¿Se ejecuta escaneo de vulnerabilidades para detectar fallos en los sistemas de seguridad?**

   ☐ SI
   ☐ NO

6. **¿Se manejan reportes de incidentes de usuarios?**

   ☐ SI
   ☐ NO

7. De las siguientes incidencias, ¿Cuáles son las que con más frecuencia afectaron a la red de la UTN en el último año?

Incidencia	Frecuencia Alto=A, Medio=M, Bajo=B	Impacto Alto=A, Medio=M, Bajo=B
Virus	A	A
Malware	B	B
Spam	M	B
Ataque de Denegación de Servicios	B	A
Phishing	M	B
Adware		
Botnets	A	A
Rogue		
Spyware		
Troyanos	B	M
Spoofing	B	B
Ataques de fuerza bruta	B	B
Ataques de Ingeniería Social	M	M
Hackers	B	B
Crackers	M	A

8. Los incidentes de seguridad informática ¿A quién son reportados?

   _____

9. ¿Cuáles son los errores y fallas cometidas, para que existan incidencias y vulnerabilidades que afecten a la red de la UTN? Enumere tres errores y fallas

   _____
   _____
   _____

10. ¿Actualmente se utilizan políticas de gestión de incidencias de seguridad informática para la gestión de incidencias? Si su respuesta es afirmativa, indique cuáles son las políticas

☐ SI
☐ NO

_____
_____
_____

11. ¿Cuáles son las herramientas de seguridad informática utilizadas para detectar incidencias?

Herramientas	Frecuencia de uso Alto=A, Medio=M, Bajo=B	Nivel de eficiencia Alto=A, Medio=M, Bajo=B
Detección y rastreo de intrusiones		
Análisis forense informático		
Pentesting		
Herramientas de Hacking ético	M	A
Antivirus	A	A
Firewall	A	B

12. ¿Realiza procedimientos de respaldo de datos de los servidores?

☐ SI
☐ NO

13. ¿En el DDTI, existe un área o unidad que se encargue de la prevención, análisis y respuesta de incidentes de seguridad informática que suceden en los servidores de la UTN?

☐ SI
☐ NO

14. ¿Estaría de acuerdo que el DDTI, trabaje conjuntamente con un CSIRT, para mejorar la gestión y respuesta a incidencias, con el fin de recuperar en el menor tiempo posible los sistemas afectados y mitigar los riesgos en los principales servidores de la UTN?

☐ SI
☐ NO

Apéndice B Modelo de encuesta aplicada al administrador de red del Dirección de Desarrollo Tecnológico e Informático

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CIERCOM

ENCUESTA AL PERSONAL DOCENTE, ADMINISTRATIVO Y ESTUDIANTES

Objetivo: Conocer acerca de la gestión de incidentes en la UTN

DATOS INFORMATIVOS

NOMBRE: _____

Seleccione una opción

- ☐ DOCENTE
- ☐ ADMINISTRATIVO
- ☐ ESTUDIANTE

¿A qué facultad Ud. pertenece?

- ☐ FICA
- ☐ FICAYA
- ☐ FECYT
- ☐ FCCSS
- ☐ FACAE

CUESTIONARIO

1. **¿Conoce o ha escuchado acerca de un Centro de Respuesta de Incidentes de Seguridad Informática?**

   - ☐ SI
   - ☐ NO

   ¿En caso de ser afirmativa su respuesta, qué conoce acerca de un CSIRT?

   _____

2. **¿Ha recibido usted, jornadas de formación, educación y sensibilización acerca de la gestión de incidencias de seguridad informática por parte de la UTN?**

   - ☐ SI
   - ☐ NO

3. **Conoce usted las incidencias informáticas que en los últimos tres años han atacado al sistema informático en la UTN**

   - ☐ SI
   - ☐ NO

   Si su respuesta es afirmativa, del listado señale las incidencias informáticas que Ud. conoce que ha tenido la UTN

   - ☐ VIRUS
   - ☐ MALWARE
   - ☐ SPAM
   - ☐ ATAQUES DE DENEGACION DE SERVICIOS
   - ☐ PISHING
   - ☐ ADWARE
   - ☐ CRACKERS
   - ☐ BOTNETS
   - ☐ SPYWARE
   - ☐ TROYANOS
   - ☐ ATAQUES DE FUERZA BRUTA
   - ☐ INGENIERIA SOCIAL
   - ☐ HACKERS

4. **Del siguiente listado seleccione los problemas o daños que han ocasionado los incidentes de seguridad informática en su área de trabajo**

   - ☐ FALLA DE COMPUTADORES Y EQUIPOS
   - ☐ BLOQUEO DE CONTRASEÑA
   - ☐ ROBO O PERDIDA DE INFORMACIÓN
   - ☐ PERDIDA DE CONFIDENCIALIDAD
   - ☐ BLOQUEOS DE INTERNET
   - ☐ FUGA DE INFORMACIÓN
   - ☐ ALTERACIÓN DE LA INFORMACIÓN
   - ☐ ACCESOS NO AUTORIZADOS A LA INFORMACIÓN EN EQUIPOS Y COMPUTADORES
   - ☐ ROBO DE IDENTIDADES
   - ☐ SATURACIÓN EN LA RED
   - ☐ DESCONOCE

5. **¿Qué tipo de software usted utiliza para mejorar la seguridad informática en sus equipos? Seleccione los más importantes**

   - ☐ Software de hacking ético
   - ☐ Antivirus
   - ☐ Antimalware
   - ☐ Firewall
   - ☐ Desconoce

6. **¿Cree usted necesario la creación de un Equipo de Respuesta de Incidentes de Seguridad Informática?**

   - ☐ SI
   - ☐ NO

Apéndice C Resultados de encuesta aplicada al administrador de red de la Dirección de Desarrollo Tecnológico e Informático

1. **Describa cuatro causas para que exista la presencia de incidencias en la red de la UTN**

   - Navegación en páginas sospechosas
   - Descargas indebidas
   - Computadores infectados de malware, virus, etc.

2. **¿Cuáles son los procedimientos realizados para el análisis de incidencias en la red de la UTN? Describa tres procesos**

   - Detectar el origen y destino del ataque
   - Bloquear en el Firewall el origen
   - Reportar al destinatario del dispositivo, o bloqueo en el Firewall

3. **Enumere los parámetros, normas y estándares utilizados por el DDTI, para realizar el manejo de incidencias de seguridad informática en la UTN**

   El DDTI, no utiliza ningún tipo de norma o estándar

4. **¿Cuáles son los procedimientos de seguridad ejecutados durante un ataque al sistema de red? Describa los más importantes**

   No se tiene un debido procedimiento para ejecutarlos

5. **¿Se ejecuta escaneo de vulnerabilidades para detectar fallos en los sistemas de seguridad?**
   - ✓ SI
6. **¿Se manejan reportes de incidentes de usuarios?**

   - NO

7. **De las siguientes incidencias, ¿Cuáles son las que con más frecuencia afectaron a la red de la UTN en el último año?**

Tabla C1 Frecuencia de Incidencias que Afectaron a la Red de la UTN

Frecuencia de Incidencias que Afectaron a la Red de la UTN

Incidencia	**Frecuencia Alto=A, Medio=M, Bajo=B**	**Impacto Alto=A, Medio=M, Bajo=B**
Virus	A	A
Malware	B	B
Spam	M	B
Ataque de Denegación de Servicios	B	A
Phishing	M	B
Adware Botnets Rogue Spyware	A	A
Troyanos	B	M
Spoofing	B	B
Ataques de fuerza bruta	B	B
Ataques de Ingeniería Social	M	M
Hackers	B	B
Crackers	M	A

8. **Los incidentes de seguridad informática ¿A quién son reportados?**

   Al DDTI, específicamente al área de Redes y Comunicaciones

9. **¿Cuáles son los errores y fallas cometidas, para que existan incidencias y vulnerabilidades que afecten a la red de la UTN? Enumere tres errores y fallas**

   - Falta de actualización de antivirus
   - Manipulación de usuario final en punto de red (flapping)
   - Parte eléctrica, no abastece el generador, se apaga el D.C, el UPS dura 20 min

10. **¿Actualmente se utilizan políticas de gestión de incidencias de seguridad informática para la gestión de incidencias? Si su respuesta es afirmativa, indique cuáles son las políticas**

    ✓ NO

11. **¿Cuáles son las herramientas de seguridad informática utilizadas para detectar incidencias?**

Tabla C2 Herramientas de seguridad informática para detección de incidentes

Herramientas de seguridad informática para detección de incidentes

Herramientas	**Frecuencia de uso Alto=A, Medio=M, Bajo=B**	**Nivel de eficiencia Alto=A, Medio=M, Bajo=B**
Detección y rastreo de intrusiones		
Análisis forense informático		
Pentesting		

Herramientas de Hacking ético	M	A
Antivirus	A	A
Firewall	A	B

12. ¿Realiza procedimientos de respaldo de datos de los servidores?

- ✓ NO

13. ¿En el DDTI, existe un área o unidad que se encargue de la prevención, análisis y respuesta de incidentes de seguridad informática que suceden en los servidores de la UTN?

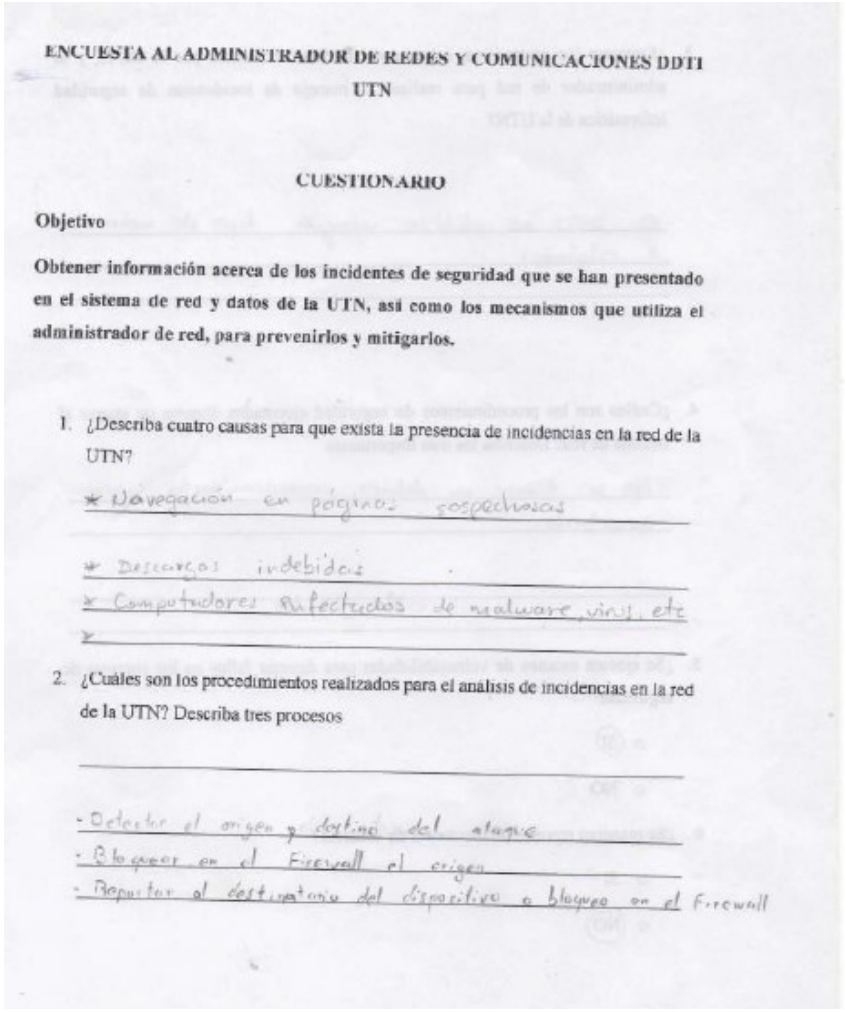
- ✓ NO

14. ¿Estaría de acuerdo que el DDTI, trabaje conjuntamente con un CSIRT, para mejorar la gestión y respuesta a incidencias, con el fin de recuperar en el menor tiempo posible los sistemas afectados y mitigar los riesgos en los principales servidores de la UTN?

- ✓ SI

Actualmente, se trabaja con CSIRT de CEDIA, y los principales servidores de la UTN, se encuentran en el CLOUD de ORACLE

Apéndice D Evidencia de Aplicación de la Encuesta Aplicada al Administrador de Red de la Dirección de Desarrollo Tecnológico e Informático



ENCUESTA AL ADMINISTRADOR DE REDES Y COMUNICACIONES DDTI UTN

CUESTIONARIO

Objetivo

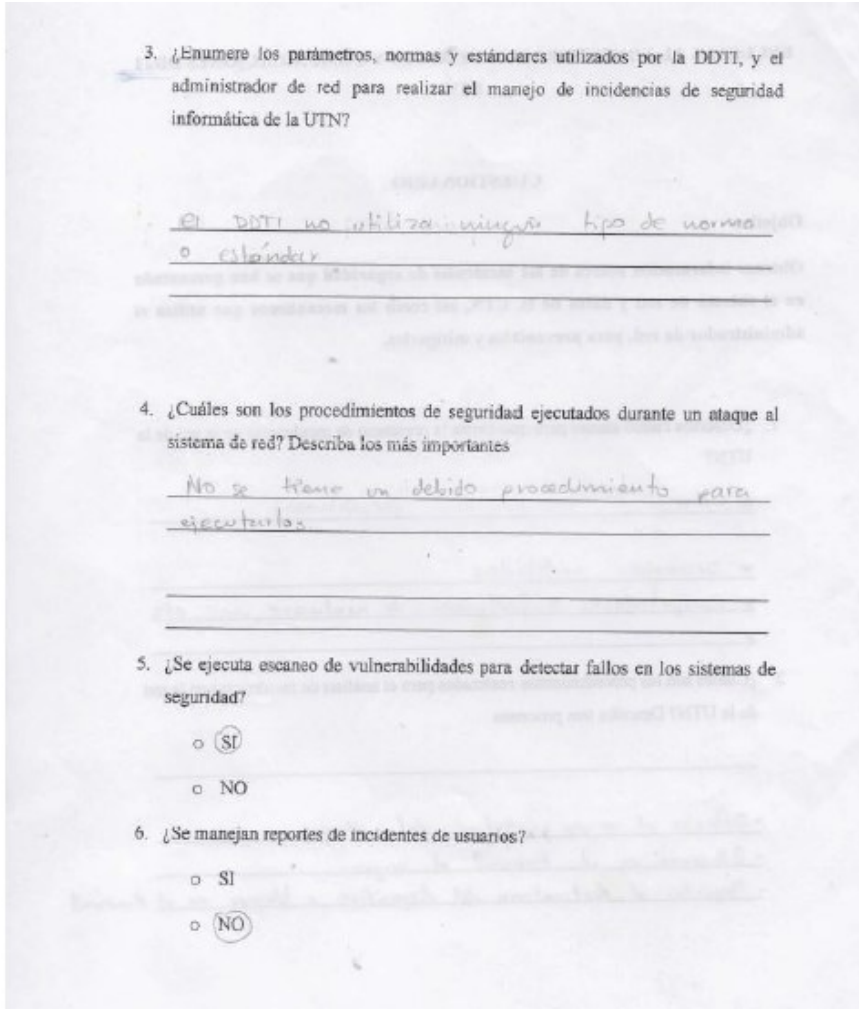
Obtener información acerca de los incidentes de seguridad que se han presentado en el sistema de red y datos de la UTN, así como los mecanismos que utiliza el administrador de red, para prevenirlos y mitigarlos.

1. ¿Describa cuatro causas para que exista la presencia de incidencias en la red de la UTN?

* Navegación en páginas sospechosas
* Descargas indebidas
* Computadores infectados de malware, virus, etc
*

2. ¿Cuáles son los procedimientos realizados para el análisis de incidencias en la red de la UTN? Describa tres procesos

- Detectar el origen y destino del ataque
- Bloquear en el Firewall el origen
- Reportar al destinatario del dispositivo o bloqueo en el Firewall



3. ¿Enumere los parámetros, normas y estándares utilizados por la DDTI, y el administrador de red para realizar el manejo de incidencias de seguridad informática de la UTN?

El DDTI no utiliza ninguna tipo de norma o estándar

4. ¿Cuáles son los procedimientos de seguridad ejecutados durante un ataque al sistema de red? Describa los más importantes

No se tiene un debido procedimiento para ejecutarlos

5. ¿Se ejecuta escaneo de vulnerabilidades para detectar fallos en los sistemas de seguridad?

- (SI)
- NO

6. ¿Se manejan reportes de incidentes de usuarios?

- SI
- (NO)

7. ¿De las siguientes incidencias, cuáles son las que con mas frecuencia afectaron a la red de la UTN en el último año?

INCIDENCIA	FRECUENCIA Alto=A, Medio=M, Bajo= B	IMPACTO Alto=A, Medio=M, Bajo= B
Virus	A	A
Malware	B	B
Spam	M	B
Ataque de denegación de servicios	B	A
Pishing Phishing	M	B
Adware	-	-
Botnets	A	A
Rogue	-	-
Spyware	-	-
Troyanos	B	M
Spoofing	B	B
Ataques de fuerza bruta	B	B
Ataques de ingeniería social	M	M
Hackers	B	B
Crackers	M	A

8. ¿Los incidentes que ocurren en las redes a quienes son reportados?

Al DDTI especificamente al área de Redes y Comunicaciones

9. ¿Cuáles son los errores y fallas cometidas, para que existan incidencias y vulnerabilidades que afecten al sistema de seguridad informática? Enumere tres errores y tres fallas (o a la red?)

- Falta Actualización de Antivirus
- Manipulación de usuario final en puntos de red (con el swd [illegible] flapping
- Poste eléctrico, no arranca el generador se apaga el D.C (20 min UPS)

10. Actualmente se utilizan políticas de gestión de incidencias de seguridad informática para la gestión de incidencias.?. ¿Si su respuesta es afirmativa indique cuales son estas politicas?

- SI
- (NO)

11. ¿Cuáles son las herramientas de seguridad utilizadas para detectar incidencias?

HERRAMIENTAS	FRECUENCIA DE USO Alto=A, Medio=M, Bajo= B	NIVEL DE EFICIENCIA Alto=A, Medio=M, Bajo= B
Detección y rastreo de intrusiones	-	-
Análisis forense informático	-	-
Test de penetración	-	-

Herramientas de Hacking ético	M	A
Software antivirus	A	A
Firewall	A	B

12. ¿Usted realiza procedimientos de respaldo de datos de los servidores?

- SI
- NO

13. ¿En el DDTI existe un área o unidad que se encargue de la prevención, análisis y respuesta de incidentes de seguridad informática que se suceden en los servidores de la UTN?

- SI
- NO

14. ¿Estaría de acuerdo que el DDTI trabaje conjuntamente con un CSIRT para mejorar la gestión y respuesta a incidencias con el fin de recuperar en el menor tiempo posible los sistemas afectados y mitigar los riesgos en los principales servidores de la UTN?

- SI
- NO

Actualmente también se trabaja con CSIRT de CEDIA, y los principales servidores de la UTN se encuentran alojados en el cloud de ORACLE

Apéndice E Resultados de encuesta aplicada al personal docente, administrativo y estudiantes

1. **¿Conoce o ha escuchado acerca de un Centro de Respuesta de Incidentes de Seguridad Informática?**

Figura E1

Resultados P1 Docentes y Personal Administrativo

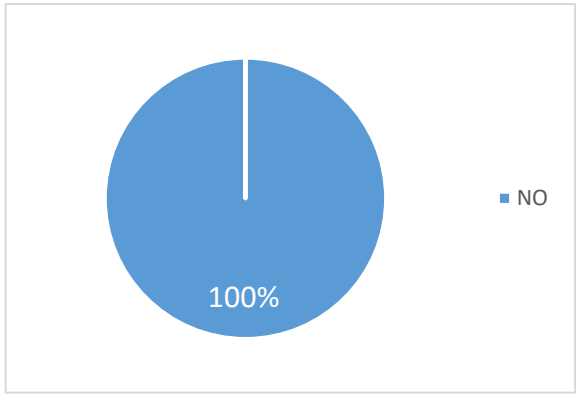
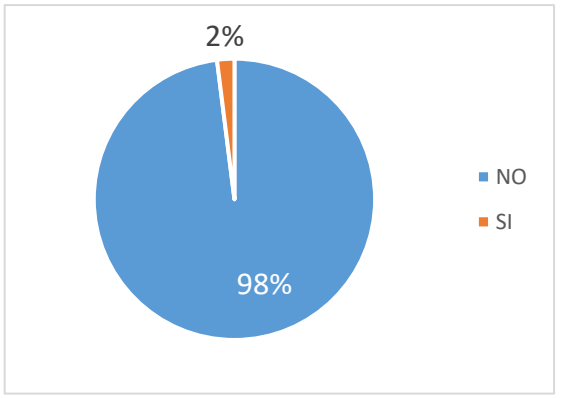


Figura E2

Resultados P1 encuesta a Estudiantes



¿En caso de ser afirmativa su respuesta, qué conoce acerca de un CSIRT?

- Brinda ayuda informática sobre un dispositivo
- Es un sistema que permite la ayuda con la protección de las plataformas
- Que ayudan a mantener seguro nuestro equipo

2. **¿Ha recibido usted, jornadas de formación, educación y sensibilización acerca de la gestión de incidencias de seguridad informática por parte de la UTN?**

Figura E3

Resultados P2 Docentes

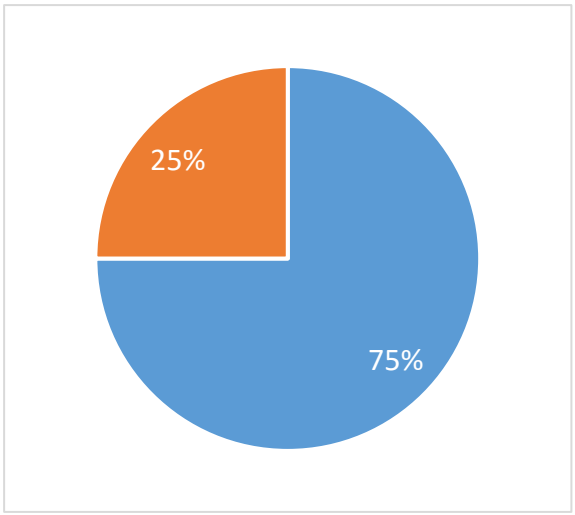


Figura E4

Resultados P2 personal Administrativo

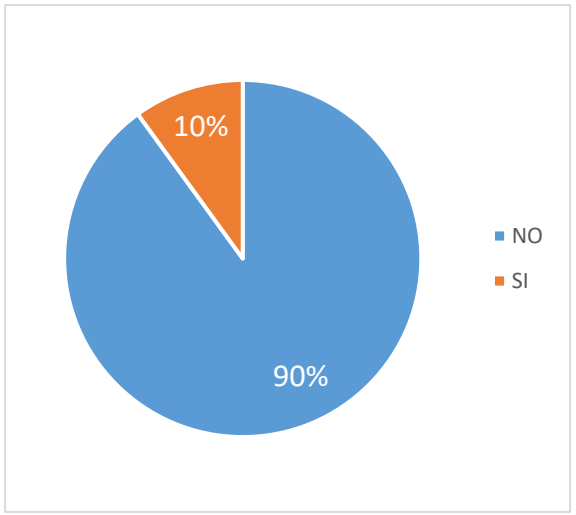
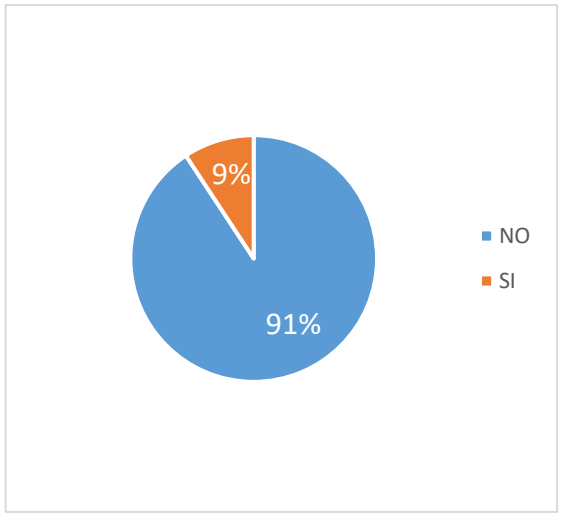


Figura E5

Resultados P2 Estudiantes



3. Conoce usted las incidencias informáticas que en los últimos tres años han atacado al sistema informático en la UTN

Figura E6

Resultados P3 Docentes

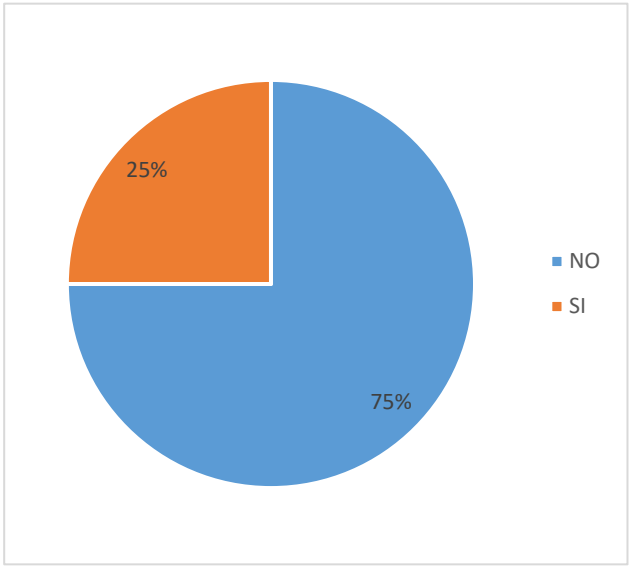


Figura E7

Resultados P3 Personal Administrativo

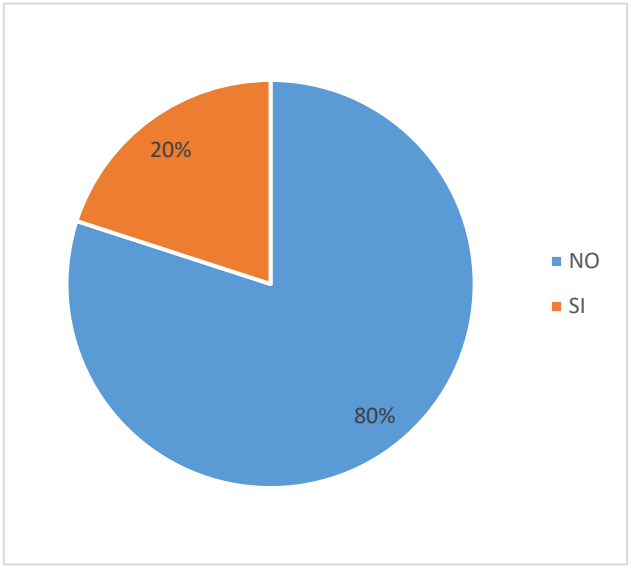
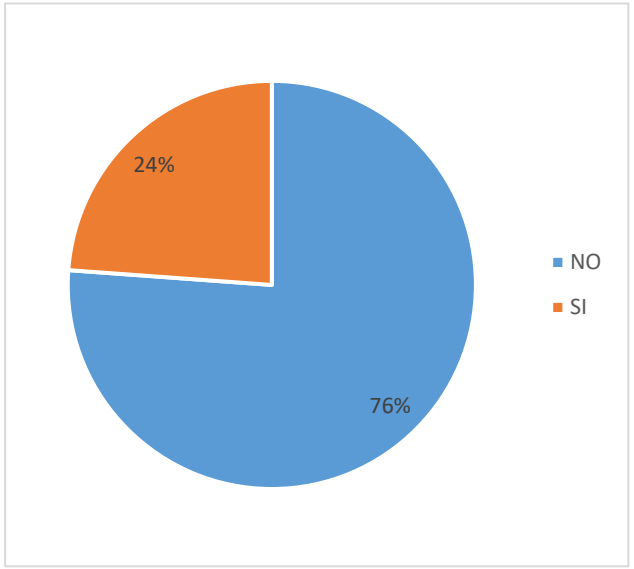


Figura E8

Resultados P3 Estudiantes



Si su respuesta es afirmativa, del listado señale las incidencias informáticas que Ud. conoce que ha tenido la UTN (1)

Figura E9

Resultados P3.1 Docentes

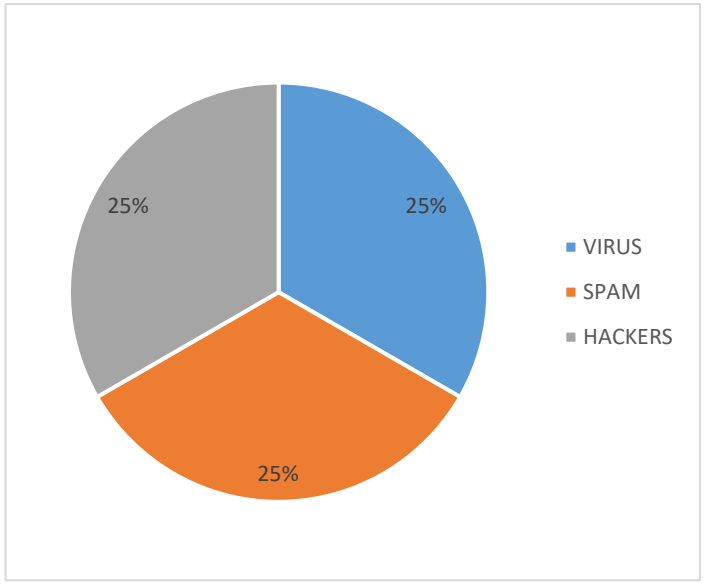
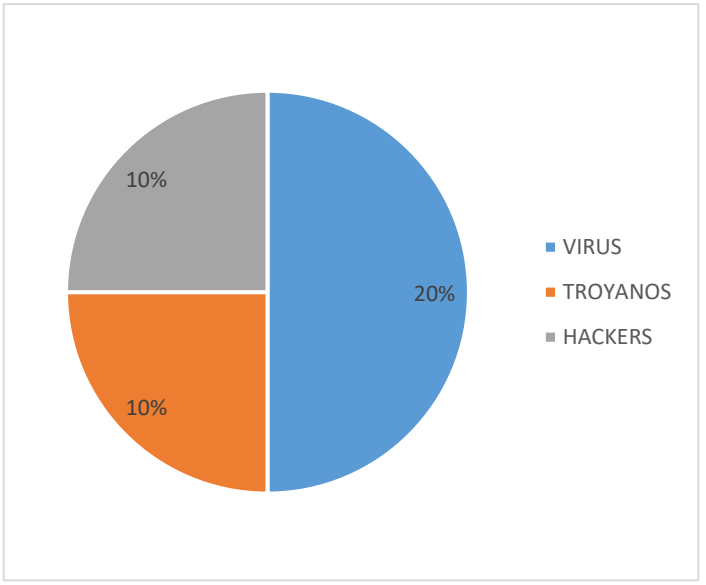


Figura E10

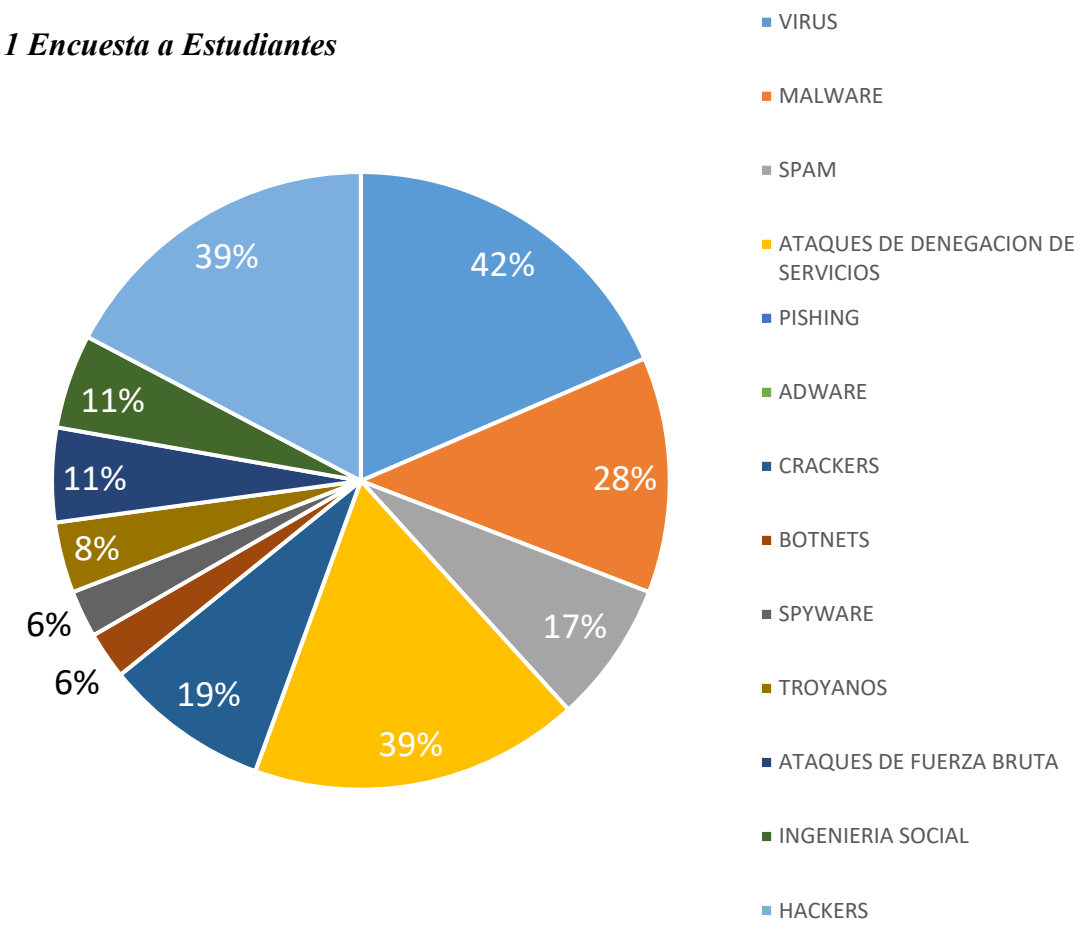
Resultados P3.1 Personal Administrativo



Si su respuesta es afirmativa, del listado señale las incidencias informáticas que Ud. conoce que ha tenido la UTN (2)

Figura E11

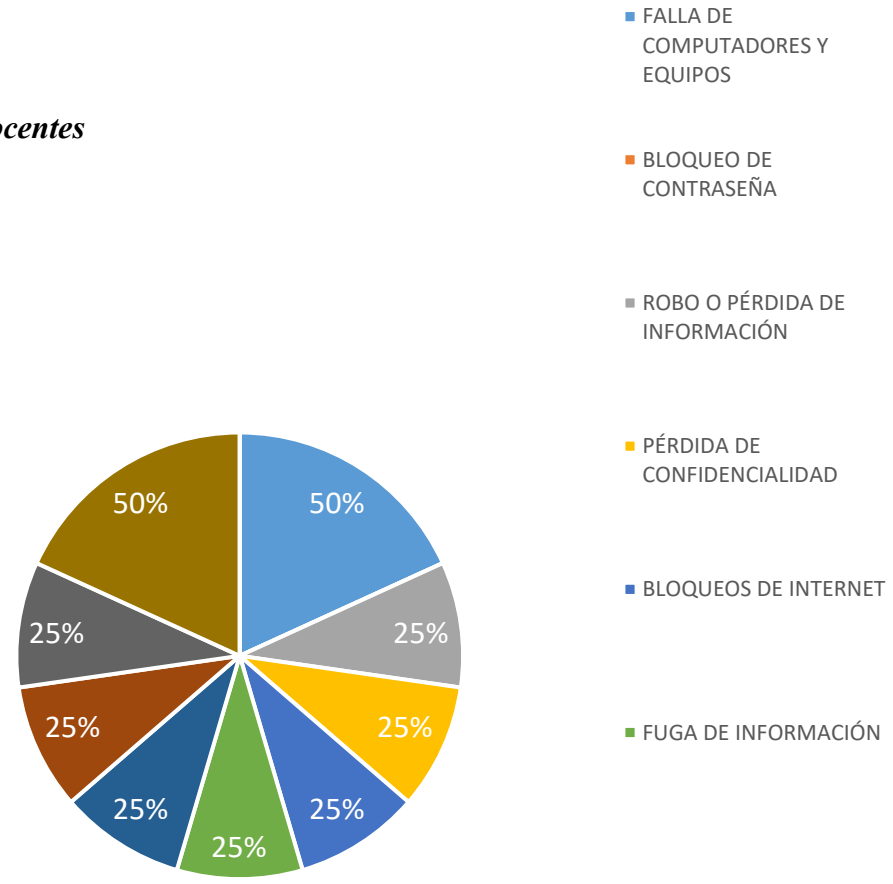
Resultados P3.1 Encuesta a Estudiantes



4. Del siguiente listado seleccione los problemas o daños que han ocasionado los incidentes de seguridad informática en su área de trabajo (1)

Figura E12

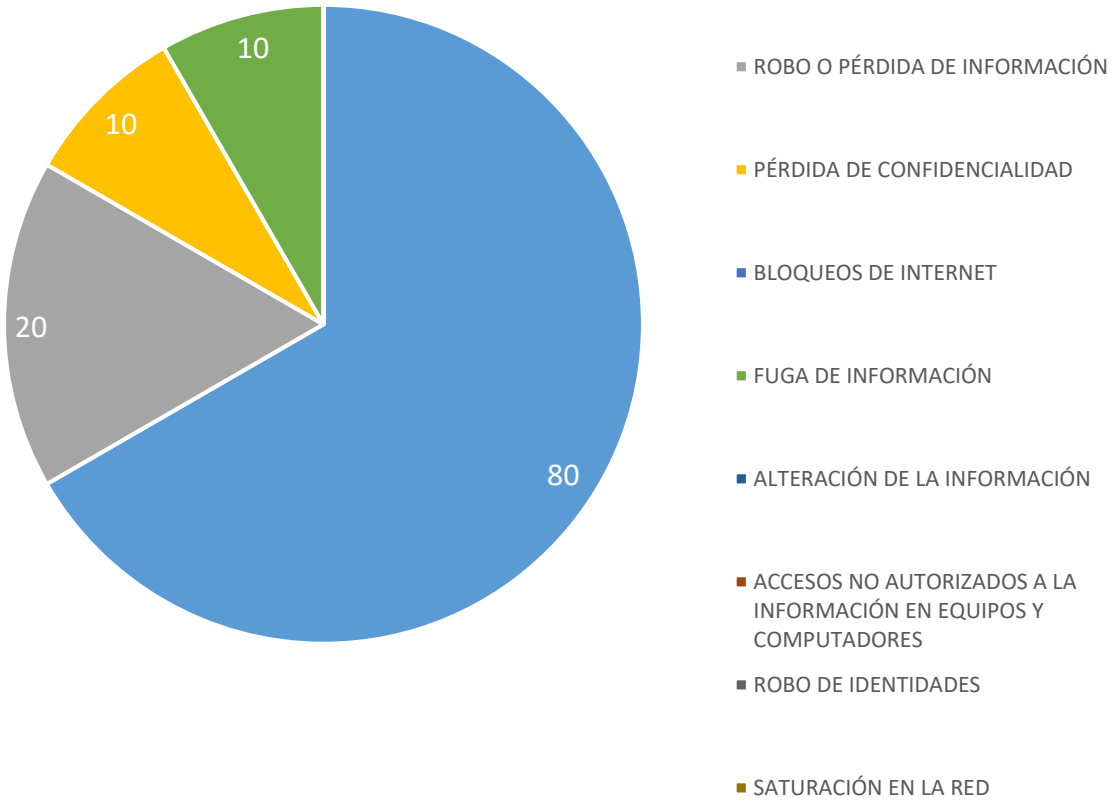
Resultados P3 Docentes



4. El siguiente listado seleccione los problemas o daños que han ocasionado los incidentes de seguridad informática en su área de trabajo (2)

Figura E13

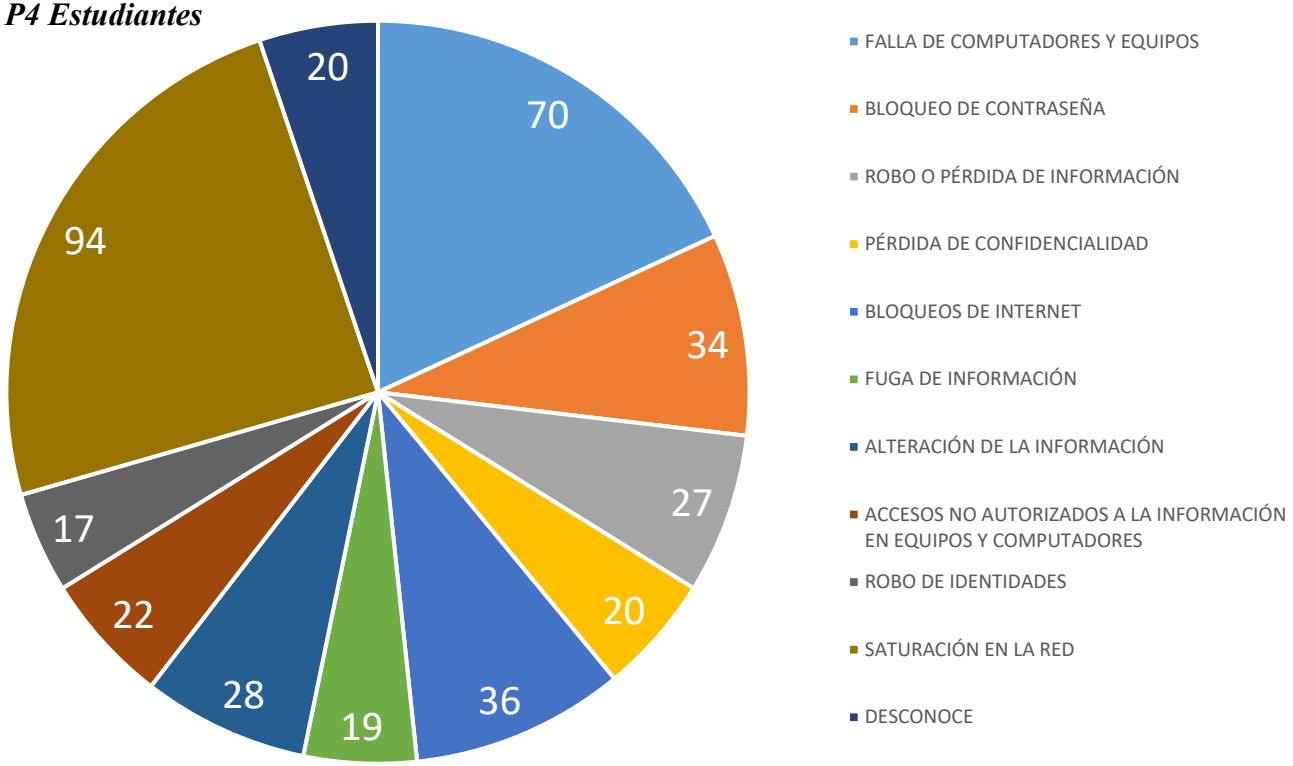
Resultados P4 Personal Administrativo



4. **Del siguiente listado seleccione los problemas o daños que han ocasionado los incidentes de seguridad informática en su área de trabajo (3)**

Figura E14

Resultados P4 Estudiantes



5. ¿Qué tipo de software usted utiliza para mejorar la seguridad informática en sus equipos? Seleccione los más importantes (1)

Figura E15

Resultados P5 Docentes

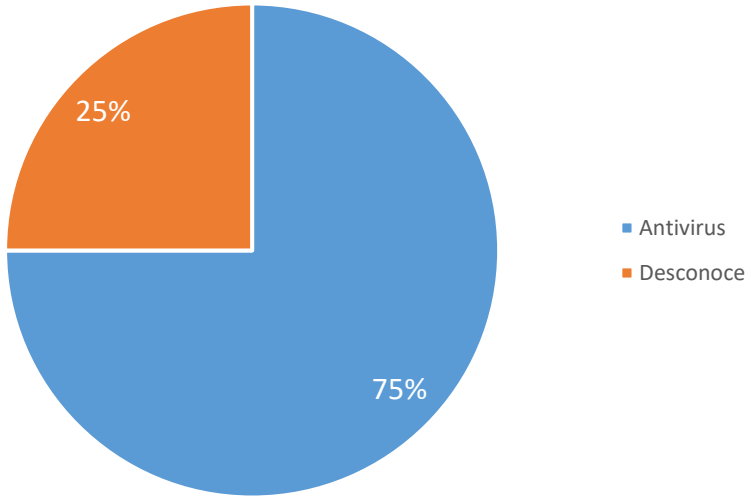
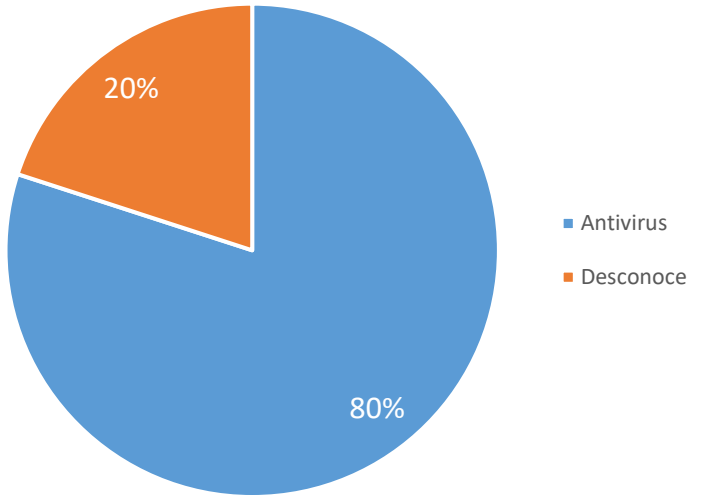


Figura E16

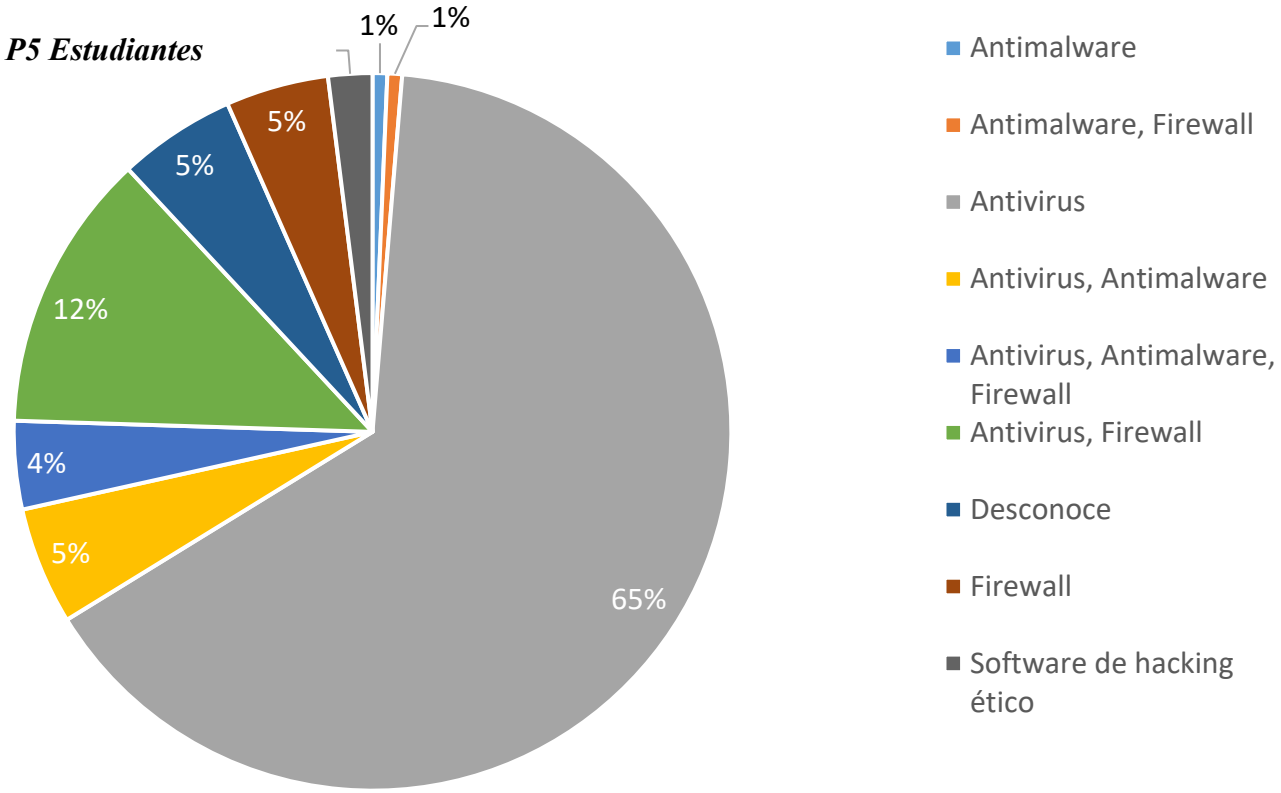
Resultados P5 Personal Administrativo



5. ¿Qué tipo de software usted utiliza para mejorar la seguridad informática en sus equipos? Seleccione los más importantes (2)

Figura E17

Resultados P5 Estudiantes



6. ¿Cree usted necesario la creación de un Equipo de Respuesta de Incidentes de Seguridad Informática?

Figura E18

Resultados P6 Docentes y personal Administrativo

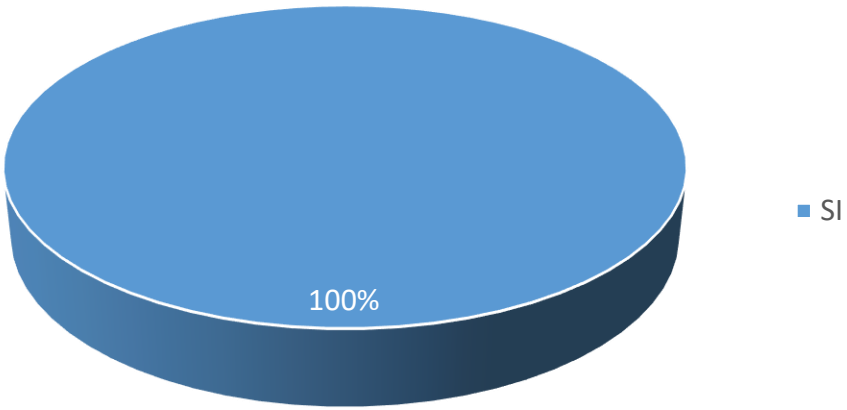
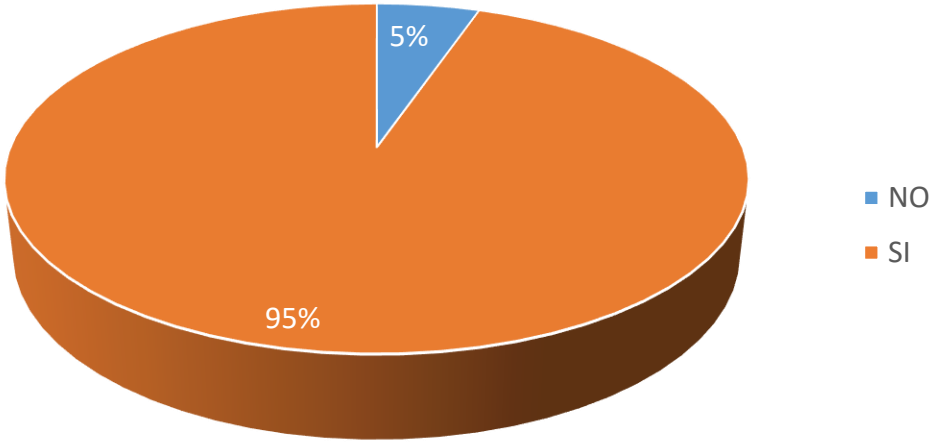
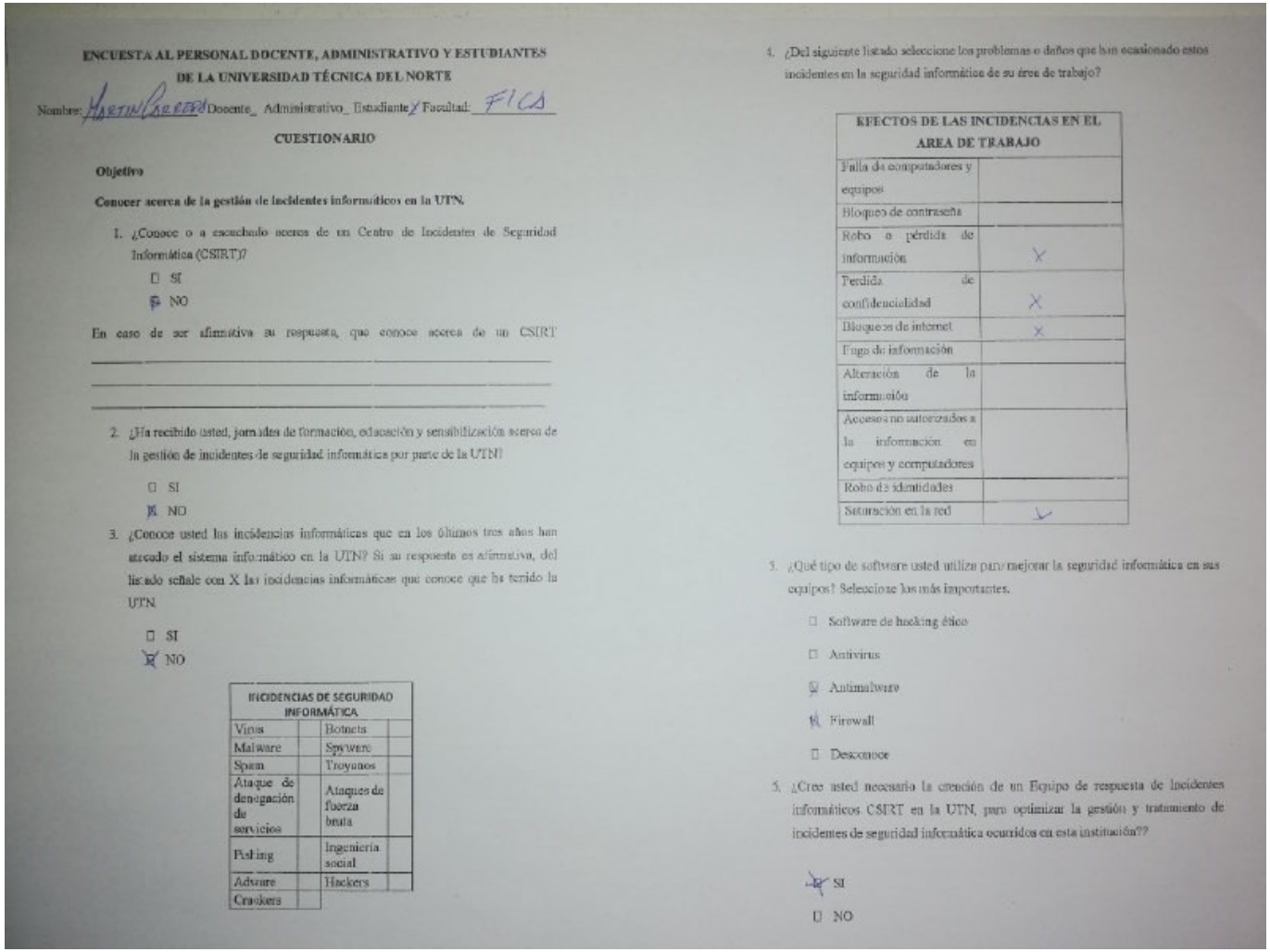


Figura E19

Resultados P6 encuesta a Estudiantes



Apéndice F Evidencia de aplicación de encuesta aplicada al personal docente, administrativo y estudiantes



ENCUESTA AL PERSONAL DOCENTE, ADMINISTRATIVO Y ESTUDIANTES DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Nombres: [illegible] Docente_ Administrativo_ Estudiante X Facultad: FICA

CUESTIONARIO

Objetivo

Conocer acerca de la gestión de incidentes informáticos en la UTN.

1. ¿Conoce o a escuchado acerca de un Centro de Incidentes de Seguridad Informática (CSIRT)?
   - ☐ SI
   - ☒ NO

En caso de ser afirmativa su respuesta, que conoce acerca de un CSIRT

2. ¿Ha recibido usted, jornadas de formación, educación y sensibilización acerca de la gestión de incidentes de seguridad informáticas por parte de la UTN?
   - ☐ SI
   - ☒ NO
3. ¿Conoce usted las incidencias informáticas que en los últimos tres años han atacado el sistema informático en la UTN? Si su respuesta es afirmativa, del listado señale con X las incidencias informáticas que conoce que ha tenido la UTN
   - ☐ SI
   - ☒ NO

INCIDENCIAS DE SEGURIDAD INFORMÁTICA			
Virus		Botnets	
Malware		Spyware	
Spam		Troyanos	
Ataque de denegación de servicios		Ataques de fuerza bruta	
Pishing		Ingeniería social	
Adware		Hackers	
Crackers			

4. ¿Del siguiente listado seleccione los problemas o daños que han ocasionado estos incidentes en la seguridad informática de su área de trabajo?

EFECTOS DE LAS INCIDENCIAS EN EL AREA DE TRABAJO	
Falla de computadores y equipos	
Bloqueo de contraseña	
Robo o pérdida de información	X
Perdida de confidencialidad	X
Bloqueos de internet	X
Fuga de información	
Alteración de la información	
Accesos no autorizados a la información en equipos y computadores	
Robo de identidades	
Saturación en la red	✓

5. ¿Qué tipo de software usted utiliza para mejorar la seguridad informática en sus equipos? Seleccione los más importantes.
   - ☐ Software de hacking ético
   - ☐ Antivirus
   - ☒ Antimalware
   - ☒ Firewall
   - ☐ Desconoce
6. ¿Cree usted necesario la creación de un Equipo de respuesta de Incidentes informáticos CSIRT en la UTN, para optimizar la gestión y tratamiento de incidentes de seguridad informática ocurridos en esta institución??
   - ☒ SI
   - ☐ NO

ENCUESTA AL PERSONAL DOCENTE, ADMINISTRATIVO Y ESTUDIANTES DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Nombre: Maria Tobar Docente__ Administrativo ✓ Estudiante__

Facultad:_____

CUESTIONARIO

Objetivo

Conocer acerca de la gestión de incidentes informáticos en la UTN.

1. ¿Conoce o a escuchado acerca de un Centro de Incidentes de Seguridad Informática?

   ☐ SI

   ☑ NO

En caso de ser afirmativa su respuesta, que conoce acerca de un CSIRT

_____

_____

_____

2. ¿Ha recibido usted, jornadas de formación, educación y sensibilización acerca de la gestión de incidentes de seguridad informática por parte de la UTN?

   ☐ SI

   ☑ NO

3. ¿Conoce usted las incidencias informáticas que en los últimos tres años han atacado el sisyema informático en la UTN? Si su respuesta es afirmativa, del listado señale con X las incidencias informáticas que conoce que ha tenido a UTN.

   ☐ SI

   ☑ NO

INCIDENCIAS DE SEGURIDAD INFORMATICA	
Virus	
Malware	
Spam	
Ataque de denegación de servicios	
Pishing	
Adware	
Botnets	
Spyware	
Troyanos	
Ataques de fuerza bruta	
Ingeniería social	
Hackers	
Crackers	

4. ¿Del siguiente listado seleccione los problemas o daños que han ocasionado estos incidentes en la seguridad informática de su área de trabajo?

EFECTOS DE LAS INCIDENCIAS EN EL AREA DE TRABAJO	
Falla de computadores y equipos	X
Bloqueo de contraseña	
Robo o pérdida de información	
Pérdida de confidencialidad	
Bloqueos de internet	
Fuga de información	

ENCUESTA AL PERSONAL DOCENTE, ADMINISTRATIVO Y ESTUDIANTES DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Nombre: Dennis Ortiz Docente X Administrativo_ Estudiante_ Facultad: FACAE

CUESTIONARIO

Objetivo

Conocer acerca de la gestión de incidentes informáticos en la UTN.

1. ¿Conoce o a escuchado acerca de un Centro de Incidentes de Seguridad Informáticos (CSIRT)?

   ☐ SI
   ☒ NO

En caso de ser afirmativa su respuesta, que conoce acerca de un CSIRT

_____

_____

_____

2. ¿Ha recibido usted, jornadas de formación, educación y sensibilización acerca de la gestión de incidentes de seguridad informática por parte de la UTN?

   ☐ SI
   ☒ NO

3. ¿Conoce usted las incidencias informáticas que en los últimos tres años han atacado el sistema informático en la UTN? Si su respuesta es afirmativa, del listado señale con X las incidencias informáticas que conoce que ha tenido la UTN

   ☐ SI
   ☒ NO

INCIDENCIAS DE SEGURIDAD INFORMÁTICA			
Virus		Botnets	
Malwre		Spyware	
Spam		Troyanos	
Ataque de denegación de servicios		Ataques de fuerza bruta	
Pishing		Ingeniería social	
Adware		Hackers	
Crackers			

4. ¿Del siguiente listado seleccione los problemas o daños que han ocasionado estos incidentes en la seguridad informática de su área de trabajo?

EFECTOS DE LAS INCIDENCIAS EN EL AREA DE TRABAJO	
Falla de computadores y equipos	X
Bloqueo de contraseña	X
Robo o pérdida de información	
Perdida de confidencialidad	
Bloqueos de internet	
Fuga de información	
Alteración de la información	X
Accesos no autorizados a la información en equipos y computadores	
Robo de identidades	
Saturación en la red	

5. ¿Qué tipo de software usted utiliza para mejorar la seguridad informática en sus equipos? Seleccione los más importantes.

   ☐ Software de hacking ético
   ☒ Antivirus
   ☐ Antimalware
   ☐ Firewall
   ☐ Desconoce

6. ¿Cree usted necesario la creación de un Equipo de respuesta de Incidentes informáticos CSIRT en la UTN, para optimizar la gestión y tratamiento de incidentes de seguridad informática ocurridos en esta institución??

   ☒ SI
   ☐ NO

Apéndice G Análisis e interpretación de resultados de las encuestas

Administrador de Red del DDTI

Los resultados de la encuesta aplicada al administrador de red, permitió conocer la gestión de incidencias que realiza el DDTI, en la cual, se conoció que, en el caso de existir algún incidente de seguridad informática, este es reportado al DDTI, específicamente al departamento de Redes y Comunicaciones, pero no poseen una herramienta en la cual puedan realizar este reporte de incidentes de manera adecuada.

Por otra parte, el administrador de la red, asegura que el DDTI utiliza herramientas de escaneo de vulnerabilidades, pero no se aplican políticas de gestión de incidencias de seguridad informática, a su vez, se tiene que, en el DDTI, no se aplican procedimientos de respaldo de la información, pudiendo generar un grave problema al perder la información.

Todos estos resultados dejan en manifiesto que es necesario un área en la que se encargue de la gestión de incidencias y vulnerabilidades, en donde el DDTI pueda trabajar en conjunto con el Equipo de Respuesta de Incidentes de Seguridad informática, para coordinar acciones para la resolución de problemas y amenazas que puedan ocurrir en la red de la UTN.

Personal Administrativo

Los resultados de las encuestas realizadas al personal administrativo, permitió conocer que ninguno de los encuestados conoce o a escuchado acerca de un Equipo de Respuesta de Incidentes de Seguridad Informática, así como también en un gran porcentaje no ha recibido jornadas de capacitación en temas de gestión de incidencias.

Así mismo, el 20% del personal administrativo, concuerda que los incidentes que han afectado sus equipos son virus, generando daños y problemas como fuga de información, pérdida de confidencialidad, en definitiva, se tiene que un gran porcentaje desconoce acerca

de los problemas o daños que hayan sido ocasionados por incidentes de seguridad informática y de este grupo de encuestados un porcentaje bajo utilizan software antivirus para proteger sus equipos, por lo que todos concuerdan en que sería factible la creación del CSIRT en la UTN, para poder optimizar la gestión y tratamiento de las incidencias de seguridad informática

Docentes

Los datos más relevantes de las encuestas realizadas a los docentes de la UTN, es que el 25% de ellos ha recibido jornadas de formación, educación y sensibilización sobre gestión de incidentes informáticos, de los cuatro docentes encuestados, el 25% dice que los virus han afectado sus equipos, de manera que, los docentes concuerdan que los incidentes informáticos han causado problemas como falla de computadores, pérdida de confidencialidad, saturación en la red, bloqueos de internet, bloqueos contraseñas, por otro lado, dentro de este grupo en su mayoría no conoce exactamente que programas utilizar para combatir las incidencias de seguridad, creando la necesidad en los docentes que se opte por la creación de un CSIRT en la universidad para la optimización de la gestión y tratamiento de los incidentes que pudieran ocurrir dentro de la academia.

Estudiantes

Los estudiantes en su gran mayoría, no conoce lo que es un CSIRT, no ha recibido jornadas de formación en temas de gestión de incidencias, el 24% de los estudiantes conocen acerca de las incidencias que han atacado a la red de la UTN, coincidiendo que el problema más grande son los virus informáticos, teniendo como consecuencias bloqueo de contraseñas, bloqueo de internet, fallas en los computadores, robo o pérdida de información, alteración de la información, para combatir estas incidencias la mayoría de los encuestados

utiliza software antivirus, además este grupo de encuestados también coincide en estar de acuerdo en la creación de un CSIRT en la UTN

Apéndice H Matriz de Asignación de Responsabilidades RACI

La matriz RACI, o matriz de responsabilidades, aplicada en la Dirección de Desarrollo Tecnológico e Informático (DDTI) de la UTN, es un documento que permite definir de forma esquemática las funciones de cada empleado del DDTI, en relación con su participación en las 7 prácticas del dominio de entrega, servicio y soporte (DSS02) relacionadas con gestión de incidencias según COBIT.

En este sentido, estas prácticas son: definir esquemas de clasificación para incidentes y de peticiones de servicio (DSS02-01), registrar, clasificar y priorizar las peticiones e incidentes (DSS02-02), verificar, aprobar y resolver peticiones de servicio (DSS02-03), investigar, diagnosticar y asignar incidentes (DSS02-04), resolver y recuperarse de los incidentes (DSS02-05), cerrar las peticiones de servicio y los incidentes (DSS02-06) y hacer seguimiento del estado de la gestión de incidentes y emitir informes (DSS02-07).

De manera que, las actividades mencionadas en el párrafo anterior son relacionadas con los recursos que posee el DDTI, que corresponde al asistente técnico, analista de sistemas, administrador de red y el director de TI, donde se asigna los siguientes roles: Responsable (R), es la persona que ejecuta la tarea, Aprobador (A), es el funcionario que aprueba el trabajo realizado y da por concluida la tarea, Consultor (C), es el encargado que presta ayuda al responsable, Informado (I), es el individuo que debe estar informado de la ejecución de la tarea, pero no participa de la misma, y no aplica (NA), en caso de que no se realice la actividad, tal como se presenta en la tabla H1.

Tabla H1

Matriz de Asignación de Responsabilidades (RACI)

ID Actividad	Prácticas claves de Gestión de Incidencias (DSS02)	Asistente Técnico	Analista de Sistemas	Administrador de Redes	Director de TI	Observaciones
DSSO2 01	Definir esquemas de clasificación de incidentes y peticiones de servicio	**NA**	**NA**	**NA**	**NA**	No se realiza
DSSO2 02	Registrar, clasificar y priorizar peticiones e incidentes	**NA**	**NA**	**NA**	**NA**	No se realiza
DSSO2 03	Verificar, aprobar y resolver peticiones de servicio	**NA**	**NA**	**NA**	**NA**	No se realiza
DSSO2 04	Investigar, diagnosticar y asignar incidentes	**R**	**C**	**R**	**I**	Si se realiza No se documenta

DSSO2 05	Resolver y recuperarse de incidentes	**R**	**C**	**R**	**I**	Si se realiza No se documenta
DSSO2 06	Cerrar incidentes y peticiones de servicio	**NA**	**NA**	**NA**	**NA**	No se realiza
DSSO2 07	Dar seguimiento del estado de la gestión de incidentes y emitir informes	**NA**	**NA**	**NA**	**NA**	No se realiza

Por lo tanto, según la tabla H1, los resultados de la matriz RACI, demuestran que de las 7 prácticas claves de gestión de incidencias según COBIT, no son ejecutadas en el DDTI, las practicas correspondientes a: DSS02-01, DSS02-02, DSS02-03, DSS02-06 y DSS02-07, además las prácticas DSS0204 y DSS0205 son realizadas, pero no son documentadas.

En consecuencia, las mejoras deben aplicarse a estos procesos, donde el CSIRT UTN, deberá designar responsables que realicen tales prácticas afines de que el proceso de gestión de incidencias sea completo. Con esto resultados podemos confirmar que los diferentes tipos de servicios de gestión de incidencias del CSIRT UTN, serán creados en base a las necesidades de gestión de incidencias del DDTI, que actualmente no se ejecutan.

Apéndice I Modelo de evaluación de procesos PAM de COBIT

El modelo PAM de COBIT, permite conocer el nivel de madurez en que se encuentra el dominio de entrega, servicio y soporte del proceso de gestión de incidentes DSSO2 en el DDTI, cuyas prácticas y responsables fueron evaluados en la Matriz RACI. De modo que, este modelo, comprende un conjunto de indicadores de desempeño y capacidad del proceso DSSO2 basados en la (BP) Prácticas Base que son necesarias para cumplir con los procesos y (WP) Productos de trabajo que se obtienen como resultado, permitiendo medir en rangos porcentuales la madurez del proceso según su nivel de cumplimientos, estos niveles de cumplimiento son asignados de acuerdo a la tabla I1, en la que COBIT propone la siguiente escala de evaluación de los procesos realizados.

Tabla I1

Escala de evaluación de PAM

Niveles de evaluación PAM de COBIT	
No conseguido	0 al 15%
Parcialmente conseguido	15% al 50%
Mayormente conseguido	50% al 85%
Completamente conseguido	85% al 100%

Nota: Tomado de (Gonzáles, 2016).

A continuación, en la tabla I2, se presenta el módulo PAM aplicado para el proceso DSSO2 de COBIT en el DDTI de la UTN:

Tabla I2

Módulo PAM aplicado para COBIT en el DDTI

PROCESO	**PRÁCTICAS DEL PROCESO DE GESTIÓN DE INCIDENCIAS**	
DESCRIPCIÓN	Permitir el uso efectivo de los sistemas y equipos de TI en el DDTI, áreas de administradores, estudiantes y docentes de la UTN, garantizando la resolución y el análisis de incidentes y vulnerabilidades de seguridad de la información	
PROPÓSITO	Lograr mayor productividad y minimizar interrupciones mediante la resolución rápida de peticiones e incidentes de los usuarios	
	RESULTADOS	
IDENTIFICADOR	**DESCRIPCIÓN**	
DSS02-01	Los servicios relacionados con TI están disponibles para su uso	
DSS02-02	Los incidentes se resuelven de acuerdo con los niveles de servicio acordados	
DSS02-03	Las solicitudes de servicio se atienden de acuerdo con los niveles de servicio y satisfacción de los usuarios	
	Practicas Base (BPs)	
IDENTIFICADOR	**DESCRIPCIÓN**	**SOPORTE**
DSS02-BP1	Definir esquemas de clasificación de incidentes y peticiones de servicio	DSS02-01
DSS02-BP2	Registrar, clasificar y priorizar peticiones e incidentes	DSS02-01/02

DSS02-BP3	Verificar, aprobar y resolver peticiones de servicio	DSS02-03
DSS02-BP4	Investigar, diagnosticar y asignar incidentes	
DSS02-BP5	Resolver y recuperarse de incidentes	DSS02-02
DSS02-BP6	Cerrar incidentes y peticiones de servicio	DSS02-03
DSS02-BP7	Dar seguimiento del estado de la gestión de incidentes y emitir informes	

Productos de Trabajo (WPs)

IDENTIFICADOR	ANÁLISIS	(0-15%)	(15-50%)	(50-85%)	(85-100%)
DSSO2-BP1 Crear procedimientos de clasificación, escalamiento y priorización de incidentes	El DDTI no posee una herramienta automatizada para clasificar ni evaluar los tiempos de escalamiento de las incidencias reportadas, por tanto, estos datos no se pueden asegurar y tampoco comprobar los tiempos de respuesta a los incidentes reportados ni su solución	N			
DSSO2-BP2 Detectar y registrar los incidentes y las	Según los resultados de las encuestas en la UTN, el DDTI si se detectan los incidentes, su origen y destino del ataque, pero no se utilizan herramientas automatizadas, para el registro de los incidentes y peticiones de servicios.		S		

peticiones de servicios	No existe un control y seguimiento de los incidentes y peticiones de servicios, este proceso es realizado de forma manual Falta un servicio de Help Desk en la UTN		
DSSO2-BP3 Verificar, aprobar y resolver peticiones de servicio	No se posee procedimientos para resolver las peticiones de los usuarios	N	
DSSO2-BP4 Investigar, diagnosticar y asignar incidentes	El DDTI resuelve el incidente, pero no maneja un reporte de gestión de incidencias para saber cuántos incidentes y de qué tipo han sido solucionados. Tampoco maneja registros o datos de incidentes recuperados. Faltan procedimiento de gestión de incidentes		S
DSSO2-BP5 Resolver y recuperarse de incidentes	Los usuarios finales no reciben información acerca de la solución de las incidencias reportadas y las garantías que este proceso aplica para seguir resolviendo los incidentes reportados. El DDTI no tiene un procedimiento para comunicar a los usuarios sobre el tratamiento que se va a dar a los incidentes reportados, además no se realiza un seguimiento a los incidentes		S

DSSO2-BP6 Cerrar solicitudes de incidentes	En el DDTI el personal encargado de la gestión de incidencias no envía reportes de cierre de incidentes	N
DSSO2-BP7 Cerrar solicitudes de incidentes	No se brinda seguimiento del estado de la gestión de incidentes y no se emite informes	N

Por lo tanto, la tabla I2, permite concluir que de las 7 prácticas de gestión de incidencias, el DDTI cumple parcialmente en 3 de sus prácticas, siendo estas BP2 (Registrar, clasificar y priorizar peticiones e incidentes), BP4 (Investigar, diagnosticar y asignar incidentes) y BP5 (Resolver y recuperarse de incidentes), y en 4 de sus prácticas no cumple con su objetivo las cuales corresponden a BP1 (Definir esquemas de clasificación de incidentes y peticiones de servicio), BP3 (Verificar, aprobar y resolver peticiones de servicio), BP6 (Cerrar incidentes y peticiones de servicio) y BP7 (Dar seguimiento del estado de la gestión de incidentes y emitir informes), por ende se evidencia la falta de procedimientos para la gestión de incidentes de seguridad de la información, por ello los procesos de gestión de incidentes realizados por el DDTI son parcialmente conseguidos según la evaluación PAM realizada.

Apéndice J Resultados de entrevista realizada a la Ingeniera Miriam López del EcuCERT

Objetivo: Establecer una primera relación con el EcuCERT, para obtener información relevante que contribuya en el Diseño del CSIRT académico de la UTN

1. **¿En qué beneficiaría la creación de un CSIRT académico en la Universidad Técnica del Norte, en la ciudad de Ibarra?**

   Se tiene como beneficios la creación de una cultura de conciencia y sensibilización de ciberseguridad en todos los usuarios, asesoría para certificación FIRST, redes de confianza entre CSIRT's, atacar las realidades locales, minimizar vulnerabilidades dentro de la comunidad universitaria, reducir brechas, e incidentes.

2. **¿Uds. como CSIRT, en qué aspectos podrían brindar apoyo para la creación del CSIRT académico en la UTN?**

   El Ecu CERT puede brindar guías para la creación de un CSIRT en el ámbito de infraestructura, estructural, organizacional, así como asesorar en el cumplimiento de políticas y procedimientos mínimos como políticas de gestión de incidentes, herramientas para la gestión de incidentes, asesoría para poder ser miembro de FIRST, y a su vez podrían colaborar como sponsor para el ingreso a FIRST conjuntamente con CEDIA

   Este proceso se lo realiza de manera formal con el envío de una carta con la cual se puede comenzar a trabajar conjuntamente

3. **¿Qué servicios recomendaría, o qué servicios debería brindar un CSIRT en una etapa inicial?**

Gestión de incidentes, notificaciones y sensibilización

4. **En cuanto a equipamiento tecnológico ¿Qué equipos serían necesarios para el correcto funcionamiento del CSIRT académico en la UTN en etapas iniciales?**

   El equipamiento va en función de los servicios a brindar, se debe contar con un servidor de gestión de tickets, correo electrónico, portal web, servidor de monitoreo de red

5. **¿En base a su experiencia y en cuanto a recursos humanos, cuantas personas serían necesarias para que el CSIRT académico de la UTN comience con sus operaciones?**

   En el tema de recursos humanos también depende de los servicios a brindar y el nivel de automatización, por ejemplo, en el caso de Ecu CERT cuentan con seis personas, CEDIA cuenta con dos personas, y el CSIRT de la politécnica cuenta con cuatro personas

6. **¿Qué políticas considera que son necesarias para un CSIRT?**

   Las políticas es otro tema que depende de los servicios que se van a brindar sin embargo se debe contar con las siguientes políticas en una etapa inicial: Gestión de incidentes, Control de accesos, contraseñas, Clasificación de la información, Protección de la información, Destrucción de la información, Difusión de la información, Cooperación con otros CSIRT

7. **¿Qué requisitos son necesarios para que se pueda establecer colaboración entre el EcuCert y el CSIRT de la UTN?**

Más que requisitos es el pedido de registro para formar parte de la red de confianza con el EcuCERT, en el cual se envía la información del CSIRT, una vez analizada la información el Ecu CERT envía el acuerdo y por último se procede a la firma el convenio

8. **En tema de capacitaciones, talleres de formación, ¿el EcuCERT puede brindar capacitaciones para el personal del CSIRT?**

   EcuCERT como CERT público no lo puede realizar, sin embargo, se brinda información de cursos brindados por otras organizaciones

Apéndice K Resultados de entrevista realizada al Ingeniero Ernesto del CSIRT CEDIA

Objetivo: Establecer una primera relación con el CSIRT de CEDIA, para obtener información relevante que contribuya en el Diseño del CSIRT académico de la UTN

1. **¿En qué beneficiaría la creación de un CSIRT académico en la Universidad Técnica del Norte, en la ciudad de Ibarra?**

   Un CSIRT tiene importancia fundamental, ya que ayuda a que la comunidad objetivo tenga un punto de contacto para el reporte y solución de incidentes de seguridad informática, además es una excelente oportunidad para los estudiantes que conozca acerca del funcionamiento de un CSIRT, así mismo puede darse la oportunidad para la realización de prácticas pre profesionales.

2. **¿Uds. como CSIRT, en qué aspectos podrían brindar apoyo para la creación del CSIRT académico en la UTN?**

   El apoyo que se puede brindar es el cruce de información acerca de vulnerabilidades, posibles vectores de ataque, campañas de concienciación en temas de ciberseguridad, brindar apoyo para tener relaciones de confianza con otros CSIRT´s, y capacitaciones como institución miembro de CEDIA

3. **¿Qué servicios recomendaría, o qué servicios debería brindar un CSIRT en una etapa inicial?**

   Los servicios recomendados son servicios básicos en una primera etapa como gestión de incidentes, concienciación de seguridad informática, alertas y avisos de seguridad

4. **En cuanto a equipamiento tecnológico ¿Qué equipos serían necesarios para el correcto funcionamiento del CSIRT académico en la UTN?**

   Infraestructura en la que pueda operar el CSIRT, en cuanto a Hardware dos servidores, uno de pruebas y otro para realizar pentesting, con memoria RAM de 8Gb

5. **¿En base a su experiencia y en cuanto a recursos humanos, cuantas personas serían necesarias para que el CSIRT académico de la UTN comience con sus operaciones?**

   Este punto es en base a los servicios que se va a ofrecer, en etapas iniciales estaría bien con dos personas, y no necesariamente que trabajen a tiempo completo

6. **Que políticas considera son necesarias para un CSIRT**

   Las políticas recomendadas, son las que FIRST propone para obtener la membresía

7. **¿Qué requisitos son necesarios para que se pueda establecer colaboración entre el CSIRT CEDIA y el CSIRT de la UTN?**

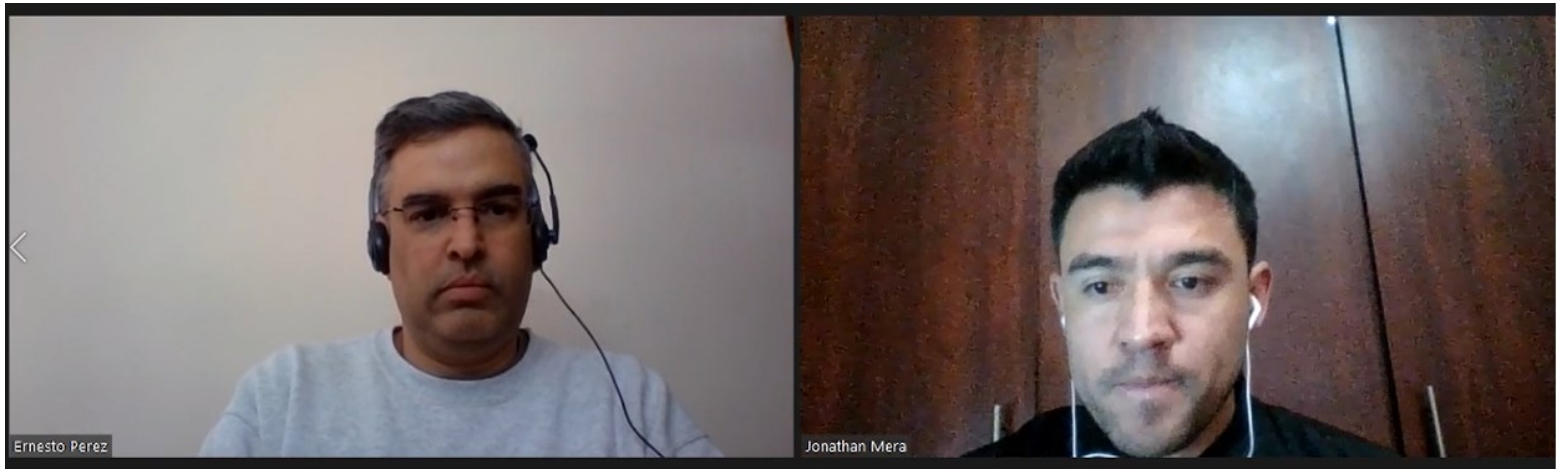
   El procedimiento comienza con el aviso de inicio de operaciones del CSIRT y a partir de allí se puede firmar convenios de cooperación y colaboración.

8. **En tema de capacitaciones, talleres de formación, ¿el CSIRT de CEDIA puede brindar capacitaciones para el personal del CSIRT?**

   CEDIA brinda cursos, con beneficios para miembros de la organización

Apéndice L Evidencia de aplicación de encuestas

Apéndice M Evidencia de entrevistas con la Ingeniera Miriam López EcuCERT e Ingeniero Ernesto Pérez de CSIRT CEDIA



Apéndice N Manual de Políticas del CSIRT-UTN

Política de Clasificación de la Información del CSIRT-UTN

UNIVERSIDAD TÉCNICA DEL NORTE

CSIRT – UTN

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Código	DDTI-CSIRT-PCI-UTN-01
Versión	1.0
Fecha de la versión	03 de marzo de 2020
Creado por	Jonathan Mera
Aprobado por	Director DDTTI

Fecha de aprobación:

Historial de modificaciones

Fecha	Versión	Elaborado por	Descripción de la modificación
03-03-2020	1.0	Jonathan Mera	Elaboración de política

Contenido

1. OBJETIVO

Establecer los lineamientos y procedimientos para clasificar los activos de información del CSIRT académico de la UTN y evitar la divulgación indebida de la misma

2. ALCANCE

La presente política aplica a todos los tipos de información del CSIRT-UTN independientemente de su formato, ya sea documentos electrónicos, en papel, base de datos, aplicaciones.

3. ROLES Y RESPONSABILIDADES

Responsable: Corresponde al jefe del DDTI, la responsabilidad de implementar la presente política dentro del CSIRT académico de la UTN

Administrador del CSIRT: Es el encargado de verificar que se cumpla con la presente política, dando a conocer su incumplimiento

Propietario de la información: es el responsable de custodiar y dar protección a los activos de información, siguiendo la presente política

4. POLÍTICA

La información que maneje el CSIRT de la UTN y el propietario de la información utilizarán el siguiente esquema de clasificación, teniendo como criterio los tres pilares de la seguridad de la información: Disponibilidad, Integridad y Confidencialidad:

Disponibilidad	
NIVEL 0	Información que, en caso de no estar disponible, no afecta a las operaciones del CSIRT-UTN
NIVEL 1	Información que, en caso de no estar disponible en el lapso de una semana, puede afectar levemente a las operaciones del CSIRT-UTN
NIVEL 2	Información que, en caso de no estar disponible en el lapso de 24 horas puede afectar de manera significativa a las operaciones del CSIRT-UTN
NIVEL 3	Información, que en caso de no estar disponible en el lapso de 1 hora puede afectar de manera significativa a las operaciones del CSIRT

Integridad	
NIVEL 0	Información que, en caso de ser modificada sin previa autorización, puede rectificarse fácilmente y en caso de no ser posible no afecta en las operaciones del CSIRT-UTN
NIVEL 1	Información que, en caso de ser modificada sin autorización, puede rectificarse a pesar de que pueda afectar a las operaciones del CSIRT-UTN
NIVEL 2	Información que, en caso de ser modificada sin autorización, la rectificación es difícil y puede afectar a las operaciones del CSIRT-UTN
NIVEL 3	Información, que, en caso de ser modificada sin autorización, no pueda ser rectificada ocasionando afectaciones en las operaciones del CSIRT-UTN

Confidencialidad		
NIVEL 0	**PÚBLICO**	Información que puede tener acceso cualquier persona sin previa autorización, pertenezca o no al CSIRT-UTN
NIVEL 1	**RESERVADA – USO INTERNO**	Información que puede tener acceso solo personal del CSIRT-UTN y algunas personas externas con su respectiva autorización, y que en caso de ser divulgada la información sin previa autorización pueda provocar riesgos o afectaciones leves al CSIRT-UTN
NIVEL 2	**RESERVADA - PRIVADA**	Información que puede tener acceso solo personal del CSIRT-UTN, y que en caso de ser divulgada la información pueda traer consigo pérdidas significativas para el CSIRT-UTN
NIVEL 3	**RESERVADA - CONFIDENCIAL**	Información que puede tener acceso solo la alta dirección del CSIRT-UTN, y que en caso de ser divulgada la información pueda traer consigo pérdidas graves para el CSIRT-UTN

Para la valorización a los activos de información se tendrá que asignar un valor para cada criterio antes mencionado, por ejemplo:

Activo	Disponibilidad	Integridad	Confidencialidad
Información XX	1	2	1

Una vez realizado la valoración, se asignará una clasificación de la información según su criticidad de acuerdo a la tabla a continuación:

Nivel de criticidad	Detalle
Alto	En caso de que algún valor asignado sea de nivel 3
Medio	En caso de que algún valor asignado sea de nivel 2
Bajo	En caso de que algún valor asignado pase del nivel 1

En base al nivel de criticidad se establecen las siguientes categorías:

- Cuando el nivel de **criticidad** sea **alto** la clasificación de la información será **CONFIDENCIAL**
- Cuando el nivel de **criticidad** sea **medio** la clasificación de la información será de **USO INTERNO**
- Cuando el nivel de **criticidad** sea **bajo** la clasificación de la información será **PÚBLICA**

5. INCUMPLIMIENTO

En caso de incumplimiento de la presente política tendrá la aplicación de sanciones ya sea administrativas o legales teniendo en cuenta la magnitud y el aspecto no cumplido.

6. VALIDEZ

Este documento entrará en vigencia y será válido desde su aprobación. El CSIRT-UTN es el propietario de este documento y por lo tanto será el encargado de verificar la efectividad del mismo.

REFERENCIAS

2700, I. (s.f.). *ISO 27000.ES*. Obtenido de ISO 27000.ES: https://www.iso27000.es/iso27002.html

Política de Protección de la Información del CSIRT-UTN

UNIVERSIDAD TÉCNICA DEL NORTE

CSIRT – UTN

POLÍTICA DE PROTECCIÓN DE LA INFORMACIÓN

Código	DDTI-CSIRT-PPI-UTN-01
Versión	1.0
Fecha de la versión	03 de marzo de 2020
Creado por	Jonathan Mera
Aprobado por	

Fecha de aprobación:

Historial de modificaciones

Fecha	Versión	Elaborado por	Descripción de la modificación
03-03-2020	1.0	Jonathan Mera	Elaboración de política

Contenido

1. OBJETIVO

Brindar protección a los activos de información del CSIRT académico de la UTN garantizando su confidencialidad y disponibilidad, asegurando el manejo adecuado de la información.

2. Roles y responsabilidades

Responsable: Corresponde al jefe del DDTI, la responsabilidad de implementar la presente política dentro del CSIRT académico de la UTN.

Aprobador: El Equipo de Respuesta ante Incidentes de Seguridad Informática, es el responsable de verificar el cumplimiento de la presenta política.

Propietario de la información: es el responsable de custodiar y dar protección a los activos de información, siguiendo la presente política

3. ALCANCE

La presente política aplica a todo tipo de información del CSIRT-UTN independientemente de su formato, ya sea documentos electrónicos, en papel, base de datos, aplicaciones.

4. POLÍTICA

Toda la información independientemente del medio, deberá tener de manera clara su clasificación teniendo en cuenta la Política de Clasificación de la Información. La protección a brindar se establecerá según los siguientes parámetros:

Información confidencial

- Cuando la información esté en formato lógico, deberá ser almacenada de manera que se asegure la confidencialidad con el uso de claves de 2048 bits como largo

mínimo, y la integridad con el uso de firmas digitales, como por ejemplo la función hash SHA-2.

- En caso de que la información sea en formato físico, deberá ser almacenado en una caja fuerte con el uso de sobre cerrado y ubicado dentro del CSIRT-UTN.
- La entrega de información impresa o que su entrega sea a mano, o información contenida de manera digital o almacenamiento magnético, deberá ser posterior a la firma de un acta de entrega-recepción, en la cual deberá contener lo siguiente:
    - Definir claramente qué información se está entregando o receptando, fecha y hora de recepción o entrega, datos de quien entrega la información y además deberá contar con imágenes que evidencien este proceso.
- Se deberá asegurar la confidencialidad e integridad al acceso remoto de información clasificada como confidencial, mediante el uso de protocolos como ssh, sftp o hhtps, y en caso de ser necesaria la transmisión de la información, se deberá cifrar con una llave pública de un mínimo de 2048 bits de longitud.

Información de uso interno

- Cuando la información esté en formato lógico, se deberá almacenar en un dispositivo de almacenamiento el cual contendrá el nombre del mismo, la versión actual, fecha de creación, fecha de publicación, el valor de la firma digital y deberá ser almacenada en una caja fuerte ubicada dentro del CSIRT-UTN.
- La información en formato físico, no podrá ser difundida fuera del CSIRT-UTN, por lo tanto, no podrá salir de sus instalaciones.
- Se deberá asegurar la confidencialidad e integridad del acceso remoto a la información.

- La información no puede ser comentada o compartida con terceros.

Información pública

- Cuando la información sea en formato lógico, deberá contener el nombre del mismo, la versión actual, fecha de creación, fecha de publicación y el valor de la firma digital, toda esta información será guardada en un dispositivo de almacenamiento no volátil, así como también en una caja fuerte ubicada dentro del CSIRT-UTN.
- La información en formato físico será válida siempre y cuando exista la misma información en formato lógico.

5. INCUMPLIMIENTO

En caso de incumplimiento de la presente política tendrá la aplicación de sanciones ya sea administrativas o legales teniendo en cuenta la magnitud y el aspecto no cumplido.

6. VALIDEZ

Este documento entrará en vigencia y será válido desde su aprobación. El CSIRT-UTN es el propietario de este documento y por lo tanto será el encargado de verificar la efectividad del mismo.

REFERENCIAS

2700, I. (s.f.). *ISO 27000.ES*. Obtenido de ISO 27000.ES: https://www.iso27000.es/iso27002.html

Política de Destrucción de la Información del CSIRT-UTN

UNIVERSIDAD TÉCNICA DEL NORTE

CSIRT – UTN

POLÍTICA DE DESTRUCCIÓN DE INFORMACIÓN

Código	DDTI-CSIRT-PDTI-UTN-01
Versión	1.0
Fecha de la versión	03 de marzo de 2020
Creado por	Jonathan Mera
Aprobado por	
Nivel de confidencialidad	

Fecha de aprobación:

Historial de modificaciones

Fecha	Versión	Elaborado por	Descripción de la modificación
03-03-2020	1.0	Jonathan Mera	Elaboración de política

Contenido

1. OBJETIVO

Garantizar que toda la información que esté almacenada ya sea de manera física o electrónica sea eliminada de manera segura

2. ALCANCE

La presente política aplica a todo tipo de información del CISRT-UTN independientemente de su formato, ya sea documentos electrónicos, en papel, base de datos, aplicaciones.

3. ROLES Y RESPONSABILIDADES

Responsable de la seguridad de la información: Es el responsable de dar cumplimiento a la presente política, definir el método seguro para la destrucción de la información según sea el caso.

Responsable de la destrucción de los activos de información: Es la persona responsable del registro del proceso y la destrucción de la información, asegurándose de que este proceso sea el adecuado y dejando una evidencia del proceso realizado.

4. POLÍTICA

El ciclo de vida de la información termina con la destrucción de la misma, por ello es importante que tenga un tratamiento adecuado de destrucción de la información, por lo tanto, es importante el uso de métodos que garanticen que la información electrónica o física sea destruida y no pueda ser recuperada de forma satisfactoria. Por lo tanto, se realiza las siguientes recomendaciones para la destrucción de la información:

Información en papel: Para la destrucción de datos almacenados en papel es necesario regirse a la norma DIN 66399, la cual establece tres clases de protección y siete niveles de seguridad a tener en cuenta, según estas directrices de seguridad el papel tiene que hacerse desde tiras hasta pequeñas partículas.

Información en dispositivos de almacenamiento: Para la destrucción de información almacenada en dispositivos de almacenamiento se puede utilizar la destrucción física, desmagnetización o la sobreescritura

Teniendo en cuenta las recomendaciones es necesario realizar el siguiente procedimiento para la destrucción de la información:

1. Solicitud al director del DDTI y del CSIRT, informando de la destrucción de información, en la cual se debe detallar la información a eliminar, qué proceso se va a utilizar y la o las personas que participarán en dicho proceso, además el documento deberá estar con sus respectivas firmas de aprobación y responsabilidad.
2. Verificar que la información que va a ser destruida no repercuta en un futuro.
3. Asegurar que en el proceso cumpla la cadena de custodia, evitando la fuga de información.
4. Informar cualquier novedad al director del DDTI y del CSIRT

5. INCUMPLIMIENTO

En caso de incumplimiento de la presente política tendrá la aplicación de sanciones ya sea administrativas o legales teniendo en cuenta la magnitud y el aspecto no complido

6. VALIDEZ

Este documento entrará en vigencia y será válido desde su aprobación. El CSIRT-UTN es el propietario de este documento y por lo tanto será el encargado de verificar la efectividad del mismo.

REFERENCIAS

2700, I. (s.f.). *ISO 27000.ES.* Obtenido de ISO 27000.ES: https://www.iso27000.es/iso27002.html

Documental, P. B. D. G. (2017, 14 junio). Norma DIN 66399. DPS Gestión Documental. https://dpsgestiondocumental.com/info-tips/norma-din-66399

Política de Divulgación de la Información del CSIRT-UTN

UNIVERSIDAD TÉCNICA DEL NORTE

CSIRT – UTN

POLÍTICA DE DIVULGACIÓN DE LA INFORMACIÓN

Código	DDTI-CSIRT-PDVI-UTN-01
Versión	1.0
Fecha de la versión	03 de marzo de 2020
Creado por	Jonathan Mera
Aprobado por	

Fecha de aprobación:

Historial de modificaciones

Fecha	Versión	Elaborado por	Descripción de la modificación
03-03-2020	1.0	Jonathan Mera	Elaboración de política

Contenido

1. OBJETIVO

Definir la información que puede ser divulgada, a quién, cómo y bajo qué circunstancias, así como la manera en que la información será compartida según su clasificación

2. ALCANCE

La presente política aplica a todo tipo de información del CSIRT-UTN independientemente de su formato, ya sea documentos electrónicos, en papel, base de datos, aplicaciones.

3. ROLES Y RESPONSABILIDADES

Responsable: Corresponde al jefe del DDTI, la responsabilidad de implementar la presente política dentro del CSIRT académico de la UTN

Administrador del CSIRT: Es el encargado de verificar que se cumpla con la presente política, dando a conocer su incumplimiento

El director del DDTI y el responsable del CSIRT, serán los encargados de etiquetar la información como pública, clasificada y de uso comunitario, así como dar autorización para su difusión.

4. POLÍTICA

La divulgación de la información que a continuación se detalla se la realizará teniendo en cuenta la política de clasificación de la información.

Información pública: Toda información que tenga un nivel de criticidad baja según la política de clasificación de la información, podrá ser divulgada de manera pública y a través de los medios oficiales del CSIRT UTN.

Información clasificada: Toda información que tenga un nivel de criticidad media según la política de clasificación de la información, antes de su divulgación, deberá tener previa autorización por el director del DDTI o el encargado del CSIRT. La divulgación de esta información deberá ser manejada de manera sigilosa, teniendo presente la política de protección de la información.

Información confidencial: Toda información que tenga un nivel de criticidad alta según la política de clasificación de la información, bajo ninguna circunstancia podrá ser revelada y la o las personas que tengan acceso a este tipo de información deberán firmar un acuerdo de confidencialidad.

5. INCUMPLIMIENTO

En caso de incumplimiento de la presente política tendrá la aplicación de sanciones ya sea administrativas o legales teniendo en cuenta la magnitud y el aspecto no cumplido.

6. VALIDEZ

Este documento entrará en vigencia y será válido desde su aprobación. El CSIRT-UTN es el propietario de este documento y por lo tanto será el encargado de verificar la efectividad del mismo.

REFERENCIAS

2700, I. (s.f.). *ISO 27000.ES*. Obtenido de ISO 27000.ES: https://www.iso27000.es/iso27002.html

Política de Gestión de Incidentes del CSIRT-UTN

UNIVERSIDAD TÉCNICA DEL NORTE

CSIRT – UTN

POLÍTICA DE GESTIÓN DE INCIDENTES

Código	DDTI-CSIRT-PGI-UTN-01
Versión	1.0
Fecha de la versión	03 de marzo de 2020
Creado por	Jonathan Mera
Aprobado por	

Fecha de aprobación:

Historial de modificaciones

Fecha	Versión	Elaborado por	Descripción de la modificación
03-03-2020	1.0	Jonathan Mera	Elaboración de política

Contenido

1. OBJETIVO

Establecer los lineamientos y procedimientos para la gestión de incidentes de seguridad informática que se presenten dentro de la UTN

2. ALCANCE

La presente política aplica a todo el campo de tecnología de la información y comunidad objetivo del CSIRT-UTN.

3. ROLES Y RESPONSABILIDADES

Responsable: Corresponde al jefe del DDTI, la responsabilidad de implementar la presente política dentro del CSIRT académico de la UTN

Técnico de soporte: Será el encargado de recibir los reportes de incidentes de seguridad informática y en caso de no poder solventarlo, éste será el responsable de escalar el incidente al Equipo de Respuesta a Incidentes de Seguridad Informática del CSIRT-UTN.

Equipo de Respuesta a Incidentes de Seguridad Informática: Será el encargado de dar una solución al Incidente de Seguridad Informática reportado.

4. POLÍTICA

- El DDTI, deberá hacer conocer al personal de la UTN, los contactos a los que puede comunicarse para el reporte de incidentes de seguridad informática.
- Es responsabilidad del DDTI, hacer conocer al personal de la UTN, sobre la existencia del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT- UTN).
- El DDTI debe elaborar y publicar los datos estadísticos acerca de los incidentes de seguridad que se producen en la Universidad.

- El Área de Soporte Técnico del DDTI escalará al CSIRT-UTN todos los incidentes de seguridad informática de los usuarios, que coincidan con la categorización de incidentes creada por el CSIRT-UTN (ver tabla de clasificación de incidentes).
- Todas las actividades concernientes al manejo de incidentes se realizarán en base a los procedimientos definidos para el manejo de los mismos.
- Por ningún motivo se deberán utilizar métodos ilegales para la resolución de incidentes, se debe tomar en cuenta que estas actividades podrían repercutir en acciones legales en contra de la UTN.
- Es importante tomar en cuenta la asesoría legal para las acciones a realizar en incidentes relacionados a: suplantación de identidad, acceso no consentido a información confidencial, incidentes relacionados con ingeniería social, y cualquier otro incidente relacionado con ciberdelitos
- Toda la información relativa a los incidentes reportados, deberá ser manejada con total confidencialidad, la clasificación de la información se realizará de acuerdo a la Política de Clasificación de la Información.
- Se deberán tomar en cuenta las herramientas, normativas y metodologías adecuadas para la recolección del contenido digital durante el proceso de respuesta a incidentes, lo que servirá como recurso o evidencia necesaria, si el caso llegara a instancias legales.
- Para la respuesta a incidentes de seguridad informática se deberá utilizar la tabla de tiempo máximo de resolución de incidentes (ver tabla de tiempo máximo de resolución de incidentes), en la cual se especifica la prioridad y el tiempo para su resolución. Es tarea del Equipo de Respuesta a Incidentes de Seguridad

Informática realizar una valoración para medir el impacto que el incidente pueda causar.

Tiempo máximo de resolución de incidentes

Prioridad	Tiempo de respuesta
Bajo	2 horas
Medio	1 hora
Alto	30 min

Clasificación de Incidentes

Clase de incidente	Tipo de incidente
Código malicioso	Virus, troyanos (malware)
Recopilación de información	Ingeniería Social, Suplantación de Identidad, Detección de Vulnerabilidades
Ataques de Autenticación	Exploits, fuerza bruta
Acceso no autorizado	Robo de información, Alteración de Información
Denegación de Servicios	Ataques DoS, DDoS
Intentos de Intrusión	Explotación de Vulnerabilidades, Intento de acceso a sistemas
Contenido abusivo	Acoso

Mal uso de Recursos Tecnológicos	Violación a las Políticas

Reporte de Incidentes de Seguridad

La comunidad objetivo del CSIRT-UTN deberá conocer el procedimiento para el reporte de incidentes de seguridad informáticos, el cual se detalla a continuación:

- Una vez identificado un incidente de seguridad informática, este deberá ser reportado a través del correo csirt.utn@gmail.com, o a su vez a través de la página web del CSIRT-UTN en la cual se deberá llenar los campos que se piden tal y como se muestra en el siguiente formulario. Para el reporte del incidente, la persona quien reporta, deberá incluir información como: nombres completos, correo electrónico, teléfono de contacto, área afectada, activo(s) de información afectados por el incidente, fecha de detección del incidente, descripción del incidente

- La persona que reporta un incidente de seguridad informática recibirá una respuesta por correo electrónico con el número de ticket correspondiente al incidente para su seguimiento.
- Una vez que se resuelva el incidente, la persona que reportó el mismo, será notificada.

Respuesta a incidentes de Seguridad Informática

- Una vez recibido el incidente reportado a través del Técnico de Soporte del DDTI, éste revisará y analizará el incidente, en caso de que el incidente conste dentro de la matriz de categorización de incidentes, el mismo será escalado al CSIRT-UTN.

- Cuando el CSIRT-UTN, recibe el escalamiento del incidente, el Equipo de Respuesta a Incidentes de Seguridad Informática realizará el proceso de gestión de incidentes, el cual consta de registro del incidente, triage, análisis y cierre del mismo.
- Una vez que se cierra el incidente, este deberá ser notificado a quién lo reportó.

5. INCUMPLIMIENTO

En caso de incumplimiento de la presente política tendrá la aplicación de sanciones ya sea administrativas o legales teniendo en cuenta la magnitud y el aspecto no cumplido.

6. VALIDEZ

Este documento entrará en vigencia y será válido desde su aprobación. El CSIRT-UTN es el propietario de este documento y por lo tanto será el encargado de verificar la efectividad del mismo.

REFERENCIAS

2700, I. (s.f.). *ISO 27000.ES.* Obtenido de ISO 27000.ES: https://www.iso27000.es/iso27002.html

Política de Seguridad de la Información del CSIRT-UTN

UNIVERSIDAD TÉCNICA DEL NORTE

CSIRT – UTN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código	DDTI-CSIRT-PSI-UTN-01
Versión	1.0
Fecha de la versión	03 de marzo de 2020
Creado por	Jonathan Mera
Aprobado por	

Fecha de aprobación:

Historial de modificaciones

Fecha	Versión	Elaborado por	Descripción de la modificación
03-03-2020	1.0	Jonathan Mera	Elaboración de política

Contenido

1. OBJETIVO

Establecer los lineamientos y procedimientos que permitan brindar protección a la información del CSIRT académico de la UTN y sus recursos tecnológicos.

2. ALCANCE

La presente política aplica a todos los tipos de información independientemente de su formato, ya sea documentos electrónicos, en papel, base de datos, aplicaciones y la comunidad de la UTN.

3. ROLES Y RESPONSABILIDADES

Responsable: Corresponde al jefe del DDTI, la responsabilidad de implementar la presente política dentro del CSIRT académico de la UTN

Administrador del CSIRT: Es el encargado de verificar que se cumpla con la presente política, dando a conocer su incumplimiento

4. POLÍTICA

A continuación, se describen las políticas por las que estará regido el CSIRT de la UTN:

Seguridad Física: Dado que el equipo CSIRT estará en las mismas instalaciones físicas del DDTI de la UTN, contará con similares medidas de seguridad, entre las que se incluyen: bitácora de registros de acceso, acceso biométrico controlado, circuito cerrado de televisión.

Plan de Respaldos y Recuperación: Todas las configuraciones y archivos ejecutables de cada uno de los sistemas que se utilicen para la operación del CSIRT, serán respaldados semanalmente en un repositorio externo previamente establecido, a cargo del Administrador del Servicio de CSIRT. De forma similar todos los registros de eventos, alarmas, incidentes y

correos que se hayan generados serán respaldados de forma diaria teniendo en cuenta la Política de Protección de la Información.

En caso de un algún problema con la operación de un sistema o que se requiera tener acceso a un histórico de registros, se deberá solicitar la información al administrador del CSIRT UTN.

Seguridad de Red Local: La seguridad de la red local de las instalaciones del CSIRT estarán regidas por las mismas condiciones de seguridad del DDTI.

Seguridad de Información Local: Toda la información generada o recibida como parte de una alerta, reporte de incidente o caso de incidente deberá ser clasificada y manejada con mucho sigilo y únicamente por personal autorizado.

Manejo de Incidentes: Una vez que se genere un reporte de incidentes por parte del equipo de analistas del DDTI, estos serán escalados al equipo CSIRT-UTN para su debido manejo. Solamente el equipo CSIRT-UTN estará autorizado para poder realizar un análisis a profundidad, aplicar acciones de remediación, solicitar información adicional y escalar con las entidades externas (si así se requiere).

5. INCUMPLIMIENTO

En caso de incumplimiento de la presente política tendrá la aplicación de sanciones ya sea administrativas o legales teniendo en cuenta la magnitud y el aspecto no cumplido.

6. VALIDEZ

Este documento entrará en vigencia y será válido desde su aprobación. El CSIRT-UTN es el propietario de este documento y por lo tanto será el encargado de verificar la efectividad del mismo.

REFERENCIAS

2700, I. (s.f.). *ISO 27000.ES*. Obtenido de ISO 27000.ES: https://www.iso27000.es/iso27002.html

Apéndice O Ficha de entrevista con el Administrador de Red del DDTI

FICHA BIBLIOGRÁFICA DE ENTREVISTA CON EL ADMINISTRADOR DEL DEPARTAMENTO DE DESARROLLO TECNOLÓGICO E INFORMÁTICO (DDTI)

Entrevista de socialización de resultados obtenidos de encuestas aplicadas a la comunidad de la Universidad Técnica del Norte, para la obtención de la situación actual de la seguridad informática en la UTN.

Fecha: 23 de noviembre 2020

Nombre entrevistado: Ing. Vinicio Guerra

Cargo: Administrador de Red del DDTI

Durante la entrevista, se dio a conocer el análisis FODA, como resultado de entrevistas anteriores con el Ing. Vinicio Guerra y resultados de encuestas realizadas al personal administrativo, docentes, estudiantes que fueron realizadas en el trabajo de titulación "Diseño de un Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT) académico en la UTN", teniendo su aceptación del mismo, además se socializó el diagnóstico de Gestión de Incidencias informáticas en la UTN, matriz de riesgos informáticos, matriz RACI, matriz PAM, los cuales fueron resultado de las encuestas, y la estructura organizacional.

Como resultado de la entrevista se obtuvo la aceptación y confirmación de estos resultados.

Medio: La entrevista fue realizada mediante la herramienta de video conferencias ZOOM, la misma que se encuentra grabada.

Firmado electrónicamente por:
EDWIN VINICIO
GUERRA MORALES

Ing. Vinicio Guerra
Administrador de Red DDTI

Jonathan Mera
Tesista

Apéndice P Ejemplo de Propuesta Para Análisis de Vulnerabilidades

UNIVERSIDAD TÉCNICA DEL NORTE

DEMO DE FUNCIONAMIENTO CSIRT ACADÉMICO UTN

ANÁLISIS DE VULNERABILIDADES CON NMAP Y MONITOREO DE RED CON NAGIOS A LOS SERVIDORES DEL DATA CENTER DE LA FICA

INTRODUCCIÓN

El objetivo principal del análisis de vulnerabilidades, consiste en enumerar las vulnerabilidades que se presentan en las diferentes aplicaciones, servidores o sistemas de una organización, para este análisis de vulnerabilidades se sigue la metodología según (Romero Castro et al., 2018), en el que establece como primer paso para el análisis de vulnerabilidades, la realización del acuerdo de confidencialidad, ya que la información obtenida como proceso del análisis, debe ser tratada con sigilo, luego de esto es importante establecer las directrices a ser realizadas dentro del análisis, estableciendo los límites a seguir, el siguiente paso es la recolección de información del objetivo a ser analizado, una vez que se tiene la información se procede a realizar el respectivo análisis de vulnerabilidades para concluir con la documentación en la cual se presenta un informe además este análisis es realizado por personal que pertenece a la organización, la finalización del análisis de vulnerabilidades consiste en la entrega de un informe técnico, en el cual se enumera las vulnerabilidades e identifica los posibles procesos de remediación. Es importante recalcar que existe diferencia entre el análisis de vulnerabilidades, un pentesting o hacking ético, estos dos últimos, llevan una o varias metodologías de realización y necesita de personal especializado, además que estos servicios no solo se encargan de descubrir las vulnerabilidades, también se encargan de explotar las vulnerabilidades encontradas.

Para el análisis de vulnerabilidades se utilizan dos herramientas la primera es Nmap, la cual es una herramienta, que permite escanear redes, puertos y servicios, brindando información del estado de los puertos, sistema operativo, hosts activos, permitiendo explorar vulnerabilidades y detectar redes y por otro lado se usará Nagios, la cual es una herramienta que permite monitorear equipos y servidores, esta

herramienta permite obtener información del estado de la red, procesos que corren, servicios, carga de la CPU y memoria, espacio de almacenamiento, con esta información da a conocer la presencia de problemas que puedan ocurrir en la red, para ello es importante el uso del protocolo SNMP (Simple Network Management Protocol) y NRPE (Nagios Remote Plugin Executor), los cuales permiten la gestión de diferentes dispositivos de la red.

CSIRT - UTN	**Documento:** Análisis de Vulnerabilidades	**Tratamiento: Pruebas**
Tipo de Documento: Propuesta de Análisis de Vulnerabilidades	**Autor:** Jonathan Mera	**Fecha:** 25-10-2020

ANÁLISIS DE VULNERABILIDADES Y MONITOREO DE RED

CLIENTE	Data Center FICA
UBICACIÓN	Universidad Técnica del Norte – Ibarra
CONTACTO	Ing. Mauricio Domínguez
CORREO	hmdominguez@utn.edu.ec

ACUERDO DE CONFIDENCIALIDAD

Toda información que se obtenga por efectos del análisis de vulnerabilidades será utilizada solo con fines informativos, por tanto, la persona encargada de realizar el análisis de vulnerabilidades y monitoreo de red se compromete a no divulgar o revelar bajo ningún motivo o circunstancia la información obtenida, además no podrá utilizar dicha información para propio beneficio o a terceras personas.

Servicios a brindar	**Análisis de Vulnerabilidades y monitoreo de red con NAGIOS**

Conceptos:

- **Análisis de Vulnerabilidades**: Servicio que permite identificar si las aplicaciones, software o sistemas de una organización presentan vulnerabilidades de seguridad. Este servicio se lo realiza mediante un escaneo automatizado.
- **Vulnerabilidad**: Es un defecto en un sistema informático el cual puede ser explotado por un atacante.
- **Modalidad caja blanca:** El responsable de realizar el análisis de vulnerabilidades posee una visión total de la red que va a ser analizada.
- **Modalidad caja negra:** El responsable de realizar el análisis de vulnerabilidades, solo posee información de acceso a la red

OBJETIVO GENERAL:

Realizar el análisis de vulnerabilidades y monitoreo a los servidores OPINA y Reactivos mediante el uso de la herramienta NMAP y nagios para monitoreo de servidores lo cual permitirá observar el funcionamiento básico de un CSIRT

OBJETIVOS ESPECÍFICOS:

- Obtener información acerca de los servidores OPINA y Reactivos para poder realizar el análisis de vulnerabilidades en modalidad caja blanca.
- Buscar vulnerabilidades en los servidores OPINA, Reactivos y Revista Universitaria mediante NMAP.
- Realizar el monitoreo a servidores mediante la herramienta nagios, con la cual permitirá conocer si presentan alguna vulnerabilidad.
- Redactar un informe con los resultados obtenidos del análisis de vulnerabilidades

Descripción:

Realizar una evaluación rápida a los servidores OPINA y Reactivos para la identificación de posibles vulnerabilidades, y poder emitir un informe de los resultados obtenidos.

Alcance:

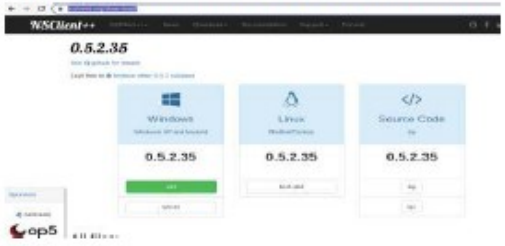
El análisis de vulnerabilidades y monitoreo de red se realizará en el Data Center de la FICA, a los servidores y dispositivos de red, el método a usar será el de caja blanca, por lo que es importante obtener información necesaria de los servidores antes mencionados
Tiempo estimado:
5 días

	LEVANTAMIENTO DE INFORMACIÓN	DETALLE
1	El análisis será interno o externo	Interno
2	Indicar la modalidad del Análisis de Vulnerabilidades	El análisis será de tipo caja blanca, por tanto, es importante dar a conocer al auditor toda la información necesaria
3	Indicar la cantidad de IPs, tipo de dispositivos, funcionalidad	Es importante dar a conocer el direccionamiento IP, y las funciones que cumplen cada servidor
4	El informe consta de resumen y las vulnerabilidades encontradas	El informe constará de las vulnerabilidades encontradas

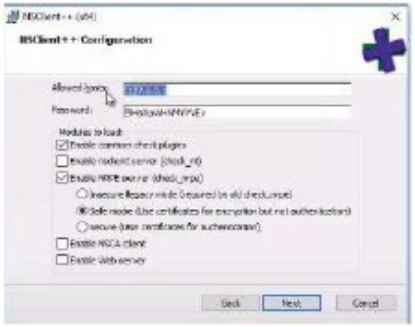
N°	ACTIVIDAD	SI	NO	RESPONSABLE	DETALLE
1	Obtener información de los servidores OPINA y Reactivos (Direccionamiento IP, funcionalidad)			Encargado Data Center FICA	Es necesario proporcionar esta información, ya que la modalidad del Análisis de Vulnerabilidades es de tipo caja blanca
2	Escaneo de direcciones IP activas **Comando a utilizar:** nmap -sP <RED>/subred			Tesista	-**sP**: sondeo Ping. -**O**: Activar la detección de sistema operativo. -sS: Análisis TCP SYNYConnect/ACK. -**A**: Detección de SO y versión. -**sV**: Sondea puertos abiertos para obtener información de los servicios y la versión. -**f**: fragmentar paquetes. -oN: guardar el escaneo enn formato
3	Obtención del SO **Comando a utilizar:** nmap -O **IP**			Tesista	
4	Escaneo de SO y servicios **Comando a utilizar:** **Nmap -A IP**			Tesista	
5	Obtener versión de los servidores **Comando a utilizar:** **nmap -sV IP**			Tesista	
6	Búsqueda de vulnerabilidades conocidas **Comando a utilizar:** **nmap -f –script vuln IP**			Tesista	
7	Comprobar existencia de usuarios con contraseñas vacías **Comando a utilizar:** **nmap -f -sS –script auth/default IP**			Tesista	
8	Obtener información de red **Comando a utilizar:** **nmap -f –script safe IP**			Tesista	
9	Guardar información del scaneo Comando a utilizar: nmap **-oN <NombredelArchivo.txt> IP**			Tesista	
10	Análisis de vulnerabilidades encontradas			Tesista	
11	Monitoreo de servidores con Nagios			Tesista	
12	Ver configuración de SNMP en Windows Server **Comando a utilizar: Get-WindowsCapability -Online -Name "SNMP*"**				En caso de no estar instalado y configurado SNMP en Windows Server, regirse a manual
13	Instalar RNPE en Linux				
14	Instalar y configurar SNMP en Windows Server			Tesista / Encargado del Data Center FICA	Es importante trabajar conjuntamente con el responsable del Data Center, ya que de ser necesario la instalación y configuración del cliente SNMP, el encargado deberá proporcionar las credenciales. Se adjunta comandos y procedimiento para la instalación de SNMP en Windows. Es importante aclarar que este procesos se lo realizará en caso de existir un servidor con Sistema Operativo Windows
15	Instalar y configurar NRPE en servidor LINUX			Tesista / Encargado del Data Center FICA	Para la instalación de NRPE es necesario trabajar conjuntamente con el responsable del Data Center, debido a que es necesario acceder al servidor LINUX para la instalación de este complemento de NAGIOS que permite la monitorización del servidor
16	Agregar Servidores a ser monitoreados en NAGIOS				Configurar para que se pueda monitorear el/los servidores
17	Informe final			Tesista	El informe presentará los siguientes parámetros: • Nombre de vulnerabilidad • Fecha de descubrimiento • Descripción de la vulnerabilidad • Posible remediación

PASOS A SEGUIR PARA CONFIGURAR SNMP EN WINDOWS

1. Descargar cliente NSClient++ de https://nsclient.org/download/

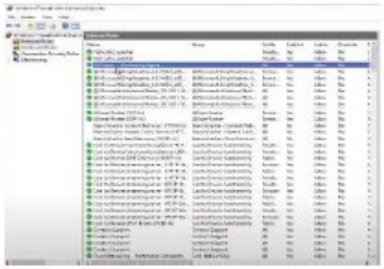


2. ejecutar instalador → genérico → Typical



- Allowed hosts: colocar ip de servidor Nagios
- colocar contraseña para mayor seguridad
- marcar las 3 primeras casillas, Insecure legacy. Enable NSCA client, Enable Web server

3. instalar
4. verificar estado en Firewall, reglas de entrada y salida



5. En el servidor Nagios ingresar al directorio cd /usr/local/nagios/etc/objects/

```
root@nagios:/usr/local/nagios/etc/objects# ls
commands.cfg   localhost.cfg   switch.cfg      timeperiods.cfg
commands.cfg~  localhost.cfg~  switch.cfg~     timeperiods.cfg~
contacts.cfg   printer.cfg     templates.cfg   windows.cfg
contacts.cfg~  printer.cfg~    templates.cfg~  windows.cfg~
```

6. editar archivo windows.cfg, y colocar el nombre del host_name, alias, y address

```
define host {

    use                     windows-server          ; Inherit default values from a template
    host_name               WINDOWS10               ; The name we're giving to this host
    alias                   ALEJO                   ; A longer name associated with the host
    address                 192.168.0.102           ; IP address of the host
}
```

7. Cambiar en todos los servicios definidos el host_name
8. Dirigirse al directorio cd /usr/local/nagios/etc/

```
root@nagios:/usr/local/nagios/etc/objects# cd /usr/local/nagios/etc/
root@nagios:/usr/local/nagios/etc# ls
cgi.cfg   htpasswd.users  nagios.cfg~  resource.cfg
cgi.cfg~  nagios.cfg      objects      resource.cfg~
```

9. Editar archivo nagios.cfg y descomentar

```
# Definitions for monitoring a Windows machine
cfg_file=/usr/local/nagios/etc/objects/windows.cfg
```

10. Reiniciar el servicio nagios systemctl restart nagios
11. Editar en Windows Server el archivo nsclient.ini

- colocar IP del servidor Nagios

```
; Undocumented key
allowed hosts = 192.168.1.244
```

- Activar lo siguiente

12. Guardar

Ingresar a servicios → NSClient → clic derecho y reiniciar

INSTALACIÓN NRPE EN LINUX

1. Descargar NRPE con el siguiente comandowget https://github.com/NagiosEnterprises/nrpe/releases/download/nrpe-3.2.1/nrpe-4.0.3.tar.gz
2. Descomprimir tar xf nrpe-4.0.3.tar.gz
3. Ingresar al directorio cd nrpe-4.0.3/
4. Configurar la compilación ./configure
5. Compilar make nrpe
6. Crear el usuario y grupo con el que va a correr NRPE sudo make install-groups-users
7. Iniciar el script del servicio sudo make install-daemon
8. Instalar los archivos de configuración sudo make install-config
9. Instalar los scripts que permitirán el manejo del servicio nrpe sudo make install-init
10. Iniciar el servicio sudo systemctl start nrpe
11. Comprobar el estado systemctl status nrpe
12. Escribir el siguiente comando para que el servicio siempre esté disponible sudo systemctl enable nrpe
13. Configurar el servidor a cliente a NAGIOS

Referencias

Castro, M. I. R., Morán, G. L. F., Navarrete, D. S. V., Cruzatty, J. E. Á., Anzúles, G. R. P., Mero, C. J. Á., Quimiz, Á. L. M., & Merino, M. A. C. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES (1.a ed.) [Libro electrónico]. 3Ciencias. https://doi.org/10.17993/IngyTec.2018.46

Nmap.org. (s. f.). Guía de referencia de Nmap (Página de manual). Recuperado 13 de abril de 2020, de https://nmap.org/man/es/

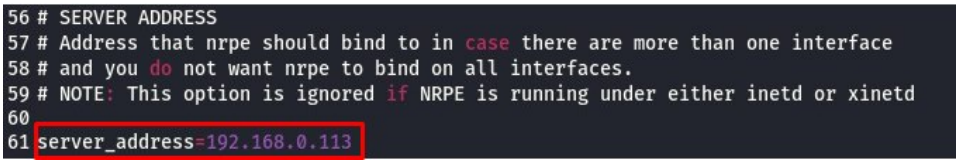
Apéndice Q Configuraciones Importantes en Nagios

Dentro de este apartado, se presentan las configuraciones importantes que se debe realizar tanto en el host monitoreado, como en el servidor Nagios, dicho en otras palabras, el host monitoreado viene a ser el equipo cliente, y Nagios el servidor de monitoreo.

Primeramente, para la monitorización de un servidor Linux (host), es necesario la instalación del plugin NRPE, este plugin es un agente que permite la ejecución de scripts para el chequeo de servidores remotos, para ello es necesario la configuración del archivo nrpe.cfg en el servidor Linux, teniendo en cuenta dos configuraciones, la primera corresponde a la asignación de la IP del host monitoreado, y la IP de Nagios, siendo así en la figura Q1 se presenta el establecimiento de la dirección IP del servidor a ser supervisado, para lo cual en la línea 61, en server_address se establece la dirección IP 192.168.0.113, siendo la IP del servidor Linux.

Figura Q1

IP del Servidor Monitoreado



Ahora bien, dentro de este archivo de configuración nrpe.cfg hay que ingresar también la IP correspondiente al servidor Nagios, como se señala en la figura Q2, para ello en la línea 106, en allowed_hosts se ingresa la dirección IP 192.168.0.112.

Figura Q2

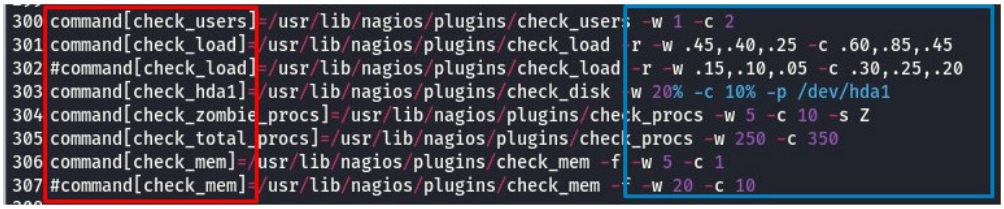
Establecimiento de IP de Nagios

Además, otro aspecto importante dentro del archivo de configuración nrpe se indica en la figura Q3, en la cual están establecidos los comandos y parámetros de los servicios que se puede monitorizar, en este archivo se puede configurar los parámetros con los cuales pueda generar las alertas del equipo que se está monitorizando. Lo que se encuentra dentro del rectángulo de color rojo son los comandos que hacen referencia a los servicios que pueden ser monitorizados, y lo que se encuentra dentro del rectángulo de color azul son los parámetros que se pueden ajustar de acuerdo a las necesidades para generar alertas.

En este sentido se tiene la posibilidad de chequear el número de usuarios (check_users), carga de procesador (check_load), disco duro (check_hda1), procesos zombies (check_zombie_procs), total de procesos (check_total_procs), memoria (check_mem), ahora bien, junto a estos comandos se encuentran los parámetros que pueden ser configurados para que generen alertas o advertencias, para ello se puede establecer los parámetros junto a las letras w (Warning) o c (Critical).

Figura Q3

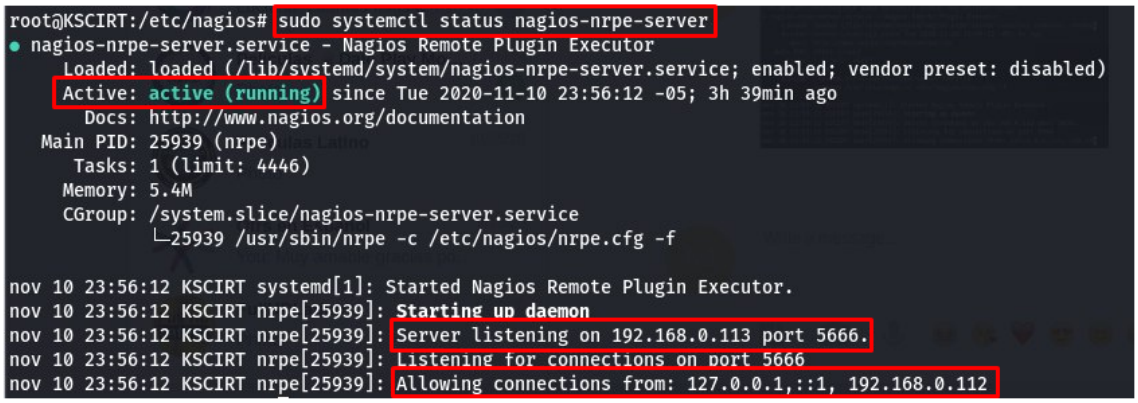
Servicios y Parámetros de Monitorización de Nagios



De forma que, una vez establecidos los parámetros a monitorizar, es importante comprobar que el servicio NRPE está corriendo en el servidor Linux que será monitoreado con Nagios, para ello se hace uso del comando systemctl status nagios-nrpe-server como se indica en la figura Q4, presentando información como la IP y puerto del servidor cliente, la IP del servidor agente, y el estado del plugin NRPE como activo.

Figura Q4

Estado de NRPE en Servidor Linux



Configuraciones en Servidor Nagios

Para poder monitorear equipos de una red con Nagios, es importante antes de la instalación, tener instalado un servidor web Apache con PHP, después proceder con la instalación de nagios y de los plugins que van a permitir la monitorización de los servicios y equipos, y finalmente se procede a instalar NRPE, en la figura Q5 se presenta el archivo de configuración denominado commands.cfg, en el cual se define mediante comandos los recursos y servicios que van a ser monitoreados con NRPE. Este comando contiene la ubicación en la cual están presentes los servicios que se pueden monitorizar, la dirección IP y los argumentos, que viene hacer los parámetros de monitorización. De manera que los servicios que se puede monitorear se presentan en la figura Q6 y en la tabla Q1 se menciona de manera detallada algunos de estos plugins.

Figura Q5

Inserción de Comandos en el Servidor Nagios Para la Comunicación de NRPE

```
# .check_nrpe. command definition
define command{
command_name check_nrpe
command_line /usr/local/nagios/libexec/check_nrpe -H $HOSTADDRESS$ -t 30 -c $ARG1$
}
```

Figura Q6

Servicios que Pueden ser Monitorizados en los Servidores

```
root@nagiosdebian:/usr/local/nagios/libexec# ls
check_apt       check_icmp          check_nntps     check_spop
check_breeze    check_ide_smart     check_nrpe      check_ssh
check_by_ssh    check_ifoperstatus  check_nt        check_ssl_validity
check_clamd     check_ifstatus      check_ntp       check_ssmtp
check_cluster   check_imap          check_ntp_peer  check_swap
check_dbi       check_ircd          check_ntp_time  check_tcp
check_dhcp      check_jabber        check_nwstat    check_time
check_dig       check_ldap          check_oracle    check_udp
check_disk      check_ldaps         check_overcr    check_ups
check_disk_smb  check_load          check_pgsql     check_uptime
check_dns       check_log           check_ping      check_users
check_dummy     check_mailq         check_pop       check_wave
check_file_age  check_mrtg          check_procs     negate
check_flexlm    check_mrtgtraf      check_real      remove_perfdata
check_fping     check_mysql         check_rpc       urlize
check_ftp       check_mysql_query   check_sensors   utils.pm
check_game      check_nagios        check_simap     utils.sh
check_http      check_nntp          check_smtp
```

Tabla Q1

Detalle de Plugins de Nagios

Plugins de Nagios	Descripción
check_apt	Busca actualizaciones de software
check_breeze	Información de la intensidad de la señal de un equipo inalámbrico Breezecom
check_by_ssh	Utiliza SSH para la ejecución de comandos en un host remoto
check_dhcp	Realiza la comprobación de la disponibilidad de servidores DHCP en la red
check_disk	Verifica la cantidad de espacio en el disco en un sistema de archivos montado

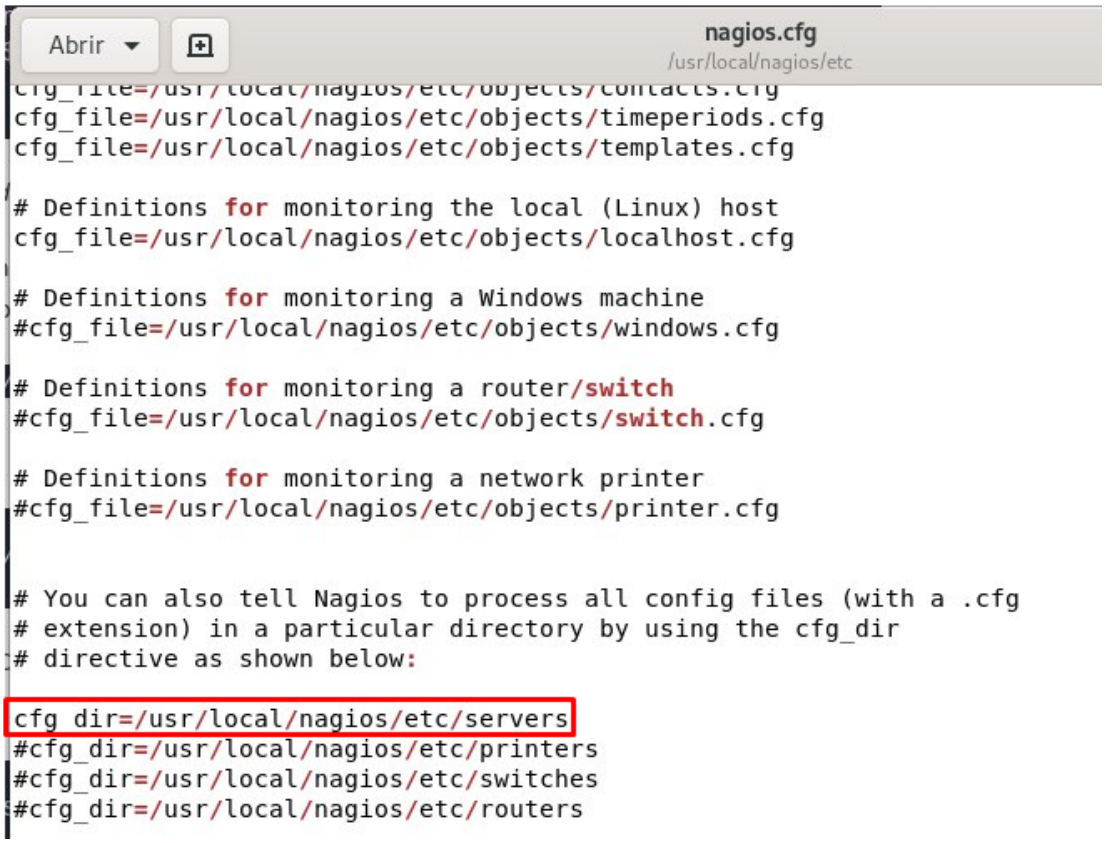
check_dns	Este complemento usa nslookup para la obtención de una dirección IP para consultar el dominio
check_ftp	Prueba las conexiones FTP con un host especifico
check_mysql	Realiza pruebas de conexión a un servidor MySQL
check_nagios	Realiza la verificación del estado del proceso de Nagios en la máquina local
check_smtp	Realiza conexiones SMPT con el host
check_users	Verifica la cantidad de usuarios conectados a un equipo
check_ping	Utiliza ping para comprobar la conexión con el equipo cliente

Fuente: (atlantixlab, 2015)

Para tal efecto, Nagios permite monitorizar servidores, routers, switches, equipos con sistema operativo Windows y Linux, para ello es necesario activar los directorios que permiten la monitorización, para lo cual en el archivo de configuración principal denominado nagios.cfg es necesario activar la respectiva línea que hace mención al dispositivo que se desea monitorear, como ejemplo en la figura Q7, se presenta la activación del directorio de servidores, para ello se procede a quitar el símbolo #.

Figura Q7

Activación de Directorio para Monitorear Servidores



Por lo tanto, una vez activado el directorio que permite monitorizar los diferentes equipos en una red es importante crear un archivo de configuración en el cual se agrega el servidor y los servicios que van a ser monitoreados, en la figura Q8, se presenta el archivo de configuración que se utilizó para las pruebas.

En efecto, este archivo de configuración contiene la dirección IP del servidor que está siendo monitoreado, la definición de los componentes como carga del CPU, el número de usuarios conectados al servidor, el número de procesos que se ejecutan y el consumo de memoria RAM, en cada uno de estos servicios se puede configurar el intervalo de tiempo que se desea monitorear, para este caso se toma datos cada minuto.

Ahora bien, de manera más explícita, el archivo de configuración, primeramente, contiene la definición del host (define host), en el cual se inserta información del nombre de

la plantilla (use), el nombre del host (host_name), un alias (alias), la dirección IP (address), el número de chequeos antes de notificar los errores (max_check_attempts), intervalo de notificaciones en segundos (notification_interval), y el periodo de monitorización (notification_period).

En segundo lugar, se tiene la definición del grupo, este parámetro permite identificar el equipo que se monitoriza, para ello presenta información como el nombre asignado (hostgroup_name), una descripción de identificación (alias) y los miembros de este grupo (members).

Y finalmente se define los servicios que se van a monitorear, para ello se define información como el nombre de la plantilla (use), el nombre del host (host_name), una descripción del servicio (service_description) que será el nombre que aparecerá en la interfaz de administración, se hace el llamado al comando (check_command), y el intervalo de monitorización (check_interval).

Figura Q8

Archivo de Configuración del Servidor Monitoreado

Abrir

cliente.cfg
/usr/local/nagios/etc/servers

```
define host {
        use                     linux-server
        host_name               servidorlinux
        alias                   servidorlinux
        address                 192.168.0.113
        max_check_attempts      5
        check_period            24x7
        notification_interval   2
        notification_period     24x7
}



define hostgroup{

            hostgroup_name          linux-server
            alias                   Linux Servers
            members                 servidorlinux
}
define service{

             use                        generic-service
             host_name                  servidorlinux
             service_description        PING
             check_command              check_ping!200.0,20%!600.0,60%
             check_interval             1

}

define service{

             use                        generic-service
             host_name                  servidorlinux
             service_description        CARGA CPU
             check_command              check_nrpe!check_load
             check_interval             1

}
define service{

             use                        generic-service
             host_name                  servidorlinux
             service_description        PROCESOS
             check_command              check_nrpe!check_total_procs
             check_interval             1

}


define service{

             use                        generic-service
             host_name                  servidorlinux
             service_description        RAM
             check_command              check_nrpe!check_mem
             check_interval             1

}


define service{

             use                        generic-service
             host_name                  servidorlinux
             service_description        Current Users
             check_command              check_nrpe!check_users
             check_interval             1

}
```

Apéndice R Configuraciones Importantes en OTRS

Para comprender las configuraciones del sistema de tickets OTRS es importante tener presente las siguientes definiciones, la primera, hace referencia a las colas en OTRS, que viene a ser el destino de los tickets, y agentes, que son los técnicos encargados de brindar soluciones a los tickets de incidencias reportados por los usuarios.

Dentro de las configuraciones importantes de la herramienta de tickets, en primer lugar, se presenta, la creación de la cola, en la cual se almacenarán todos los correos de los incidentes reportados, es decir, cualquier correo enviado a la dirección de correo de OTRS llega a la cola denominada Mesa de Servicios CSIRT UTN, de esta cola, serán derivados los tickets según la cantidad y nivel de criticidad a los técnicos de soporte (agentes).

Ahora bien, el proceso para la creación de colas en OTRS, es el siguiente, como primer paso es ingresar a la cuenta de administrador, seguido de eso, dirigirse en la parte superior en el apartado Admin, e ingresar en colas, como se muestra en la figura R1, posterior a esto se accede a la opción añadir cola, que se encuentra en el panel izquierdo como se indica en la figura R2, y finalmente se rellenan los campos correspondientes a nombre, para este caso es Mesa de Servicios CSIRT UTN, se le asigna al grupo admin, es necesario ingresar el correo de OTRS, así como una plantilla de saludo y firma que posteriormente se indica el proceso de edición de las mismas y se guarda toda la información ingresada, estos pasos se ponen en manifiesto en la figura R3.

Figura R1

Acceso a panel de administración para crear colas

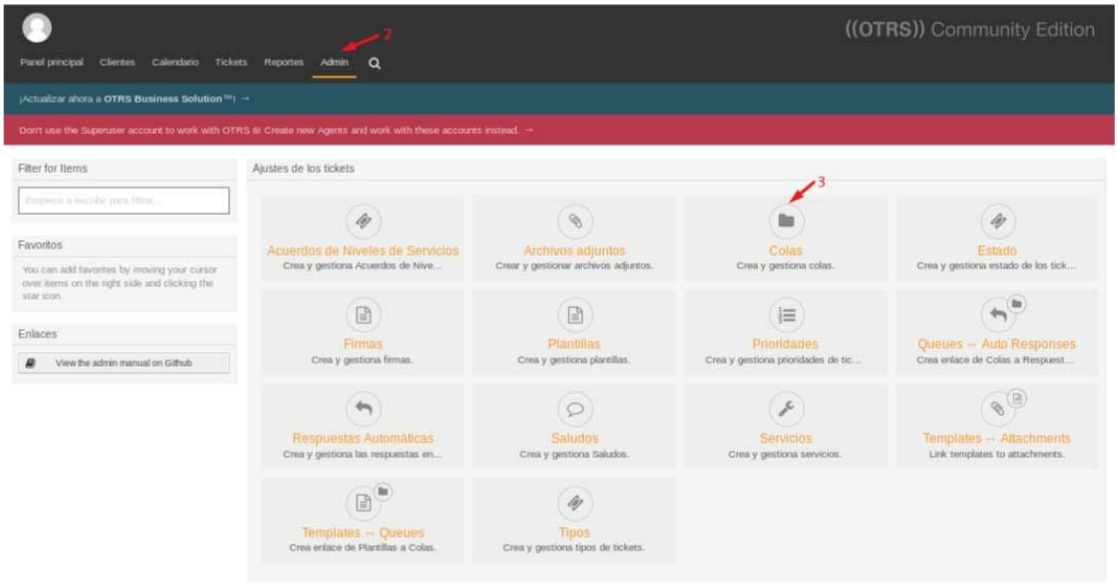


Figura R2

Agregar Cola

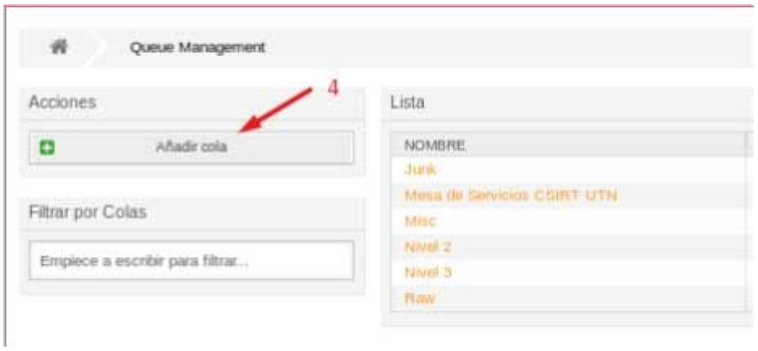
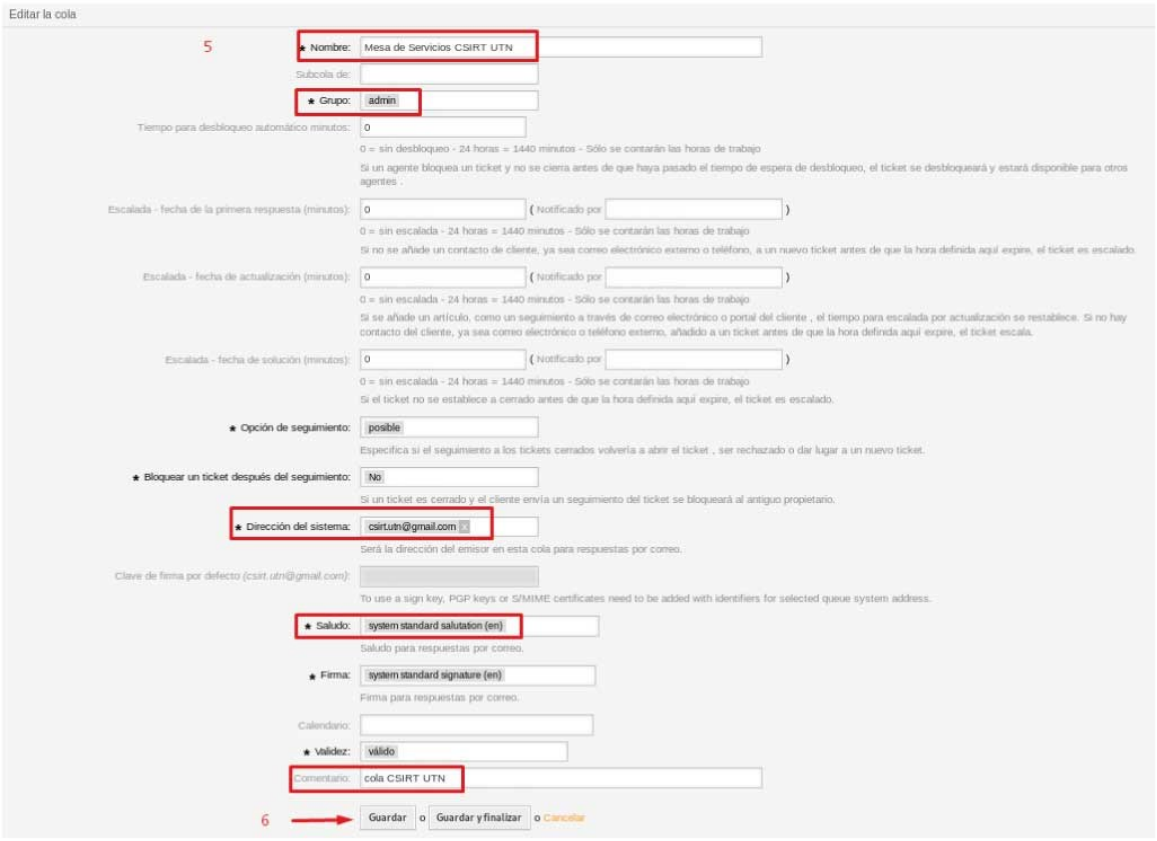


Figura R3

Configuración de Cola para la Recepción de Tickets



En este sentido, dentro del panel de administración se tiene la opción de personalizar firmas, respuestas automáticas y saludos, como se indica en la figura R4. En consecuencia, para la configuración de firmas existe dos opciones la de añadir firma o editar la plantilla de OTRS, en este caso se opta por la edición de la plantilla existente, para ello se accede a la opción de firmas, seguido se ingresa en la plantilla y se procede a la edición, en la figura R5 se señala dicho proceso. Por otro lado, para la edición de saludos, de igual manera es necesario ingresar en dicha opción y se edita el saludo, como se indica en la figura R6.

Por último, se edita la respuesta automática, que se genera cuando un usuario reporta un incidente a la mesa de ayuda del CSIRT académico de la UTN, el cual es enviado al correo. Dentro de esta configuración, se establece el nombre que se asigna a esta respuesta, el asunto,

en el cual genera de manera automática un número de ticket, el texto de la respuesta, y el correo correspondiente a la mesa de ayuda, para ello ingresar en la opción de respuesta automática, y seguido de eso seleccionar la plantilla que hace referencia a respuesta automática, como se puede observar en la figura R7.

Figura R4

Configuración de Firmas, Respuestas Automáticas y Saludos

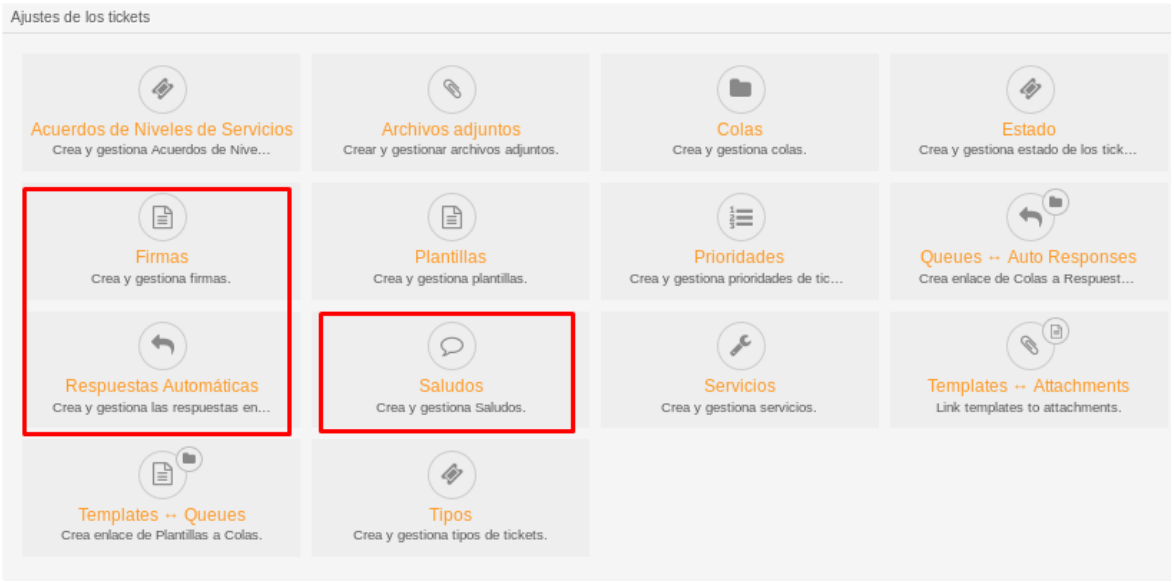


Figura R5

Edición de Firmas

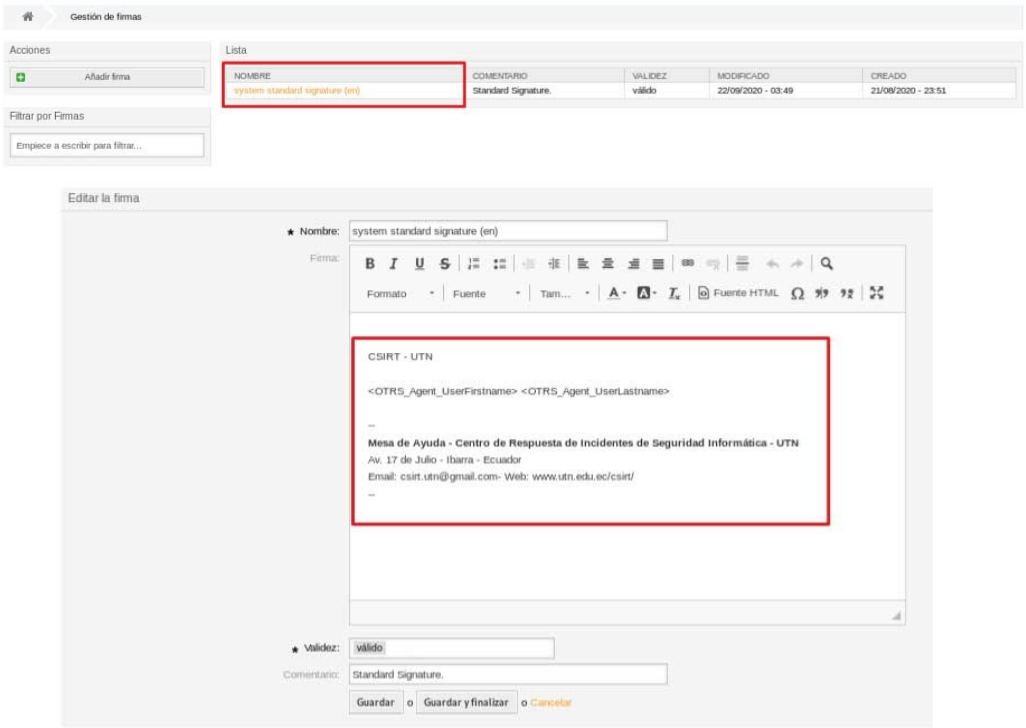


Figura R6

Edición de Saludo

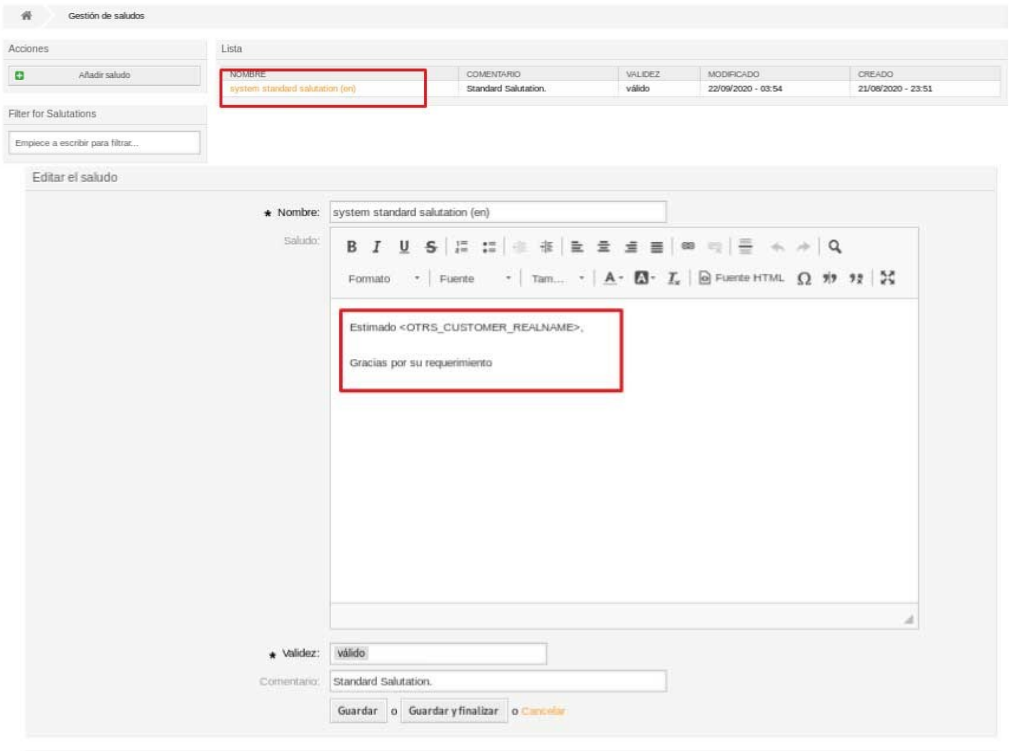
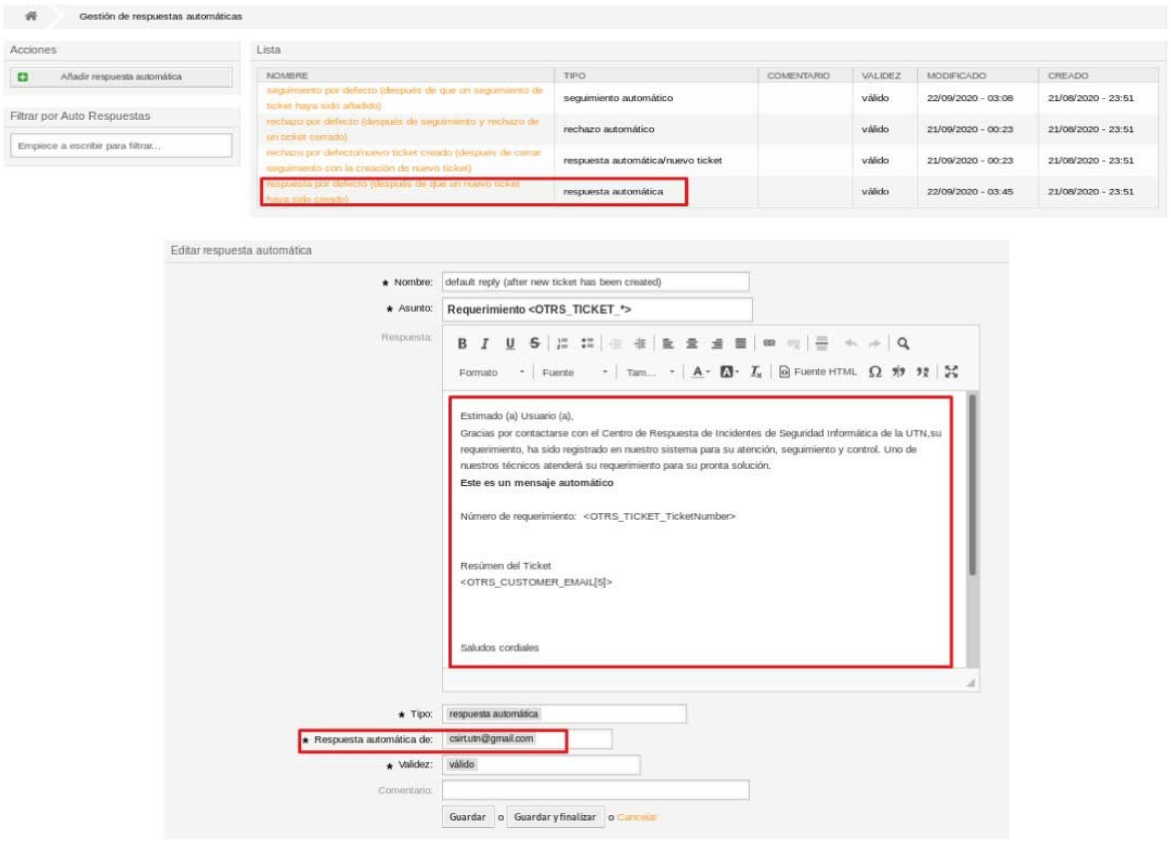


Figura R7

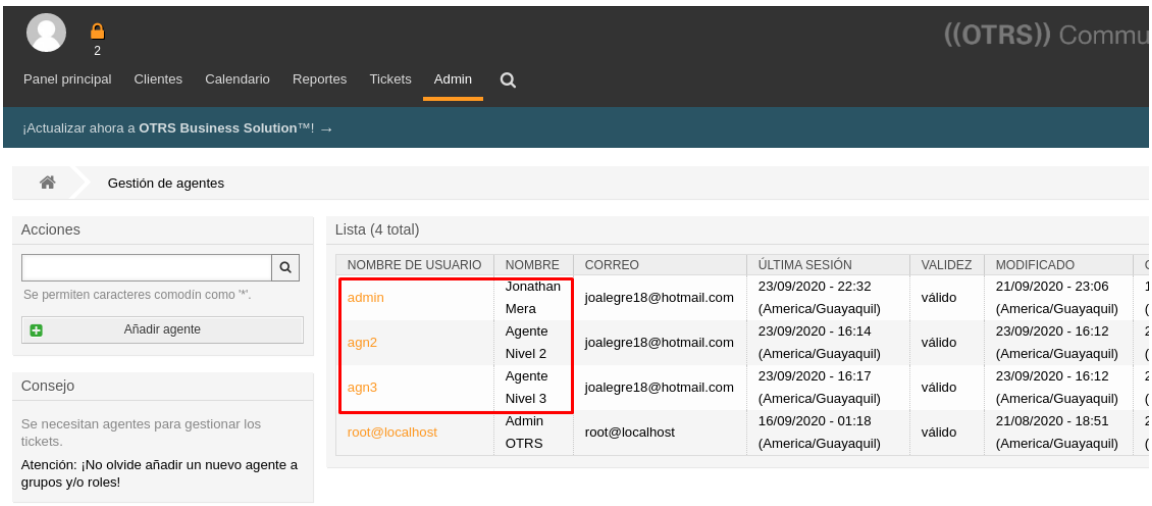
Configuración de Respuesta Automática



Pasando a otro aspecto, otra de las configuraciones se presenta en la figura R8, y corresponde a la creación de agentes, que son los encargados de brindar una solución a los incidentes reportados, en este caso se crearon 3 agentes, el primer agente es denominado admin, quien es el encargado de receptar y derivar los tickets, el segundo agente como “agn2” que es el técnico de soporte de nivel 2 y el tercer agente “agn3” que es el técnico de soporte de nivel 3.

Figura R8

Creación de Agentes OTRS



De manera que el procedimiento para la creación de agentes, se señala en la figura R9, para ello en el panel de administración se accede al apartado denominado Users, Groups & Roles, y se selecciona la opción agentes. Una vez seleccionado la opción de Agentes, se escoge la opción de añadir agentes, como se presenta en la figura R10, posterior a eso se procede a editar la cuenta del agente, ingresando el nombre y apellido, nombre de usuario, contraseña y el correo del agente, y como último paso se guarda la configuración como indica la figura R11.

Figura R9

Creación de Agentes

Figura R10

Añadir Agente

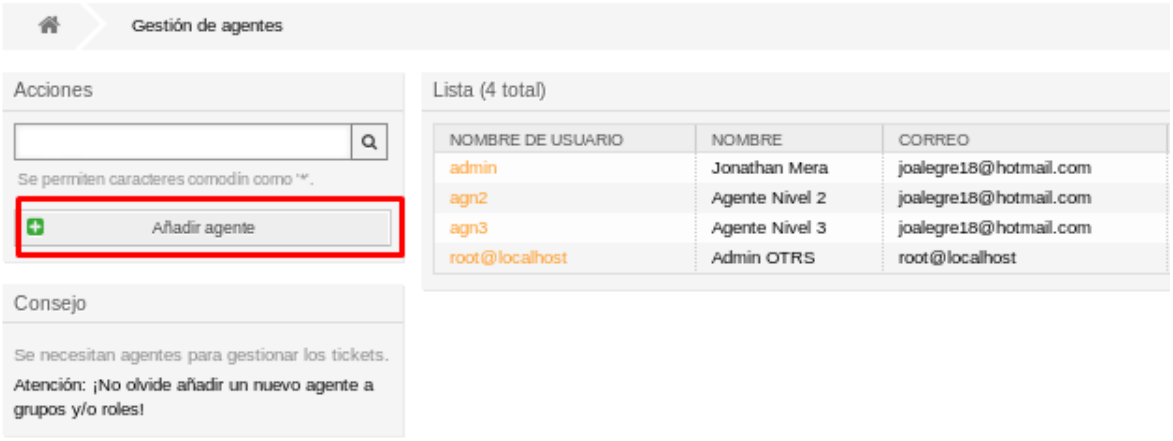
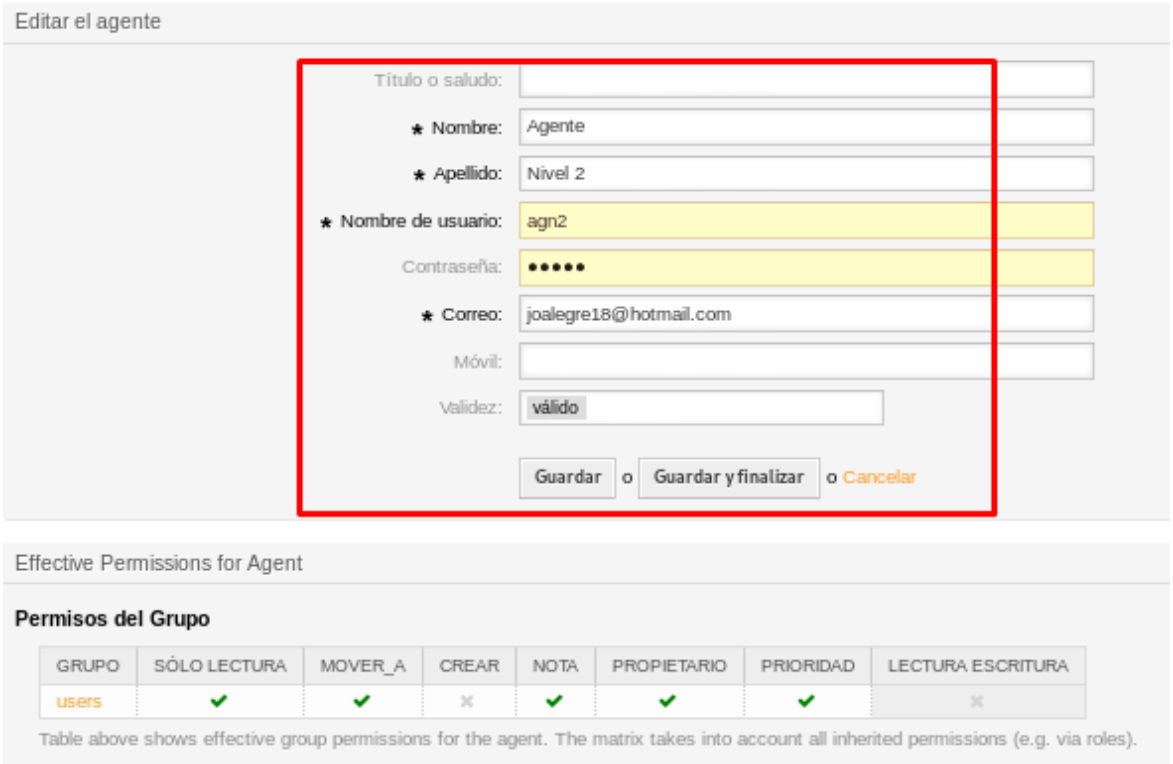


Figura R11

Configuración de las Cuentas de los Agentes



En efecto a los agentes es necesario darles permisos para la gestión de los tickets, en la figura R12 se presenta los permisos de administrador, a quien se le da todos los permisos por ser quien administra la mesa de ayuda y en la figura R13 se presenta los permisos que tienen los técnicos de soporte de la mesa de ayuda.

Figura R12

Permisos para la Gestión de Tickets al Agente Administrador de la Mesa de Ayuda

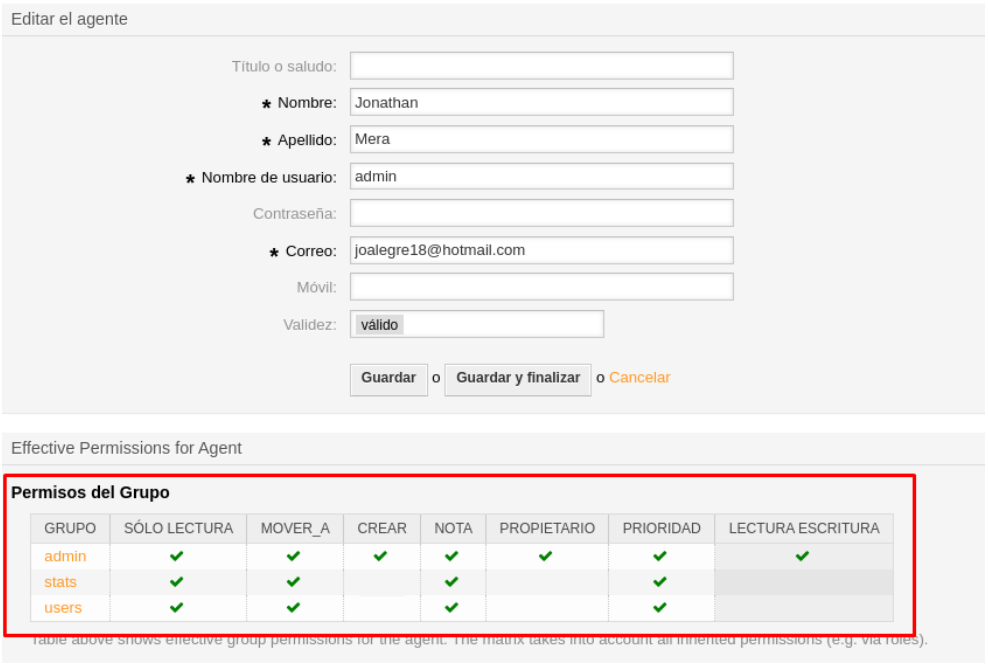
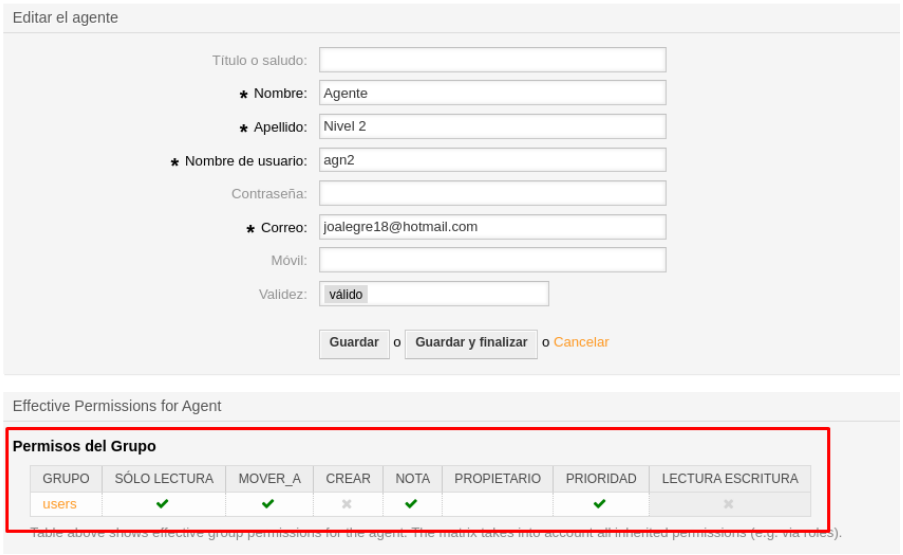


Figura R13

Permisos para la Gestión de Tickets a los Técnicos de Soporte



De modo que, los permisos que se pueden otorgar a los agentes son los siguientes:

Solo lectura: Puede leer y tener acceso a los tickets.

Mover a: Tiene opción de mover los tickets y asignarlos a otros agentes.

Crear: Permite la creación de nuevos tickets.

Propietario: Puede cambiar al propietario del ticket.

Prioridad: Permite establecer o cambiar la prioridad de un ticket.

Lectura y escritura: Son permisos completos, mencionados anteriormente.

Por otra parte, ahora se menciona la gestión de los tickets en OTRS, para ello se presenta en la figura R14, desde la cuenta del agente, en el panel principal puede observar los tickets que han sido asignados para su solución, para tal efecto, en el apartado nuevos tickets selecciona el incidente y puede visualizar la información del mismo, como se indica en la figura R15.

Figura R14

Bandeja de Tickets

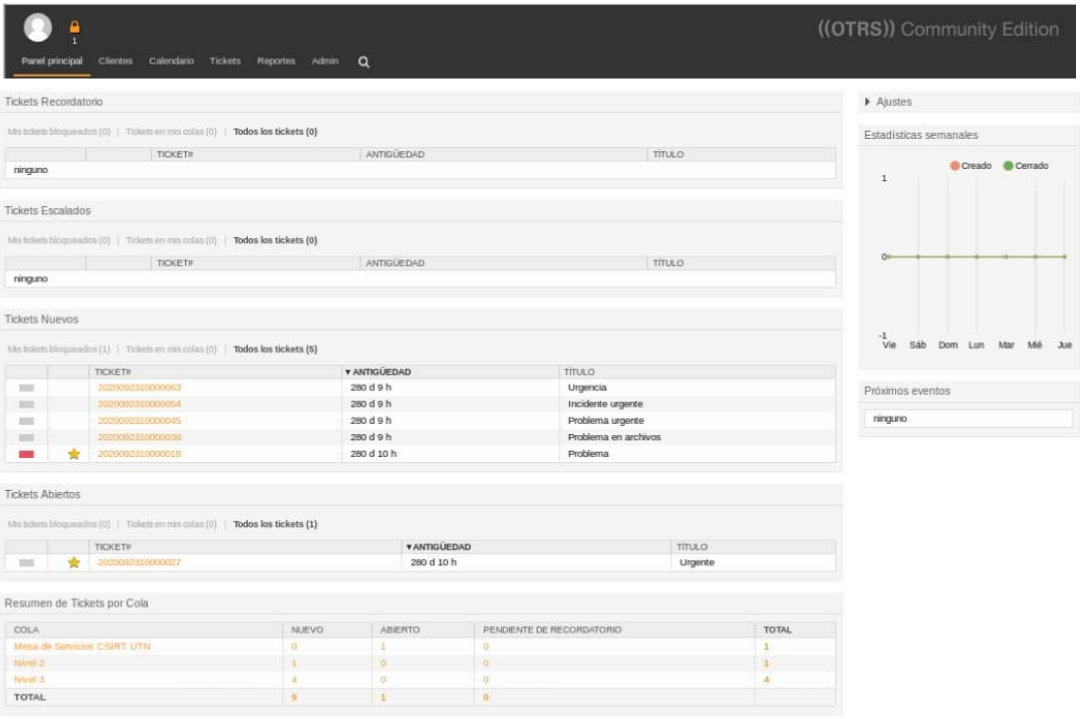


Figura R15

Visualización de Información del Ticket

Una vez que se ha dado el tratamiento al incidente se procede a dar una respuesta mediante OTRS de manera que quede como evidencia, en este caso, en la opción contestar se selecciona respuesta vacía como se indica en la figura R16, seguido de esto se abre otra ventana en la cual se inserta un mensaje de respuesta y se procede a cerrar el ticket, cabe mencionar que existen varias opciones en estado del ticket, en caso de que no se brinde una

solución, los estados son: abierto, cerrado sin éxito, y pendiente, como se muestra en la figura R17.

Figura R16

Respuesta a Ticket

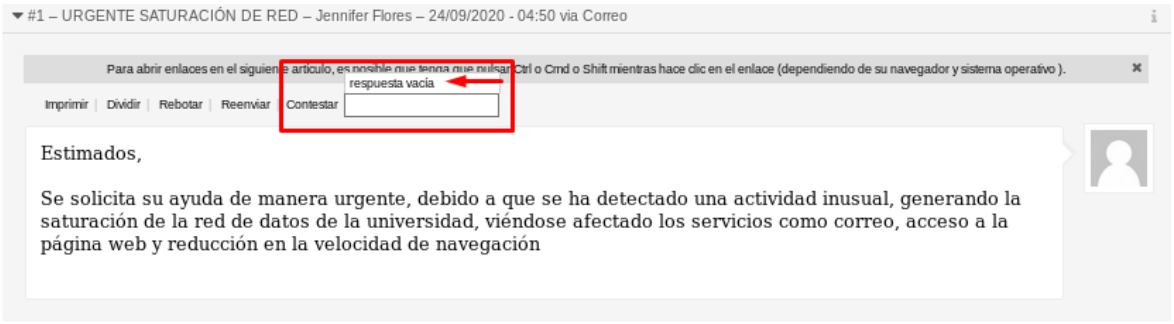
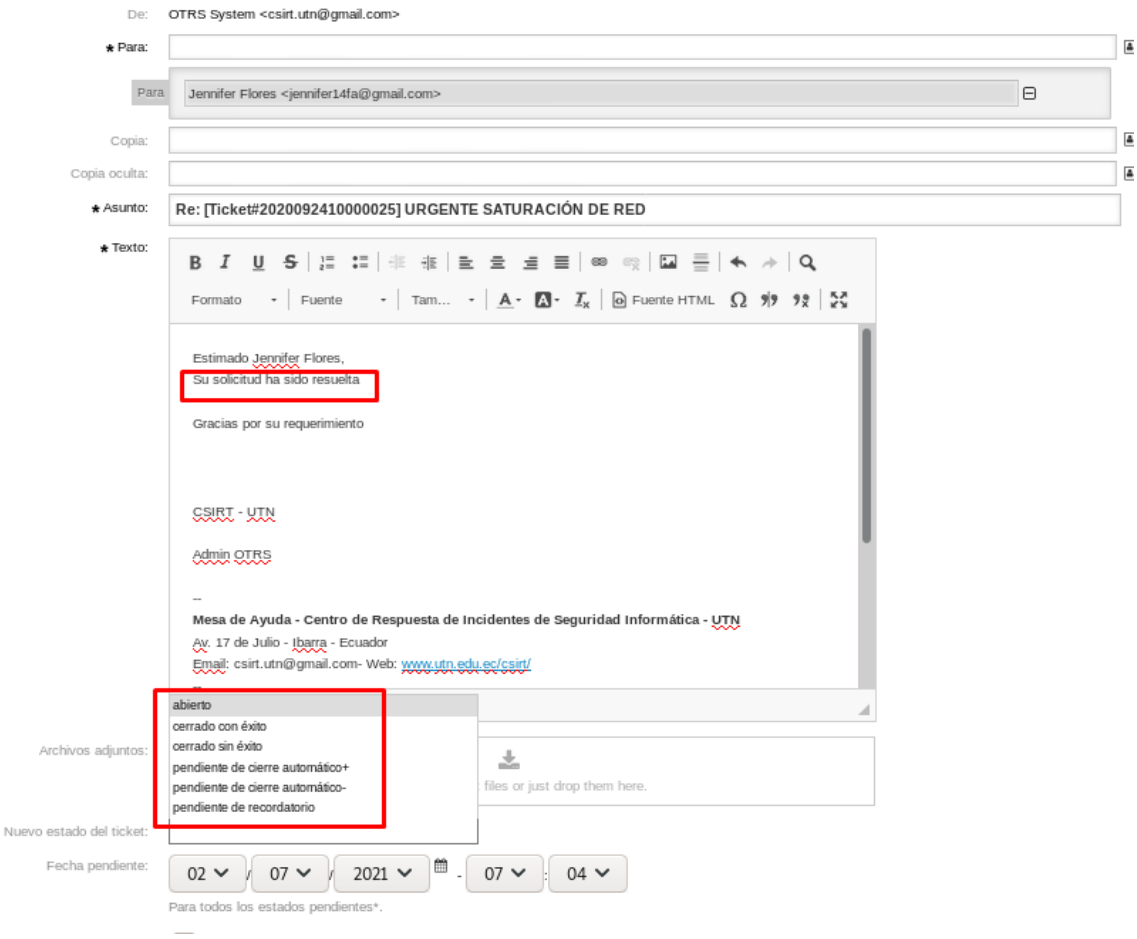


Figura R17

Cierre de Ticket



Finalmente, en caso de que el incidente sea reportado mediante llamada telefónica, se procede a la creación del ticket, para su posterior análisis y escalado en caso de requerirlo, para este particular, el procedimiento es el siguiente, desde el panel principal, en la opción de Tickets, se selecciona nuevo ticket por teléfono, como se señala en la figura R18, a continuación se despliega una nueva ventana, y se procede a ingresar la información del incidente, comenzando por los nombres de la persona que reporta el incidente, se asigna la cola, se ingresa el asunto, la información del incidente y finalmente se crea el ticket, como se indica en la figura R19.

Figura R18

Creación de Ticket

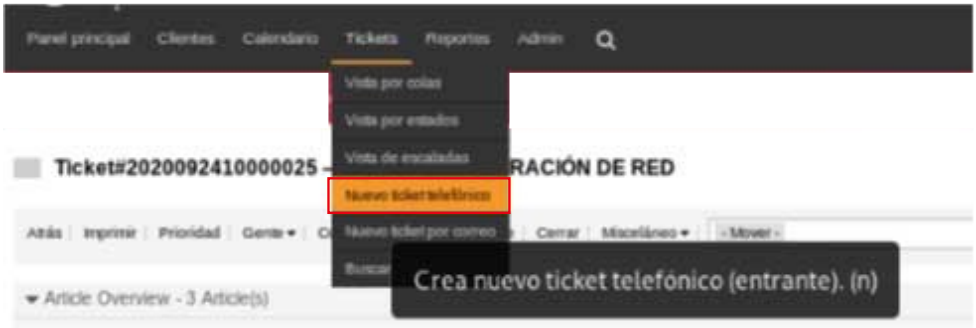
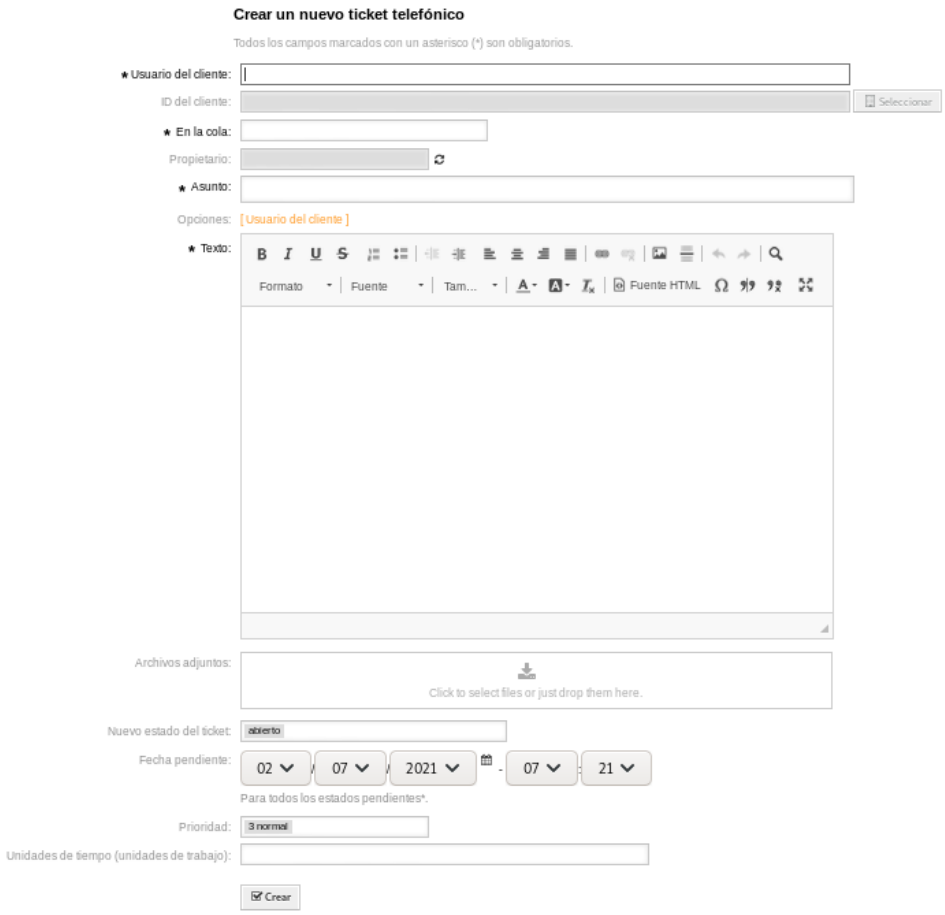


Figura R19

Información del Ticket



Apéndice S Configuraciones Importantes en SIMPROCESS

Para poder realizar la simulación en SIMPROCESS, se recibió una licencia de 10 días por parte de la empresa dueña de esta herramienta, la cual en la figura S1, se presenta como evidencia el correo con el archivo de activación.

Por consiguiente, en este apartado se presenta el ingreso de valores y configuraciones para cada caso simulado, el cual corresponde primeramente la gestión de incidentes sin la presencia del CSIRT, y el segundo caso, corresponde a la simulación con la presencia del CSIRT.

En este sentido, para comprensión de la simulación en Simprocess es necesario tener en cuenta los componentes y objetos de SimProcess. Los componentes son: procesos y actividades, recursos, entidades y conectores, presentando en la tabla S1 el detalle de cada uno ellos.

Figura S1

Archivo de Activación Proporcionada por Parte de CACI

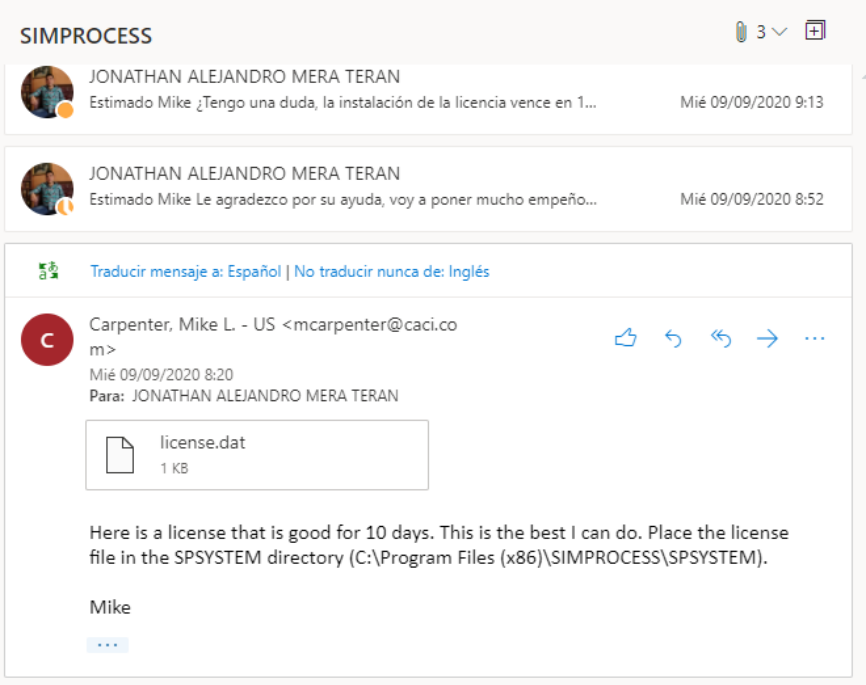


Tabla S1

Componentes de Simprocess

Componentes SIMPROCESS	Función
Procesos y actividades	SimProcess permite modelar procesos de forma jerárquica, permitiendo descomponer en subniveles, subprocesos y actividades. Las actividades se pueden modelar mediante bloques denominados DELAY, siendo este el tiempo en la que una entidad puede permanecer en la actividad.
Recursos	Un recurso es una herramienta limitada, por tanto, Simprocess permite definir costos, la capacidad de estos recursos.
Entidades	Las entidades son objetos que pasan a través de los procesos, las entidades se pueden simular con bloques denominados GENERATE, finalizando estas entidades en bloques denominados DISPOSE.
Conectores	Los conectores permiten la unión de las actividades definiendo el camino a seguir de una entidad desde la entrada hasta la finalización del proceso

Fuente: (CACI, 2012)

Por otro lado, en la tabla S2 se detalla la función y simbología de los objetos como: generate, dispose, delay, branch y join, los mismos que son parámetros importantes que hay que conocer, y que son de ayuda para la realización de la simulación de cada proceso.

Tabla S2

Objetos de Simprocess

Símbolo	Objetos	Descripción
	Generate	Su función es la de modelizar la llegada de las entidades a los procesos.
	Dispose	Es el punto en el cual llegan las entidades que circulan en el proceso.
	Delay	Se encarga de definir los tiempos de las actividades.
	Branch	Distribuye las entidades entre las rutas alternativas.
	Join	Transforma varias entidades en una sola.

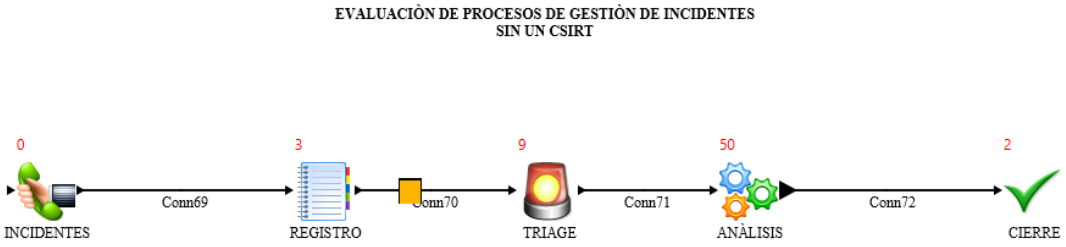
Fuente: (CACI, 2012)

Caso 1: Simulación de Procesos de Gestión sin un CSIRT

Hay que tener presente que, en el DDTI, tienen conocimiento de los procesos necesarios para gestionar los incidentes, por tanto, el esquema simulado consta de: reporte, registro, triage, análisis y cierre del incidente, siendo este esquema representado en la figura S2 a continuación.

Figura S2

Esquema de Resolución de Incidentes DDTI



El proceso de gestión de incidencias comienza con el reporte, cabe considerar que el DDTI no cuenta con una herramienta que permita este primer paso, por tanto, estos son reportados vía telefónica, la cantidad de incidentes reportados por hora consta en la tabla 44 (Distribución de incidentes), y está distribuido de la siguiente manera: 2 incidentes de prioridad alta, 4 de prioridad media y 7 de prioridad baja.

En este sentido, para el ingreso del número de incidentes en simprocess, es necesario primeramente la creación de entidades, las cuales, en otras palabras, son definidos como incidentes, que están distribuidos según su nivel de criticidad, siendo de prioridad alta, media y baja tal como se ilustra en la figura S3, enfatizando que, para este caso, los incidentes tienen la misma prioridad, ya que en el DDTI no se cuenta con procesos que permitan la clasificación de incidentes reportados. De forma que se crean tres entidades, denominadas incidentes de prioridad alta, media y baja, con su respectivo color rojo, naranja y verde, que permite una mejor identificación, y finalmente se les asigna la misma prioridad, siendo asignado el valor de 1.

Figura S3

Creación de entidades para la generación incidentes

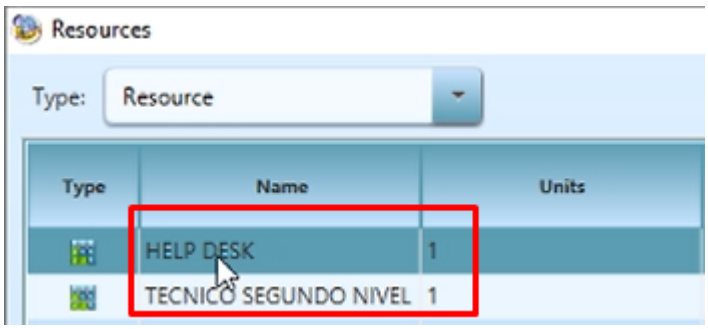
Entity Types

Name	Icon	Priority	Preempt	Entity Stats
INCIDENTES PRIORIDAD ALTA	RedSquare	1		
INCIDENTES PRIORIDAD MEDIA	OrangeSquare	1		
INCIDENTES PRIORIDAD BAJA	GreenSquare	1		

Entonces, una vez definido los tipos de entidades(incidentes), se procede con la creación de los recursos (resources), haciendo referencia a los encargados de atender los incidentes reportados, este proceso se expone en la figura S4, para lo cual se tiene dos recursos, un técnico de nivel 1 (Helpdesk) y un técnico de segundo nivel.

Figura S4

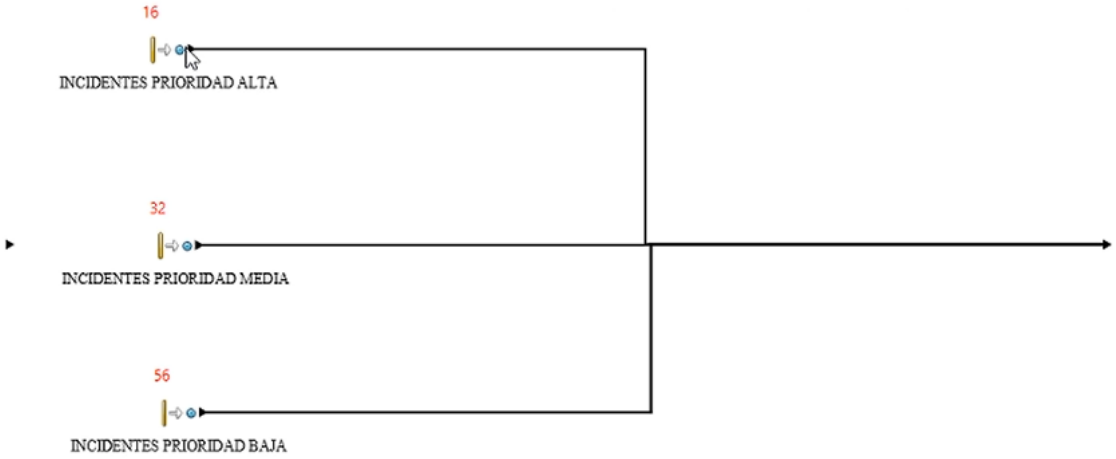
Creación de recursos, encargados de atender los incidentes reportados



Dentro del proceso de reporte de incidentes se parametriza los valores con el objeto denominado “Generate”, estos valores corresponden al número de incidentes que se reportan en la jornada laboral de 8 horas, estableciendo 16 incidentes de prioridad alta, 32 de prioridad media y 56 incidentes de prioridad baja, esta parametrización se presenta en la figura S5.

Figura S5

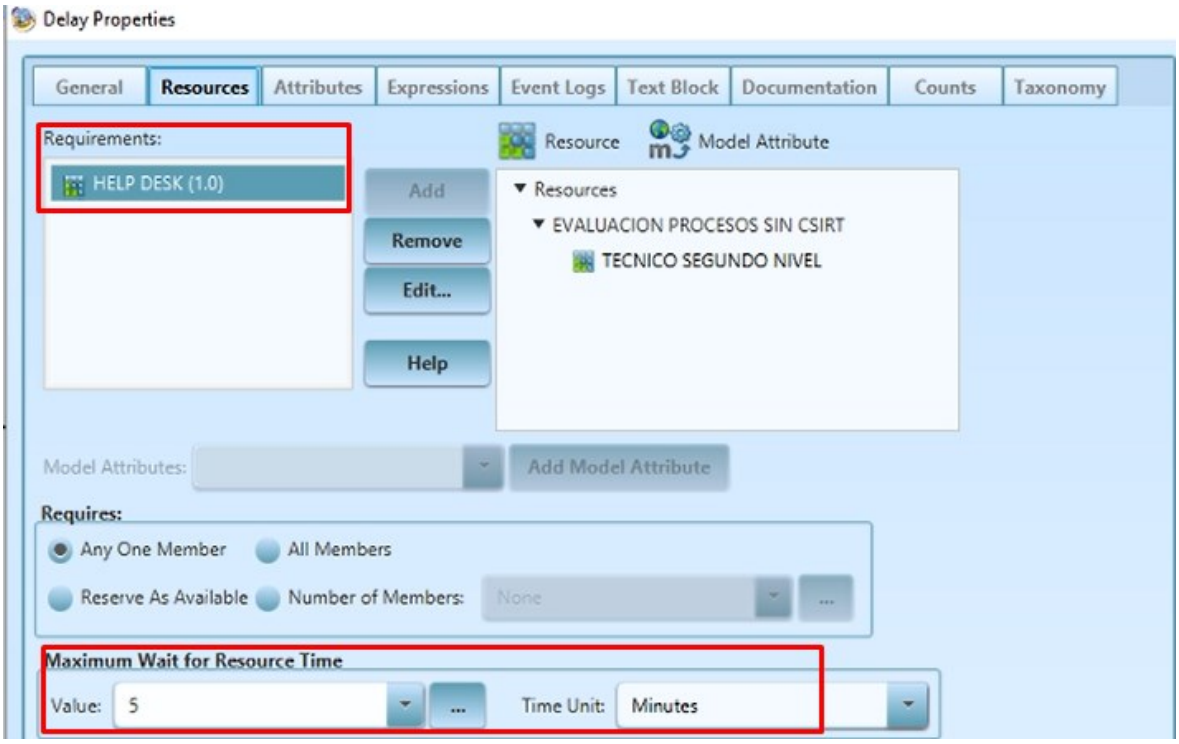
Simulación de Incidentes Reportados



En efecto, a continuación, se asigna el tiempo (delay) que toma el registro de los incidentes reportados y el recurso (resource) encargado de este proceso, en este sentido el recurso corresponde al técnico de nivel 1 (Help Desk), y el tiempo de 5 minutos, para ello en la figura S6 se manifiesta esta parametrización.

Figura S6

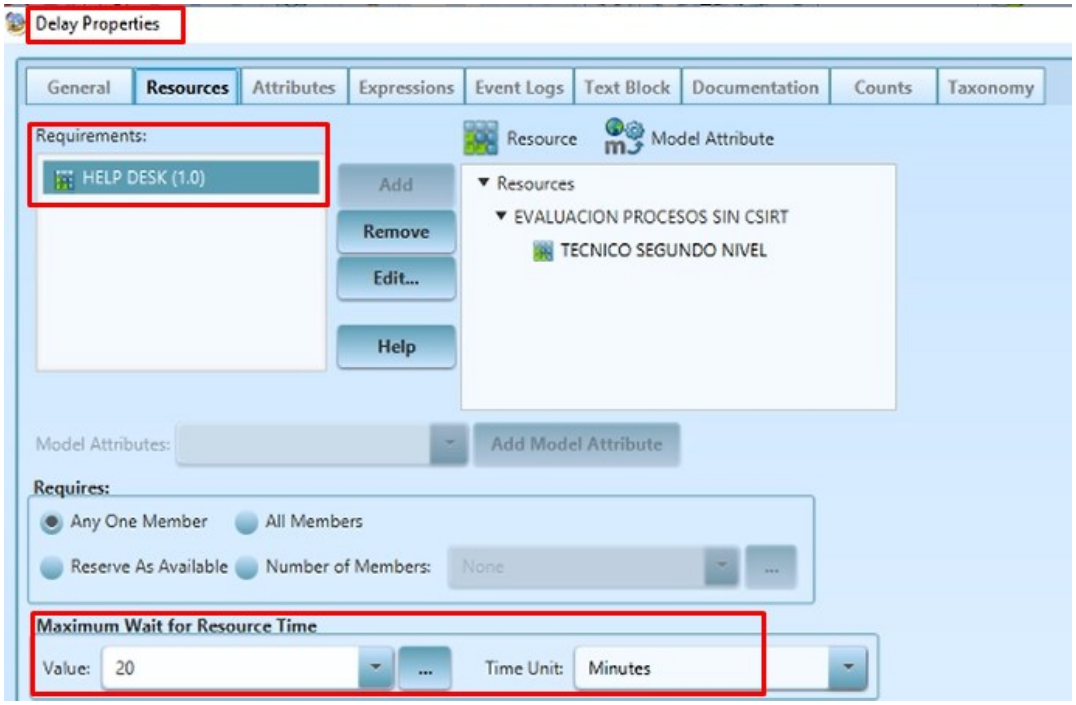
Tiempo de registro de incidentes reportados y recurso encargado de la actividad.



Seguidamente, en la figura S7 se detalla la etapa de Triage, este paso este compuesto por la clasificación y asignación del incidente al técnico correspondiente según el nivel de prioridad, cabe mencionar, que el DDTI no aplica un proceso adecuado para la gestión de incidentes por tanto no se realiza una correcta priorización de los incidentes reportados. En consecuencia, el tiempo estimado para este proceso de triage corresponde a 20 minutos, y el encargado es el técnico de nivel 1.

Figura S7

Tiempo y Recurso para la Etapa de Triage



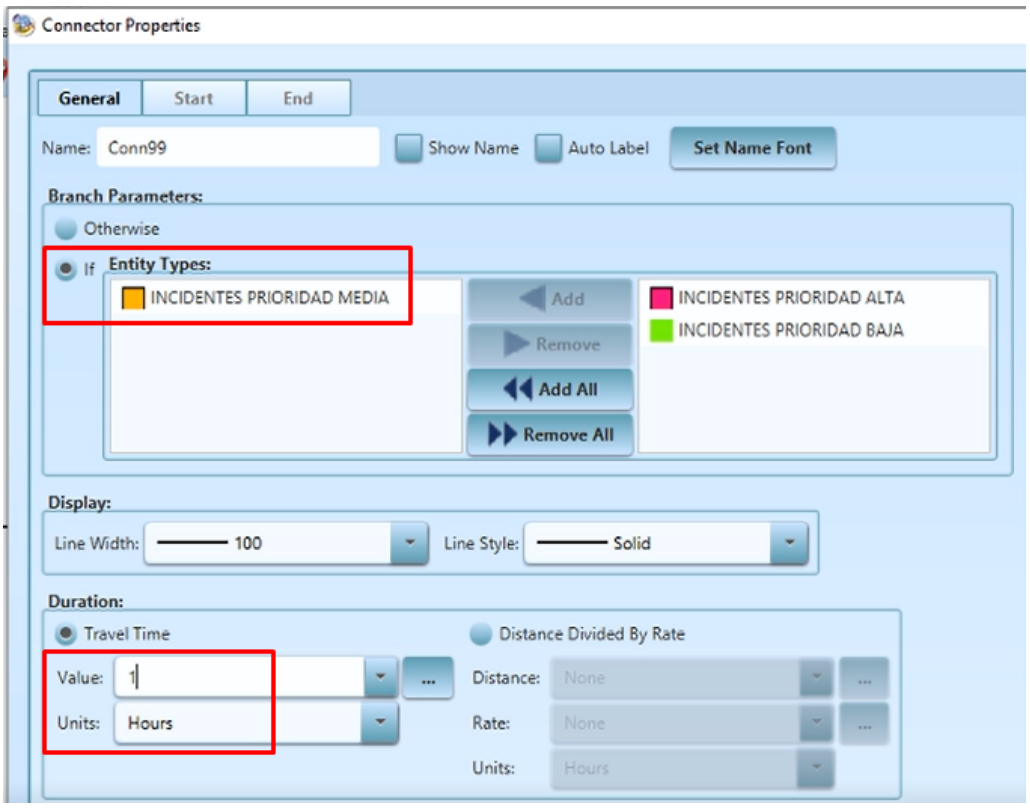
Luego del análisis realizado por el técnico de nivel 1, los incidentes son distribuidos según el nivel de prioridad, para ello se utiliza el objeto denominado “Branch”, que es el encargado de simular la distribución de los incidentes según su criticidad, recordando que se tiene 16 incidentes de prioridad alta, 32 de prioridad media y 56 en prioridad baja, para ello en la figura S8 se presenta la distribución de los incidentes, además, en esta fase se ingresa el tiempo estimado para la resolución de los incidentes según la prioridad, siendo los valores los siguientes: 2 horas para incidentes de prioridad baja, 1 hora para los de prioridad media y 30 minutos para los de prioridad alta, en la figura S9, a manera de ejemplo se ilustra el ingreso del tiempo para incidentes de prioridad media, para ello se selecciona la entidad (incidentes), y se ingresa el tiempo de resolución.

Figura S8

Distribución de Incidentes

Figura S9

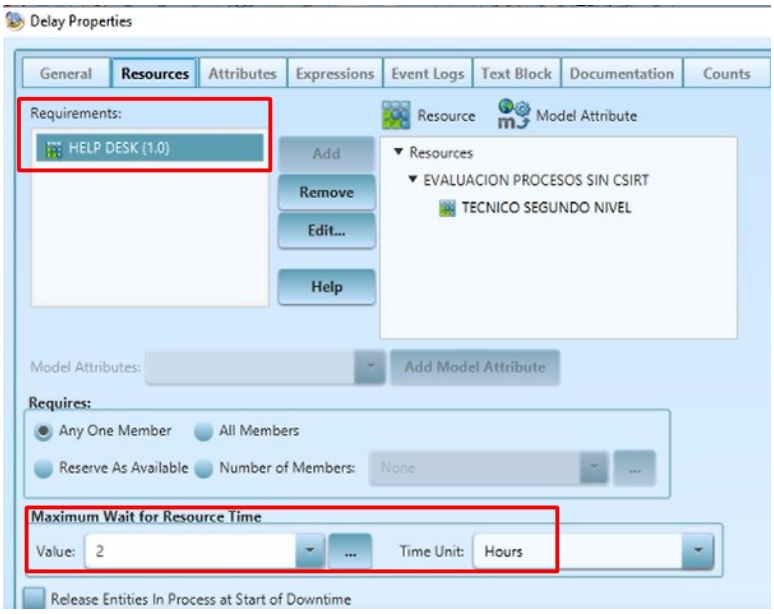
Tiempo de Resolución de Incidentes Según Nivel de Prioridad



De forma que, luego de ingresar el tiempo para la resolución del incidente, según el nivel de prioridad, es necesario asignar un recurso que se encargue de este proceso, en la figura S10, se presenta esta parametrización.

Figura S10

Asignación de Recurso Encargado de Brindar Solución



Finalmente, una vez solucionado el incidente se procede a cerrar el mismo, es importante señalar que esta herramienta brinda un reporte de la simulación el cual se presenta en la figura S11, este reporte brinda datos como la duración de la simulación, el número total de incidentes registrados, solucionados, sin solución y porcentajes de utilización de los recursos.

De esta manera los resultados que destacan corresponden a la cantidad de incidentes solucionados y que se encuentran distribuidos de la siguiente manera: 10 incidentes de prioridad alta, 8 de prioridad media y 0 incidentes de prioridad baja, presentando un total de 18 incidentes solucionados de un total de 104 incidentes reportados, por otro lado, se presenta un total de 86 incidentes sin solución.

Figura S11

Reporte de la Simulación Caso 1

Standard Report

Simulation Initiated: Fri Sep 11 19:42:02 2020
Simulation Concluded: Fri Sep 11 19:46:10 2020
Simulation Run Duration: 00:04:07.759

Model Start Date/Time: 01/01/2020 08:00:00:000:000:000
Model End Date/Time: 01/01/2020 16:00:00:000:000:000
Actual Start Date/Time: 01/01/2020 08:00:00:000:000:000
Actual End Date/Time: 01/01/2020 16:00:00:000:000:000
Actual Run Duration: 08:00:00:000:000:000

Entity : Total Count - Observation Based : Replication 1

Name	Total Generated	Remaining In	Total Disposed
INCIDENTES PRIORIDAD ALTA	16	6	10
INCIDENTES PRIORIDAD BAJA	56	56	0
INCIDENTES PRIORIDAD MEDIA	32	24	8

Entity : Count By State - Time Weighted : Replication 1

	Total In System		Processing		Wait For Resources		Hold For Conditions		Traveling	
Name	Avg	Max	Avg	Max	Avg	Max	Avg	Max	Avg	Max
INCIDENTES PRIORIDAD ALTA	6.40	8	0.00	0	3.35	6	0.00	0	3.04	7
INCIDENTES PRIORIDAD BAJA	31,50	56	1,95	2	9,29	14	0,00	0	20,28	48
INCIDENTES PRIORIDAD MEDIA	16.52	28	0.00	0	6.75	12	0.00	0	10.17	21

Entity : Cycle Time (in Hours) By State - Observation Based : Replication 1

		Total In System		Processing		Wait For Resources		Hold For Conditions		Traveling	
Name	#Obs	Avg	Max	Avg	Max	Avg	Max	Avg	Max	Avg	Max
INCIDENTES PRIORIDAD ALTA	10	3.52	3.52	0.00	0.00	1.52	1.52	0.00	0.00	2.00	2.00
INCIDENTES PRIORIDAD BAJA	0	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
INCIDENTES PRIORIDAD MEDIA	8	6.42	6.42	0.00	0.00	2.42	2.42	0.00	0.00	4.00	4.00

Resource : Number of Units By State - TimeWeighted : Replication 1

		Idle		Busy		Planned Downtime		Unplanned Downtime		Reserved	
Name	Cap	Avg	Max	Avg	Max	Avg	Max	Avg	Max	Avg	Max
HELP DESK	1.00	0.00	1.00	1.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
TECNICO SEGUNDO NIVEL	1,00	0,05	1,00	0,95	1,00	0,00	0,00	0,00	0,00	0,00	0,00

Resource : Percent Utilization By State : Replication 1

Name	Idle	Busy	Planned	Unplanned	Reserved
HELP DESK	0.00%	100.00%	0.00%	0.00%	0.00%
TECNICO SEGUNDO NIVEL	5,21%	94,79%	0,00%	0,00%	0,00%

Resource : Percent Utilization By State When Available : Replication 1

Name	Idle	Busy	Reserved
HELP DESK	0.00%	100.00%	0.00%
TECNICO SEGUNDO NIVEL	5,21%	94,79%	0,00%

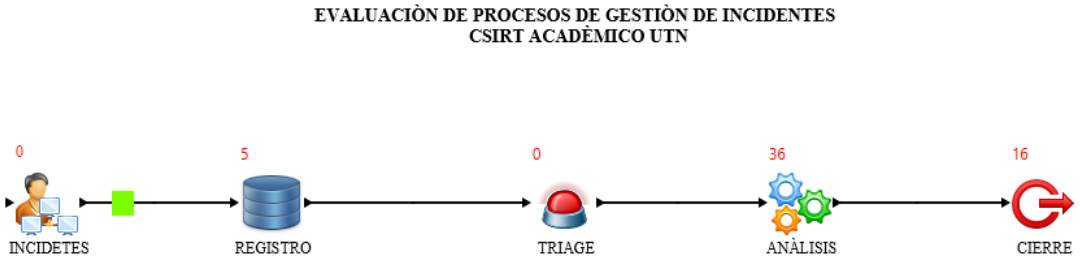
Caso 2: Simulación de Procesos de Gestión con la presencia del CSIRT

Dentro de este apartado se presentarán los parámetros que difieren del caso 1, debido a que las configuraciones son similares.

El esquema del proceso de gestión de incidentes es similar, pero con la presencia del CSIRT, se lleva procesos organizados, utilizando normas, estándares y marcos de referencia que sirven de soporte para la resolución de incidentes, en la figura S12, se presenta el esquema de resolución de incidentes.

Figura S12

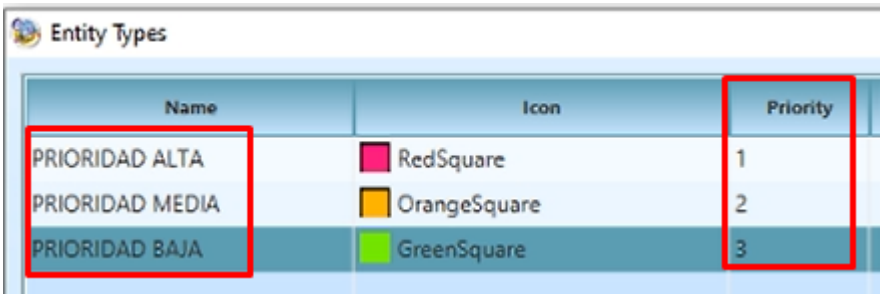
Esquema de Gestión de Incidentes con la Presencia del CSIRT



Con la presencia del CSIRT, se utiliza OTRS como herramienta para el reporte de incidentes, por tanto, se reduce el tiempo de registro, las entidades son las mismas, con la diferencia que, en cada tipo de incidente se asigna una prioridad, la cual se puede observar en la figura S13, para los incidentes de prioridad alta se asigna el valor de 1, para los de prioridad media se asigna el valor de 2 y 3 para los de prioridad baja.

Figura S13

Asignación de Prioridad a cada Entidad



Por otra parte, hay que considerar que se tiene un recurso más para brindar solución a los incidentes, los cuales corresponden a: dos técnicos de soporte y un experto en seguridad informática, los mismos que se evidencian en la figura S14.

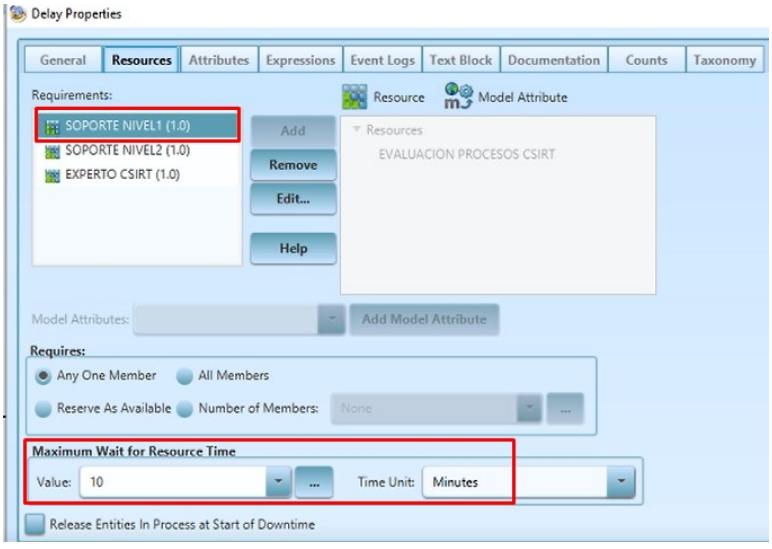
Figura S14

Recursos para la resolución de incidentes con la presencia del CSIRT

En definitiva, el contar con una herramienta de tickets para el reporte de incidentes, ayuda a disminuir el tiempo de registro, por tanto, el tiempo se disminuye a un minuto, y la etapa de Triage también se reduce a 10 minutos, ya que se cuenta con procesos para la gestión de incidentes, estos datos se muestran en la figura S15 a continuación, estableciendo que el recurso encargado del triage es el técnico de nivel 1.

Figura S15

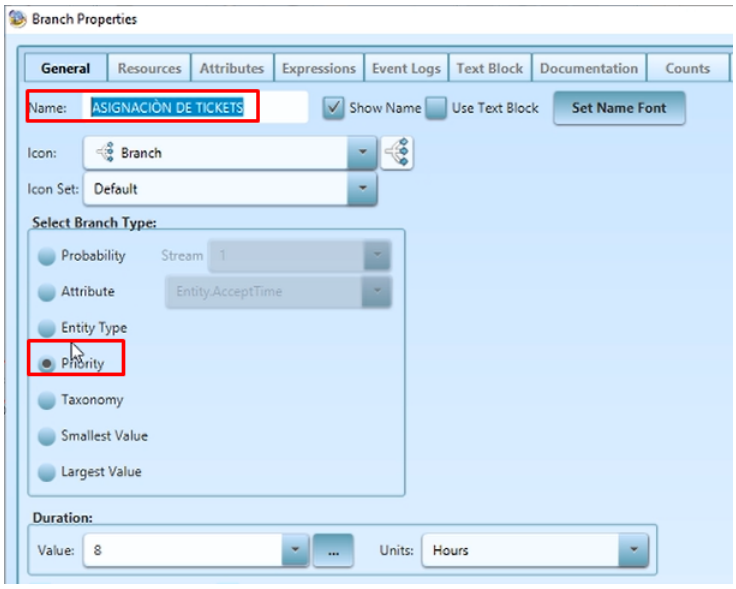
Definición de recurso encargado del Triage y tiempo establecido



Ahora bien, para la asignación de los incidentes, en este caso con el objeto “Branch” se asigna la prioridad según la criticidad del incidente, esta configuración se presenta en la figura S16.

Figura S16

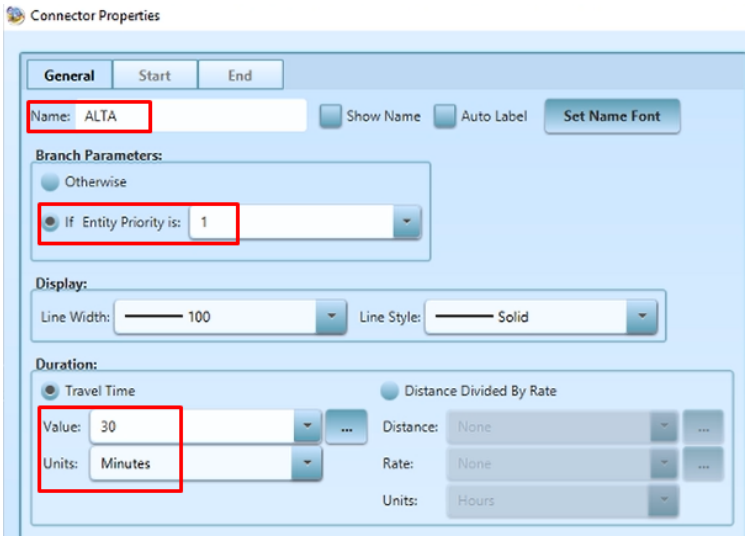
Asignación de Prioridad para la Distribución de Incidentes



Agregando a lo anterior, en esta etapa se configura los parámetros según el nivel del incidente, la prioridad y el tiempo estimado para la resolución, en la figura S17, se muestra a manera de ejemplo, si la prioridad corresponde a nivel 1 (prioridad alta), que el tiempo de resolución sea de 30 minutos. Cabe destacar, que este proceso es la principal diferencia entre ambos casos, ya que para este particular se realiza la priorización de los incidentes, según la entidad o nivel de priorización (alta, media, baja) y que se relaciona con el tiempo de resolución.

Figura S17

Establecimiento de Prioridad según Nivel de Criticidad del Incidente



De esta manera se presenta en la figura S18 el reporte generado con la simulación para el caso 2, brindando el total de incidentes reportados según el nivel, para lo cual se tiene 16 incidentes de prioridad alta (A), 32 de prioridad media (M) y 56 de prioridad baja (B), siendo los resultados más considerables, el total de incidentes solucionados que corresponde a 12 incidentes de prioridad alta, 24 de prioridad media y 32 de prioridad baja, siendo un total de 68 incidentes solucionados, y 36 incidentes sin solución, siendo apreciable que se brinda solución a un porcentaje alto, incluyendo a los incidentes de prioridad baja, lo cual difiere del caso 1, ya que no se brinda solución a estos incidentes.

Figura S18

Reporte de la Evaluación de Incidentes con la Presencia del CSIRT

Standard Report

Simulation Initiated: Fri Sep 11 17:23:20 2020
Simulation Concluded: Fri Sep 11 17:27:48 2020
Simulation Run Duration: 00:04:28.205

Model Start Date/Time: 01/01/2020 08:00:00:000:000:000
Model End Date/Time: 01/01/2020 16:00:00:000:000:000
Actual Start Date/Time: 01/01/2020 08:00:00:000:000:000
Actual End Date/Time: 01/01/2020 16:00:00:000:000:000
Actual Run Duration: 08:00:00:000:000:000

Entity : Total Count - Observation Based : Replication 1

Name	Total Generated	Remaining In	Total Disposed
A	16	4	12
B	56	24	32
M	32	8	24

Entity : Count By State - Time Weighted : Replication 1

	Total In System		Processing		Wait For Resources		Hold For Conditions		Traveling	
Name	Avg	Max	Avg	Max	Avg	Max	Avg	Max	Avg	Max
A	4.03	6	0.00	0	3.15	6	0.00	0	0.88	3
B	21,05	31	3,00	3	12,46	21	0,00	0	5,59	15
M	3.55	12	0.00	0	6.55	12	0.00	0	2.62	5

Entity : Cycle Time (in Hours) By State - Observation Based : Replication 1

		Total In System		Processing		Wait For Resources		Hold For Conditions		Traveling	
Name	#Obs	Avg	Max	Avg	Max	Avg	Max	Avg	Max	Avg	Max
A	12	2.18	2.18	0.00	0.00	1.68	1.68	0.00	0.00	0.50	0.50
B	32	3,20	3,35	0,02	0,18	2,18	2,18	0,00	0,00	1,00	1,00
M	24	2.68	2.68	0.00	0.00	1.93	1.93	0.00	0.00	0.75	0.75

EVALUACION PROCESOS CSIRT Standard Report

Resource : Number of Units By State - TimeWeighted : Replication 1

		Idle		Busy		Planned Downtime		Unplanned Downtime		Reserved	
Name	Cap	Avg	Max	Avg	Max	Avg	Max	Avg	Max	Avg	Max
HD	1.00	0.00	1.00	1.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
N2	1,00	0,00	1,00	1,00	1,00	0,00	0,00	0,00	0,00	0,00	0,00
N3CSIRT	1.00	0.00	1.00	1.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00

Resource : Percent Utilization By State : Replication 1

Name	Idle	Busy	Planned	Unplanned	Reserved
HD	0.00%	100.00%	0.00%	0.00%	0.00%
N2	0,00%	100,00%	0,00%	0,00%	0,00%
N3CSIRT	0.00%	100.00%	0.00%	0.00%	0.00%

Resource : Percent Utilization By State When Available : Replication 1

Name	Idle	Busy	Reserved
HD	0.00%	100.00%	0.00%
N2	0,00%	100,00%	0,00%
N3CSIRT	0.00%	100.00%	0.00%