FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS PARA LA CREACIÓN DE UN EQUIPO CSIRT ACADÉMICO EN LA UNIVERSIDAD DE LAS AMÉRICAS

AUTOR

Oscar Alberto Amagua Mena

AÑO

2020

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS PARA LA CREACIÓN DE UN EQUIPO CSIRT ACADÉMICO EN LA UNIVERSIDAD DE LAS AMÉRICAS

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Ingeniero Electrónico y Redes de Información.

PROFESIR GUÍA

Ms. William Eduardo Villegas Chiliquinga

AUTOR

Oscar Alberto Amagua Mena

AÑO

2020

DECLARACIÓN PROFESOR GUÍA

“Declaro haber dirigido el trabajo, Análisis para la creación de un equipo CSIRT académico en la Universidad de la Américas, a través de reuniones periódicas con el estudiante Oscar Alberto Amagua Mena, en el semestre 202020, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

William Eduardo Villegas Chiliquinga

Doctor en Informática

CI: 171533826

DECLARACIÓN PROFESOR CORRECTOR.

“Declaro haber revisado este trabajo, Análisis para la creación de un equipo CSIRT académico en la Universidad de la Américas, del Oscar Alberto Amagua Mena, en el semestre 202020, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

Iván Patricio Ortiz Garcés
Magister en Redes de Comunicaciones
CI: 0602356776

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE.

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

Oscar Alberto Amagua Mena

CI: 1718128539

AGRADECIMIENTOS

Agradezco a mi familia por siempre brindarme su apoyo y amor, por ser una parte fundamental en la consecución de esta meta, a mis compañeros por siempre estar presentes en los momentos de alegría y sobre todo de en los de tristeza, a mi querida universidad por brindarme una educación de excelencia y prepararme para mis nuevos retos en la vida. Finalmente puedo decir y expresar, que no hay nada más gratificante que culminar estos años de estudio en un lugar que para mí fue considerado un hogar.

Oscar Amagua.

DEDICATORIA

Dedico este trabajo a mi familia, quienes se merecen un profundo agradecimiento, por su apoyo moral y económico para la culminación de esta maravillosa etapa, en la cual he conocido amigos, compañeros y sobre todo he adquirido el conocimiento para poder alcanzar mis metas.

Oscar Amagua.

RESUMEN

El proyecto de titulación propone un análisis para la creación de un equipo de respuesta ante incidentes de seguridad informática en la Universidad de las Américas. Debido al incremento de los servicios, productos y experiencias ofertadas. Esto también conlleva a un aumento de las incidencias y amenazas dentro de la organización.

El objetivo principal de este proyecto se centra en el análisis de los diferentes modelos organizacionales establecidos y reconocidos por organismos de control a nivel nacional e internacional. De manera que los servicios e infraestructura con los que cuente actualmente la universidad puedan adaptase o ser tomados como referencia para la puesta en marcha de un equipo de respuesta ante incidencias de seguridad Informáticas (en inglés, *Computer Security Incident Response Team o CSIRT*). Permitiendo a futuro la mejora constante de los procesos, servicios y aumentando el nivel de seguridad en la institución.

La idea es que las personas y organizaciones sin importar el rol de la empresa, puedan desarrollar las primeras fases de un análisis para el manejo de problemas informáticos y a su vez la implementación de un equipo especializado en el monitoreo, gestión, control y mitigación de incidentes de seguridad informática. De manera que la red de miembros nacionales crezca y se pueda detectar las vulnerabilidades en los sistemas de manera rápida y sin que el problema escale exponencialmente dentro de la empresa.

ABSTRACT

The degree project proposes an analysis for the creation of a computer security incident response team at the University of the Americas, due to the increase in services, products and experiences offered. This also implies an increase in incidents and threats within the organization.

The main objective of this project is focused on the analysis of the different organizational models established and recognized by control bodies at national and international level. So, the services and infrastructure that the university currently has can be adapted or used as a reference for the implementation of a computer security incident response team or CSIRT. Allowing a future, the constant improvement of processes, services and changes the level of security in the institution.

The idea is that people and organizations, regardless of their role in the company, can develop the first phases of an analysis for incident management or, in turn, the implementation of a specialized team to handle, monitor and mitigate incidents or threats. So that the member network grows, and vulnerabilities can be detected in the systems quickly and without the problem escalating exponentially.

ÍNDICE

1. CAPÍTULO I. INTRODUCCIÓN

Preservar la información de nuestra organización en un escenario informático interconectado es cada vez más difícil, con la implementación de nuevos servicios y el aumento de los métodos de intrusión en la red. Por tal motivo, la seguridad de las redes de comunicación se volvió un problema que afecta a la población mundial. Los ciberataques se han convertido en una de las principales amenazas para los países y gobiernos. Pueden ocurrir en cualquier instante, independientemente del tipo de organización, ya sea esta grande, mediana, pequeña o de alta relevancia.

En el 2004 se crea una agencia europea de seguridad con el fin de permitir garantizar un elevado nivel de conocimiento de seguridad de las redes y la información denominado “ENISA”, lo cual a su vez permitió desarrollar una cultura de seguridad informática hacia la comunidad europea. En latino América se ha puesto en práctica implementaciones de equipos de respuesta, pero no se ha obtenido los resultados esperados. Esto se debe en su mayoría a la falta de información e importancia hacia este tema de carácter mundial, que principalmente provocaría pérdidas económicas.

Por tal motivo, las naciones ven como una necesidad conformar Equipo de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT - *Computer Security Incident Response Team*) que permiten a las organizaciones lograr limitar el daño, tolerar ataques, consolidar la continuidad de los servicios, además de ser una buena práctica a futuro y de igual manera tener una mejor cultura de seguridad en nuestro país.

Las instituciones educativas están en constante riesgos debido a los servicios que manejan y prestan a los estudiantes, esto aumenta en gran medida los medios de acceso no autorizado a nuestra información, es por tal motivo que contar con un Equipo de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT - *Computer Security Incident Response Team*) ayudará a mitigar en gran medida los ataques informáticos, el alcance del equipo de respuesta dependerá

de las políticas, requerimientos y áreas de alto impacto de manera que puedan actuar de mejor manera en cada campo.

1.1 Alcance

El alcance de este trabajo de titulación busca plantear un modelo CSIRT Académico que cumpla con los estándares internacionales y aplicados en la Universidad de las Américas (UDLA). Se planea seguir un lineamiento de acuerdo con guías aprobadas y abaladas por ENISA (Agencia Europea de Seguridad de las Redes - *Union Agency for Network and Information Security*) Para ello se desarrollarán las fases iniciales establecidas en los diferentes modelos de creación de un equipo CSIRT. Teniendo en cuenta los recursos, requerimientos y políticas que están establecidas en la unidad educativa, con el fin de no poner en riesgo la seguridad de la institución y preservar la integridad de los datos. Para lograr dar una visión más general y práctica de cómo se ejecuta y quien coordina la parte organizacional del proyecto. Se deberá, tomar referencias de Equipo de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT - *Computer Security Incident Response Team*) ya establecidos.

1.2 Justificación

La red se ha convertido en una forma de negocios en la sociedad actual, pero esto también conlleva nuevos retos para proteger nuestros datos e información de ataques cibernéticos. Según expertos la única manera de protegerte en la red y evitar el robo de información es no usar en absoluto el internet, pero esta medida es casi imposible en la actualidad. Esto puede ocurrir debido a la poca seguridad de la que gozan nuestras redes o aplicaciones y la falta de cultura en seguridad por parte de los usuarios.

El principal problema en la Universidad de las Américas (UDLA) se da debido al uso de diferentes servicios, entre los cuales, el más importante es el acceso al internet, ya que los estudiantes lo utilizan para prácticamente todo, ya sean búsquedas, correo electrónico, aulas virtuales, oros, etc. Se encuentran

constantemente expuestos a ataques perpetrados por terceras personas, que dado el caso suplantarían la identidad o robarían información del usuario.

1.3 Objetivos

1.3.1 Objetivo general

Analizar y documentar los diferentes factores necesarios para el desarrollo futuro de un CSIRT académico en la Universidad de las Américas.

1.3.2 Objetivos específicos

- Determinar las áreas o servicios de alto impacto en la Universidad de las Américas (UDLA).
- Analizar los diferentes estándares y diseños de modelos ya establecidos en diferentes organizaciones.
- Formular una propuesta de modelo inicial para la puesta en marcha de un CSIRT académico en la Universidad de las Américas (UDLA).

2. CAPÍTULO II. MARCO TEÓRICO

Este capítulo se desarrollará con el objetivo de familiarizarnos con el documento, de manera que se logre comprender las frases, palabras o citaciones que se emplearan durante el desarrollo del trabajo de titulación. Defiendo conceptos, modelos CSIRT (*Computer Security Incident Response Team),* estableciendo características y diferencias de cada estructura, de esta manera se podrá complementar la idea transmitida y evitar la redundancia del escrito.

2.1 Seguridad de la información

2.1.1 Incidentes de seguridad informática

Se define como incidente de seguridad al intento de acceso sin privilegios, eliminar información sin la respectiva autorización, modificación de información, divulgación de los datos, no permitir el funcionamiento normal de los servicios,

redes y sistemas. Realizar acciones que no se encuentren permitidas en las políticas de seguridad de la universidad. (Centro Nacional de Respuesta ante Incidentes de Seguridad Informática, 2018)

2.1.2 Amenaza de seguridad informática

Las amenazas surgen a partir de las vulnerabilidades, ya que estas pueden ser utilizadas para comprometer la seguridad de la información. En la actualidad el incremento y las nuevas técnicas de intrusión en la red, han hecho cada vez más creciente el número de ataques intencionales a la red de una organización. Las amenazas se clasifican en dos tipos:

- Amenazas intencionales: Sucede cuando se intenta poner en riesgo a la organización, por ejemplo, el robo de información mediante el uso de técnicas como: trashing lógico (buscar en la basura o papelera información que sirva para provocar fraudes, robos y divulgaciones de datos).
- Amenazas no intencionales: Son amenazas que no buscar exponer una vulnerabilidad, pero ponen en riesgo la información de una organización. Por ejemplo, cuando acontecen desastres naturales y la infraestructura se ve afectada, así como los equipos que manejan los datos.

2.1.3 Vulnerabilidades de seguridad informática

Una vulnerabilidad es una debilidad de un sistema o software, del cual un atacante pueda aprovecharse con el fin de violentar la confidencialidad, integridad, disponibilidad de la información y aplicaciones. Las vulnerabilidades son producidas por fallos o el incorrecto diseño de un software, no obstante, también puede ser producido por las limitaciones del dispositivo o aplicación, ya que, al no contar con un sistema actualizado, estará presto a sufrir ataques más sofisticados. (Universidad Internacional de Valencia, 2018)

2.1.4 Reporte de incidentes

2.1.5 Reporte de incidentes manuales

Ejemplo de ingreso de un incidente de forma manual, en el cual se detallan los datos del solicitante, encargado de resolver el requerimiento e información que permitirá determinar el grado de urgencia con la cual deberá ser tratado. En la parte inferior se deberá ingresar la información del incidente, teniendo en cuenta que los usuarios no conocen en su totalidad un lenguaje técnico y colocaran una descripción en sus palabras.

ACTA DE REGISTRO MANUAL DE UN INCIDENTE INFORMATICO

FECHA DE NOTIFICACIÓN:	HORA DE NOTIFICACIÓN:

DATOS SOLICITANTE	
SOLICITANTE:	
CEDULA/ID:	
CORREO:	
TELEFONO O EXT(EXTENSIÓN):	
DEPARTAMENTO:	
UBICACIÓN:	

ENCARGADO DEL REQUERIMIENTO	
ASIGNADO A:	
CEDULA/ID:	
CORREO:	
TELEFONO O EXT(EXTENSIÓN):	
DEPARTAMENTO:	
UBICACIÓN:	

ESTATUS DEL REQUERIMIENTO	
ESTADO:	NUEVO INCIDENTE
URGENCIA:	☐ ALTA ☐ MEDIA ☐ BAJA
IMPACTO	☐ ALTA ☐ MEDIA ☐ BAJA
PRIORIDAD:	MEDIA
ELEMENTOS ASOCIADOS:	

DATOS DEL REQUERIMIENTO	
NÚMERO DE REQUERIMIENTO:	
TITULO:	
DESCRIPCIÓN:	

FIRMA SOLICITANTE

FIRMA ENCARGADO

Figura 1. Descripción manual de un incidente

2.1.6 Reporte de incidentes vía web

Ingreso de un requerimiento de manera virtual, donde se establecerán varios parámetros que nos permitirán identificar y clasificar los incidentes, se ingresarán los datos de la misma forma que se realiza un incidente manual. Es importante tener en cuenta que, al contar con un programa destinado a la gestión de incidentes, se podrá controlar y obtener estadísticas precisas de la resolución de los incidentes en cuanto a tiempo transcurrido hasta resolverlo, incidentes similares, frecuencia de los incidentes, además de enviar el estado del incidente por el correo institucional.

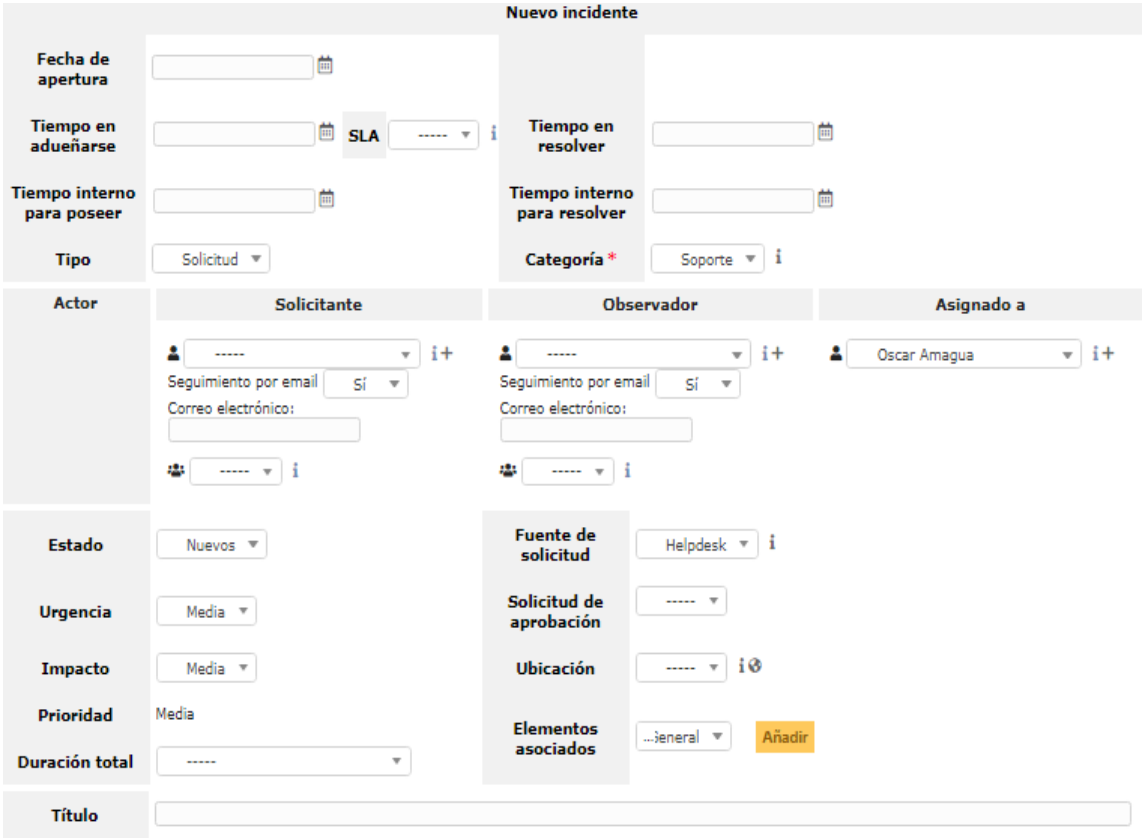

Figura 2. Ingreso vía web de un incidente.

Tomado de “ÉTICA, Metropolitana Touring: Plataforma de gestión de incidentes”, 2019.

2.2 CSIRT

Equipo de respuesta ante incidentes de seguridad informática (*CSIRT - Computer Security Incident Response Team*), es un grupo de trabajo conformado por expertos encargados de la seguridad informática, mediante la creación de medidas preventivas, proactivas, políticas de seguridad. De tal manera que se logre dar una respuesta de forma rápida y eficiente ante un incidente o amenaza, ya sea esta interna o externa, disminuyendo el impacto en la organización. Una de las funciones más importantes de un CSIRT es compartir la información recopilada del incidente con otros CSIRT de este modo se podrá analizar la forma en la que se actuó ante esta vulnerabilidad del sistema y como proceder para eliminarla de raíz. (Cedia, 2019)

2.2.1 Nombres Asociados al acrónimo CSIRT

Existen varios nombres asociados al acrónimo CSIRT de los cuales destacaremos los tres más importantes, ya que comparten las mismas responsabilidades y sus estándares son parecidos, pero cuentan con ligeras diferencias.

- Centro de Operaciones de Seguridad (SOC - Security Operations Center): Un SOC permite analizar, supervisar, prevenir y controlar la seguridad informática de una empresa ya sea esta pública o privada. Las funciones de un SOC no se encuentran limitadas únicamente a dar solución a un incidente, dado que entre sus características más importantes se encuentra el prevenir futuros ataques y a su vez monitorizar la red de tal manera que pueda identificar posibles actividades fuera de lo común. Un SOC emplea métricas que permiten evaluar la gestión de riegos dentro de una organización y lograr una respuesta ante incidentes más efectiva.

- Equipo de Respuesta ante Emergencias Informáticas (CERT - Computer Emergency Response Team): El termino CERT se caracteriza por ser una marca registrada por la Carnegie Mellon University desde 1997. Por tal motivo,

se debe pedir autorización para utilizar dicha terminología, caso contrario se estaría incurriendo en un delito contra la propiedad y se tendría problemas legales. Un CERT se enfoca en la metodología, desarrollo de herramientas avanzadas (aplicaciones preventivas) y análisis de las amenazas que vayan surgiendo día a día durante el desarrollo de las actividades diarias de la organización. (Carnage Mellon University, s.f.)

- Equipo de Respuesta ante Emergencias Informáticas (CSIRT - Computer Security Incident Response Team): Organización conformada por una o más personas, las cuales cumplen la función de mitigar o prevenir incidentes, un CSIRT puede prestar sus servicios para Naciones, Gobiernos, Organizaciones, Empresas sin fines de lucro, etc. El objetivo de un CSIRT es reducir el impacto de las amenazas e incidentes, mediante la creación de guías de respuesta, métodos de recuperación ante incidentes y medidas proactivas para evitar incidencias futuras. (Mendoza, 2015)

2.3 Funciones de un CSIRT

- Determina la importancia de un incidente, tipo de incidente y el impacto que tendrá en la organización.
- Permite conocer las derivaciones de un incidente, y a al mismo tiempo dar una solución más efectiva.
- Dar soluciones preventivas, recomendaciones para evitar futuros incidentes e investigar alternativas que permitan solucionar un requerimiento de seguridad.
- Implementar políticas de seguridad en diferentes áreas de la empresa (Recursos humanos, gerentes de negocio, contabilidad, etc.), de manera que puedan actuar de forma más eficiente ante un incidente hasta que se comuniquen con el departamento de TI.
- Comunicar información relevante sobre temas de seguridad, riesgos de seguridad, mecanismos de alerta, estrategias de mitigación de amenazas, sitios maliciosos, etc. De esta manera el usuario, podrá frenar el alcance del incidente y evitar que se propague por toda la organización.

- Elaboración de un repositorio que contenga información de los incidentes ocurridos en la organización, para solventar de manera más eficiente el incidente o amenaza. Al contar con experiencia y lecciones aprendidas de incidentes pasados y también se podrá emplear una mejor gestión de incidentes.
- Trabajar con grupos externos para solventar incidentes de gran magnitud o de un alto riesgo para la empresa, ya sean estos proveedores, CSIRT externos, grupos de seguridad, etc.
- Realizar políticas de seguridad, configuraciones más robustas, medidas de protección para la red, capacitaciones sobre seguridad, seguridad de la información crítica o prevención de incidentes.
- Realizar monitoreo de redes, sitios web, correo electrónico, equipos tecnológicos, amenazas sociales, amenazas políticas, monitorear avances tecnológicos para siempre contar con tecnología actualizada y de vanguardia.

2.4 Tipología de un CSIRT

En la actualidad los CSIRT cumplen distintas funciones o ámbitos en la sociedad u organizaciones, debido al constante crecimiento de las amenazas y formas de corromper la seguridad, por lo cual es necesario conocer los estándares, medidas y funciones que se aplican en cada sector.

2.4.1 CSIRT/CERT para el sector de las pymes

Por el tamaño de las empresas no es factible emplear un CSIRT/CERT individual, por lo cual se deberá recurrir a CSIRT privados o públicos que presten sus servicios. Un ejemplo es, CSIRT-CEDIA el cual fue creado el 21 de marzo del 2011 con el propósito de brindar servicios de seguridad informática a los miembros que pertenecen a la red CEDIA. (CSIRT Cedia, 2019)

Servicios prestados por CEDIA

- Acceso a sitios web con información preventiva sobre políticas de seguridad para miembros del grupo CEDIA.

- Sistemas de detección de intrusos para miembros del grupo CEDIA
- Bases de conocimientos que albergaran información de incidentes ocurridos, reportes y métodos de solución.
- Sistemas que permiten verificar mediante listas negras direcciones falsas para prevenir el spam.
- Capacitaciones sobre aspectos de seguridad informática dictados para miembros de grupo CEDIA.
- Apoyar a miembros del grupo CEDIA en la creación de medidas proactivas y preventivas en ámbito de seguridad informática.
- Soporte de incidencias, monitoreo y emisión de alertas.
- Responder ante incidentes cuando estos se presenten y dar seguimiento de las amenazas.

Miembros del Grupo CEDIA

- Universidades**:** Universidad de las Américas (UDLA), Universidad Central del Ecuador (UCE), Universidad Politécnica Nacional (UPN), Universidad Politécnica Salesiana (UPS), Universidad Tecnológica del Ecuador (UTE), entre otras.
- Institutos**:** Instituto Superior Tecnológico “Vida Nueva”, Instituto Superior Tecnológico Bolivariano (ITB), Instituto Tecnológico Superior Cordillera (ITSCO), entre otros.
- Colegios**:** Unidad Educativa particular Borja (UEPB), Fundación Colegio Americano de Quito (FCAQ), Centro Educativo Naciones Unidas (CENU), entre otros.
- Corporaciones**:** Conquito

(CSIRT Cedia, 2019)

2.4.2 CSIRT/CERT comercial

Un CSIRT comercial se enfoca en prestar sus servicios a clientes finales que contratan un servicio (Ejemplo: Internet), de esta forma se puede prevenir abusos de las tarifas o comprobar que el servicio ofertado es el que se está recibiendo.

Los CSIRT comerciales establecen acuerdos por sus servicios con sus clientes a cambio de una compensación económica.

2.4.3 CSIRT/CERT sector militar

Centran sus funciones en organizaciones militares, en el área de TI con propósitos de defensa, permitiendo de esta manera responder ante incidentes que afecten la estructura del Estado. Como por ejemplo tenemos el Comando de Ciberdefensa de las FF.AA.

Estructura en forma piramidal, que jerarquiza la gestión de ciberdefensa, dividiéndola en tres niveles: Sector estratégico, sector gerencial y por último el nivel técnico, mediante el cual podremos direccionar los problemas a las áreas y mejorar el actuar ante incidentes que involucren la soberanía de un país. (Revista Latinoamericana de Estudios de Seguridad, 2017)

Figura 3. Direccionamiento estratégico de ciberseguridad.

Adaptado de “Revista Latinoamericana de estudios de seguridad”, 2019.

2.4.4 CSIRT/CERT gubernamental

Un CSIRT Gubernamental se enfoca en asegurar los servicios de TIC que son suministrados a la población de una nación, por ejemplo, servicios de telecomunicaciones, además de preocuparse por el bienestar de los ciudadanos. Este tipo de CSIRT esta orientados a direcciones públicas y sus trabajadores. Los CSIRT gubernamentales son patrocinados por organizaciones estatales. De acuerdo con las políticas manejadas por el estado, se podría dar el caso de que un CSIRT militar pueda ser tratado como un CSIRT gubernamental o cada uno puede ser independiente. (Ministerio del interior y seguridad pública de Chile, 2018)

La mayoría de las naciones ven como una buena práctica a futuro que los CSIRT/CERT compartan estrategias comunes, por lo cual se ha buscado mecanismos y modelos que permitan la creación de alianzas y/o colaboraciones del sector público y privado para logran la creación de un CSIRT Nacional y gestionar de mejor manera las crisis e incidentes que afecten a todo un estado.

2.4.5 CSIRT/CERT nacional

Se encarga de la coordinación de todos los sectores tratados anteriormente, además de atender amenazas y requerimientos nacionales como internacionales. Según la Agencia Europea de Seguridad de Redes y de la Información (*ENISA - European Network and Information Security Agency*), un CSIRT nacional funciona como punto de contacto entre dos CSIRT nacionales (Miembros de UE y el resto del mundo) para el intercambio de información sobre amenazas o vulnerabilidades. En muchos casos un CSIRT nacional puede ser tratado como un CSIRT gubernamental. Los estándares varían de acuerdo con las políticas o medidas que se manejen en casa estado. (Ministerio del interior y seguridad pública de Chile, 2018)

CSIRT/CERT nacional “de facto”

Actúa como un CSIRT nacional cuando en un país no se ha oficializado un CSIRT, De esta manera las otras naciones lo percibirán como un CSIRT nacional, y podrá tratar temas fronterizos e internacionales. Además de poder actuar ante amenazas o incidentes que afecten a todo un estado. (Ministerio de defensa de España, 2011)

Centro de respuesta a incidentes informáticos del Ecuador (EcuCERT)

ECUCERT es el grupo de respuesta ante incidentes por parte de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), el cual presta sus servicios para el cumplimiento de la Ley Orgánica de Telecomunicaciones. A continuación, se enunciarán sus funciones.

- Ser el punto de contacto de otros equipos de respuesta ante incidentes internacionales, para dar solución a amenazas que tengan impacto crítico sobre un país.
- Encargados de promover la creación de equipos de respuesta ante incidentes (CSIRT), y cuya función se desarrolle en el ámbito de las telecomunicaciones.
- Dar capacitaciones, actividades de prevención ante incidentes, buenas prácticas para el correcto uso de las telecomunicaciones estatales y manejo de herramientas que no afecten el adecuado funcionamiento o trabajo de las redes de telecomunicaciones de una nación.
- Monitorización de proveedores de servicios de telecomunicaciones, para que cumplan con los estatutos establecidos en la Ley Orgánica de Telecomunicaciones (LOT).
- Establecer políticas y medidas entre EcuCERT, ARCOTEL y proveedores para mantener una correcta gestión de incidentes de seguridad, asegurando un correcto uso de las telecomunicaciones y evitando vulnerabilidades en la red.

2.4.6 CSIRT/CERT académico

Está enfocada para instituciones académicas, ya sean estas escuelas, colegios, institutos y universidades. Los requerimientos y el personal limitaran el número de servicios prestados y además se tendrá que ajustar a las políticas y reglas establecidas en la Unidad Educativa, de esta manera se podrá determinar el campo sobre el cual actuara el Equipo de respuesta ante incidentes de seguridad. (Nacional, 2011)

CERT académico – CertUNLP

Ejemplo tomado de la Universidad Nacional de la Plata, en el cual se podrán analizar los datos obtenidos durante su primer año de funcionamiento. Este proyecto surgió dada la necesidad de contar con un CSIRT ante el creciente número de incidencias y amenazas en la universidad. Durante el primer año se recopilaron los datos de las amenazas e incidentes suscitados, lo que permitió conocer el trabajo conjunto que realizan los miembros del equipo de respuesta ante incidentes de seguridad y las diferentes áreas involucradas. De igual manera, se realizaron procesos de mejora del servicio, es decir se agregó valor al actuar del equipo de respuesta, mediante el desarrollo de herramientas de automatización, monitoreo proactivo, capacitaciones, procedimientos, políticas, análisis preventivos, etc. (Lanfranco, Macia, Venosa, Molinari, & Díaz, 2010)

Uno de los principales objetivos del CERTUNPL es prestar servicios de seguridad contra incidentes, para salvaguardar activos críticos y solventar incidencias producidas en la red.

Resultados obtenidos

- Elaboración una página web pública http://www.cert.unlp.edu.ar donde encontraremos recomendaciones, prácticas preventivas de seguridad y se podrá solicitar ayuda para solventar un incidente, ya sea este interno o externo a la institución.

- Entablar relaciones con otros CERT, para solucionar incidentes de mayor escala, por lo cual se realizó una alianza de trabajo conjunto con ArCERT (CERT Gubernamental Argentino).
- Se realizaron charlas continuas de seguridad a todos los miembros de la universidad.
- Lograr un reconocimiento por parte de la universidad, tomando el proyecto como referente al hablar de temas de seguridad, hackers, prácticas preventivas, políticas de seguridad, etc. (Lanfranco, Macia, Venosa, Molinari, & Díaz, 2010)
- Brindar de forma oportuna recomendaciones de seguridad, vulnerabilidades, amenazas a la red, prevención de ataques cibernéticos.
- Realizar capacitaciones de seguridad y medidas de seguridad tecnológica.
- Implementación de sensores de seguridad y HoneyPots en toda la red, de tal manera que se puedan identificar posibles ataques a nuestra red informática.
- Monitoreo de la red, teniendo en cuenta las restricciones establecidas para cada área.
- Garantizar la disponibilidad de los servicios de red y un rápido restablecimiento de los servicios, si se diera el caso de una falla o incidente del sistema. (Lanfranco, Macia, Venosa, Molinari, & Díaz, 2010)

2.5 Brechas de seguridad

Una brecha de seguridad puede ser producida de forma accidentalmente o provocada, teniendo consecuencias que afectan directamente a la información de usuarios u organizaciones, provocando daños materiales o inmateriales. De manera general se puede definir a una brecha de seguridad como el: robo de información, alteración de la información, acceso no autorizado, difusión de información personal, etc. (Agencia española de datos, 2019).

Un claro ejemplo de una brecha de seguridad informática se dio en la Universidad de Valladolid (UVA), el denominado hacker “takedownroot” expuso una serie de falencias en el sistema al enviar varios expedientes de estudiantes

a personal administrativo de la institución. Debido a que no se contaba con un sistema de gestión de riesgos robusto, lo que hizo posible el filtrado de los datos. Dentro del contenido se encontraba información como: el número de cuenta bancaria del estudiante, teléfonos personales, datos de la cedula de identidad, direcciones postales, etc. (Rey, 2019)

2.6 CSIRT en Europa

European union agency for cybersecurity

Prestan servicios de seguridad desde el año 2004, localizados en Atenas - Grecia. Actualmente se encuentran colaborando con los estados que son participes de la Unión Europea, para brindar apoyo sobre incidentes cibernéticos de gran magnitud y se desarrollen fuera de los límites fronterizos. Realizan trabajos conjuntos con empresas privadas para brindar asesorías y soluciones a requerimientos. Apoyan la creación, desarrollo e implementación de políticas de seguridad de la información. (Enisa, 2019)

Capacidades

- Estrategias de prevención y seguridad nacional.
- Análisis sobre la tecnología IoT (Internet of things - Internet de las cosas), infraestructura robusta e inteligente, métodos de protección de la información, servicios confiables, análisis de amenazas cibernéticas, etc.
- Realizar recomendaciones de seguridad y métodos de mitigación de amenazas
- Creación de políticas de seguridad ajustadas a los diferentes tipos de estructuras.

Estadísticas de los países miembros de la UE (Unión Europea) que prestan servicios de CSIRT, donde encontraremos información que nos permitirá determinar el número de miembros que integran esta comunidad y a su vez los que no la conforman, además de obtener datos sobre el nivel de infraestructura o madurez con el que cuentan los diferentes equipos, ya que al contar con estos

datos se podrá verificar que la información proporcionada durante un incidente será verídica, eficiente y efectiva. De esta manera una organización o usuario podrá escoger el CSIRT correcto o que se ajuste a sus necesidades. (TF-CSIRT, 2019)

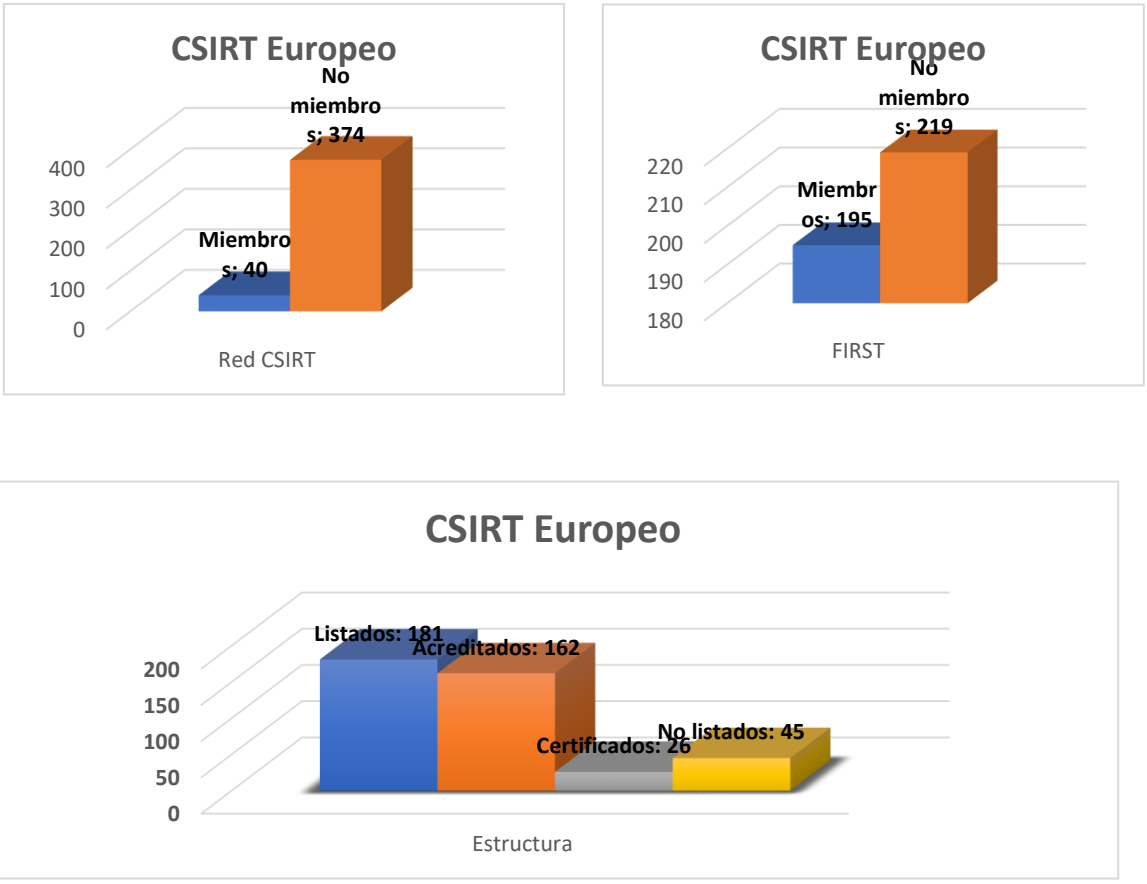

Figura 4. CSIRT por países – Mapa interactivo

Adapt ado de “CSIRTs by Country: Interactive Map”, 2019

Red CSIRT

Sitio en el cual se expone, dialoga, recomienda, da información, métodos de solución de incidentes informáticos. Los miembros podrán acudir en cualquier momento y solicitar ayuda para solventar incidentes fronterizos de alto impacto

para una nación. La red CSIRT se encuentra conformada por miembros pertenecientes a CERT-EU y UE. ENISA apoyar de manera activa la solución de incidentes bajo pedido, con el fin de tener una cooperación y confianza entre los estados miembros y solventar una incidencia de manera rápida y efectiva. (CSIRT España, 2019)

2.7 CSIRT en América Latina

En la siguiente imagen observamos los países de América Latina que cuentan con equipos CSIRT nacionales o gubernamentales, se puede constatar que no todos los países emplean la marca registrada CERT por Carnegie Mellon University, por el contrario, emplean un modelo que se ajuste a sus necesidades y conveniencias, de igual manera podrán transmitirse conocimientos o prestar ayuda si fuera necesario para evitar que un incidente sea mucho más grave y tenga un impacto sobre otras naciones.

Figura 5. CSIRT en América Latina

Tomado de (Sullivan, Tendencias de Seguridad Cibernética en América Latina y el Caribe, 2014).

Al surgir por primera vez el nombre FIRST (Foro de Equipos de Respuesta a Incidencias Informáticas) en 1989, se vivía un ambiente diferente al actual. En esos años los equipos de respuesta trabajaban ya en problemas críticos a nivel mundial, no obstante, al propagarse el gusano informático Morris, el cual en 1988 empezó a infectar los ordenadores conectados a la red, y afectando a aproximadamente un 10 % de máquinas en el mundo, alrededor de 6000 computadores aproximadamente, lo cual en esa época era una cifra inimaginable. (FIRST, 2019)

Trasladándonos al presente, podemos nombrar unos cuantos problemas complejos como:

- Ataques de denegación de servicio distribuido (DDoS) de hasta 500 Gbps, además estos ataques se generan debido a una ineficiente configuración de miles de terminales, por lo cual es casi imposible que una sola nación pueda resolver este incidente.
- Código malicioso, que aprovechan vulnerabilidades en los sistemas para realizar ataques informáticos.

2.7.1 Ataques cibernéticos en América Latina

La vulnerabilidad de seguridad de la información en las empresas ha provocado que los incidentes y amenazas aumenten de manera exponencial, por lo cual los gobiernos y países han buscado alternativas para mitigar el gran número de problemas relacionados con la ciberseguridad, como lo es la implementación de CSIRT o CERT en América Latina. En la siguiente imagen podremos observar los ataques de programas malignos por país. ESET realiza anualmente un informe en el cual se analizan las interrogantes, preguntas, incidentes, controles, respuestas, preocupaciones de más de 2500 empresas de América Latina, de esta manera se puede determinar el nivel vulnerabilidad de los países. (Harán, 2018)

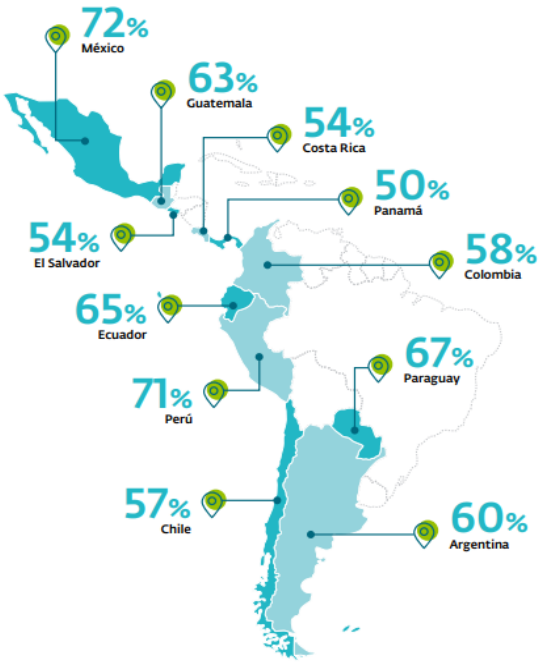

Figura 6. Incidentes de ciberseguridad por país

Tomado de (ESET, 2019).

Según estadísticas del Banco Interamericano de Desarrollo (BID) y la organización de Estados Americanos (OEA), la mayoría de los países carecen de estrategias de seguridad robustas o no las tienen, por lo cual son un foco mundial para el intento de acceso a información confidencial, no obstante, hay países que ven como buena práctica el implementar políticas de seguridad nacionales y conformar equipos de respuesta más estructurados y organizados.

El mundo cibernético está creando un gran crecimiento económico y mejorando la calidad de vida. Pero al mismo tiempo nos expone a problemas que hace unas décadas, eran vistos como incidentes inimaginables, es por tal motivo que América Latina debe mejorar la seguridad cibernética si desea contar con un entorno beneficioso a futuro. El acceso a internet ha impulsado la productividad en un 25%, obteniendo ganancias de crecimiento de PIB (Producto interno bruto) de más 72%. De manera que será necesario cerrar brechas con otras naciones y cooperar por un bien común. Afortunadamente se ve una clara iniciativa de desarrollo de las tecnologías y alianzas que permitirán mejorar las capacidades

y conocimientos sobre ciberseguridad, y la implementación de políticas de seguridad, así como la creación de nuevas. (Powell, 2018)

2.8 Foro de equipos de seguridad y respuesta a incidentes.

Organización líder en el ámbito de respuesta a incidentes, contar con una membresía para el foro de equipos de seguridad y respuesta a incidentes (*FIRST - Forum of Incident Response and Security Teams)*, permitirá solventar inconvenientes de seguridad tanto reactivos como proactivos. FIRST trabaja juntamente con varios equipos de respuesta a incidentes de seguridad nacionales, gubernamentales, educativos, comerciales. El objetivo de FIRST consiste en fomentar la cooperación entre los países miembros y la coordinación de una respuesta rápida y eficiente, promoviendo el intercambio de la información entre los participantes y la comunidad. (FIRST, 2019)

2.8.1 Servicios prestados

- Brindar acceso a documentación útil para solventar un incidente o requerimiento.
- Recomendar mejores prácticas de seguridad informática.
- Clases prácticas y teóricas de seguridad informática.
- Acceso a conferencias anuales sobre la respuesta a incidentes de seguridad informática.
- Publicaciones y foros de interés, para los miembros.
- Compartir información, métodos, procedimientos y mejores prácticas.
- FIRST se encarga de fomentar el buen uso y creación de políticas de seguridad de calidad.

2.9 Recursos comunitarios internacionales

2.9.1 ITU

La UIT o ITU es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación (TIC). Fue fundada con el fin de

ayudar a las comunicaciones internacionales, además de conceder el espectro radioeléctrico global, se encarga del desarrollo de las normas técnicas que permitan una conexión sin problemas e interferencias. Uno de los objetivos más importantes y desatacados por la ITU es el buscar que todas las zonas que no cuenten con servicios de comunicaciones (telefonía celular, internet, enviar mensajes electrónicos, etc.), tengan en algún momento los servicios que en la actualidad son de uso cotidiano, conectando a cada persona del mundo. (Unión Internacional de Telecomunicaciones)

2.9.2 ITU servicios prestados

- Servicios de llamadas telefónicas, ya sean estas nacionales o internacionales. Las normas y métodos proporcionados por la UIT permiten contar con un sistema de comunicaciones global.
- Organiza los satélites que se encuentran orbitando la tierra, permitiendo realizar una gestión del espectro y las orbitas, ofreciéndonos servicios como la televisión, GPS, datos meteorológicos, etc.
- Permite el acceso al servicio de la internet.
- La UIT presta servicios comunitarios en caso de desastres naturales o emergencias, habilitando canales de transmisión exclusivos o dedicados.

3. CAPÍTULO III. RIESGO TECNOLÓGICO

3.1 Introducción

En el presente capitulo se analizarán las zonas y puntos de alto riesgo tecnológico dentro de las organizaciones, teniendo en cuenta los factores y amenazas que causan un gran impacto en la seguridad de la información, tomando como punto de partida los criterios que nos ofrece la norma ISO/IEC 27002 para el análisis de dominios y su escala de cumplimiento, de manera que se puedan establecer los procesos de mayor impacto en la universidad. (UNAM, 2018)

3.2 Criterios para la evaluación del riesgo

Definir los criterios para la evaluación de riesgos, permitirá identificar de manera más precisa las áreas de riesgo que existen dentro y fuera de la organización y que afecten el trabajo diario e información de los miembros, de tal manera que se pueda establecer prioridades que permitan tratar los incidentes, teniendo en cuenta como base los factores que han sucedido en años anteriores y de los cuales se tenga registro, entre los cuales se debe considerar: (CEDIA, 2014)

- El valor estratégico del proceso
- El nivel crítico de los activos de la organización
- La ocurrencia de los incidentes
- Valor de los activos
- Definir el número de niveles críticos

3.2.1 Impacto en la organización

En este nivel se podrá identificar el impacto y daño del incidente de seguridad informática, además de las consecuencias que tendrá la organización, al no cumplir los objetivos propuestos. Comúnmente todos los incidentes tienen un impacto financiero sobre la empresa, por lo cual se debe considerar: (CEDIA, 2014)

- La afectación de las operaciones
- El atraso de los procesos y entregas
- Problemas legales
- La gravedad y nivel crítico de los incidentes
- Integridad, confidencialidad y disponibilidad de la información.

3.2.2 Nivel de impacto del riesgo

Permite definir el nivel del riesgo y aceptación de un problema en la organización, dependiendo de las políticas de seguridad y sus objetivos. Evaluar la criticidad

del riesgo en la empresa permitirá establecer una estrategia para abordar el problema sin importar el nivel (alto, medio o bajo). De manera que se pueda mitigar el menor tiempo posible y con la menor afectación para la organización. Se debe tener en cuenta lo siguiente: (CEDIA, 2014)

- Aspectos y normas legales
- Área financiera
- Problemas sociales
- Problemas operacionales
- Infraestructura
- Planes a futuro
- Naturaleza del riesgo

3.3 Riesgo Tecnológico

El riesgo tecnológico crece exponencialmente junto con el incremento de las herramientas empleadas y servicios prestados, uno de los factores que influye directamente con el problema son las constantes actualizaciones y cambios de las medidas de protección tecnológicas, las cuales suelen presentar bugs o fallas del programa, este percance suele ser usado como puente o medio de intrusión y permitir ataques intencionados a los sistemas educativos y sus servicios. (Universidad Internacional de Valencia, s.f.)

3.3.1 Factores que influyen en la seguridad tecnológica

Al profundizar dentro de los objetivos, metas y estándares de cada organización y empresa podemos comprender que detrás de los servicios y planteamientos ofrecidos se encuentran sobre una base de infraestructura tecnológica que permite el correcto funcionamiento de las operaciones y a su vez la continuidad del negocio, por tal motivo es indispensable mantener un cuidado y conservación de la estructura tecnológica y todo lo que lo conforma. (SGSI, 2017)

3.3.1.1 Infraestructura tecnológica

Lo que conforma el nivel físico o hardware se podría considerar lo más costoso dentro de un sistema informático y por ende las medidas de seguridad que permitan asegurar su integridad son primordiales en cualquier organización. Los mecanismos de mitigación ante un incidente físico son de carácter técnico, es decir procedimientos y controles físicos que permitan prevenir daños o accesos no autorizados a los recursos e información. (SGSI, 2017)

- Acceso físico a los recursos e información en áreas específicas.
- Control de acceso mediante carnet de identificación o reloj biométrico.
- Interacción de los sistemas con los servicios básicos (Agua y energía) utilizados en la empresa
- Métodos y mecanismos de control de hardware
- Mantenimiento de los equipos físicos

3.3.1.2 Nivel lógico

Emplear técnicas y métodos que permitan incrementar los niveles de seguridad informática dentro de una organización, de manera que se logre asegurar los datos y servicios utilizados. Estas medidas permitirán un control de acceso dependiendo de los permisos y privilegios establecidos para cada usuario. Una brecha de seguridad lógica implica una vulnerabilidad en los sistemas, no necesariamente afectando la parte física o hardware, logrando mantenerse imperceptible hasta el momento de visualizar o realizar procesos con datos, por lo cual la extensión del problema es desconocido. (Universidad Internacional de Valencia, s.f.)

- Virus, gusanos, troyanos
- Emplear software sin su respectivo testeo
- Errores de los usuarios
- Uso indebido de los equipos
- Accesos no autorizados internos y externos

3.3.1.3 Recurso Humano

El factor humano es el más crítico dentro de las organizaciones, debido a las diferentes personalidades y criterios de cada persona, por lo cual es impredecible determinar el accionar de los usuarios. La metodología empleada está enfocada en los procedimientos, políticas y acuerdos. Además, todos los errores que sean cometidos por el usuario serán referenciados hacia el equipo o departamento de TI, ya que todos los incidentes deberán ser prevenidos y a su vez contar con un plan de contingencia. (Universidad Internacional de Valencia, s.f.)

- Procedimientos de manejo de la información
- Aceptación de las políticas de seguridad
- Capacitación continua de las herramientas empleadas
- Capacitación continua de sobre seguridad Informática
- Normativas de uso de la red y equipos

3.4 Servicios tecnológicos empleados en la UDLA.

El nivel educativo de alto nivel es uno de los factores que caracterizan a la UDLA, por ende, el contar con un amplio catálogo de servicios ayudará a cumplir con los estándares que se desea ofrecer a los estudiantes y al personal que forma parte de la institución, de tal manera que la gestión de TI y el uso de tecnologías actualizadas aumentará de manera exponencial los riesgos y beneficios dentro de la institución.

3.4.1 Catálogo de servicios

1. Soporte técnico	
• Soporte de Equipos (Hardware)	• Ayuda Telefónica • Conexión Remota • Mantenimiento Preventivo • Mantenimiento Correctivo • Garantías • Soporte presencial
• Antivirus	• Kaspersky antivirus

• Software Utilitario	• Matlab • Office 2013 • Adobe • Windows/MacOS/Linux/Android/iOS
2. Correo electrónico	
• Servicios en línea	• Microsoft office 365
3. Servicios Tecnológicos	
• Impresión	• Cambio de tóner impresora • Cambio tinta
• Parqueadero	• Máquina boletos parqueadero
• Telefonía	• Extensiones Telefónicas
4. **Conectividad**	
• Wifi	• SSID • Calidad de la señal
• Navegación	• Bloqueo de páginas con contenido de spam, virus e inseguras.
5. **Accesibilidad**	
• Contraseña	• Bloqueo de usuario • Cambio de contraseña • Permisos de usuario

Tabla 1. Catálogo de servicios

3.4.2 Activos primarios

Categorías	**Activos**
• Nivel Físico	• Computadoras • Impresoras • Periféricos • Equipos tecnológicos • Cableado estructurado • Dispositivos de acceso • Almacenamiento de los equipos (discos duros) • Acceso biométricos • Equipos de comunicación
• Nivel Lógico	• Aplicaciones

	• Antivirus • Servicio en la nube • Equipos móviles • Manejo de la información • Acceso a la red
• Recurso Humano	• Personal técnico • Personal administrativo • Personal de mantenimiento • Personal de seguridad

Tabla 2. Activos primarios

3.4.3 Vulnerabilidades y amenazas

Categorías	**Amenazas**
• Nivel Físico	• Daño de equipos • Robo de hardware • Desastres naturales • Daño de los activos físicos • Venta o cambio de equipos sin el protocolo de eliminación de información correcto.
• Nivel Lógico	• Robo de identidad • Contraseñas débiles • Actualizaciones de software • Brechas de seguridad • Cierre de sesión • Phishing, spyware, virus • Emplear contraseñas distintas • Actualización de aplicaciones • Malware

	• Denegación de servicios
• Recurso Humano	• Robo de información • Daño de información • Incidentes accidentales y provocados • Implementación de software sin licencia • Enlaces y sitios dudosos

Tabla 3. Vulnerabilidades y amenazas

3.5 Aplicación del estándar ISO/IEC 27002

En este apartado se recomendarán las mejores prácticas de seguridad de la información para preservar la confidencialidad e integridad de los datos en la UDLA, tomando como referencia el estándar de seguridad ISO/IEC 27002, en el cual se deberán definir una serie de directrices para aplicar y administrar controles, tomando en cuenta el análisis de riegos dentro de la universidad. (ECU RED, s. f.)

Dominio	Característica del dominio
Objetivos de control	Numero de objetivos de control
Controles	Número de controles por objetivo
Descripción	Definición del objetivo agrupado en un dominio
ID	Importancia del dominio
CC	Cumplimiento del control
IC	Importancia del control
Escala	Escala de cumplimiento del control

Tabla 4. Definiciones y abreviaturas ISO 27002.

En la siguiente plantilla serán establecidos los dominios y criterios propuestos como los puntos más críticos dentro de la organización, compartiendo una idea

general de la implementación de la norma ISO 27002, definiendo un objetivo principal para cada criterio a ser tratado y los procesos que lo conforman.

- Escala de valoración

	Alto	70 % al 100%
	Medio	31% al 69 %
	Bajo	0 % al 30 %

Tabla 5. Dominios ISO 27002.

- Dominios de la norma ISO 27002

Dominio	Objetivos de Control	Controles	Descripción	% Cumplimiento			
				ID	CC	IC	Escala
5	1	**2**	**Políticas de seguridad**	**100**	**90**		
		1	Documento de nivel superior con las políticas de seguridad			**90**	
		2	Revisión documental			**90**	
6	1	**5**	**Organización de la seguridad**	**100**	**84**		
		1	Designar responsables para la administración de la seguridad de la información			**80**	
		2	Establecer esquemas de administración de la seguridad de la información			**80**	
		3	Aprobación por parte de los involucrados sobre el acuerdo de confidencialidad			**90**	
		4	Evaluación de riegos de la seguridad de la información			**80**	
		5	Revisión de procesos críticos dentro de la organización			**90**	
7	1	**4**	**Seguridad de los recursos humanos**	**100**	**65**		
		1	Inducciones y capacitaciones al personal nuevo			**50**	
		2	Revisión de las políticas de seguridad			**70**	
		3	Utilización de la información			**70**	
		4	Revisión de los procesos disciplinarios			**70**	
8	1	**5**	**Gestión de los activos**	**100**	**64**		
		1	Revisión de los activos empleados diariamente			**50**	
		2	Administración de inventarios informáticos			**70**	
		3	Conocimiento de los activos de información			**70**	
		4	Conocimiento de los activos de hardware			**70**	
		5	Conocimiento de los activos de software			**60**	
9	**1**	**7**	**Control de acceso**	**100**	**80**		
		1	Control de acceso a la información			**80**	
		2	Control de uso de los servicios			**80**	
		3	Seguridad de equipos, usuarios y servicios			**80**	
		4	Prevención de amenazas internas y externas			**90**	

		5	Política de acceso			**70**	
		6	Designar privilegios a usuarios			**80**	
		7	Autenticación de ingreso y salida de los usuarios			**80**	
		3	**Cifrado de información**	**100**	**83.33**		
10	**1**	1	Evaluación de riegos de la seguridad de la información			**80**	
		2	Proceso de validación de la información			**80**	
		3	Protección de los dispositivos			**90**	
		5	**Seguridad física y ambiental**	**100**	**72**		
		1	Ingreso físico no autorizado			**80**	
11	**1**	2	Controles de seguridad			**80**	
		3	Estudios de la zona de trabajo			**70**	
		4	Protocolos de protección y seguridad			**70**	
		5	Eliminación completa o parcial de los equipos			**60**	
		5	**Seguridad de operaciones**	**100**	**82**		
		1	Proceso de manejo y uso de datos			**90**	
12	**1**	2	Operaciones de mantenimiento			**70**	
		3	Proceso de actualización			**80**	
		4	Renovación de sistemas y equipamientos			**80**	
		5	Seguridad de la información enviada y recibida			**90**	
		6	**Seguridad de las comunicaciones**	**100**	**90**		
		1	Monitoreo de la redes			**90**	
		2	Protocolos ante software malicioso			**90**	
13	**1**	3	Monitoreo de los servicios			**90**	
		4	Políticas de manejo de información			**90**	
		5	Capacitaciones sobre el uso del o los sistemas			**90**	
		6	Revisión de la creación de Backus			**90**	
		5	**Adquisición de sistemas, desarrollo y mantenimiento**	**100**	**88**		
		1	Procesos y mecanismos de protección de la información			**80**	
14	**1**	2	Mantenimiento de software de operaciones			**90**	
		3	Actualización de los sistemas			**90**	
		4	Manejo de las vulnerabilidades			**90**	
		5	Integridad de la información			**90**	
		3	**Relación con proveedores**	**100**	**86.67**		
15	**1**	1	Controles de seguridad de la información			**90**	
		2	Monitoreo de los servicios de terceros			**80**	
		3	Verificación de los acuerdos de servicio			**90**	
		4	**Gestión de incidencias**	**100**	**85**		
		1	Mecanismos de alerta ante incidentes			**90**	
16	**1**	2	Administración de la base de conocimiento			**80**	
		3	Medidas activas y proactivas de seguridad			**90**	
		4	Reporte y registro de las actividades			**80**	
17	**1**	**4**	**Continuidad del negocio**	**100**	**87.5**		
		1	Mecanismos de respuesta ante incidentes, amenazas o emergencias			**90**	

		2	Servicios en línea las 24 horas			**80**	
		3	Estrategias para reactivación inmediata del negocio			**90**	
		4	Análisis de los riegos producidos por la incidencia			**90**	
		4	**Cumplimiento**	**100**	**90**		
		1	Cumplimiento de las normas legales			**90**	
18	**1**	2	Conocimiento de las sanciones civiles y penales			**90**	
		3	Cumplimiento de las políticas y normas empresariales			**90**	
		4	Protección de la información			**90**	

Tabla 6. Plantilla dominios ISO 27002.

4. CAPÍTULO IV. ANÁLISIS INICIAL

4.1 Introducción

En el presente capitulo se analizarán los procedimientos de seguridad de la información que emplea la Universidad de las Américas, los recursos existentes para mitigar una incidencia, se estudiara el modelo estructural que utiliza y se examinara la situación en la que se encuentra actualmente la universidad, de tal manera que se pueda determinar las áreas con mayor impacto positivo al establecer un equipo de respuesta ante incidentes de la información.

4.2 Estado actual de la UDLA

La Universidad de las Américas (UDLA) fue creada en el año de 1994, con el objetivo de ofrecer servicios académicos, tomando en cuenta los aspectos económicos y sociales, a partir de su creación el catálogo académico fue creciendo exponencialmente, hasta la actualidad en la cual se ofrecen 37 alternativas de carreras en las diferentes modalidades y horarios. A partir del 2006 la UDLA incursiona en un nuevo campo ofreciendo servicios académicos de cuarto nivel, a la fecha se ofrecen 20 alternativas de maestrías. En este corto pero fructífero periodo la UDLA ha buscado posicionarse como una universidad de vanguardia, dedicando un gran esfuerzo en las áreas de investigación, desarrollo académico y una interacción directa con la comunidad. (Universidad de las Américas, 2019)

4.2.1 Estructura organizacional

La UDLA cuenta con una estructura organizacional jerárquica en la cual el máximo órgano académico es el consejo superior o consejo universitario conformado por:

- Canciller: Carlos Alfonso Larreátegui Nardi
- Rector
- Vicerrector académico
- Vicerrector administrativo
- Decanos de las facultades
- Representantes del personal académico
- Representantes de los estudiantes
- Representante de los empleados y trabajadores de la institución

(Universidad de las Américas, 2019)

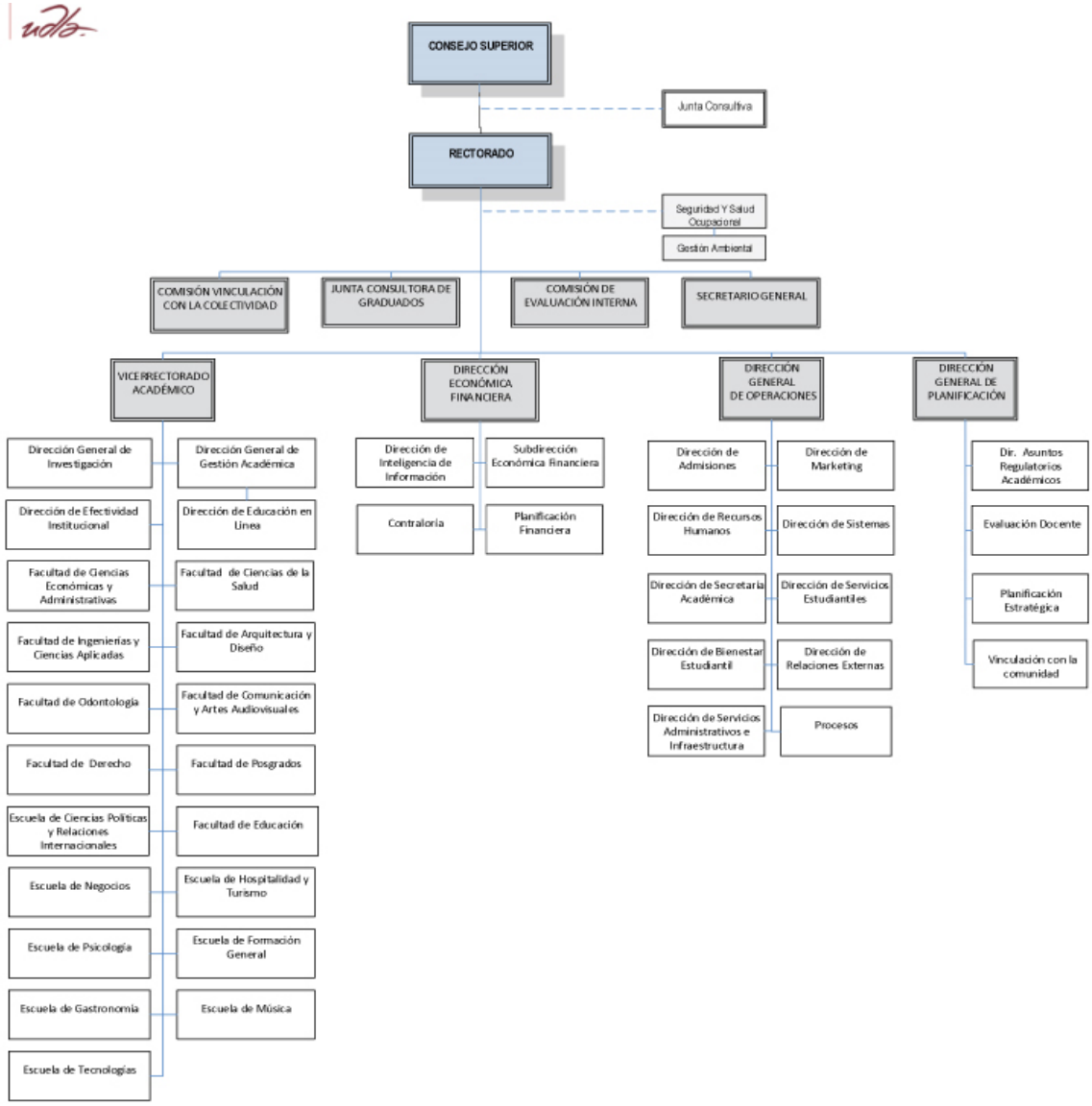

Figura 7. Estructura organizacional UDLA.

Tomado de “Universidad de las Américas: Estructura organizacional”, 2019.

4.3 Áreas de gestión estratégica

La UDLA emplea un plan estratégico desarrollado e implementado en el 2015 por parte del Consejo Superior, el cual a su vez representa el máximo organismo dentro de la universidad. La dirección general de planificación y desarrollo fue la

encargada de desarrollar el análisis FODA, mediante el cual fue posible el desarrollo de los objetivos y estrategias que son implementadas actualmente, para ello se tomó en cuenta a todos los miembros que conforman la Universidad de las Américas.

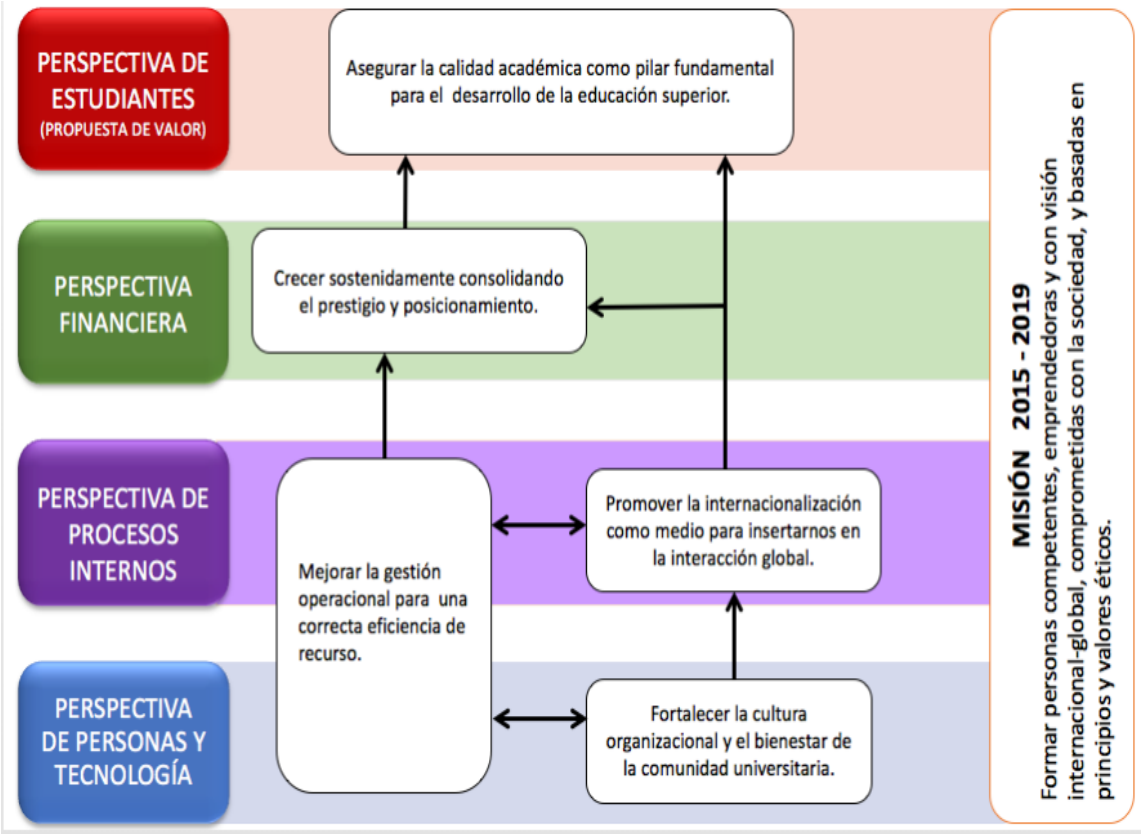

Figura 8. Áreas de gestión estratégicas.

Tomado de “Universidad de las Américas: Misión”, 2019.

4.4 Análisis de seguridad de la información

Al diseñar nuestro CSIRT académico nos encontramos con varios obstáculos, debido a los diferentes roles instituciones (docentes, estudiantes, administrativos, investigadores) que forman parte de la UDLA, además de contar con diferentes áreas o departamentos pertenecientes al campus (cafetería, biblioteca, salones de clase, áreas recreativas, etc.) y por último los servicios

(office 365, internet, telefonía, etc.) que son ofrecidos, de manera que existirán inevitablemente problemas que condicionen el éxito total de un equipo de TI, además de dificultar el diseño de metodologías, estándares de uso, y por sobre todo asegurar la confidencialidad e integridad de la información de los usuarios.

La evaluación de riesgos, mediante medidas técnicas y operacionales nos permitirá, actuar de manera más precisa y profunda al tener claro en qué área se corre un riesgo de seguridad más alto, esto conllevará a la realización de buenas prácticas y el establecimiento de una excelente política de seguridad. (Salvatierra, Díaz, Fara, & Salvatierra, 2016)

4.4.1 Estándar ISO/IEC 27002

Proporciona varias recomendaciones que nos permitirán realizar un mejor manejo de la seguridad informática, la cual se encuentra definida en el estándar ISO como: “la preservación de la confidencialidad, integridad y disponibilidad de la información”. En la siguiente tabla se definirán los dominios empleados en el estándar ISO/IEC 27002, con el fin de poder adaptarlos a la realidad de la universidad. (ISO, 2013)

ISO/IEC 27002	
Dominio	Descripción
Políticas de seguridad	Procesos empleados por la universidad para actuar frente a un riegos, amenaza o incidente de seguridad. Descritos sobre un documentos de nivel superior en cual se establecen los acuerdos de seguridad informática dentro de la organización. (ISO tools excellence, 2018)
Organización de la seguridad de la información	En este dominio se establecerán los esquemas para administrar la

	seguridad informática dentro de la organización, de manera que podamos asignar las tareas y responsabilidades al personal o área específica y que cuente con las herramientas necesarias para asegurar la protección de los datos. (ISO tools excellence, 2018)
Seguridad de los recursos humanos	En esta dominio se dará un gran enfoque en las inducciones y capacitaciones al personal nuevo y de planta sobre seguridad informática dentro de la empresa, para evitar o disminuir errores humanos que afecten el desarrollo de sus tareas diarias, asi como también se revisará las políticas de seguridad establecidas en la organización. (ISO tools excellence, 2018)
Gestión de los activos	Dar a conocer a los miembros de una entidad los activos con los que se trabaja diariamente y los riegos que estos conllevan al no adoptar las medidas y políticas de seguridad establecidas en la organización. (ISO tools excellence, 2018)
Control de accesos	Administrar los accesos a la información y servicios dependiendo de las funciones realizadas por el usuario en una organización. (ISO tools excellence, 2018)

Cifrado	Mecanismos de cifrado de la información, de manera que se pueda asegurar la integridad, confidencialidad y legitimo uso de los datos. (ISO tools excellence, 2018)
Seguridad física y ambiental	Se establecerá medidas de seguridad, asi como áreas restringidas para el personal no autorizado, de manera que se logre asegurar la integridad y disponibilidad de los servicios dentro de la organización. (ISO tools excellence, 2018)
Seguridad de las operaciones	Procesos de seguridad al realizar las operaciones de mantenimiento o actualización de la información, asi como el análisis de los cambios o renovaciones de los sistemas y equipamientos, de manera que se asegure su correcta implementación en la organización. (ISO tools excellence, 2018)
Seguridad de las comunicaciones	Mecanismos y procesos que permitan asegurar la confidencialidad, al utilizar sistemas de datos, voz y video, etc. De manera que se pueda asegurar el acceso seguro a los servicios internos y externos que se conecten a la red corporativa. (ISO tools excellence, 2018)
Adquisición de sistemas, desarrollo y mantenimiento	Evaluar y asegurar el proceso de desarrollo, adquisición y mantenimiento de los sistemas, de

	manera que se logre dar cumplimiento a los objetivos de la organización. También se determinarán los procesos y mecanismos de protección de la información.
Relación con los proveedores	Controles de seguridad de la información de los servicios contratados y verificación del cumplimiento de los acuerdos de servicio establecidos en los contratos con terceras personas. (ISO tools excellence, 2018)
Gestión de incidencias que afectan a la seguridad de la información	En este dominio se establecen los mecanismos para la notificación y resolución de incidentes de la manera más efectiva. Es indispensable contar con una base del conocimiento en la cual se almacenará la información de los incidentes solucionados, de tal manera que se puedan solucionar incidentes parecidos en un menor tiempo. (ISO tools excellence, 2018)
Aspectos de la seguridad de la información para la gestión de la continuidad del negocio	Mecanismos y procedimientos que permitan una rápida respuesta ante amenazas, incidentes o emergencias. Además de una rápida puesta en línea de los servicios afectados, de manera que se vean afectados en lo más mínimo posible los procesos del negocio. (ISO tools excellence, 2018)
Conformidad	Cumplimiento de las normas legales y reglamentarias de los sistemas

	empleados en la organización, con el fin de evitar sanciones civiles o penales. (ISO tools excellence, 2018)

Tabla 7. Análisis de seguridad informática UDLA

4.4.2 Requerimientos informáticos orientados a Help Desk

Los salones se han convertido en lugares donde los estudiantes pueden realizar discusiones desde cualquier dispositivo tecnológico que pueda acceder a la red, por tal motivo las instituciones han destinado sus esfuerzos en modernizar y adaptarse a los cambios continuos de la tecnología y al mismo tiempo mejorar sus sistemas de gestión para ofrecer un mejor servicio. Es por eso por lo que los miembros que prestan servicios de soporte deberán buscar las soluciones más prácticas y rápidas para dar una solución de primer nivel efectivo, estas soluciones pueden también escalar incluyendo a otros departamentos. (Rodríguez Gallardo, 2018)

En la siguiente figura se podrán observar los tipos de incidentes asociados al: funcionamiento del computador, acceso a servicios, software, impresoras, antivirus y otros. También podremos observar las estadísticas de estos sucesos que se producen en instituciones universitarias.

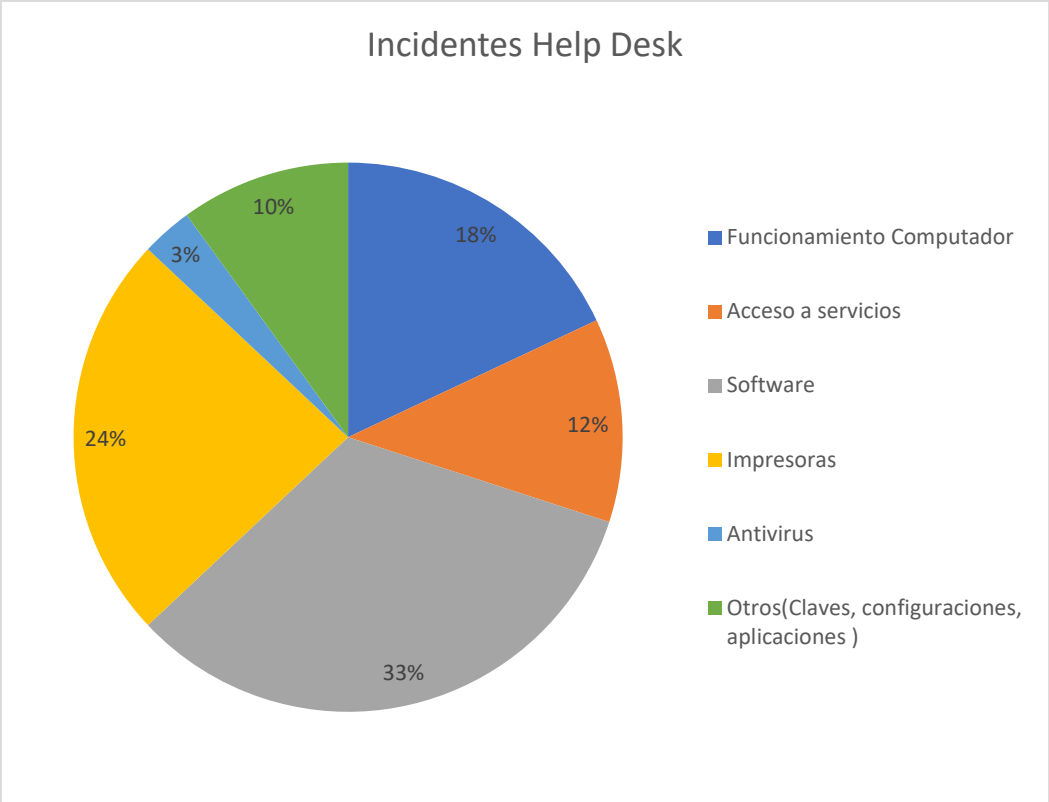

Figura 9. Incidentes reportados.

4.5 Mejores prácticas para la creación de un CSIRT

4.5.1 Elaboración de un CISRT

En esta sección se describen todas tareas, actividades, y servicios que serán necesarios para que un CSIRT pueda realizar sus funciones. Se deberán seguir las mejores prácticas para en un futuro ser miembro de los diferentes CSIRT internacionales, de manera que podamos compartir intereses, asi como consejos, políticas de seguridad, aportes tecnológicos e iniciativas. La mayoría de los CSIRT comparten los mismos requisitos para formar parte o cooperar entre ellos por tal motivo tomar estas buenas prácticas hará que el proceso sea más sencillo. (ETDA, 2017)

4.5.2 Misión de un CSIRT

La misión del equipo debe ser puntual y clara, explicando el propósito de un CSIRT académico, dando énfasis en los objetivos y ambiciones a futuro. Una

buena práctica es realizarlo en dos o tres líneas, la misión no cambiara hasta pasados algunos años ya que siempre se establecen las metas a futuro. (Cedia, 2019)

Propuesta de misión CSIRT-UDLA

CSIRT-UDLA: Asegurar la navegación, prevención y atención de incidentes dentro de la universidad, siendo este el punto de contacto para otros CSIRT académicos, promoviendo el intercambio de información y apoyo a otras instituciones.

4.5.3 Destinatarios del servicio

Comprender a quien va dirigido el servicio prestado por un CSIRT, ayudara a determinar las necesidades de la organización, los activos críticos que deberán ser protegidos y como estos interactuarán con el CSIRT, estos parámetros estarán establecidos en cualquier informe, acuerdo de servicio, misión, documentos que describan la función y propósito de un CSIRT. El modelo planteado para la UDLA es un modelo académico, debido a que está enfocado para una universidad. (UNICAMP, 2019)

Área	Enfoque	Destinatarios
CSIRT académico	Instituciones, universidades, unidades educativas, etc.	Estudiantes, investigadores, visitantes, docentes, administrativos y comunidad universitaria.

CSIRT comercial	Proveedor de servicios, Proveedores de servicios de internet, proveedor de acceso, proveedores independientes.	Clientes y organizaciones
CSIRT gubernamental	Gobierno o estado.	Ministerios, agencias gubernamentales y todo departamento que tenga relación con el gobierno.
CSIRT interno	Instituciones, organizaciones y empresas públicas o privadas	Área de TIC, usuarios y administradores.
CSIRT militar	Fuerzas armadas del Ecuador	Departamento de TIC de las fuerzas armadas del Ecuador
CSIRT nacional	Gobierno o estado, el cual tramita incidentes fuera de los límites fronterizos.	El CSIRT gubernamental, a veces es nombrado como CSIRT nacional.
CSIRT pymes	Pequeñas y medianas empresas	Representan el 99% de las empresas en el Ecuador. Personal administrativo.
CSIRT/PCIRT	Enfocados en productos específicos o en ataques específicos.	Usuarios que adquieren el producto

Tabla 8. Sectores de trabajo de un CSIRT

4.5.4 Servicios prestados por un CSIRT

Servicios reactivos	Servicios Proactivos
• Sistema de alerta temprana • Gestión de incidentes • Help Desk • Analizar vulnerabilidades • Respuesta ante incidentes • Respuesta a vulnerabilidades • Analizar incidentes • Gestión de vulnerabilidades • Soporte de nivel 1	• Comunicados • Políticas de seguridad • Auditorias informáticos • Mantenimiento de los sistemas • Implementación de herramientas de seguridad • Desarrollo de herramientas de seguridad • Transmisión de información • Capacitaciones • Consultoría de seguridad • Análisis de riesgos

Tabla 9. Catálogo de servicios CSIRT

4.5.5 Potestad de un CSIRT

La potestad hace referencia al nivel de acción de un CSIRT, es decir los limites sobre lo cuales podrá actuar. Esto puede cambiar dependiendo del acuerdo de servicio, ya sea únicamente como asesor de incidentes o con el poder de modificar, crear y eliminar servicios vulnerables o que se encuentren corrompidos. Es recomendable que un CSIRT únicamente sea el encargado de los aspectos técnicos, también se deberá contar con un supervisor o jefe de departamento encargado de anunciar las repercusiones, asi como también las medias de mitigación preventivas para evitar nuevamente incidencias similares. Los usuarios al no comprenden en su totalidad la parte técnica no podrían determinar el nivel de gravedad del incidente, por tal motivo es indispensable contar con una buena socialización con los usuarios, debido a que podrían dejar de reportar los incidentes por temor a represalias o castigos. (ETDA, 2017)

4.5.6 Responsabilidades

Se definen las actividades que debe cumplir un CSIRT, comúnmente los CSIRT cumplen tareas o monitorean servicios específicos (capítulo 2, tabla 3), y a su vez podrían realizar funciones adicionales como consultorías o relacionarse con fuerzas de seguridad como: la policía nacional. Al permitir a un CSIRT actuar en funciones externas a la organización se debe tener en cuenta que no se produzcan conflictos de intereses en las actividades donde puede tener un rol critico el manejo de la información. Para los CSIRT nacionales y gubernamentales estas normas son manejadas como políticas o leyes. (CSIRT-CV, 2019)

4.5.7 Estructura organizacional

La clasificación de un CSIRT nos permitirá determinar el área sobre el cual un incidente será resuelto o gestionado de una manera más práctica, para lo cual existen cinco tipos de clasificaciones (ver figura 8). Dependiendo del modelo organizacional que sea seleccionado, se podrán brindar diferentes servicios, teniendo en cuenta que la calidad y el nivel serán diferentes entre ellos, para determinar el área correspondiente se toma mucho en cuenta la madurez y experiencia del CSIRT.

- Equipo de seguridad: Se forma al no existir un CSIRT formal en la organización, las responsabilidades sobre los incidentes de seguridad son asumidas por el departamento de TI y resueltos como una actividad o tarea diaria.
- Modelo centralizado: Esta conformado por un CSIRT de tiempo completo dentro de la organización, el cual asume todo incidente relacionado a la seguridad informática dentro de la organización.
- Modelo distribuido: Este modelo debe constar de por lo menos un gerente de seguridad o jefe de departamento que supervise y coordine a los miembros que forman parte del CSIRT, generalmente son miembros de la organización, a los que se les puede asignar un incidente parcial o total dependiendo de la

dificultad o nivel crítico, este modelo es adecuado para empresas grandes en las cuales un CSIRT centralizado no será suficiente. (Muñoz & Rivas, 2017)

- Modelo combinado: Se podría decir que es un modelo hibrido entre el modelo centralizado y distribuido, el cual se contara con un gerente del equipo y miembros capacitados que realizaran tareas designadas. (Muñoz & Rivas, 2017)
- Modelo coordinador: Conformada por organizaciones externas que facilitan y coordinan la resolución de incidentes de seguridad, generalmente asisten a comunidades u organizaciones específicas. (Muñoz & Rivas, 2017)

Figura 10. Modelos de un CSIRT.

- Modelo Campus: Este modelo va enfocado a los CSIRT académicos y de investigación, conformado por varias universidades de diferentes locaciones, haciendo posible que este servicio se extienda por toda una nación. Una de las principales características de este modelo es que se encuentra coordinado

por un CSIRT madre o central, este CSIRT es el encargado de la comunicación con los demás CSIRT académicos, asi como de brindar información a todos los miembros que conforman o emplean el modelo campus, permitiendo una colaboración entre ellos y de igual manera disminuir los costos al solo utilizar el servicio. (ETDA, 2017)

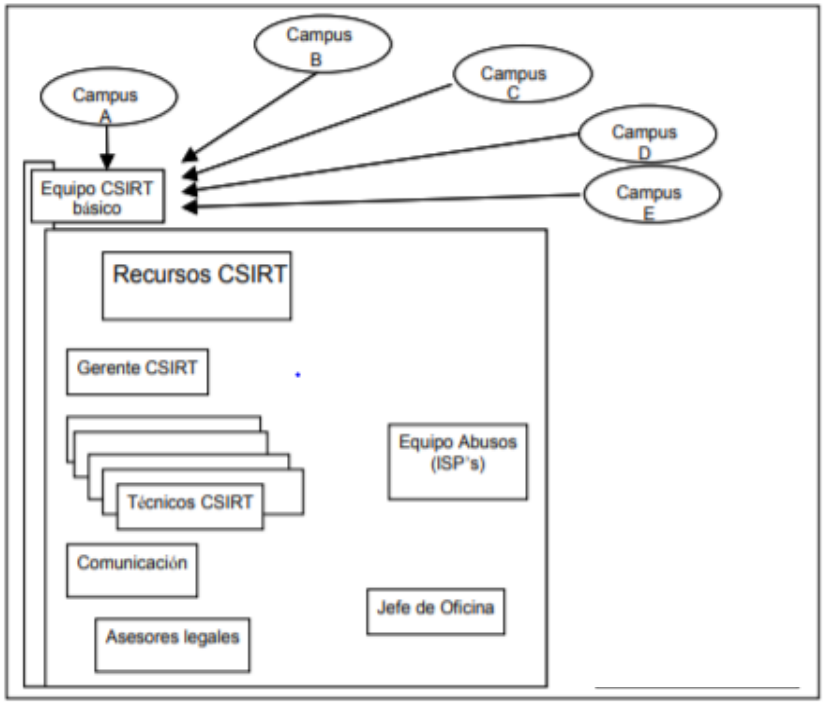

Figura 11. Modelo campus

4.5.8 Disponibilidad de los servicios

La disponibilidad de los servicios prestados por un CSIRT estará sujeto al horario de trabajo de las organizaciones, a menos que se encuentre establecido un CSIRT 24/7 (24 horas, 7 días a la semana), todo dependerá del manejo de incidencias, en cuyo caso se podrán reportar las incidencias fuera de horario de oficina y realizarlas en la siguiente jornada laboral, para esto se deberá asignar un miembro que monitoree o este de turno en horario extraordinario. De acuerdo, a la gravedad (baja, media, alta) del incidente se tomarán medidas para solventar de manera rápida en algunos casos o se lo podría dejar de lado

momentáneamente hasta la resolución de los incidentes más críticos. Contar con un equipo a tiempo completo podría ser beneficioso, pero por el contrario involucraría un costo adicional el realizar estas tareas. (ETDA, 2017)

4.5.9 Servicios propuestos al iniciar

Al momento de creación de un CSIRT no se debe ofertar más de uno o dos servicios, debido a que mientras se van fortaleciendo las capacidades del equipo se podrán ir añadiendo, dependiendo de las necesidades de la organización. Se debe seleccionar los servicios de manera específica para solventar las necesidades de la organización de una manera más optima, ya que añadir un nuevo servicio implicara un presupuesto adicional teniendo un impacto directo en los recursos disponibles. De esta manera, será mejor ofrecer un catálogo de servicios menor, pero de alta calidad. (ETDA, 2017)

4.5.9.1 Descripción de los servicios

Servicios reactivos

Los servicios reactivos nos permiten responder ante solicitudes, informes e incidentes que se encuentren dentro de la jurisdicción de un CSIRT, los servicios reactivos también pueden ser reportados por terceros, o durante monitoreos o alertas.

Alertas y amenazas

Al hablar de alertas nos enfocamos en la difusión de información que nos ayude a determinar un ataque malicioso, virus, spoofing, spam, etc. Las alertas son enviadas por los sistemas como medio de advertencia o notificación de que algo anormal sucede en la red. Al ser detectada una alerta los CSIRT deberán apoyar en la mitigación o aportando información para proteger los sistemas, información o recuperarse ante una caída del sistema. (Sophos Central Admin, 2019)

Manejo de incidentes

El manejo de incidencias hace referencia a la recuperación, evaluación, solución, repuesta ante un incidente de un sistema, permitiendo su correcto funcionamiento y mitigación del impacto en la organización. Enumeraremos unas cuantas actividades que son realizadas para tener un manejo de incidentes de efectivo. (ETDA, 2017)

- Establecer estrategias de mitigación o formas de actuar ante una alerta o amenaza con el fin de disminuir el impacto de un incidente.
- Monitorear constantemente la red, de esta manera se podrá identificar tempranamente una posible amenaza.
- Filtrar el tráfico de nuestra red.
- Realizar actualizaciones y mantenimientos periódicamente.
- Contar con estrategias de mitigación alternativas.
- Creación de políticas de seguridad.

Análisis de un incidente

Analizar un incidente, se refiere a la descripción de toda la información, evidencia y dispositivos empleados en la mitigación de una solicitud, incidente o problema de seguridad informática. El efectuar esta tarea nos ayudara a conocer el alcance del incidente, asi como la naturaleza de este, los daños causados a la organización ya sean estos económicos o materiales. Un CSIRT podrá utilizar esta recopilación de información para realizar estrategias de mitigación, un informe completo de lo acontecido durante el ataque informático, además se podrán realizar comparativas que nos permitan determinar las tendencias, patrones y pautas para limitar y evitar ataques similares. Un CSIRT podrá compartir información con otros CSIRT, y de esta manera tener un mayor entendimiento de estas amenazas. (ETDA, 2017)

Respuesta inmediata local

Un CSIRT deberá actuar ante un incidente, analizando de manera presencial los sistemas con afectaciones, de modo que si fuese necesaria una recuperación de

la información o del sistema se la realice lo más rápido posible. Si un CISRT se encuentra en otra sede o realizando otra actividad deberá acudir inmediatamente al sitio y dar respuesta al incidente. En la mayoría de los casos los CSIRT se encontrarán en la locación y procederán a dar el soporte correspondiente, asumiendo estos incidentes como funciones normales de su trabajo. (ETDA, 2017)

Respuesta ante incidentes

Un CSIRT ayuda a la recuperación ante un ataque vía telefónica, remotamente, correo electrónico o por medio de documentación que ayude en la resolución de un incidente. Para ello un CSIRT deberá interpretar la información recopilada por el usuario y transmitirle una solución sencilla y efectiva. La respuesta ante incidentes no hace referencia a una respuesta local como se mencionó anteriormente, en este caso se deberá dar solución remotamente para que el usuario o personal que se encuentre en el sitio pueda solventar el problema. (Microsoft, 2017)

Servicios Proactivos

Un servicio proactivo está diseñado para dar información o soporte de manera preventiva, mejorando en su gran mayoría la infraestructura y gestión de incidentes, uno de los objetivos principales es la reducción del número de incidentes y su gravedad. (Goode, 2018)

Anuncios

Las alertas se encuentran ligadas a los anuncios, los cuales nos permitirán aumentar los mecanismos de mitigación de incidentes al brindarnos la posibilidad de enviar advertencias, avisos y vulnerabilidades de los sistemas. De tal manera que los usuarios conozcan los nuevos mecanismos aplicados por los intrusos o hackers, el impacto que provocara estas nuevas formas de ataques y a su vez permitirá que los involucrados puedan prevenir problemas en sus sistemas antes de que estos sucedan. (ETDA, 2017)

Auditorias y evolución de los sistemas

Este servicio permitirá analizar detalladamente una infraestructura de seguridad, determinar el cumplimiento de los estándares y políticas de una organización. Existen diferentes tipos de auditorías de los sistemas de información. (ETDA, 2017)

- Auditorias de páginas web.
- Revisar las configuraciones de los equipos y realizar las actualizaciones necesarias.
- Revisión de las políticas de seguridad.
- Realizar pruebas de ataques con el objetivo de determinar la vulnerabilidad de los sistemas.
- Auditoria de la codificación de las aplicaciones.
- Análisis forenses.

Configuración y mantenimiento de los sistemas

Al implementar este servicio, se logrará aplicar de la forma más adecuado la configuración de un sistema, dotando al usuario de las herramientas necesarias, aplicaciones, servicios, y además de la infraestructura informática. Este servicio es empleado por los CSIRT dado que se podrá prestar este servicio como parte de sus funciones diarias. Un CSIRT podrá escalar este servicio hasta la gestión de incidentes, si fuera necesario para evitar la vulnerabilidad de un sistema. (ETDA, 2017)

A continuación, se enumerarán algunos de los servicios de configuración y mantenimiento:

- Monitoreo de la red
- Firewall
- Mecanismos de autenticación
- Mantenimiento y configuración de servidores
- Hardware

- Telefonía
- VPN

Herramientas de seguridad

Comprende los requerimientos y solicitudes de un CSIRT, esto puede incluir el desarrollo de parches que permitan evitar una vulnerabilidad en un sistema, herramientas que faciliten el monitoreo de la red (*PRTG - Paessler Router Traffic Grapher*), instalación de antivirus (ESET Antivirus), dispositivos de detección de ataques, etc. De esta manera se podrá conocer una incidencia de manera temprana o si es posible eliminarla antes de que aumente su nivel de peligrosidad. (Universidad Internacional de Valencia, 2019)

4.5.10 Requerimientos de personal

4.5.10.1 Personal necesario

No hay estudios claros de un mínimo recomendable de personas para conformar un CSIRT debido a que cada equipo trabaja en entornos diferentes, con políticas y estándares diferentes, sin embargo, tomando como referencia a la comunidad de los CSIRT's. Al ofertar dos servicios como mínimo se deberá contar con nada menos que cuatro personas capacitadas a tiempo completo, los CSIRT que laboran una jornada completa y ofertan todo el catálogo de servicios, como se muestra anteriormente (véase tabla 3), deberán contar con un mínimo de seis a ocho miembros a tiempo completo. Si se desea proveer de un servicio 24/7 (24 horas, 7 días) se deberá contar con un personal de doce trabajadores realizando tres turnos diarios divididos en grupos, estas estadísticas contemplan vacaciones y permisos por enfermedad. (TELCONET, 2018)

4.5.10.2 Competencias

4.5.10.2.1 Competencias Personales

- Capacidad de expresar un problema técnico en palabras sencillas para el entendimiento del usuario.

- Ser analítico.
- Ser confiable.
- Rápido aprendizaje.
- Contar con flexibilidad laboral.
- Sociable.
- Ser organizado.
- Ser comunicativo.

4.5.10.2.2 Competencias Técnicas

- Conocimiento tecnológico.
- Conocimiento de diferentes sistemas operativos.
- Tener un amplio conocimiento de redes, asi como de sus componentes.
- Tener un alto conocimiento de seguridad informática.
- Conocimiento sobre la evaluación de riesgos.
- Conocimiento de aplicaciones.

4.5.10.2.3 Competencias adicionales

- Nivel de educación acorde a las funciones que va a realizar.
- Experiencia lidiando con problemas de seguridad informática.
- Contar con el tiempo para realizar viajes (en ocasiones será necesario el soporte de manera presencial para solventar una incidencia.).

4.5.10.3 Capacitaciones

Las capacitaciones pueden ser realizadas internamente para nuevos miembros en la organización, con el fin de conocer el funcionamiento y modo de operar del CSIRT aplicado en la empresa, de igual manera se podrá realizar capacitaciones externas de manera periódica para conocer las nuevas tecnologías y de esta forma se conseguirá aumentar el catálogo de servicios, aprender nuevos mecanismos de solución de incidentes, mejora de las habilidades, toma de decisiones, etc. (CEC-EPN, 2019)

A continuación, se mencionarán ciertas organizaciones que ofrecen periódicamente capacitaciones o entrenamiento para CSIRT:

- FIRST
- CERT/CC
- SANS institute
- TRANSITS

4.5.11 Herramientas e infraestructura

Infraestructura hace referencia a todo software y hardware sobre el cual se ejecutan los servicios de la organización, se debe tener mucho cuidado al diseñar e implementar las redes, telecomunicaciones y las instalaciones sobre las cuales operara un CSIRT, debido a que se manejara información confidencial de la empresa, también se debe precautelar la seguridad de los CISRT proporcionando ambiente de trabajo acorde a las funciones que se realizaran. (ETDA, 2017)

4.5.11.1 Estructura física

- Es necesario la implementación de un cuarto de seguridad en el cual se colocará cualquier servidor que almacene información o recopile información. Se suele también establecer centros de operaciones de seguridad *(SOC – security operation center).*
- Salas insonorizadas evitando la fuga de información en las discusiones y actividades de los CSIRT.
- Herramientas que permitan la eliminación total de información, que ya no sea necesaria.
- Áreas seguras para almacenar información no digitalizada.
- Área dedicada únicamente para operaciones de un CISRT, se deberá contar con alguna seguridad adicional.

4.5.11.2 Herramientas especificas

- Sistemas de tickets para ingresar un incidente de manera digital.
- Herramientas para el análisis forense.
- Herramientas de seguridad (antivirus).
- Mecanismos de comunicación segura.
- Sistema de alarma.
- Sistemas de vigilancia.
- Sistemas de respaldos de información, para poner un sistema en línea lo más pronto posible.
- Red destina para las operaciones de un CSIRT.

5. CAPÍTULO V. PROPUESTA DE DISEÑO

En este capítulo se dará a conocer la propuesta de las primeras fases de un CSIRT académico, tomando como referencia lo descrito en los anteriores capítulos del trabajo de titulación, asi como los diferentes modelos de creación de un CSIRT. Cumpliendo el objetivo principal de esta investigación y proponiendo una guía para la protección de la información crítica en la UDLA, de manera que se pueda ofrecer un mejor servicio a los usuarios y permitirnos formar parte de la comunidad CSIRT en el Ecuador.

5.1 Planificación

Al planificar el desarrollo e implementación de un CSIRT en la UDLA, se tendrá en cuenta el acoplamiento de este sobre la estructura ya establecida en la universidad, de tal manera que la nueva propuesta logre mejorar los procesos, ya sean estos actualizados o simplemente cambiados por nuevos procedimientos, con el fin de lograr disminuir la abertura de seguridad informática y ofreciendo un catálogo de servicios mejorado acorde a las necesidades de la universidad.

5.1.1 Partes interesadas

El catálogo de servicios prestados por el CSIRT-UDLA estará destinado para toda la comunidad universitaria, en la cual se encuentran incluidos estudiantes, docentes, personal administrativo, investigadores y visitantes. De manera que se abarque todas sus sedes, y asi formar parte de la comunidad CSIRT académica en el Ecuador.

5.1.2 Servicios prestados

Según datos obtenidos durante el desarrollo de este documento, se logró determinar el número aproximado de incidentes orientados al Help Desk (véase la figura 9). Teniendo en cuenta el grado de dificultad de algunos incidentes, se desarrolló un diagrama de flujo que permite analizar el proceso por el cual deberá ser tratado un incidente desde su etapa inicial o registro del incidente, hasta el cierre de este. Se debe contar con una buena gestión de incidentes para determinar el área, sobre la cual el incidente será resuelto de la manera más optima y rápida. (EPN, s.f.)

En la siguiente figura observaremos el procedimiento para el cierre de un incidente, en el cual la fase inicial será la solicitud del usuario, quien a su vez realizará el registro del incidente de manera manual o digital. El equipo de soporte nivel uno determinará el área a la cual será asignado el incidente, siempre siendo la primera opción para la resolución del incidente, en este punto los miembros de nivel uno, deberán verificar similitudes con incidentes anteriores valiéndose de herramientas como la base del conocimiento que recopila información de incidentes pasados, de esta forma se solucionará y procederá a dar cierre del incidente. Dado el caso de no culminar la resolución del incidente o requerimiento se deberá reasignar el ticket a personal de nivel dos y de esta manera sucesivamente hasta dar por finalizado y cerrar el incidente.

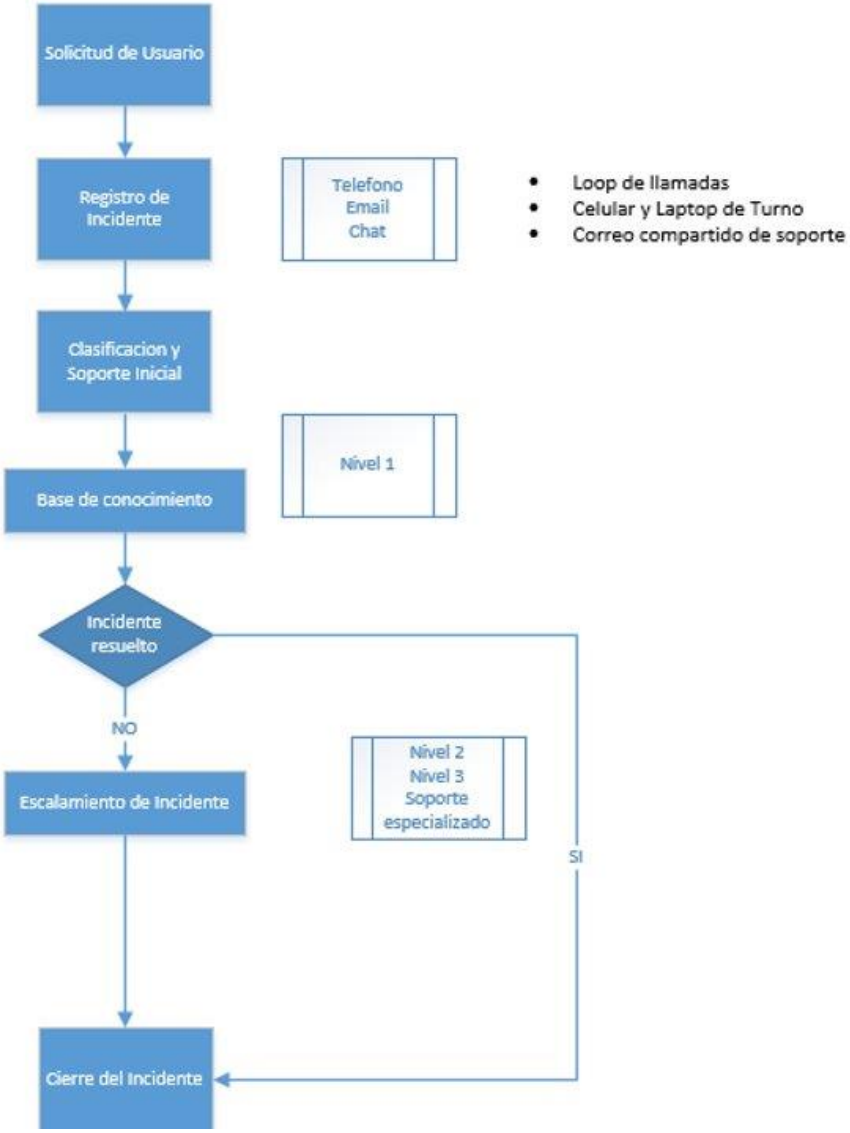

Figura 12. Tratamiento de un incidente.

5.1.3 Misión

CSIRT-UDLA: Asegurar la navegación, prevención y atención de incidentes dentro de la universidad, siendo este el punto de contacto para otros CSIRT académicos, promoviendo el intercambio de información y apoyo a otras instituciones.

5.1.4 Visión

CSIRT-UDLA: Ser la universidad con el CSIRT académico más efectivo en la resolución de incidentes de seguridad y fomentar una cultura de ciberseguridad en el país.

5.1.5 Objetivos estratégicos

- Incentivar el intercambio de información con CSIRT académicos de otras universidades, con la finalidad de apoyarse ante incidentes de escala nacional.
- Ser el punto de contacto con para los CSIRT nacionales o gubernamentales, de manera que podamos tener acceso tempranamente a información sobre incidentes que afecte directamente a la universidad.
- Realizar constantemente capacitaciones e inducciones a la comunidad universitaria, de manera que se logre prevenir y disminuir el número de incidentes dentro y fuera de las instalaciones educativas.

5.1.6 Estructura organizacional

Equipo Coordinador

Emplearemos el modelo estructural equipo coordinador debido a que la UDLA cuenta con varias sedes distribuidas por toda la ciudad de quito, este modelo nos permite contar con un coordinador encargado de los centros de respuesta ante incidentes, que interactuará directamente con los departamentos distribuidos en cada sede de manera que se establezca y busque un objetivo en común. La principal función de este modelo es coordinar la resolución optima de incidentes, asi como la interacción con las demás áreas, de manera que se logre obtener un análisis por sectores y a su vez uno global. Se debe tener como consideración al escoger un modelo, los servicios que se brindarán, ya que ciertos modelos estructurales no permiten cumplir por completo ciertos requerimientos. En

nuestro caso al ser una organización grande y con un índice alto de requerimientos podremos implementar este modelo sin problemas. (OEA, 2016)

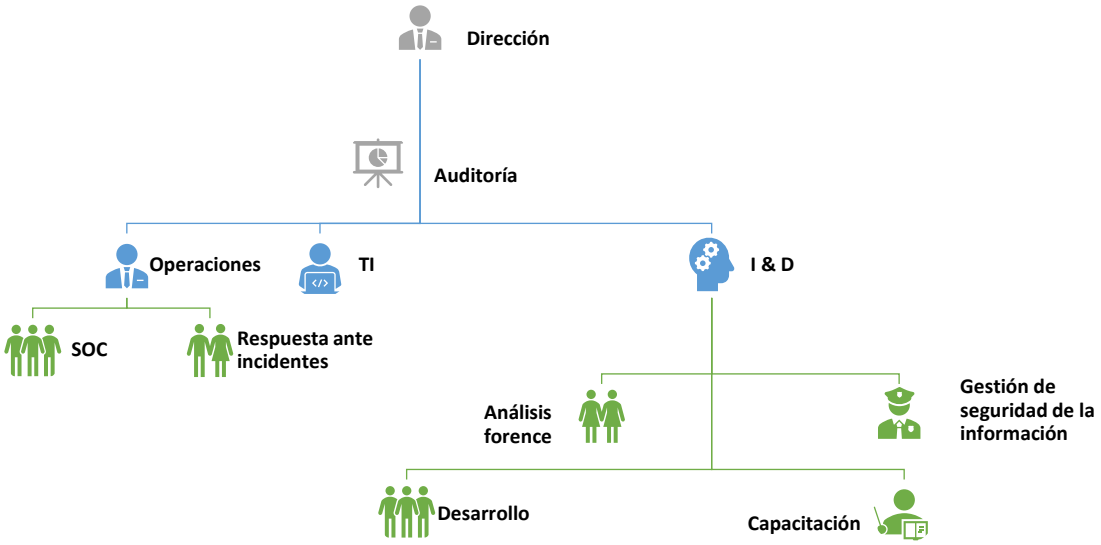

Figura 13. Diagrama estructural CSIRT

Adaptado de “OEA: Buenas prácticas para establecer un CSIRT nacional”, 2016.

5.1.7 Políticas de seguridad

5.1.7.1 Infraestructura de hardware

5.1.7.1.1 Responsabilidades de TI

Responsabilidades del departamento de TI, al adquirir, instalar, dar mantenimiento y funcionamiento de los equipos de la organización:

- Comprobar las especificaciones de los equipos adquiridos con los establecidos en el contrato de compra, de no ser asi se deberá devolver inmediatamente el dispositivo.
- Gestionar el mantenimiento técnico preventivo de los dispositivos utilizados en la organización, juntamente con el proveedor.

- Realizar capacitaciones sobre el correcto uso de los dispositivos y programas instalados.
- Encargados de realizar las instalaciones de los dispositivos y programas, asi como verificar la correcta ubicación del dispositivo en el puesto de trabajo.
- Verificar el área física donde se instalará el dispositivo sea la óptima y cuente con energía eléctrica, cableado estructurado, temperatura, etc.

5.1.7.1.2 Políticas para los usuarios de infraestructura de hardware

En este apartado detallaremos una serie de normas que deberán ser cumplidas por los usuarios al utilizar dispositivos provistos por la organización.

- No se receptarán peticiones de reparación de equipos que no sean provistos por la organización.
- Los equipos entregados por la organización serán únicamente utilizados para realizar tareas dentro de la empresa y no para fines personales.

5.1.7.2 Infraestructura de Software

5.1.7.2.1 Responsabilidad de TI

El departamento de TI estará encargado de monitorear los programas, con la finalidad de mantenerlos actualizados a su última versión.

- Inventario de las aplicaciones y programas instalados en los dispositivos, precautelando que todos se encuentren con licencias válidas.
- Determinar si el dispositivo se encuentra activo o en operación y de igual manera los que no se encuentren activos.
- Responsable del almacenamiento de los programas informáticos.

5.1.7.2.2 Responsabilidades de los usuarios

- Prohibición de descarga e instalación de software que presente una amenaza para la organización.

- Negado el ingreso de dispositivos de almacenamiento que no fueron dotados por la organización.
- Prohibido alterar las funciones del antivirus, asi como desactivarlo o desinstalarlo.

5.1.7.3 Cuarto de equipos

Lugar en el cual se alojan todos los servidores utilizados para las tareas diarias dentro de la organización. El cuarto de equipos es un espacio centralizado para los equipos empleados dentro de la organización, albergando de manera segura los equipos que influyen directamente con la red de datos y sistemas de soporte.

5.1.7.3.1 Responsabilidad de TI

- Acceso limitado para personal autorizado, debe contar con una seguridad adicional o de otro nivel en comparación con las demás áreas.
- Se permitirá el acceso a terceras personas, únicamente si se encuentran con un miembro del departamento de TI.

5.2 Ejecución

5.2.1 Relaciones con la comunidad CSIRT

Entablar relaciones con otros CSIRT académicos permitirá a la UDLA formar parte de la comunidad CSIRT dentro del Ecuador en la cual podrá apoyarse y de igual manera apoyar en la resolución de incidentes más complejos y que tengan un nivel de impacto mayor en las organizaciones. Estar incluido en este grupo hace posible el intercambio de información, capacitaciones, aportes tecnológicos, recomendaciones, políticas de seguridad, etc. A continuación, se enlistarán algunos CSIRT en cuales podremos apoyarnos.

- CSIRT CEDIA
- CSIRT UTPL
- CSIRT-EPN

- ECUCERT
- CSIRT FFAA
- CSIRT TELCONET

Para esto se deberá alcanzar un nivel alto de madurez con respecto a la seguridad de la información, asi como en la gestión de incidentes e infraestructura. Al comunicarse entre CSIRT se deberá pensar en un mecanismo o servicio que permita asegurar la privacidad de las comunicaciones, por lo que se recomienda emplear herramientas como privacidad bastante buena (*PGP – Pretty Good Privacy) o GNU Privacy Guard (abreviado como GnuPG o GPG),* las cuales básicamente realizan la misma función de encriptar el tráfico de internet mediante una criptografía de clave pública. (GnuPG, 2019)

5.2.2 Base del conocimiento

Se deberá desarrollar y emplear una base del conocimiento, en la cual se registren los incidentes resueltos, asi como el método que se empleó para dar solución a estos. De manera que los miembros del CSIRT puedan acceder y analizar las mejores prácticas y soluciones más efectivas de incidentes similares. Las bases del conocimiento también están destinadas para albergar información como: manuales de usuario, artículos, anuncios, entre otros. Es importante emplear esta herramienta debido a que se podrá compartir la información con la comunidad CSIRT. (GB Advisors, 2018)

5.3 Gestión de incidentes

5.3.1 Clasificación de los incidentes.

Los incidentes se clasificarán de acuerdo con la norma ISO 27001 en la que se establece el impacto y la urgencia de un requerimiento, realizando una relación entre ambas podemos determinar la prioridad de cada incidente, de manera que se lo pueda resolver de una forma adecuada teniendo en cuenta el impacto actual y a futuro que tendrá el posponer o resolver inmediatamente el requerimiento. (ISO tools excellence, 2018)

Urgencia \ Impacto	Alta	Media	Baja
Alta	1	2	3
Media	2	3	4
Baja	3	4	5

Tabla 10. Clasificación de los incidentes

5.3.2 Tiempo de resolución

Los tiempos de respuesta deberán estar establecidos acorde al nivel de urgencia e impacto del incidente, en la siguiente tabla se mostrará el tiempo máximo en el cual un miembro del TI deberá adueñarse del requerimiento y resolverlo, de manera que la calidad del servicio ofrecido por el área de TI sea el óptimo. Es importante contar con una buena gestión de incidentes para realizar un buen tratamiento del incidente, de forma que el incidente sea direccionado al personal más capacitado o cuente con las herramientas para la solución del requerimiento. (ISO tools excellence, 2018)

Clasificación del riegos	Tiempo de respuesta
Alta	30 min o inmediatamente
Media	1 a 2 horas
Baja	2 horas en adelante

Tabla 11. Tiempo máximo de resolución de un incidente

Se debe tener en cuenta que, al ser un requerimiento de riego bajo, se lo puede obviar momentáneamente, pero se deberá asignar una hora o fecha específica

para su resolución, ya que podría verse afectado el trabajo diario del usuario que solicito el requerimiento.

5.3.3 Tratamiento del incidente

El proceso de tratamiento de un incidente será establecido mediante el diagrama de gestión de un requerimiento desde su ingreso o pedido por el usuario, hasta el cierre e ingreso de información en la base del conocimiento. (véase figura 12). De igual manera será determinante el establecer un catálogo de servicios inicial acorde al personal, infraestructura y herramientas que están en posesión.

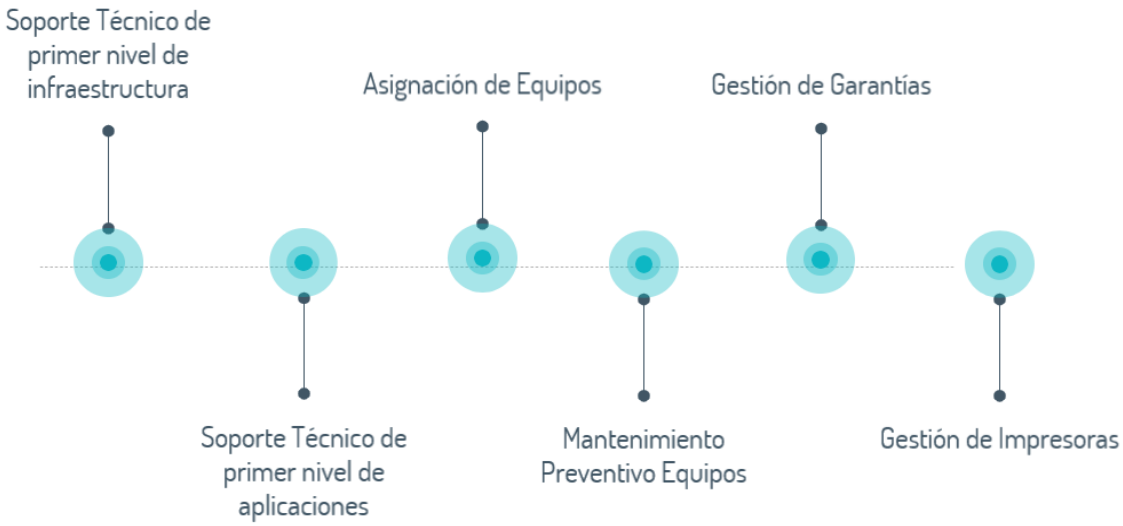

Figura 14. Servicios ofertados

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- Se concluyó mediante el desarrollo del trabajo de investigación que el servicio con el mayor riesgo es internet, al convertirse actualmente en una herramienta de trabajo, intercambio de información, generación de contenidos, comunicación y facilitar las actividades humanas. Dentro de la universidad este servicio se emplea en todas las áreas, siendo indispensable el contar con medidas y políticas de seguridad de alto nivel, de manera que la privacidad y datos de los usuarios no sean comprometidos.
- Para determinar el nivel de riesgo de un problema empleamos una clasificación de incidentes, esta categorización puede cambiar según la urgencia e impacto, añadiendo más campos que permitan ubicar al incidente en la categoría correcta y a su vez otorgarle un tiempo de resolución acorde a al nivel crítico del problema dentro de la organización.
- Durante el desarrollo de la investigación se determinó la necesidad de contar un plan de tratamiento de un incidente, por lo cual se diseñó un diagrama de flujo que permitirá el desarrollo de los diferentes procesos necesarios durante del ciclo de vida de un incidente. El diagrama puede ser modificado, para adaptarse a los cambios estructurales y tecnológicos dentro de la organización, de igual manera añadir más procesos con el fin de aumentar el detalle y la calidad del análisis de un problema.
- En Ecuador contamos con varios CSIRT académicos, uno de los más importantes y empleados dentro de la universidad es la red académica CEDIA, la cual presta como servicio un software de alerta temprana de incidentes de seguridad, y también asesoría en su uso por especialistas en CSIRT.
- El aumento de los incidentes, además de su grado de dificultad hace imposible que los mecanismos o métodos de seguridad tradicionales sean suficientes, es por ello que las organizaciones optan por el uso de herramientas de gestión de eventos e información de seguridad (*en inglés, Security Information and Event Management o SIEM*), las cuales nos ofrecen funcionalidades como: integrar entornos de trabajo en la nube, gestión de incidentes, auditoria,

cambios de configuraciones en los dispositivos, reglas de seguridad, sistemas híbridos, configurar alertas, etc.

- La protección de los activos de una organización depende en su gran mayoría de la seguridad empleada por el departamento de TI, por tal motivo se debe contar con métodos de seguridad más sofisticados que los empleados para las demás áreas de la empresa. Teniendo en cuenta que la seguridad física o hardware es la más costosa dentro de una estructura organizacional, se deberá tener esto muy en cuenta al elaborar el análisis de las áreas con un mayor riesgo de incidencias.

6.2 Recomendaciones

- Es recomendable la creación de herramientas que permitan el ingreso de los incidentes de forma digital, ya que de esta manera se podrán obtener reportes, estadísticas y dar seguimiento de todo el ciclo de vida de un problema de forma rápida.
- Las normas establecidas dentro de las políticas de seguridad no serán aplicadas de manera correcta si los estudiantes y miembros que conforman la comunidad universitaria no conocen el uso de estas. El establecer una metodología que permita la socialización de estas normas dentro de la universidad lograra una disminución de las incidencias menos críticas, y por tanto el equipo de TI priorizara los problemas que causen un mayor impacto en la organización.
- El dialogo y unión entre las universidades, permitirá en un futuro contar con una red universitaria sólida que permita la interacción y apoyo en la resolución de incidentes de seguridad a mayor escala.
- Se recomienda que la universidad preste todas las facilidades en el levantamiento de información, con el objetivo de emplear datos reales al realizar el análisis y desarrollo de proyectos.
- Los métodos de seguridad e intrusión informática cambian constantemente, por lo que se deben realizar campañas de concienciación sobre seguridad

informática para la comunidad universitaria, con el fin de disminuir y prevenir las amenazas e incidentes dentro y fuera de la universidad.

- El personal de TI deberá estar constantemente inmerso en capacitaciones, de manera que conozcan de inmediato las nuevas tendencias, tecnologías y mecanismos de mitigación de incidentes.
- Se deberá contar con varios métodos de comunicación para reportar un incidente informático, de manera que un CSIRT pueda actuar de la manera más eficiente y rápida, evitando que un incidente se convierta en un problema que afecte a toda la comunidad universitaria.

REFERENCIAS

Universidad Nacional de Luján. (s.f). Reporte de incidente de seguridad de la información. Recuperado el 05 de noviembre del 2019 de http://www.seguridadinformatica.unlu.edu.ar/sites/www.seguridadinformatica.unlu.edu.ar/files/site/Formulario%20reporte%20incidente.pdf

Centro Nacional de Respuesta ante Incidentes de Seguridad Informática. (2018). Reporte de incidente de seguridad de la información. Recuperado el 05 de noviembre del 2019 de *https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/que-es-un-incidente*

Universidad Internacional de Valencia. (2018). Vulnerabilidad informática, tipos y debilidades principales. Recuperado el 05 de noviembre del 2019 de *https://www.universidadviu.com/vulnerabilidad-informatica-tipos-debilidades-principales/*

CSIRT Cedia. (2019). Quiénes somos. Recuperado el 05 de noviembre del 2019 de https://csirt.cedia.org.ec/quienes-somos/

Carnegie Mellon University. *(s.f.).* Software Engineering Institute - Cybersecurity *.* Recuperado el 05 de noviembre del 2019 de *https://www.sei.cmu.edu/research_capabilities/cybersecurity/index.cfm*

Mendoza M . (2015). ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?*.* Recuperado el 05 de noviembre del 2019 de *https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/*

Lanfranco, Macia, Venosa, Molinari, & Díaz. (2010). Tendencias en incidentes de seguridad atendidos por el CERT académico CertUNLP. Recuperado el 05 de noviembre del 2019 de *http://sedici.unlp.edu.ar/bitstream/handle/10915/19431/Documento_completo.pdf?sequence=1&isAllowed=y*

Agencia española de protección de datos. (2019). Brechas de seguridad de datos personales: qué son y cómo actuar. Recuperado el 05 de noviembre del 2019 de *https://www.aepd.es/blog/2019-06-17.html*

Revista Latinoamericana de estudios de seguridad. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa, 31-45. Recuperado el 05 de noviembre del 2019 de *DOI: http://dx.doi.org/10.17141/urvio.20.2017.2571*

TF-CSIRT Trusted Introducer. (2019). Services for Security and Incident Response Teams. Recuperado el 05 de noviembre del 2019 de *https://www.trusted-introducer.org/index.html*

FISRT. (2019). FIRST History. Recuperado el 08 de noviembre del 2019 de *https://www.first.org/about/history*

Sullivan .B. (2014). Tendencias de Seguridad Cibernética en América Latina y el Caribe. Recuperado el 08 de noviembre del 2019 de *https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf*

Harán .J. (2018). ESET Security Report 2018: el estado de la seguridad de la información en las empresas de la región. Recuperado el 08 de noviembre del 2019 de *https://www.welivesecurity.com/la-es/2018/06/19/eset-security-report-2018-el-estado-de-la-seguridad-de-la-informacion-en-las-empresas-de-la-region/*

UDLA. (2018). Principales hitos de la planificación. Recuperado el 06 de diciembre del 2019 de https://www.udla.edu.ec/planificacion-estrategica-institucional/

Salvatierra, Díaz, Fara, & Salvatierra. (2016). La importancia de la seguridad informática en las instituciones gubernamentales (ecuador). Recuperado el 06 de diciembre del 2019 de http://www.eumed.net/rev/caribe/2016/11/seguridad.html

Robin, y Otros (2017). Computer Security Incident Response Team Development and Evolution in IEEE Security & Privacy, vol. 12, no. 5, pp. 16-26, doi: 10.1109/MSP.2014.89. Recuperado el 14 de diciembre del 2019 de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6924672&isnumber=6924618

Duncan. G. (2017). A Service Experience Designed to Deliver Peace of Mind: HPE Proactive Care. Recuperado el 20 de diciembre del 2019 de https://community.hpe.com/t5/Transforming-IT/A-Service-Experience-Designed-to-Deliver-Peace-of-Mind-HPE/ba-p/7019709#.Xfm67mRKhPa

ECURED. (s.f.). ISO/IEC 27002. Recuperado el 22 de diciembre del 2019 de https://www.ecured.cu/ISO/IEC_27002

UNICAMP. (2019). CSIRT UNICAMP. Recuperado el 22 de diciembre del 2019 de https://www.security.unicamp.br/

CSIRT-CV. (2019).Qué es y cómo traba un CSIRT en la respuesta ante incidentes. Recuperado el 22 de diciembre del 2019 de https://www.csirtcv.gva.es/es/noticias/qu%C3%A9-es-y-c%C3%B3mo-trabaja-un-csirt-en-la-respuesta-ante-incidentes.html

CEC-EPN. (2019). Aplicación de la Norma ISO 27001 y Código de Prácticas ISO 27002. Recuperado el 22 de diciembre del 2019 de https://www.cec-epn.edu.ec/cursos/curso/aplicacion-de-la-norma-iso-27001-y-codigo-de-practicas-iso-27002

TELCONET. (2018). CSIRT. Recuperado el 22 de diciembre del 2019 de https://www.telconet.net/index.php/csirt

Microsoft. (2017). Respuesta a incidentes de seguridad de TI. Recuperado el 22 de diciembre del 2019 de https://docs.microsoft.com/es-es/security-updates/security/respuestaaincidentesdeseguridaddeti

Sophos Central Admin. (2019). Alertas de protección contra amenazas. Recuperado el 22 de diciembre del 2019 de https://docs.sophos.com/central/Customer/help/es-es/central/Customer/concepts/AlertsMalware.html

UIV. (2019). Herramientas de seguridad informática más recomendadas en 2018. Recuperado el 22 de diciembre del 2019 de https://www.universidadviu.com/herramientas-seguridad-informatica-mas-recomendadas-2018/

EPN. (s.f.). Soporte interno Help Desk. Recuperado el 22 de diciembre del 2019 de https://www.epn.edu.ec/soporte-interno-help-desk/

GnuPG. (2019). The GNU Privacy Guard. Recuperado el 22 de diciembre del 2019 de https://www.gnupg.org/index.es.html

Rivas. G. (2018). Base de conocimientos de TI: ¿Cuáles son sus ventajas?. Recuperado el 22 de diciembre del 2019 de https://www.gb-advisors.com/es/base-de-conocimientos-de-ti/

Rivas. G. (2018). Base de conocimientos de TI: ¿Cuáles son sus ventajas?. Recuperado el 22 de diciembre del 2019 de https://www.gb-advisors.com/es/base-de-conocimientos-de-ti/

SGSI. (2018). Norma ISO 27002: El dominio política de seguridad. Recuperado el 25 de diciembre del 2019 de https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

SGSI. (s.f.). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.*. Recuperado el 25 de diciembre del 2019 de *https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf*

UIV. (s.f.). *Conceptos de seguridad lógica informatica.*. Recuperado el 27de julio del 2019 de *https://www.universidadviu.com/conceptos-seguridad-logica-informatica/*