Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

Trabajo Final de Máster

Desarrollo e implementación de un SOC en el Consejo de Aseguramiento de la Calidad de la Educación Superior.

Christian Rubén Molina Caza
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Seguridad Empresarial

Daniel Brande Hernandez

Víctor García Font

29 de diciembre de 2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Desarrollo e implementación de un SOC en el Consejo de Aseguramiento de la Calidad de la Educación Superior*
Nombre del autor:	*Christian Molina Caza*
Nombre del consultor/a:	*Daniel Brande Hernández*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	12/2020
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*Seguridad empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*SOC, Seguridad de la información, Centro de Operaciones de Seguridad*

Resumen del Trabajo:

Hoy en día se considera a la "información" como el principal activo, de carácter estratégico, dentro de cualquier organización independiente de su tamaño y del sector en el que se desenvuelven.

Se realizó un estudio de tipo exploratorio tomando como base los relatos de buenas prácticas, modelos y arquitecturas de los Centros de Operaciones de Seguridad (SOC) que permitieron una abstracción e interpretación propia durante la ejecución del Trabajo de Fin de Máster.

En esta realidad el Consejo de Aseguramiento de la Calidad de la Educación Superior busca implementar controles en los procesos y actividades que garanticen la seguridad en la información que maneja y administra para evitar que personal no autorizado tenga acceso a la información sensible de la Institución y pueda comprometerla causando daños considerables a la imagen institucional.

Es así como el diseño aquí planteado constituye el primer hito que permitirá proteger los servicios críticos de la Institución. En este sentido, su posterior implementación debe identificar e integrar las interrelaciones existentes entre las diferentes áreas de la organización de tal forma que se puedan identificar los impactos directos e indirectos que afecten la normal operación. Es así como la realidad actual de la mayoría de las organizaciones evidencia que, ante la presencia de un incidente de seguridad de la información que tenga afectación sobre alguno de los servicios críticos de la misma, no se cuente con los protocolos de respuesta adecuados que permitan a la organización saber cómo actuar para mitigar los riesgos presentados.

Abstract:

Today, "information" is the main asset, of a strategic nature, within any organization

independent of its size and the sector in which it is developed.

An exploratory study was carried out on the basis of the accounts of good practices, models and architectures of the Security Operations Centers (SOCs) that allowed an abstraction and interpretation of their own during the execution of the End of Master's Work.

In this reality, the Higher Education Quality Assurance Council seeks to implement controls on processes and activities that ensure the security of the information it handles and manages to prevent unauthorized personnel from accessing sensitive information in the Institution and can compromise it by causing considerable damage to the institutional image.

This is how the design proposed here is the first milestone that will protect the critical services of the Institution. In this sense, its subsequent implementation must identify and integrate the interrelationships between the different areas of the organization in such a way that direct and indirect impacts that affect the normal operation can be identified. This is how the current reality of most organizations shows that, in the presence of an information security incident affecting any of the critical services of the information, there are no adequate response protocols in place to enable the organization to know how to act to mitigate the risks presented.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

INTRODUCCIÓN

En la actualidad, podemos afirmar sin temor a equivocarnos que, la "información" se ha constituido en el activo más importante y valioso que posee cualquier organización ya sea del ámbito público o privado. En este sentido, para las organizaciones resulta sumamente relevante el hecho de disponer de los mecanismos que sean necesarios con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información generada y de los sistemas de procesamiento existentes.

Al experimentar hoy en día un mayor uso de sistemas, tecnologías y comunicaciones se ha incrementado también la gama de amenazas cibernéticas encaminadas, bajo cualquier medio, a aprovechar las vulnerabilidades existentes en las organizaciones con la finalidad de obtener beneficios de tipo económico o vulnerar las infraestructuras tecnológicas y de comunicaciones para demostrar los fallos existentes en los diferentes niveles de seguridad de la información.

Esto lleva sin duda a que, sin importar el tamaño de las organizaciones, las mismas tengan que adoptar controles y medidas que les permitan gestionar de una forma proactiva y/o reactiva todos aquellos eventos, amenazas, vulnerabilidades e incidentes de tal forma que estos mecanismos de acción y protección ayuden a mitigar y controlar el impacto que la presencia de estos eventos adversos pudieran ocasionar sobre el funcionamiento normal de las operaciones diarias de las organizaciones.

Desde la perspectiva de la seguridad de las tecnologías de la información y las comunicaciones es necesario combinar tanto los conocimientos de tipo técnico como los conocimientos de gestión de tal forma que estemos en capacidad de realizar una articulación entre los dispositivos, las tecnologías, los sistemas de detección, los procesos y las personas.

No debemos olvidar que uno de los pilares importantes dentro de cualquier estrategia de tecnologías de la información y comunicaciones es el relacionado con la gestión de la seguridad de la información ya que si llegase a existir una afectación a la disponibilidad o calidad de los sistemas y plataformas informáticas podríamos ver comprometido el hecho de lograr alcanzar los objetivos estratégicos dispuestos por las autoridades institucionales.

Siendo así, cuando nos referimos a un Centro de Operaciones de Seguridad (SOC por sus siglas en inglés) debemos tener conciencia de que nos referimos a una herramienta de gestión que nos permitirá garantizar la continuidad y calidad en las operaciones diarias que realiza la organización. En este sentido considerando que podemos abordar al Centro de Operaciones de Seguridad desde la perspectiva técnica especializada y desde el punto de vista de las buenas prácticas tendientes a la construcción efectiva de sistemas de gestión de la seguridad de la información trataremos de abordar el presente trabajo de una visión que nos permita de forma general realizar una vinculación entre los procesos, las personas y las tecnologías.

Con estos matices expuestos anteriormente podemos mencionar que el presente trabajo hace énfasis en una propuesta de modelo el cual se encuentra basado en las mejores prácticas, estándares y normativa internacional que permita al Consejo de Aseguramiento de la Calidad de la Educación Superior registrar, gestionar y analizar los eventos presentados mediante un Centro de Operaciones de Seguridad que permita tener bajo control las amenazas, brindar respuestas oportunas a los incidentes reportados y sobre todo generar indicadores e informes que permitan conocer de primera mano la forma en la que se está gestionando la seguridad de la información al interno de la Institución. Todas estas acciones se encontrarán encaminadas al único propósito de proteger y salvaguardar la información institucional de posibles ataques malintencionados efectuados por ciberdelincuentes, posibles descuidos de parte de los empleados de la organización y errores maliciosos o de carácter involuntario que pudiesen ocasionar afectación o pongan en riesgo los activos de información institucional.

CAPÍTULO I. MARCO METODOLÓGICO

1.1. CONTEXTO Y JUSTIFICACIÓN DEL TRABAJO

Hoy en día se considera a la "información" como el principal activo, de carácter estratégico, dentro de cualquier organización independiente de su tamaño y del sector en el que se desenvuelven. Hay que destacar que en función de los niveles en los cuales haya clasificado internamente su información la Institución, de acuerdo con su sensibilidad, debemos tener presente en todo momento que debemos de forma primordial garantizar la confidencialidad, integridad y disponibilidad de la información existente.

Cuando hablamos de gestión de seguridad de la información lo que primero se nos viene a la mente es implementar mecanismos o controles que ayuden a la Institución a evitar el acceso no autorizado a la información sensible de la organización y si este escenario no ha podido ser controlado y la información ha sido comprometida deben llevarse a cabo acciones que permitan que la imagen de la Institución no se vea afectada, que no se pierda la confianza de los usuarios internos y externos de los servicios y más aún que no existan pérdidas económicas irreparables.

El Consejo de Aseguramiento de la Calidad de la Educación Superior además de administrar los datos provistos por parte de las Instituciones de Educación Superior (IES), gestionan la información personal de los docentes, estudiantes y administrativos que laboran en las IES. Por esta razón, podemos indicar que la información organizacional se convierte en un blanco de los delincuentes informáticos para la ejecución de ataques.

Es en este contexto que si queremos mejorar los procesos de detección y respuesta frente a las amenazas e incidentes debemos considerar un nuevo enfoque de seguridad de la información que nos permita hacer uso de la totalidad de la información disponible en la Institución la misma que puede tener como origen los procesos internos, sistemas de información y los servicios que son utilizados por parte de los usuarios externos de tal forma que podamos prevenir amenazas futuras y detectar proactivamente aquellas amenazas existentes.

Un modelo de seguridad enmarcado en una plataforma de administración de seguridad como un Centro de Operaciones de Seguridad (SOC), sin duda nos es de vital importancia al momento de realizar una eficiente selección de las tecnologías de la información que proveen seguridad, basada en políticas y atendiendo a necesidades propias de la Institución.

Es así como el Centro de Operaciones de Seguridad (SOC) deberá basarse en cuatro ejes importantes:

a) **Prevención:** El objetivo de este eje es el de disminuir las probabilidades de que se haga presente cualquier incidente. Es necesario realizar vigilancia permanente de nuevos ataques que puedan comprometer la seguridad de la información, así como la aplicación de medidas preventivas que reduzcan la probabilidad de materialización de amenazas.
b) **Detección:** Este eje consiste en el monitoreo permanente con la finalidad de detectar amenazas, vulnerabilidades, intrusiones, ataques de seguridad, o cualquier indicio que refleje un posible incidente de seguridad de la información.
c) **Análisis:** El objetivo de este eje es principalmente el estudio de los incidentes descubiertos por la detección con la finalidad de poder entender y descifrar entre la existencia de amenazas reales o falsos positivos que puedan atentar contra la seguridad de la información.
d) **Respuesta:** El objetivo de este eje brinda la posibilidad de reaccionar ante la presencia de cualquier tipo de incidente real de seguridad de la información.

En este sentido se constituye en un factor sumamente importante el hecho de que las organizaciones en estrecha colaboración con sus equipos de trabajo tengan siempre presente como premisa en la realización de sus actividades la imperiosa necesidad de proteger y

resguardar el activo más valioso que hoy en día constituye la información para las organizaciones.

Es así como las funciones principales de un Centro de Operaciones de Seguridad las podemos resumir en las siguientes:

- ✓ Monitorización continúa de la seguridad.
- ✓ Detección y gestión de vulnerabilidades.
- ✓ Centralización, tratamiento y custodia de logs.
- ✓ Respuesta de resolución.
- ✓ Asesoría de seguridad.
- ✓ Programas de prevención.

El Consejo de Aseguramiento de la Calidad de la Educación Superior busca implementar controles en los procesos y actividades que garanticen la seguridad en la información que maneja y administra. Especialmente a nivel de la gestión de la seguridad de la información se requiere poder evitar que personal no autorizado tenga acceso a la información sensible de la Institución y pueda comprometerla, en el caso de que la información llegara a estar comprometida de cualquier manera podría afectar gravemente los servicios que la Institución ofrece, lo que conllevaría a un daño en su imagen, en la confianza de sus clientes y usuarios externos e inclusive podría tener un efecto político de grandes consecuencias. Para esto es necesario que la Institución defina e implemente controles y procesos que ayuden a garantizar la seguridad de la información, considerando todas las actividades, activos, sistemas y/o herramientas que la Institución maneja.

Debido a esto, la necesidad que tiene el Consejo de Aseguramiento de la Calidad de la Educación Superior de garantizar la seguridad de la información de sus usuarios externos, en los diferentes servicios que se ofrece, surge el planteamiento para la definición de procesos que ayuden a detectar, prevenir y solventar posibles fallos de seguridad en los servicios y sistemas que se administran dentro de la Institución. Con esta necesidad expuesta se requiere contar con un área especializada en las actividades relacionadas con la seguridad de la información que tendrán que ejecutarse diariamente.

Uno de los más grandes retos para el Comité de Seguridad de la Información del Consejo de Aseguramiento de la Calidad de la Educación Superior es la implementación de mecanismos que ayuden en la mitigación de riesgos asociados a la seguridad de la información basados en procesos de gestión de las operaciones y monitoreo permanente de las actividades que se realizan, esto conjuntamente con personal capacitado y entrenado que dé respuesta a los incidentes que se presenten, logrando con esto la prevención, evasión, reducción y detección de posibles ataques a los que pudiera encontrarse expuesta la Institución.

Por esta razón, la implementación de un Centro de Operaciones de Seguridad (SOC) dentro del Consejo de Aseguramiento de la Calidad de la Educación Superior se constituye de vital importancia para poder garantizar mayor seguridad a los servicios que brinda la Institución. Debemos tener presente siempre que la función primordial de un Centro de Operaciones de Seguridad (SOC) es prevenir y/o evitar que se produzcan incidentes relacionados con la seguridad de la información y de llegar a presentarse responder de manera ágil y adecuada.

Este trabajo se enfocará en los puntos principales que el Consejo de Aseguramiento de la Calidad de la Educación Superior debe tomar en cuenta para poder establecer los procesos de un Centro de Operaciones de Seguridad (SOC) con personal especializado en la materia y el uso de herramientas adecuadas para poder gestionar la seguridad de la información de toda la Institución tanto de sus empleados como de sus clientes y usuarios externos.

Tomando en consideración que en la actualidad no existe un estándar que hable de la implementación de un Centro de Operaciones de Seguridad (SOC) paso a paso, con la realización

de este Trabajo de Fin de Máster (TFM) buscaremos establecer un proceso para la implementación de un Centro de Operaciones de Seguridad (SOC) dentro del Consejo de Aseguramiento de la Calidad de la Educación Superior, basándonos en las mejores prácticas que a nivel mundial son utilizadas hoy en día.

1.2. OBJETIVOS Y METODOLOGÍA DEL TRABAJO

1.2.1. OBJETIVO GENERAL

Elaborar una propuesta de diseño e implementación que le permita al Consejo de Aseguramiento de la Calidad de la Educación Superior centralizar los eventos e incidentes de seguridad de la información, con la finalidad de brindar una solución a los problemas de seguridad que se identifiquen.

1.2.2. OBJETIVOS ESPECÍFICOS

a) Establecer el alcance del Centro de Operaciones de Seguridad (SOC) en concordancia con la estructura orgánica de la Institución.
b) Identificar los procesos, procedimientos y políticas que se requieren para una gestión adecuada del Centro de Operaciones de Seguridad (SOC).
c) Plantear los recursos necesarios tanto humanos como de infraestructura necesarios para la conformación del Centro de Operaciones de Seguridad (SOC).
d) Proponer las herramientas y soluciones tecnológicas que podrían ser utilizadas para ejecutar las actividades diarias dentro de un Centro de Operaciones de Seguridad (SOC).

1.2.3. METODOLOGÍA DEL TRABAJO

El enfoque de este trabajo, al encontrarse contextualizado dentro del ámbito organizacional que constituye el Consejo de Aseguramiento de la Calidad de la Educación Superior, consistirá en investigar si es viable la implementación de un Centro de Operaciones de Seguridad (SOC) que centralice los eventos e incidentes de seguridad que pudiesen comprometer los activos de información institucional.

Para alcanzar los objetivos propuestos en el desarrollo del presente trabajo haremos uso de la metodología de investigación exploratoria descriptiva relacionada con los Centros de Operaciones de Seguridad (SOC).

Realizaremos un estudio de tipo exploratorio relacionado con el marco teórico existente en la actualidad, así como los relatos de buenas prácticas, modelos y arquitecturas de los Centros de Operaciones de Seguridad (SOC) que permitan obtener una abstracción e interpretación propia durante la ejecución que aborde los tópicos más esenciales desde el punto de vista tanto técnico como gerencial.

Al estudio de carácter teórico iremos incorporando la observación empírica y algunos de los resultados que se hayan obtenido en experiencias similares de conformación de un Centro de Operaciones de Seguridad (SOC) en organizaciones tanto públicas como privadas a nivel internacional.

Estas experiencias internacionales nos serán de gran utilidad en tanto y en cuanto podamos obtener consistencia entre lo establecido en la teoría y la madurez alcanzada en la implementación de acuerdo con los criterios de profesionales que hayan aportado con su contingente en el desarrollo e implementación de un Centro de Operaciones de Seguridad (SOC).

Haremos uso de información relevante que nos permita realizar el análisis comparativo de ciertos estándares adoptados internacionalmente, tal como constituye ISO/IEC 27001, y los lineamientos emanados de estos estándares que puedan ser aplicados en la gestión de un Centro de Operaciones de Seguridad (SOC).

1.3. ESTADO DEL ARTE

En los últimos años ha generado verdadera importancia el estudio de la seguridad de la información basados en el punto primordial de que la "información" la llegado a constituirse en el activo más importante para las organizaciones, de cualquier tamaño, por el valor que brinda al cumplimiento de los objetivos esenciales del negocio.

Cuando hablamos de seguridad de la información generalmente lo relacionamos con un factor de preocupación para las autoridades institucionales independiente del sector en el cual se desenvuelven ya que en la mayoría de las veces no tienen un conocimiento fidedigno del estado actual y real de la seguridad de la información en la Institución.

En la actualidad debido al contexto globalizado en el que desempeñamos nuestras actividades cotidianas podemos conocer muchas de las preocupaciones que tienen las organizaciones con respecto a la seguridad de la información. Sin embargo, podemos indicar que las más trascendentales y que influyen de manera directa en las actividades operacionales son las siguientes:

a) **Ransomware:** Es un software malicioso que infecta nuestra computadora y muestra mensajes a través de los cuales se exige el pago de una tarifa para que nuestro sistema vuelva a funcionar. Tiene la capacidad de bloquear la pantalla de una computadora o encriptar archivos importantes predeterminados con una contraseña.
b) **Vulnerabilidades:** Constituyen una debilidad que puede poner en peligro toda la plataforma tecnológica y de comunicaciones y que demanda la existencia de un grupo de expertos que permita identificar las amenazas y sus correspondientes tipos de vulnerabilidades.
c) **Malware:** Es el nombre colectivo de una serie de variantes de software malicioso, incluidos virus, ransomware y spyware. Consiste en código desarrollado por ciberatacantes, diseñado para causar grandes daños a los datos y sistemas o para obtener acceso no autorizado a una red.
d) **Robo de información:** El robo de información, sean estos datos personales o de otra naturaleza, se producen como consecuencia de la falta de protección de esos datos que deben ser objeto de protección. Para enfrentar de manera proactiva esto debemos incidir en la concienciación de parte de los usuarios por cuanto el desconocimiento es uno de nuestros mayores enemigos.

Hoy en día existen una extensa gama de amenazas y vulnerabilidades que atentan contra la seguridad de los sistemas de información de las organizaciones, por lo cual se ha convertido en primordial para las mismas establecer controles de seguridad que minimicen el riesgo de operación. En función del tamaño de la organización los tipos de controles de seguridad pueden variar, desde controles de seguridad basados en la tecnología, hasta controles de seguridad basados en la gestión de la seguridad.

Esto se origina en gran medida en virtud de que las organizaciones de tamaño grande tienen actividades y procesos más estructurados basados en estándares, normativas y mejores prácticas que aconsejan que la gestión de la seguridad de la información es uno de los principales requisitos en la actualidad, de igual manera este tipo de empresas posee un mayor presupuesto económico para poder invertir en la gestión de la seguridad y herramientas especializadas.

Entre las organizaciones que utilizan controles basados en la gestión de la seguridad, se observa la adopción de los siguientes tipos de controles:

- ✓ Política de seguridad de la información.
- ✓ Clasificación de la información.
- ✓ Plan de continuidad del negocio.
- ✓ Auditoría externa e interna.

- ✓ Plan de respuesta a incidentes.

En la actualidad el control referente a la Política de Seguridad de la Información es uno de los controles más utilizados por parte de las organizaciones ya a través de este medio se establecen todos los lineamientos y pautas de seguridad con los que los empleados deben cumplir. Estas políticas se encuentran en todo momento alineadas directamente con la estrategia del negocio para poder cumplir con los requisitos de la Institución.

Este tipo de controles son parte del proceso integral de la gestión de la seguridad de la información y para poder administrarlos, monitorearlos y evaluarlos de mejor manera es necesario que dentro del Consejo de Aseguramiento de la Calidad de la Educación Superior se encuentre definida un área exclusivamente dedicada a la gestión de seguridad, ya que al momento la gestión de la seguridad de la información es realizada por otras área o personal no especializado en la materia. Esta forma de gestionar la seguridad de la información puede en algún momento convertirse en un inconveniente de conflicto de intereses debido a que es el personal del área de tecnologías de la información el encargado de implementar controles de seguridad y evaluarlos, cuando las mejores prácticas recomiendan que el área de seguridad de la información no sea parte del área de tecnologías de la información, sino un ente independiente que supervise y monitoree las actividades de las demás áreas.

Se puede mencionar que para las organizaciones constituye una verdadera decisión de tipo estratégico el adoptar internamente un sistema de gestión de seguridad de la información y cuyo éxito de implementación estará dado por las necesidades y objetivos de la Institución, los requisitos esenciales en cuanto a seguridad, los procesos internos y la estructura orgánica de la Institución.

Las organizaciones, de manera independiente del sector en el que se desenvuelven y del tamaño de las mismas, han comprendido y entendido la importancia que representa el realizar inversiones en el ámbito de la gestión de la seguridad de la información, sobre todo el aporte a garantizar el cumplimiento de los objetivos estratégicos de la Institución que le puede dar la definición e implementación de un Centro de Operaciones de Seguridad (SOC) que constituyéndose en una área especializada dentro de la organización interna ayude considerablemente a prevenir y evitar la posibilidad de ocurrencia de ataques a los que puede encontrarse la plataforma tecnológica y de comunicaciones de la Institución.

La utilidad de un Centro de Operaciones de Seguridad (SOC), hoy en día, se ven plasmados en la necesidad que tienen las organizaciones de poder realizar de manera efectiva el monitoreo y evaluación de las actividades realizadas de tal forma que podamos efectuar una adecuada correlación de eventos, predicción de ataques y evasión de infecciones, además que nos permite contar con profesionales especializados en el campo de la seguridad de la información y la ejecución de procesos plenamente definidos que sumados todos estos factores ayuden a incrementar los niveles de seguridad de la Institución y por ende la prestación de servicios transparentes a la ciudadanía en general.

1.4. PLANIFICACIÓN DEL TRABAJO

En esta parte nos centraremos en la elaboración de un calendario en el que hagamos constar las fechas de inicio y finalización de cada una de las acciones y actividades previstas para el desarrollo del Trabajo de Fin de Máster (TFM).

Para poder visualizar el cronograma propuesto hemos empleado un diagrama de Gantt el cual consiste en crear una tabla en la que haya barras de distintos tamaños, proporcionales a su duración, donde las filas serán las actividades que hay que desarrollar, y las columnas, una escala de tiempo, en la cual se visualizan los eventos que se solapan. (Estanyol i Casals, 2017)

El desarrollo constará de cuatro (4) fases y cinco (5) entregables, las cuales coinciden con las

fechas establecidas por la Universidad para la presentación de las Pruebas de Evaluación Continua (PEC) que corresponden al Trabajo de Fin de Máster (TFM).

a) **Fase 1 – Planificación:** En esta fase del Trabajo de Fin de Máster (TFM) realizaremos una breve introducción al contexto y la justificación del trabajo, enumerando los objetivos que queremos alcanzar con la realización del trabajo, haremos una descripción de la metodología a ser usada durante el desarrollo y presentamos un esquema de planificación que nos oriente en la realización de las distintas tareas a realizar con la finalidad de alcanzar los objetivos que nos hemos propuesto con la realización del trabajo.

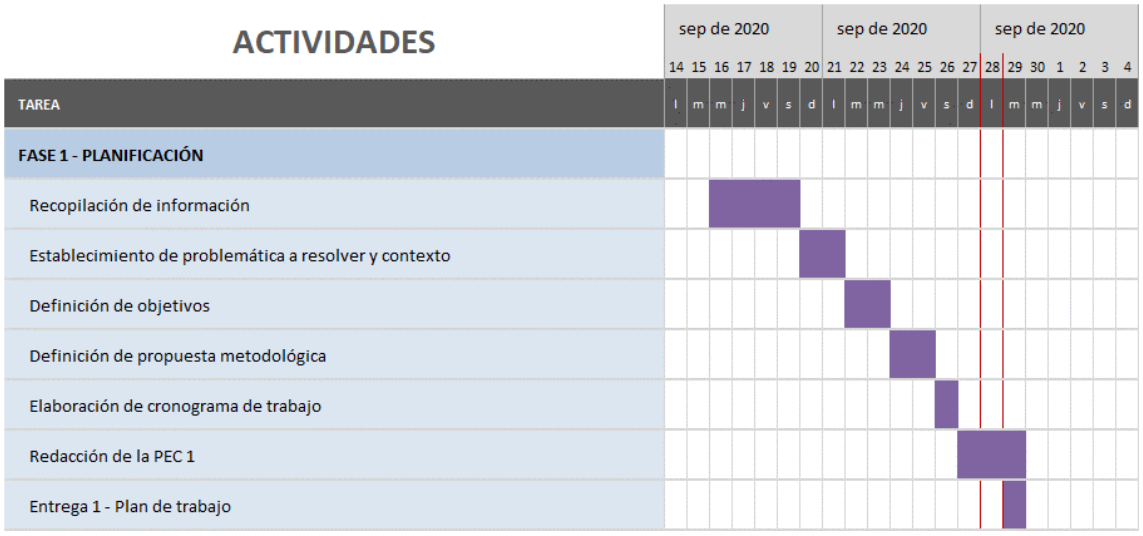

Ilustración 1. Diagrama de Gantt de la Fase 1 del TFM

b) **Fase 2 – Investigación:** En esta fase del Trabajo de Fin de Máster (TFM) haremos hincapié en el marco referencial el cual se encuentra constituido por el marco teórico y legal además de la revisión de todos los conceptos que nos permitan avanzar en un diseño metodológico y establezcan las pautas necesarias que nos permitan tener una comprensión clara sobre la temática que hemos escogido para la realización del trabajo. De igual forma en esta fase del trabajo haremos un análisis descriptivo del Consejo de Aseguramiento de la Calidad de la Educación Superior que nos permita tener un acercamiento y entendimiento de la situación actual de la organización que permitan contrastar si al momento existen o no controles del Centro de Operaciones de Seguridad (SOC) que pudiesen encontrarse ya implementados.

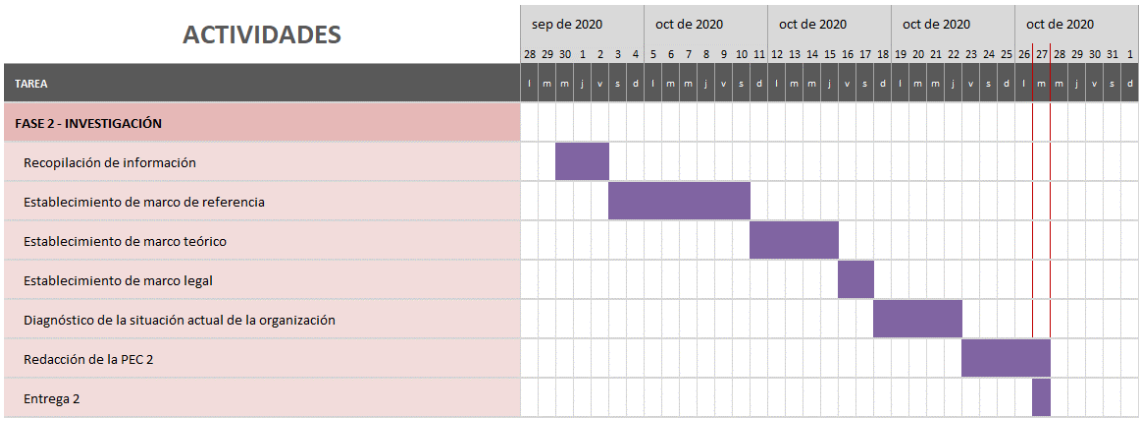

Ilustración 2. Diagrama de Gantt de la Fase 2 del TFM

c) **Fase 3 – Propuesta de Implantación:** En esta fase del Trabajo de Fin de Máster (TFM) nos enfocaremos en todos aquellos aspectos que cobran relevancia e importancia al momento que diseñemos y definamos las características de un Centro de Operaciones de Seguridad (SOC) dentro del Consejo de Aseguramiento de la Calidad de la Educación Superior. Trataremos sobre las principales funciones y aspectos, analizaremos la normativa legal vigente en el Ecuador en materia de seguridad de la información en contexto con el estándar internacional ISO/IEC 27000 para presentar una propuesta de implantación basada en responsabilidades, procesos, procedimientos, métricas, indicadores e infraestructura necesaria que le permitan a la Institución la implementación efectiva a mediano plazo.

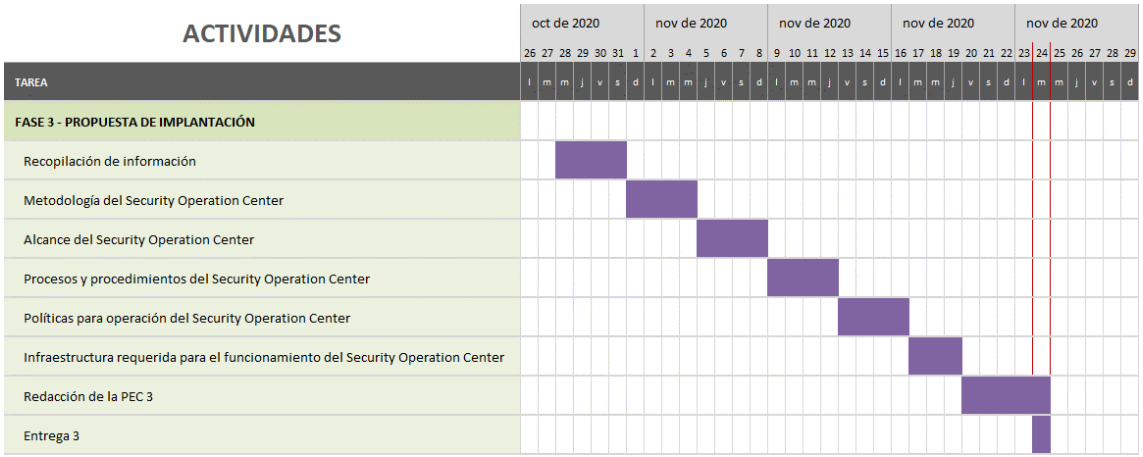

Ilustración 3. Diagrama de Gantt de la Fase 3 del TFM

d) **Fase 4 – Presentación:** En esta fase del Trabajo de Fin de Máster (TFM) presentaremos aquellas conclusiones más relevantes que hayamos obtenido con la ejecución del trabajo y de ser el caso dejaremos planteadas líneas de acción para la realización de trabajos futuros. En la redacción de la memoria final estableceremos las referencias y los anexos que correspondan de tal forma que el Trabajo de Fin de Máster (TFM) quede plenamente complementado además de las explicaciones del caso plasmadas en la presentación en video del trabajo realizado.

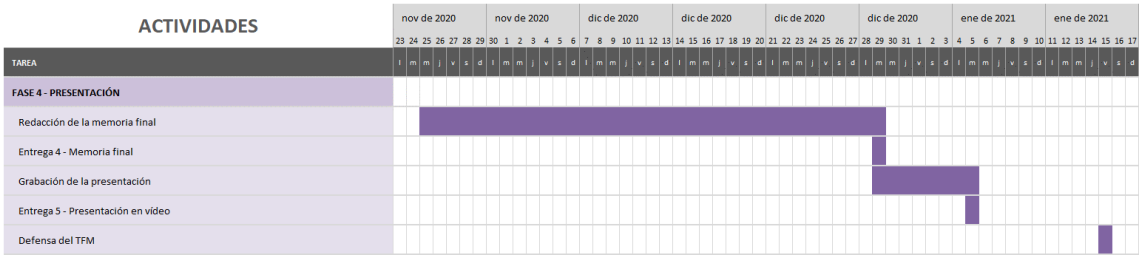

Ilustración 4. Diagrama de Gantt de la Fase 4 del TFM

1.5. ESTRUCTURA DEL TRABAJO

Una vez que creamos conciencia en las organizaciones de que hoy en día la seguridad de la información se ha convertido en uno de los principales ejes dentro de todos los procesos y actividades, que ayuda en la prevención de posibles amenazas que pudiesen llegar a poner en riesgo la funcionalidad de los servicios y llegar a perjudicar a los clientes internos y externos, se hace necesario mantener un proceso oportuno de detección de ataques y en conjunto con un proceso adecuado de respuesta ante incidentes de seguridad que puedan materializarse. Es por ello por lo que en las organizaciones deben siempre considerar a la seguridad de sus activos de información como uno de los principales requisitos a exigir en todos los procesos.

El Trabajo de Fin de Máster pretende abarcar todos aquellos aspectos que se consideran necesarios para definir e implementar un Centro de Operaciones de Seguridad (SOC), para lo cual el trabajo proporcionará un proceso para la implementación dentro del Consejo de Aseguramiento de la Calidad de la Educación Superior que pretende mejorar el rendimiento de los procesos de detección y respuesta ante las amenazas.

El presente Trabajo de Fin de Máster consta de cinco capítulos, todos ellos ordenados y estructurados con el fin de mantener una secuencia coherente e intuitivamente lógica que permitirá trazar un claro camino hacia el objetivo del trabajo: una propuesta de diseño e implementación.

a) **Capitulo I. Marco Metodológico:** Este capítulo proporciona una breve introducción sobre el planteamiento del problema que justifica la realización del presente trabajo. Es en este capítulo donde el objetivo del trabajo es presentado y se propone la metodología a seguir.
b) **Capítulo II. Marco Teórico:** Este capítulo tiene como finalidad adentrarnos en el marco teórico del trabajo. Se presentan los antecedes que conforman la situación problemática en cuestiones de seguridad de la información, así como conceptos generales del Centro de Operaciones de Seguridad (SOC). Esto permitirá establecer las bases sobre las cuales se sustentará la propuesta de diseño e implementación.
c) **Capítulo III. Diagnóstico de la situación actual del Consejo de Aseguramiento de la Calidad de la Educación Superior:** Este capítulo nos proporciona una radiografía sobre la situación actual del Consejo de Aseguramiento de la Calidad de la Educación Superior, organización para la cual se pretende dejar los lineamientos de diseño y posterior implementación de un Centro de Operaciones de Seguridad (SOC).
d) **Capitulo IV. Propuesta de implantación de un Centro de Operaciones de Seguridad (SOC):** Este capítulo constituye el núcleo del Trabajo de Fin de Máster. Se enfoca en los aspectos relevantes que permitan entender el funcionamiento del SOC y sean la base al momento de diseñar y definir el Centro de Operaciones de Seguridad para el Consejo de Aseguramiento de la Calidad de la Educación Superior.
e) **Capitulo V. Conclusiones:** Este capítulo expone las conclusiones de la realización del Trabajo de Fin de Máster, así como aportes que podrían a futuro enriquecer y aportar valor a futuros trabajos que sean realizados referentes al tema tratado.

CAPÍTULO II. MARCO TEÓRICO

Para poder avanzar en el desarrollo e implementación de un Centro de Operaciones de Seguridad (SOC) en el Consejo de Aseguramiento de la Calidad de la Educación Superior será necesario conocer aquellos conceptos primordiales que requerimos sobre la seguridad de la información y su relación con el funcionamiento y gestión de un SOC.

Es necesario tener claro que la importancia de la seguridad de la información sigue incrementándose a diario en relación directamente proporcional a la extensión cada vez con mayor amplitud en el uso de la información y la necesidad de las organizaciones de llegar a proteger la misma de una manera estructurada y organizada.

Contrapuesto a la realidad que hoy en día vivimos, años atrás la seguridad tradicional consistía en la implementación de algunos firewalls que requerían contar con un número considerables de profesionales que administren este equipamiento con la finalidad de descubrir invasores, a través del análisis de datos provenientes de distintos equipos con diferentes formatos y significados que demandaban no solo comprender los principios de seguridad de una red, sino que estuvieran en capacidad de entender varios métodos de seguridad.

2.1. SEGURIDAD DE LA INFORMACIÓN

En la actualidad el principal activo que las organizaciones consideran en su accionar diario es la "información", por lo que en función de su importancia y sensibilidad cada vez se hace más necesario contar con medidas de protección adecuadas y robustas que eviten que la información organizacional se vea comprometida en cualquier manera.

El estándar internacional ISO/IEC 27001:2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. (ISO, 2013)

Cuando nos encontramos inmersos en el campo de la seguridad de la información sin duda alguna una de las primeras cosas que debemos tomar en cuenta es la protección que debemos tener ante los riesgos que pudiesen afectar a una o varias de sus tres principales propiedades:

- ✓ Confidencialidad: Esta propiedad garantiza que la información solo tiene que ser accesible o divulgada a aquellos que se encuentran autorizados. En caso de ser accedido por usuarios no autorizados el mensaje original deberá ser incomprensible para ellos.
- ✓ Integridad: Esta propiedad garantiza que la información debe permanecer correcta, como el emisor la originó y sin manipulaciones por parte de terceros no autorizados. Esto ayuda a detectar posibles modificaciones o eliminación de datos que sean parte del mensaje original.
- ✓ Disponibilidad: Esta propiedad garantiza que los sistemas de información e infraestructura tecnológica se encuentre disponible y siempre accesible para aquellos usuarios que se encuentran autorizados.

Existen también otras propiedades que deben ser consideradas como importantes dentro de la seguridad de la información:

- ✓ Autenticidad: Esta propiedad es de ayuda al momento de verificar que el emisor de un mensaje es realmente la persona correcta que originó dicho mensaje.
- ✓ No Repudio: Esta propiedad consiste en poder implementar mecanismos que ayuden a demostrar que un determinado usuario generó y envió un mensaje para de esta forma dicho usuario no pueda negar esta acción posteriormente del envío del mensaje.

- ✓ Responsabilidad: Esta propiedad permite registrar y monitorear el uso de los distintos recursos tecnológicos por parte de usuarios previamente conectados y autorizados, de esta manera poder detectar situaciones sospechosas que podría permitir que posibles amenazas se materialicen.
- ✓ Confiabilidad: Esta propiedad garantiza que las propiedades antes mencionadas se cumplen de manera correcta en los activos de información.

2.1.1. DISEÑO DE LA SEGURIDAD DE LA INFORMACIÓN

La planeación de la seguridad de la información trae consigo el desarrollo del análisis de vulnerabilidades, análisis de riesgo y evaluaciones de amenazas. En este sentido se hace necesario incluir factores asociados que refieran el hecho de cómo estamos usando y gestionando la información, y la efectividad y relevancia que tienen las medidas de seguridad implementadas actualmente.

Conscientes de que la Política de Seguridad no trata de convertirse en una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los colaboradores de la organización, la política debe centrarse de manera principal en alcanzar los siguientes objetivos:

a) Reducir los riesgos a un nivel aceptable.
b) Garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información.
c) Cumplir con las leyes y reglamentaciones vigentes.

2.1.2. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información tiene como objetivo precautelar los activos de información que representan mayor valor o importancia para las personas u organizaciones.

Un activo de información para la organización puede constituirse desde una hoja de cálculo en la cual se almacena información de proveedores y clientes hasta el mismo centro de procesamiento de datos.

Los principales objetivos de un buen responsable de seguridad de la información son los siguientes:

a) Minimizar y gestionar los riesgos, así como identificar las posibles amenazas a la seguridad de la información de la organización.
b) Garantizar el uso adecuado de los bienes y recursos con los cuales la organización desempeña sus actividades diarias.
c) Establecer los mecanismos adecuados para una inmediata recuperación, después de un desastre, en el menor tiempo y con la menor afectación y daño posible a las actividades de la organización.
d) Cumplir con el marco legal vigente referente al sector en el cual se desenvuelve la organización.

2.1.3. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Cuando nos referimos a un Sistema de Gestión de la Seguridad de la Información mencionamos un conjunto de políticas que facilitan la administración de la información.

La abreviatura de un SGSI es ampliamente utilizada por la ISO/IEC 27001 la cual especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información apalancándose para esto en el enfoque de la mejora continua según lo define el Ciclo de Deming (PDCA).

a) **Plan (Planificar):** Consiste en una fase de diseño del Sistema de Gestión de Seguridad de la Información en la cual realizamos la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
b) **Do (Hacer):** Consiste en una fase que involucra la implantación y operación de los controles.
c) **Check (Controlar):** Consiste en una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del Sistema de Gestión de Seguridad de la Información.
d) **Act (Actuar):** Consiste en una fase en la cual realizamos cambios cuando sea necesario para llevar de vuelta el Sistema de Gestión de Seguridad de la Información a máximo rendimiento.

Un Sistema de Gestión de Seguridad de la Información busca asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información a la vez que debe ser sostenible en el tiempo a través de la adaptación a los cambios internos de la organización, así como los externos del entorno.

2.1.4. PROTOCOLOS DE SEGURIDAD DE LA INFORMACIÓN

Los protocolos de seguridad de la información consisten en un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información.

Los protocolos de seguridad de la información se encuentran compuestos de:

a) **Criptografía (Cifrado de datos):** Se encarga de la transposición u ocultación del mensaje enviado por el emisor hasta que llega a su destino y puede ser descifrado por el receptor.
b) **Lógica (Estructura y secuencia):** Se encarga de estructurar el orden en el cual se agrupan los datos del mensaje el significado del mensaje y saber cuándo se va a enviar el mensaje.
c) **Identificación (Autenticación):** Se encarga de la validación de identificación es mediante la cual un proceso comprueba que el compañero de comunicación es quien se supone que es y no se trata de un impostor.

2.2. ANÁLISIS Y GESTIÓN DE RIESGOS

En la actualidad las organizaciones a nivel mundial se han hecho cada vez más dependientes de las tecnologías de la información. Sin tecnologías de la información, los procesos de negocio de cualquier organización no funcionan. Esto ha dado la pauta para que la información se convierta en un activo esencial y por ende la seguridad de la información es la llamada a proteger dicho activo.

2.2.1. DEFINICIÓN DE RIESGO

Podemos definir al riesgo como la posibilidad de que ocurra algún evento negativo para las personas y/o empresas. Ya que cualquier persona o entidad está expuesta a una serie de riesgos derivados de factores internos y externos, tan variables como su propio personal, su actividad, la situación económica, la asignación de sus recursos financieros o la tecnología utilizada.

Hoy por hoy los activos de las organizaciones se encuentran expuestas a que ocurra alguna eventualidad que los dañe y debido a que no existe una seguridad total y las medidas de seguridad no pueden asegurar total protección en contra de las vulnerabilidades, se hace imprescindible realizar periódicamente un análisis de riesgos, que nos permita identificar las consecuencia probables o los riesgos asociados con las vulnerabilidades, y así, lograr un manejo de riesgo tras la implementación y mantenimiento de controles que reduzcan los efectos de éste a un nivel aceptable.

2.2.2. ANÁLISIS DE RIESGOS

El análisis de riegos por su parte nos proporciona herramientas útiles que nos permiten cuantificar el riesgo y evaluar si el análisis realizado es adecuado, tomar medidas para reducirlo, además intenta mantener un balance económico entre el impacto de los riesgos y el costo de las soluciones de un programa efectivo de seguridad destinadas a manejarlos.

2.2.2.1. ANÁLISIS CUANTITATIVO DEL RIESGO

Para el análisis cuantitativo del riesgo todos los activos, sus recursos y los controles se identifican, y se evalúan en términos monetarios. Todas las amenazas potenciales se identifican y se estima la frecuencia de su ocurrencia, estas amenazas se comparan con las vulnerabilidades potenciales del sistema de tal forma que se identifiquen las áreas que son sensibles.

De esta manera podremos decidir si los controles existentes son adecuados o si se requiere la implementación de otros adicionales. El problema con este tipo de análisis de riesgo radica en que generalmente existe falta de fiabilidad e inexactitud en los datos que podrían terminar en una interpretación errónea de los resultados obtenidos.

2.2.2.2. ANÁLISIS CUALITATIVO DEL RIESGO

Para el análisis cualitativo del riesgo en lugar de que establezcamos valores exactos proporcionamos notaciones como alto, bajo, medio que representan la frecuencia de ocurrencia y el valor de los activos. El problema con este tipo de análisis de riesgo radica en que pueden existir áreas significativamente expuestas que no hayan sido identificadas como posibles fuentes de riesgo.

2.2.3. GESTIÓN DE RIESGOS

Cuando nos referimos a la gestión de riesgos debemos mencionar que consiste en un enfoque claramente estructurado que nos permite manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo mediante la utilización de recursos gerenciales.

Entre las estrategias que se pueden adoptar como parte de la gestión de riesgos se incluyen el transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

El objetivo primordial de la gestión de riesgos es reducir diferentes riesgos relativos a un ámbito preseleccionado a un nivel aceptado por la organización.

Algunas veces, el manejo de riesgos se centra en la contención de riesgo por causas físicas o legales lo que nos proporciona un modelo del sistema en términos de activos, amenazas y controles que permite monitorear todas las actividades de manera claramente fundamentada. En síntesis, la gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis.

Ilustración 5. Análisis y gestión de riesgos

2.3. AMENAZAS

Podemos dar una definición diciendo que una amenaza se representa a través de una persona, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño en las tecnologías de la información, produciendo pérdidas materiales, financieras o de otro tipo.

2.3.1. AMENAZAS HUMANAS

Este tipo de amenazas surgen debido a la ignorancia, existente en las organizaciones, en cuanto al manejo de la información, derivadas del descuido, la negligencia o la inconformidad.

2.3.2. AMENAZAS DE INGENIERÍA SOCIAL

Este tipo de amenazas consisten en la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no realizan de forma que revelen datos indispensables que permitan superar las barreras de seguridad de la información establecidas en la organización con la finalidad de averiguar nombres de usuarios y contraseñas.

2.3.3. AMENAZAS DE HARDWARE

Este tipo de amenazas se da por fallas físicas que pueden hacerse presentes en cualquier momento y que pueden afectar cualquiera de los elementos que conforman los dispositivos y equipos informáticos.

2.3.4. AMENAZAS DE RED

Este tipo de amenazas se presenta una amenaza cuando no se realiza un buen cálculo o diseño del flujo de información que va a circular por el canal de comunicación, con lo cual un atacante podría terminar saturando el canal de comunicación provocando la no disponibilidad de la red. Adicional también debe considerarse que puede darse la desconexión del canal.

2.3.5. AMENAZAS LÓGICAS

Este tipo de amenazas se presenta cuando pese a que tengamos un diseño bien elaborado de

un mecanismo de seguridad lo hayamos implementado mal y sin cumplir con las especificaciones del diseño. También la comunicación entre procesos puede constituir una amenaza cuando un intruso utilice una aplicación que permita enviar y recibir información, que le brinden los elementos necesarios para la generación de un ataque a la organización.

2.3.6. AMENAZAS POR FENÓMENOS NATURALES

Este tipo de amenazas se relaciona directamente con los distintos fenómenos naturales que provocan desastres. Este tipo de amenaza constituye uno de los riesgos más fuertes y debido a la existencia de éstos se tiene la necesidad imperativa de desarrollar planes de contingencia y aplicarse medidas en pro de salvaguardar la seguridad de la información.

2.4. VULNERABILIDADES

Otro de los factores que ponen en riesgo la seguridad de la información constituyen las vulnerabilidades que consisten en elementos que pueden ser aprovechados por los atacantes para violar la seguridad y que pueden derivar en daños por sí mismos sin tratarse de un ataque intencionado.

2.4.1. VULNERABILIDADES HUMANAS

Este tipo de vulnerabilidades se presenta comúnmente por la falta de capacitación y concientización sobre los empleados de la organización, lo que puede dar lugar a la negligencia en el seguimiento de las políticas de seguridad, y mal uso de los equipos de cómputo.

Los actos contra la seguridad realizados a conciencia por un elemento humano pueden ser el fruto de una vulnerabilidad humana, ya sea porque un usuario que accidentalmente revela las contraseñas de acceso o porque no revisa periódicamente las bitácoras de actividades de los equipos de cómputo a fin de buscar actividades sospechosas.

2.4.2. VULNERABILIDADES FÍSICAS

Este tipo de vulnerabilidades se encuentra relacionada con el acceso físico a los sistemas e instalaciones de la organización. De manera general esta vulnerabilidad se hace presente cuando no existen adecuadas prácticas en cuanto a las políticas de acceso de personal a los sistemas y uso de medios físicos de almacenamiento de información que permitan extraer datos del sistema de manera no autorizada.

2.4.3. VULNERABILIDADES NATURALES

Este tipo de vulnerabilidades se hace presente de manera principal cuando se tienen deficiencias en cuanto a las medidas adoptadas por las organizaciones para afrontar los desastres naturales.

2.4.4. VULNERABILIDADES DE HARDWARE

Este tipo de vulnerabilidades representa la probabilidad de que los componentes físicos de los sistemas fallen dando como consecuencia que los sistemas se encuentren desprotegidos o inoperables. Se hace referencia también a las formas en las cuales el hardware puede ser usado por personas internas o ajenas a la organización para atacar la seguridad del sistema.

2.4.5. VULNERABILIDADES DE SOFTWARE

Este tipo de vulnerabilidades se hace presente cuando un programa puede ser utilizado como medio para atacar a un sistema más grande, debido a los errores de programación que puedan existir en las aplicaciones, o porque en el diseño de estas no se consideraron aspectos relevantes de seguridad.

2.4.6. VULNERABILIDADES DE RED

Este tipo de vulnerabilidades consiste en el ataque a toda la red de la organización penetrando

primero en uno de los equipos y posteriormente expandiéndose a los equipos restantes. Se debe tener claridad que en una red el objetivo primordial es la transmisión de la información, por lo que las vulnerabilidades se centran en la posible intercepción de la información por personas no autorizadas y con fallas en la disponibilidad del servicio.

2.5. INCIDENTES DE SEGURIDAD

Se considera como incidente de seguridad a la materialización de una amenaza, es decir, es cualquier evento que pueda producir una interrupción del funcionamiento normal de los servicios tecnológicos que ofrece la organización, y que puede conllevar a pérdidas materiales y financieras.

Un incidente de seguridad de la información es producido por un solo evento o una serie de eventos inesperados que poseen una probabilidad alta de comprometer las operaciones del negocio y amenazar contra la seguridad de la información.

2.6. CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Al referirnos a un Centro de Operaciones de Seguridad (SOC) mencionamos una parte o a la totalidad de una plataforma cuyo propósito es de brindar servicios de detección y reacción ante incidentes de seguridad.

Un Centro de Operaciones de Seguridad (SOC) se encargar del monitoreo y administración de todos los aspectos de seguridad de la información de la organización en tiempo real desde una ubicación única y centralizada.

Al mismo tiempo que el Centro de Operaciones de Seguridad (SOC) requiere de estándares y mejores prácticas que nos provean la ayuda necesaria que nos permita resolver las brechas entre enfoques teóricos, implementaciones propietarias y sistemas independientes con la finalidad de poder cumplir de una manera completa, efectiva y medible cada uno de los objetivos y requerimientos que plantea la implementación, los objetivos, las funciones y la operación exitosa de un SOC el cual estará encaminado a proveer servicios de detección y reacción a incidentes de seguridad y dar resultados confiables, así como cumplir con los requerimientos técnicos y de negocio establecidos por parte de la organización.

2.6.1. POR QUÉ SE REQUIERE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Desde siempre los sistemas de detección de intrusos (IDS) han ayudado a la gestión de los analistas de seguridad a reconocer e identificar amenazas, mediante la emisión de alertas que van describiendo el detalle de las posibles intrusiones. Estas alertas generadas por los sistemas IDS de forma general suelen ser muy molestas al momento de revisar la información que contienen además que en varias ocasiones las alertas mostradas pueden desencadenar en falsos positivos.

Para esto, el personal encargado de la administración de la seguridad debe de forma obligatoria combinar la experiencia y el conocimiento que disponen sumados a un entendimiento del contexto tanto interno como del entorno que rodea a la organización para de esta manera encontrarse en plena capacidad de determinar con exactitud la severidad de cada alerta emitida. En este escenario, y a medida que día a día las redes van creciendo en cuanto a su tamaño y complejidad estas tareas se van volviendo cada vez más complicadas de ejecutar y por ende existe dificultades para el personal encargado del monitoreo de la red actuar proactivamente para lograr encontrarse un paso adelante sobre los atacantes.

A esto se suma que en la actualidad los sistemas de detección de intrusos tienen a disposición numerosas soluciones de seguridad en el mercado, tales como software antivirus, firewalls, sistemas de prevención de intrusos, control de acceso, Identity Management, sistemas de autentificación, entre otros. Sin embargo, el inconveniente que se tiene ante este sin número

de soluciones existentes es que cada solución nos presenta información en diferentes formatos, la almacena en diferentes lugares y la reporta a ubicaciones diferentes lo cual complica a las organizaciones en el sentido de tener que tratar con incompatibilidades en cuanto a las tecnologías de seguridad de la información implementadas, lo que genera una sobrecarga al equipo de seguridad, además que los esfuerzos de parte del equipo se duplican dando como resultados debilidad en los modelos de seguridad implementados así como inconvenientes o resultados no deseados al momento de las auditorías.

Para poder hacer frente a la diversidad y fragmentación que se tiene en cuanto a los eventos de seguridad que se presentan diariamente y poder poner a buen recaudo las operaciones del negocio, los administradores de seguridad hoy en día necesitan contar con soluciones que les permitan responder de una manera rápida y efectiva ante los incidentes de seguridad, a través de herramientas que permitan la integración, centralización y análisis en tiempo real de los incidentes que se llegaren a presentar.

Es así como un Centro de Operaciones de Seguridad (SOC) nos puede brindar la facilidad de contar con información en tiempo real del estado de la seguridad de la red de nuestra organización, actuando de manera más proactiva a través de la generación de alertas automáticas, emisión de reportes más detallados y sobre todo contar con aspectos que nos permitan ejecutar la remediación necesaria ante un incidente de seguridad desde una ubicación centralizada y que nos permita sobre la marcha ir realizando los ajustes y tomando los correctivos necesarios a la estrategia de seguridad de la información implementada en la organización.

Mediante el diseño, implementación y operación de un Centro de Operaciones de Seguridad (SOC) la organización puede obtener algunos beneficios entre los cuales podemos citar los siguientes como los más destacados:

a) Preparación para actuar de manera efectiva ante los incidentes de seguridad que se puedan presentar.
b) Minimización de los riesgos potenciales que pueden existir para los clientes tanto internos como externos.
c) Mejora en los tiempos de respuesta de los equipos de seguridad.
d) Incremento en la eficiencia operacional de la organización.
e) Reducción de costos para la organización.
f) Asistencia a los clientes internos y externos para el cumplimiento de las regulaciones y la normativa legal vigente.

Si bien es cierto el plantear la necesidad de parte de la organización de implementar un Centro de Operaciones de Seguridad (SOC) puede constituirse en una decisión relativamente fácil de tomar, tenemos una contraposición de opiniones al momento de diseñarlo e implementarlo, especialmente cuando no existe homogeneización de los grupos operativos de seguridad y de red que vienen desarrollando sus actividades de manera independiente y aislada uno del otro.

2.6.2. DEFINICIÓN GENERAL DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Podemos empezar definiendo a un Centro de Operaciones de Seguridad (SOC) como “un término genérico que describe una parte o el todo de una plataforma cuyo propósito es proveer servicios de detección y reacción a incidentes de seguridad”.

El Centro de Operaciones de Seguridad (SOC) se ha convertido en la actualidad en una tendencia relativa a la infraestructura de seguridad ya que el SOC es un espacio de monitoreo avanzado constituido como un centro de respuestas de seguridad informática, cuya principal responsabilidad radica en la detección y respuesta ante incidentes de seguridad de la información que ocurren dentro de la organización.

Para lograr los niveles deseados de seguridad de la información que en la actualidad demandan las organizaciones, el Centro de Operaciones de Seguridad (SOC) necesita cumplir con una serie de funcionalidades por decirlo menos básicas que garanticen su normal funcionamiento:

- ✓ Debe ser en tiempo real, y permitir la administración y monitoreo de las redes privadas virtuales, firewalls, sistemas de prevención y detección de intrusos y otros sistemas de seguridad.
- ✓ Debe analizar datos de seguridad, información de vulnerabilidades, información de los activos y las alertas respectivas ante cada uno de los eventos que se presenten.
- ✓ Debe tener la capacidad de responder de forma inmediata ante las amenazas potenciales de seguridad y poder resolver de manera rápida y oportuna los problemas de seguridad que se hayan presentado.
- ✓ Debe brindar vistas de información en tiempo real de las posturas de seguridad de los clientes internos y externos de la organización.
- ✓ En todo momento debe proteger a los clientes internos y externos ante todo tipo de ataques de red que puedan surgir.
- ✓ Debe proteger las inversiones tecnológicas realizadas por parte de la organización.

El Centro de Operaciones de Seguridad (SOC) debe también tener la capacidad de poder generar la siguiente información, la cual se evidencia en forma de reportes de tipo gerencial que ayuda a la toma de decisiones. Esta información mínima que debe presentar se resume de la siguiente manera:

- ✓ Monitoreo de seguridad para la administración de riesgos.
- ✓ Análisis de riesgos de seguridad de la información en la organización.
- ✓ Acceso seguro al portal de administración de la plataforma basado en roles.
- ✓ Reportes de políticas de seguridad de la información implementados en la organización.
- ✓ Reportes de incidentes de seguridad de la información ocurridos en la organización.
- ✓ Atención en tiempo real a incidentes, así como reportes semanales y mensuales.
- ✓ Información requerida para preparase para auditorías de cumplimiento a regulaciones internacionales y a la normativa legal vigente.
- ✓ Reportes de SLA (Service Level Agreement).
- ✓ Evidencia de cumplimiento de la política de seguridad de la información establecida en la organización.
- ✓ Tendencias de incidentes de seguridad y eventos ocurridos.

Es así que la clave del éxito de un Centro de Operaciones de Seguridad (SOC) constituye sin duda alguna el hecho de aprovisionar un escenario en el cual tanto los administradores de seguridad como la organización en su conjunto se encuentren siempre en conocimiento de la realidad y de la situación actual de la seguridad de la información, ya que el SOC es el facilitador de esa radiografía de la situación actual por la que está atravesando la organización en un momento determinado a través de la acumulación de información proveniente de una gran variedad de dispositivos, que luego son normalizados y correlacionando la información, de tal forma que el SOC pueda proveer los reportes en tiempo real de lo que está sucediendo, de tal modo que los administradores de seguridad puedan manejar y responder a las intrusiones antes de que éstas pongan en riesgo inminente a la organización.

2.6.3. IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Hoy en día existen varios casos de implementaciones exitosas de Centros de Operaciones de Seguridad (SOC) alrededor del mundo. El punto en común entre cada una de ellas es que el SOC provee a las organizaciones un análisis de seguridad en tiempo real, basados en una detección temprana de advertencias y que brinda la posibilidad de reaccionar rápida y proactivamente ante eventos sospechosos, de tal forma que los equipos de seguridad de la organización estén en capacidad de monitorear todos los eventos que suceden en la red a través de un portal

seguro.

La misión de un Centro de Operaciones de Seguridad (SOC) es integrar la información de los eventos de seguridad y de red, de manera que el equipo de seguridad y operaciones de la organización puedan tener una perspectiva bastante clara y amplia de cada uno de los eventos suscitados y las afectaciones que estos podrían generar sobre la red de tal forma que la organización este en capacidad de tomar decisiones basadas en la información que permita reaccionar de mejor manera según lo establecido en las políticas de seguridad de la información definidas en la organización.

Uno de los puntos a tomar en cuenta es que la complejidad en la implementación del Centro de Operaciones de Seguridad (SOC) obedece a una correcta y adecuada integración de los sistemas de seguridad existentes antes que implementación de herramientas individuales. Es así como el SOC se configura como un proceso que requiere la incorporación de estándares encaminados de manera primordial a referenciar lo siguiente:

a) **Sensores como generadores de eventos:** Determinado por la variedad de técnicas que existen para la recolección de datos de múltiples fuentes de información con niveles de detalle distintos y con especificidades propias según cada uno de los fabricantes o desarrolladores.
b) **Bases de datos de mensajes con formato:** Al ser bases de datos en si estos módulos son los que tienen mayor estandarización al momento de establecer la arquitectura del Centro de Operaciones de Seguridad (SOC).
c) **Análisis de eventos:** Responde a la mayor parte de investigaciones que se están llevando a cabo alrededor del mundo en la actualidad enfocado en gran medida en la realización de futuras implementaciones. Sin embargo, al estar enfocado a la investigación se ha estancado en la realización de pruebas de concepto que lleven en algún momento al diseño de un módulo estandarizado para operación del Centro de Operaciones de Seguridad (SOC).
d) **Reacción a eventos y reportes:** Al estar los Centros de Operaciones de Seguridad (SOC) implementados para responder a necesidades específicas en función de las organizaciones se tiene que cada organización emita sus consejos y mejores prácticas las cuales estarán basadas en las experiencias de la vida real que las organizaciones han ido experimentando a través del tiempo.

Es así como la implementación y operación de un Centro de Operaciones de Seguridad (SOC) les trae a las organizaciones una serie de interesantes beneficios entre los cuales podemos mencionar los siguientes como los más relevantes:

a) **Preparación para lidiar efectivamente con incidentes de seguridad:** Al operar un Centro de Operaciones de Seguridad (SOC), la organización se mueve de una postura reactiva a una proactiva, teniendo un proceso bien establecido que permita un movimiento rápido y efectivo para aislar, contener y mitigar la amenaza. Además, permitirá dedicar los esfuerzos de los administradores de seguridad al desarrollo de estrategias de red en lugar de perseguir soluciones después de cada ocasión que surja una amenaza.
b) **Reducción de riesgos para los clientes:** Un Centro de Operaciones de Seguridad (SOC) permite minimizar el tiempo muerto de la red en relación con la seguridad de esta, así como proteger más efectivamente el tráfico de información de los clientes internos y externos y de esta manera evitar su pérdida o manipulación, controlando mejor los servicios de seguridad de la información.
c) **Mejora en la respuesta de seguridad:** Al operar un Centro de Operaciones de Seguridad (SOC) se cuenta con una definición clara de los niveles de escalamiento a seguir, de tal forma que se esté en capacidad de analizar las razones potenciales de la anomalía en el

tráfico y se pueda resolver el incidente de forma apropiada eliminando problemas potenciales en servicios críticos y procesos de negocio.

d) **Incremento de la eficiencia operacional:** Al definir reglas y políticas de seguridad de la información claras, los especialistas del Centro de Operaciones de Seguridad (SOC) estarán en capacidad de identificar las amenazas más rápidamente que permitan aplicar remedios a sitios en riesgo antes que las amenazas de red los alcancen.
e) **Reducción de costos:** Dado que un Centro de Operaciones de Seguridad (SOC) basa su funcionamiento sobre las tecnologías, herramientas y procedimientos de seguridad de la información, es posible emplear eficientemente los costosos especialistas de seguridad de tecnologías de la información sin que se vea comprometida la calidad de los entregables del SOC. obviamente el hecho de los expertos en seguridad se concentren en amenazas legítimas, ayuda considerablemente a optimizar el uso de sus habilidades.
f) **Asistencia a clientes para cumplir con regulaciones:** Los clientes tanto internos como externos generalmente necesitan cumplir con regulaciones y políticas sobre el uso, protección y privacidad de la información. Es posible que los clientes usen los reportes que el Centro de Operaciones de Seguridad (SOC) genera para adherirse a estas regulaciones y políticas.

2.6.3.1. REQUERIMIENTOS DE NEGOCIO

Se han propuesto entre algunas mejores prácticas para construir un Centro de Operaciones de Seguridad (SOC), algunos requerimientos de negocio:

a) **Reducción de riesgos y tiempo muerto:** Hace algún tiempo podía haber sido posible para una organización apagar, por ejemplo, el servidor de correo cuando un virus se empezaba a expandir rápidamente, pero para la mayoría de las organizaciones esto ya no es una opción.
b) **Control y prevención de amenazas:** Prevenir y controlar amenazas involucra una notificación temprana de actividad sospechosa, así como la habilidad de implementar rápidamente un mecanismo de contingencia.
c) **Aligeramiento de la carga de trabajo administrativa:** El Centro de Operaciones de Seguridad (SOC) debe ser diseñado para involucrar la menor cantidad posible de sobrecarga humana. La meta es habilitar a unos cuantos administradores con la mejor información, para lograr respuestas rápidas y automatizadas.
d) **Personal y responsabilidades:** Las responsabilidades que necesitan ser definidas incluyen el quién es encargado de ciertas tareas específicas y asignar responsabilidades de respuesta y control para cada unidad de negocio.
e) **Trayectoria de escalamiento:** Este requerimiento implica saber el cómo y el cuándo escalar los eventos.
f) **Auditorías y soporte de cumplimiento:** Uno de los requerimientos más críticos del negocio implica la necesidad de auditorías para cumplir con regulaciones corporativas, gubernamentales y de la industria.
g) **Respuesta a incidentes y recuperación:** Un Centro de Operaciones de Seguridad (SOC) bien diseñado pone en manos de los administradores el poder de ver los incidentes atacando la red, y usa efectivamente herramientas de administración de incidentes para ayudar a los administradores a encontrar y remediar los problemas.

2.6.3.2. REQUERIMIENTOS TÉCNICOS

Se han propuesto entre algunas mejores prácticas para construir un Centro de Operaciones de Seguridad (SOC), algunos requerimientos técnicos:

a) **Rapidez de agregación y correlación:** Suprimir información repetida, validando alertas para confirmar su impacto, y priorizar las alertas más críticas caracteriza un verdadero y útil producto de administración de seguridad de la información.
b) **Cobertura de sistemas y dispositivos:** Para que un Centro de Operaciones de Seguridad (SOC) pueda generar verdadero valor, debe ser capaz de soportar todos los dispositivos de seguridad y cubrir todo servidor y aplicaciones.
c) **Habilidad para responder rápidamente:** El centro de comandos y control del Centro de Operaciones de Seguridad (SOC) necesita ser capaz de proveer información en tiempo real o casi en tiempo real, habilitando a los operadores para tomar acciones rápidamente.
d) **Actividad 24x7:** Si la red está corriendo 24x7, el Centro de Operaciones Seguridad (SOC) también debe hacerlo. El SOC debe estar corriendo y reportando en tiempo real.
e) **Soporte para ambientes federados y distribuidos:** El Centro de Operaciones de Seguridad (SOC) debe soportar vistas federativas y roles administrativos. La herramienta debe basarse en roles de manera flexible para acomodar estas diferentes necesidades.
f) **Capacidades forenses:** Las herramientas de administración de seguridad de la información que registran las actividades de eventos y pueden visualizar estos datos, habilitan a los administradores para aprender lecciones valiosas y evitar que se repita la historia.
g) **Integración inteligente entre SOC y NOC:** El Centro de Operaciones de Seguridad (SOC) y el Centro de Operaciones de Red (NOC) necesariamente conviven dentro de una organización y juntas estas herramientas proveen una vista de red y seguridad a lo largo de la organización, la cual el negocio necesita para maximizar su eficiencia.

2.7. ESTÁNDARES INTERNACIONALES Y MARCOS DE REFERENCIA APLICABLES AL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

En la actualidad se tienen disponibles varias normas, estándares, guías y buenas prácticas que pueden ser implementadas en cualquier organización con la finalidad de mejorar los servicios, procesos, productos, tiempo de respuesta, desarrollo e inclusive la seguridad de la información.

Si bien no nos enfocaremos a establecer una norma específica que regule las funciones y componentes de un Centro de Operaciones de Seguridad (SOC) a continuación bosquejaremos de manera general aquellas normas y estándares internacionales que a través de su reconocimiento a nivel mundial guardan relación y tienen acápites relacionados con la seguridad de la información que terminan siendo aplicables a las funciones y actividades de un Centro de Operaciones de Seguridad (SOC).

2.7.1. ISO

Cuando nos referimos a ISO podemos hacer referencia a un acrónimo de (International Organization for Standardization) que consiste en una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de normalización.

Es una organización independiente y no-gubernamental formada por las organizaciones de normalización de sus 164 países miembros. Es el mayor desarrollador mundial de estándares internacionales voluntarios y facilita el comercio mundial al proporcionar estándares comunes entre países promoviendo el uso de estándares privativos, industriales y comerciales a nivel mundial.

2.7.1.1. ISO 27001:2013

ISO/IEC 27001:2013 es el estándar internacional que establece la especificación para un sistema de gestión de seguridad de la información (SGSI).

Su enfoque de mejores prácticas ayuda a las organizaciones a administrar la seguridad de su

información al dirigirse a las personas y los procesos, así como a la tecnología.

La certificación acreditada de forma independiente para el estándar se reconoce en todo el mundo como una indicación de que su sistema de gestión de la seguridad de la información se encuentra alineado con las mejores prácticas de seguridad de la información.

2.7.2. NIST

Cuando nos referimos a NIST podemos hacer referencia a un acrónimo de (National Institute of Standards and Technology) que consiste en un laboratorio de ciencias físicas y una agencia no reguladora del Departamento de Comercio de los Estados Unidos.

Su misión es promover la innovación y la competitividad industrial. Las actividades del NIST están organizadas en programas de laboratorio que incluyen ciencia y tecnología a nanoescala, ingeniería, tecnología de la información, investigación de neutrones, medición de materiales y medición física.

2.7.2.1. CYBERSECURITY FRAMEWORK

Los gobiernos, los sectores de la industria y las organizaciones de todo el mundo están reconociendo cada vez más el Marco de seguridad cibernética (CSF) de NIST como una base de seguridad cibernética recomendada para ayudar a mejorar la gestión del riesgo de la seguridad cibernética y la resistencia de sus sistemas.

Las aplicaciones más comunes del CSF se han manifestado en tres situaciones diferentes:

a) La evaluación de la posición y la experiencia de la empresa en materia de seguridad cibernética mediante la evaluación del modelo CSF (perfil actual) determina la posición deseada en seguridad cibernética (perfil objetivo) y planifica y prioriza los recursos y los esfuerzos para conseguir el perfil objetivo.
b) La evaluación de los productos y los servicios actuales y propuestos para cumplir con los objetivos de seguridad junto con las categorías y subcategorías del CSF para identificar las deficiencias en la capacidad y las oportunidades de reducir el solapamiento/duplicado de las mismas y lograr una mayor eficiencia.
c) Una referencia para la reestructuración de sus equipos de seguridad, los procesos y la formación.

2.7.3. ITIL

Cuando nos referimos a ITIL podemos hacer referencia a que es un acrónimo de (Information Technology Infrastructure Library) que consiste en un conjunto reconocido a nivel mundial de mejores prácticas para la gestión de servicios de tecnología de la información.

La definición oficial de ITIL consiste en “Un conjunto de publicaciones de mejores prácticas para Gestión de servicios de TI. ITIL proporciona asesoramiento sobre la provisión de servicios de TI de calidad y de los procesos, funciones y demás capacidades necesarias para darles apoyo. El marco de ITIL está basado en un ciclo de vida del servicio y consiste en cinco etapas (estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio) que cuentan con su propia publicación de apoyo. También hay un conjunto de publicaciones complementarias de ITIL que brindan asesoramiento específico para distintos sectores económicos, tipos de organizaciones, modelos de operación y arquitectura de tecnología”.

2.7.3.1. GESTIÓN DE LA SEGURIDAD

La gestión de la seguridad debe siempre tener en cuenta todos aquellos riesgos generales a los que se encuentra expuesta la infraestructura de tecnologías de la información de la organización de tal forma que se asegure que no existan peligros potenciales que afecten la continuidad del

servicio.

Debe tratarse en todo momento que la gestión de la seguridad sea dinámica y evalúe de forma anticipada los riesgos de seguridad que pueden suponer los cambios realizados en la infraestructura, nuevas líneas de negocio, entre otros.

2.7.3.2. GESTIÓN DE INCIDENTES

Cuando nos referimos a una incidencia mencionamos toda interrupción o reducción de la calidad no planificada del servicio. Pueden ser fallos o consultas reportadas por los usuarios, el equipo del servicio o por alguna herramienta de monitorización de eventos.

Un proceso de gestión de incidentes adecuadamente implementado en una organización consigue que el flujo de trabajo y servicio no se vea interrumpido durante periodos de tiempo prolongados e inaceptables.

Para que un servicio funcione de forma óptima es necesario que disponga de una gestión de incidencias eficiente, capaz de solucionar cualquier problema o adversidad de forma eficaz, en el menor tiempo posible.

2.7.4. COBIT

Cuando nos referimos a COBIT podemos hacer referencia a que es un acrónimo de (Control Objectives for Information and related Technology) que constituye un conjunto de propósitos definidos y controles de tecnologías de la información que tiene como principio la implementación de un marco para el gobierno y gestión de tecnologías de la información.

La seguridad de la información y los datos personales es algo imprescindible hoy en día en cualquier organización. Si la tecnología utilizada en una organización es importante para los directivos, la seguridad de la información lo es aún más.

Por este motivo, es importante que todos los empleados conozcan los servicios, infraestructuras, aplicaciones, competencias, principios y procesos existentes en la organización. En este sentido, COBIT ayuda a las organizaciones a minimizar los perfiles de riesgos mediante la administración adecuada de la seguridad.

Dentro de la familia de documentos de COBIT, en la última versión existe uno completamente enfocado en la seguridad de la información (COBIT 5 for Information Security), que tiene como base el framework de mejores prácticas, con la característica de que agrega guías prácticas detalladas para la protección de la información para todos los niveles en las organizaciones.

2.7.4.1. GESTIÓN DE LA SEGURIDAD

Establece la necesidad de definir, operar y supervisar un sistema para la gestión de la seguridad de la información con el propósito de mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la organización.

2.7.4.2. GESTIÓN DE LA CONTINUIDAD

Establece la necesidad de mantener un plan para permitir al negocio y a tecnología de la información responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios requeridos y mantener la disponibilidad de la información a un nivel aceptable para la organización con el propósito de continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable ante el evento de una interrupción significativa.

2.7.4.3. GESTIÓN DE SERVICIOS DE SEGURIDAD

Establece la necesidad de proteger la información de la organización para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad.

Establece y mantiene los roles de seguridad y privilegios de acceso de la información y realiza la supervisión de la seguridad con el propósito de minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.

2.7.5. MITRE

Es una empresa sin fines de lucro que proporciona sistemas de ingeniería, investigación, desarrollo y soporte en información tecnológica. Opera con recursos federales la investigación y desarrollo tecnológico en seguridad nacional, aviación civil y militar entre otros. Actualmente atiende a diversas agencias gubernamentales de gran nivel mediante centros de investigación y desarrollo financiados con fondos federales, en los ámbitos de defensa, aviación, sistemas civiles, seguridad nacional, justicia, salud y ciberseguridad. Es un laboratorio considerado como recurso nacional en los Estados Unidos, en la misma categoría de Los Alamos National Laboratory y el Jet Propulsion Laboratory.

2.7.5.1. ATT&CK

Tácticas, Técnicas y Conocimiento Común de Adversarios describe y categoriza los comportamientos adversos basados en las observaciones de todo el mundo. ATT&CK es una lista estructurada de comportamientos conocidos de los atacantes que se recopilaron en tácticas y técnicas y se expresaron en un par de matrices y también mediante STIX y TAXII. Ya que esta lista es una representación integral de los comportamientos que los atacantes usan cuando ponen en peligro las redes, es útil para una variedad de medidas, representaciones y otros mecanismos ofensivos y defensivos.

2.8. MARCO LEGAL APLICABLE AL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Cuando nos referimos a la normativa relacionada con la seguridad de la información debemos tener siempre presente que la misma debe garantizar los derechos y accesibilidad a los mismos, el cumplimiento de las obligaciones y el aseguramiento.

A continuación, se referencia las normativas de la legislación ecuatoriana que se han tenido en cuenta para el desarrollo del trabajo.

2.8.1. LEY ORGÁNICA DE PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

La Ley Orgánica de Protección de los Datos de Carácter Personal (LOPD), establece un conjunto de principios, derechos y deberes que las organizaciones deben dar cumplimiento.

El responsable de los datos/ficheros, es la entidad, persona u órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales. Sobre el responsable del fichero recaen las principales obligaciones establecidas por la LOPD y le corresponde velar por el cumplimiento de la Ley en su organización.

2.8.2. LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS

Regula la gestión de los datos públicos y su acceso. Promueve el derecho de las personas al acceso de la información y servicios públicos, derecho a la identidad personal y colectiva, y a la protección de los datos de carácter personal.

2.8.3. LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

Se aplica el derecho a la publicidad de la información pública. Reconocida en el Pacto Internacional de Derechos Civiles y Políticos, la Convención Interamericana de Derechos Humanos, la Ley Orgánica de la Contraloría General del Estado.

Para su aplicación se ampara en la Norma Técnica de Aplicación y el Reglamento a la LOTAIP.

2.8.4. LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJE DE DATOS

Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

A los mensajes de datos se les reconoce el mismo valor jurídico que los documentos escritos, así como se otorga reconocimiento jurídico de la firma electrónica como si se tratar de la firma manuscrita.

2.8.5. NORMAS TÉCNICAS DE SEGURIDAD ADOPTADAS DE LOS ESTÁNDARES INTERNACIONALES ISO/IEC 27000

- ✓ NTE INEN ISO/IEC 27000: Descripción General y Vocabulario.
- ✓ NTE INEN ISO/IEC 27001: Requisitos de un SGSI.
- ✓ NTE INEN ISO/IEC 27002: Guía de buenas prácticas. Describe objetivos de control y controles (39 objetivos y 133 controles) en 11 dominios.
- ✓ NTE INEN ISO/IEC 27003: Guía de Implementación. Uso modelo PDCA.
- ✓ NTE INEN ISO/IEC 27004: Medición, especifica métricas y técnicas de medida para determinar la eficacia del SGSI.
- ✓ NTE INEN ISO/IEC 27005: Gestión del Riesgo.

2.8.6. NORMAS DE CONTROL INTERNO DE LA CONTRALORÍA GENERAL DEL ESTADO

Para entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos.

2.8.7. ACUERDO 166 DE LA SECRETARÍA NACIONAL DE LA ADMINISTRACIÓN PÚBLICA

Normativa del Esquema Gubernamental de Seguridad de la Información (EGSI).

CAPITULO III. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DEL CONSEJO DE ASEGURAMIENTO DE LA CALIDAD DE LA EDUCACIÓN SUPERIOR

Las instituciones del Sistema Nacional de Educación Superior Ecuatoriano tienen como misión la búsqueda de la verdad, el desarrollo de las culturas universal y ancestral ecuatoriana, de la ciencia y tecnología, mediante la docencia, la investigación y la vinculación con la colectividad.

Las instituciones del Sistema Nacional de Educación Superior Ecuatoriano son esencialmente pluralistas, están abiertas a todas las corrientes y formas del pensamiento universal expuestas de manera científica. Dirigen su actividad a la formación integral del ser humano para contribuir al desarrollo del país y al logro de la justicia social, al fortalecimiento de la identidad nacional en el contexto pluricultural del país, a la afirmación de la democracia, la paz, los derechos humanos, la integración latinoamericana y la defensa y protección del medio ambiente. Les corresponde producir propuestas y planteamientos para buscar la solución de los problemas del país; propiciar el diálogo entre las culturas nacionales y de éstas con la cultura universal, la difusión y el fortalecimiento de sus valores en la sociedad ecuatoriana, la formación profesional, técnica y científica y la contribución para lograr una sociedad más justa, equitativa y solidaria, en colaboración con los organismos del estado y la sociedad.

3.1. DATOS BÁSICOS DE LA INSTITUCIÓN

3.1.1. NOMBRE

Consejo de Aseguramiento de la Calidad de la Educación Superior – CACES –.

3.1.2. FUNCIÓN PRINCIPAL

La regulación, planificación, coordinación del Sistema de Aseguramiento de la Calidad de la Educación Superior.

3.2. BASE LEGAL

3.2.1. CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR

La Constitución de la República en su artículo 275 señala: “El régimen de desarrollo es el conjunto organizado, sostenible y dinámico de los sistemas económicos, políticos, socioculturales y ambientales, que garantizan la realización del Buen Vivir, del Sumak Kawsay”.

“El Estado planificará el desarrollo del país para garantizar el ejercicio de los derechos, la consecución de los objetivos del régimen de desarrollo y los principios consagrados en la Constitución. La Planificación propiciará la equidad social y territorial, promoverá la concertación y será participativa, descentralizada, desconcentrada y transparente. El Buen Vivir requerirá que las personas, comunidades, pueblos y nacionalidades gocen efectivamente de sus derechos, y ejerzan responsabilidades en el marco de la interculturalidad, del respeto a sus diversidades, y de la convivencia armónica con la naturaleza”.

Mediante artículo 280, ibidem: “El Plan Nacional de Desarrollo es el instrumento al que se sujetarán las políticas, programas y proyectos públicos; la programación y ejecución del presupuesto del Estado; y la inversión y la asignación de los recursos públicos; y coordinar las competencias exclusivas entre el Estado central y los gobiernos autónomos descentralizados. Su observancia será de carácter obligatorio para el sector público e indicativo para los demás sectores”.

3.2.2. LEY ORGÁNICA REFORMATORIA A LA LEY ORGÁNICA DE EDUCACIÓN SUPERIOR

La Asamblea Nacional discutió el “Proyecto de Ley Orgánica Reformatoria a la Ley Orgánica de Educación Superior” en primer debate los días 19 y 26 de septiembre y 10 de octubre de 2017, y en segundo debate el 15 de mayo de 2018. El 14 de junio de 2018 fue objetado parcialmente

por el Presidente Constitucional de la República del Ecuador; y posteriormente aprobado por la Asamblea Nacional el 12 de julio de 2018 con el nombre "LEY ORGÁNICA REFORMATORIA A LA LEY ORGÁNICA DE EDUCACIÓN SUPERIOR", publicada en el Registro Oficial 297 del 2 de agosto de 2018.

El artículo 171 de la Ley Orgánica Reformatoria a la Ley Orgánica de Educación Superior determina que: "El Consejo de Aseguramiento de la Calidad de la Educación Superior: Es el organismo público técnico con personería jurídica y patrimonio propio, con independencia administrativa, financiera y operativa que tiene a su cargo la regulación, planificación y coordinación del sistema de aseguramiento de la calidad de la educación superior; tendrá facultad reguladora y de gestión".

3.2.3. NORMAS DE CONTROL INTERNO DE LA CONTRALORÍA GENERAL DEL ESTADO

La Unidad de Tecnología de Información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además, debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.

Las entidades u organismos del sector público establecerán una estructura organizacional de tecnología de información que refleje las necesidades institucionales, la cual debe ser revisada de forma periódica para ajustar las estrategias internas que permitan satisfacer los objetivos planteados y soporten los avances tecnológicos. Bajo este esquema se dispondrá como mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica y soporte interno y externo de ser el caso, considerando el tamaño de la entidad y de la unidad de tecnología."

La norma de control 410-10 Seguridad de tecnología de información determina que: "La Unidad de Tecnología de Información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos.".

3.3. ANÁLISIS SITUACIONAL

3.3.1. PLANIFICACIÓN, ORGANIZACIÓN Y CULTURA

El macroproceso gobernante "Direccionamiento Estratégico" establece las directrices y gestión de política pública de aseguramiento de la calidad que se instrumentaliza a través del proceso de gestión estratégica –que se guía en los instrumentos y metodologías emitidas por las instancias gubernamentales rectoras y se articula al Plan de Desarrollo del Ecuador – y la cadena de valor de la Institución.

La responsabilidad de la gestión y liderazgo recae en el Pleno del Consejo (máxima autoridad) y Comisiones Permanentes, donde se establecen los lineamientos y directrices estratégicas que guían el accionar de la Institución.

3.3.2. CONTEXTO POLÍTICO

El apoyo político del Ejecutivo es un factor determinante para el cumplimiento de los objetivos institucionales y que ha dado la legitimidad que permite al Consejo de Aseguramiento de la Calidad de la Educación Superior seguir adelante en el camino hacia la promoción de la cultura de calidad en el sistema de educación superior.

3.3.3. CONTEXTO ECONÓMICO

La economía del Ecuador no goza de buena salud, solamente un manejo responsable, transparente y disciplinado de los recursos y de las finanzas devolverá al país la prosperidad y

esperanza. No se puede gastar más de lo que se tiene.

Es el Estado quien más gasta y quien debe asumir el mayor esfuerzo para cambiar las cosas. Estos cambios toman tiempo; requieren de disciplina y constancia. La Ley de Fomento Productivo es un primer paso para recuperar la competitividad. Esta garantiza un marco regulatorio con una ruta clara hacia el equilibrio fiscal y menor endeudamiento para tener una economía dinámica, diversa y que ofrezca oportunidades de empleo, desarrollo y bienestar.

3.3.4. ANÁLISIS SECTORIAL DE LA EDUCACIÓN SUPERIOR

Después de los procesos de evaluación con fines de acreditación el Consejo ha realizado actividades para dar seguimiento y acompañamiento a las Instituciones de Educación Superior – IES – no acreditadas, con el objetivo de apoyarlas en la superación de debilidades para que enfrenten de mejor manera nuevos procesos de acreditación. Este esquema ha respondido a una lógica lineal en la que el aseguramiento de la calidad ha sido un proceso posterior al de acreditación y clasificación. Este esquema cambia sustancialmente con la aprobación de la Ley reformatoria a la LOES 2018, ya que se constituye el Sistema Interinstitucional de Aseguramiento de la Calidad (LOES 2018, Art. 94), y el aseguramiento de la calidad pasa a ser un proceso central y permanente, sustentado sobre todo en la autoevaluación de las IES y los procesos de evaluación externa.

3.3.5. MICROENTORNO (GRUPOS DE INTERÉS)

De los actores identificados en instrumentos como el Modelo de Gestión y el Análisis de Presencia Institucional, se realizó el mapeo y análisis de influencia de cada uno de ellos. El análisis va encaminado a las instituciones receptoras de los productos y servicios que realiza el CACES y que se convierten en proveedores de información para la institución, de acuerdo con las atribuciones estipuladas en la LOES y su reglamento, el estatuto orgánico por procesos y demás instrumentos legales que determinan el funcionamiento de este Consejo, con el fin de determinar el relacionamiento y el actuar en la entrega de los productos y servicios. Estos son:

- ✓ Instituciones de Educación Superior – IES – (Universidades, Escuelas Politécnicas, Institutos Superiores Técnicos, Tecnológicos, Pedagógicos, de Artes y Conservatorios Superiores del país, Consejos universitarios, Comités Regionales Consultivos de Planificación de la Educación Superior).
- ✓ Estudiantes y egresados que deberán rendir las pruebas de habilitación del ejercicio profesional.
- ✓ Consejo de Educación Superior – CES –, Secretaría de Educación Superior, Ciencia, Tecnología e Innovación – SENESCYT –, Asamblea Nacional, Presidencia de la República, Ciudadanía en general, Organizaciones Internacionales (agencias, redes, organismos públicos y privados internacionales).

3.4. DIRECCIONAMIENTO ESTRATÉGICO

3.4.1. MISIÓN

Regular, coordinar y planificar los procesos participativos de acompañamiento, evaluación, acreditación y cualificación para garantizar el desarrollo de una cultura de la calidad en las instituciones de educación superior, enfocada en el equilibrio de la docencia, la investigación e innovación y la vinculación con la sociedad.

3.4.2. VISIÓN

Al 2030, el Consejo de Aseguramiento de la Calidad de la Educación Superior –CACES –, será un organismo público referente a nivel nacional y regional en la innovación y promoción de la construcción colectiva de la cultura de la calidad en las IES, institucionalizando procesos de garantía de la calidad de la Educación Superior.

3.4.3. OBJETIVOS ESTRATÉGICOS

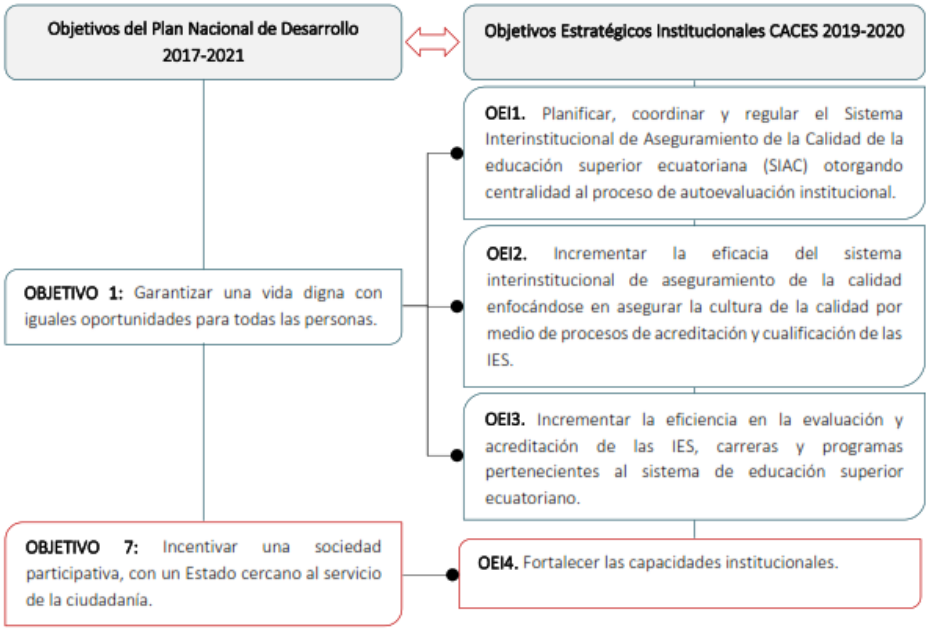

Ilustración 6. Alineación de los Objetivos Estratégicos Institucionales a los objetivos del Plan Nacional de Desarrollo

3.4.4. CADENA DE VALOR

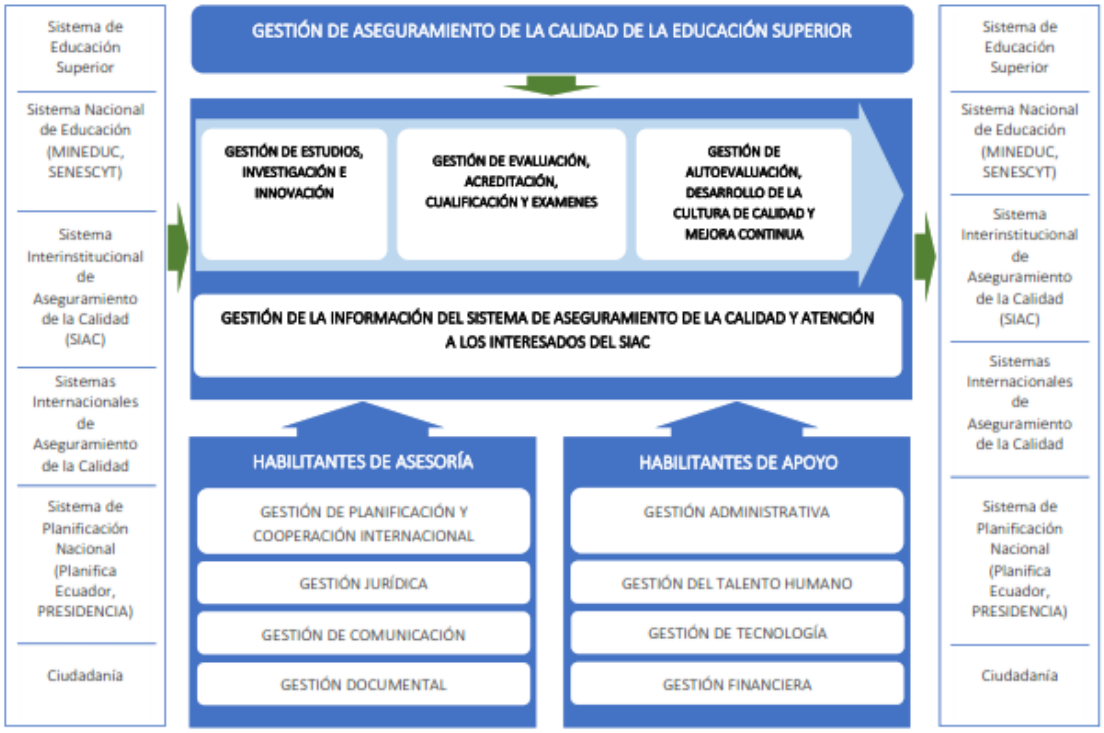

Ilustración 7. Cadena de Valor del Consejo de Aseguramiento de la Calidad de la Educación Superior

3.4.5. MAPA DE PROCESOS

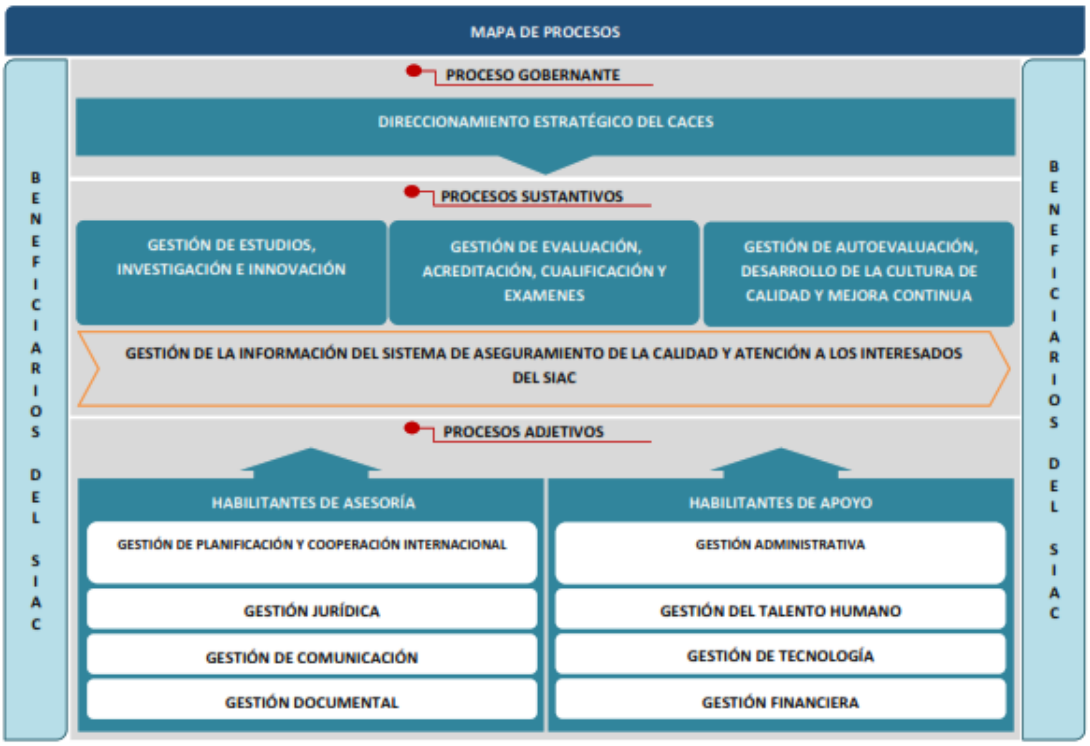

Ilustración 8. Mapa de Procesos del Consejo de Aseguramiento de la Calidad de la Educación Superior

3.4.6. MAPA ESTRATÉGICO

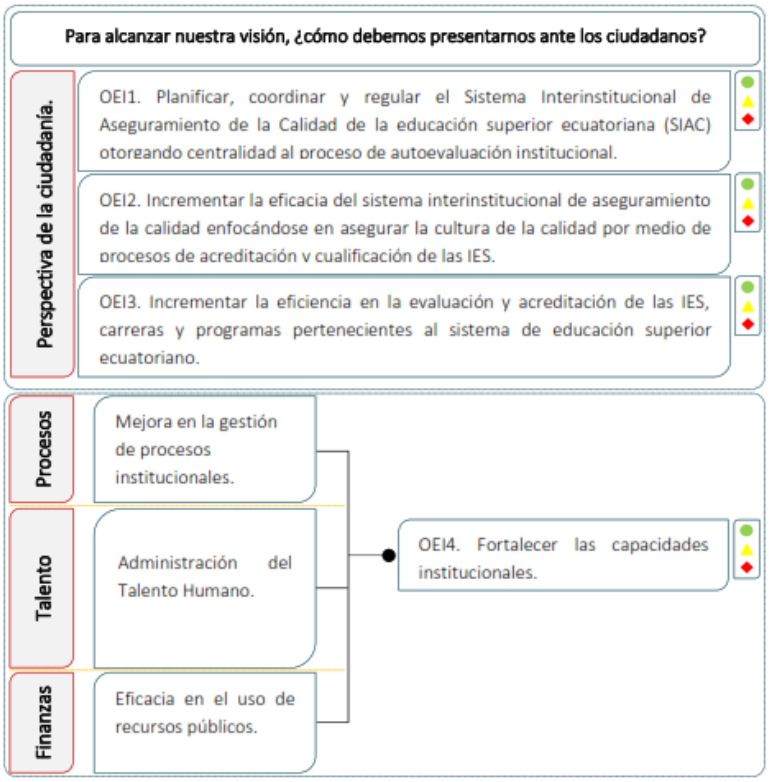

Ilustración 9. Mapa Estratégico del Consejo de Aseguramiento de la Calidad de la Educación Superior

3.4.7. POLÍTICAS PARA EL SISTEMA DE GESTIÓN DE LA CALIDAD INTERNA

El alcance del Sistema de Gestión de la Calidad del Consejo de Aseguramiento de la Calidad de la Educación Superior corresponde a todos los procesos directamente relacionados con los servicios en operación. Se fundamenta en las mejores prácticas y normas técnicas nacionales e internacionales generalmente aceptadas priorizadas por la máxima autoridad de la Institución, excluyendo conceptos que no sean aplicables de acuerdo con la naturaleza de la Institución (pública), sus procesos y reglamentos internos. Su objetivo es aumentar la satisfacción de las necesidades y expectativas de los usuarios, cumplir con la legislación vigente aplicable y normativa relacionada.

3.4.7.1. POLÍTICA DE CALIDAD

El Consejo de Aseguramiento de la Calidad de la Educación Superior, como institución reguladora, planificadora y coordinadora del Sistema Interinstitucional de Aseguramiento de la Calidad de la educación superior, está comprometido en generar procesos transparentes, articulados y eficientes que guíen los sistemas internos y promuevan la cultura de calidad en las IES. En este marco, el propósito fundamental es la certificación objetiva y transparente del cumplimiento de criterios y estándares de calidad establecidos participativamente con las IES para la ejecución efectiva de procesos de evaluación externa, acreditación de la calidad, cualificación académica y habilitación profesional.

3.4.7.2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Es responsabilidad del Consejo de Aseguramiento de la Calidad de la Educación Superior, y compromiso con la ciudadanía, garantizar la legitimidad, objetividad, imparcialidad y transparencia de los procesos de aseguramiento de la calidad de la educación superior, mediante la adopción de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001, que permita minimizar los riesgos y prevenir eventos e incidentes de seguridad que atenten contra la integridad, disponibilidad y confidencialidad de la información interna y externa usada para el cumplimiento de los objetivos de la Institución.

3.5. INFRAESTRUCTURA TECNOLÓGICA

El Esquema Gubernamental de Seguridad de la Información (EGSI), establece un conjunto de directrices prioritarias para la gestión de la seguridad de la información e inicia un proceso de mejora continua en las instituciones de la administración pública. Las entidades que generan utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el EGSI para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera.

La arquitectura tecnológica actual del Consejo de Aseguramiento de la Calidad de la Educación Superior está apoyada en dos pilares fundamentales, por medio de los cuales es posible el acceso, la integración y despliegue de los servicios tecnológicos de la información y comunicaciones:

3.5.1. PROCESAMIENTO Y ALMACENAMIENTO

Comprende toda la infraestructura ligada a servidores físicos, servidores virtuales y almacenamiento. Al momento la Unidad de Tecnologías de la Información no cuenta con infraestructura de almacenamiento y procesamiento local en la Institución. La infraestructura con la cual se cuenta se encuentra bajo la modalidad IaaS, como servicio contratado con la Corporación Nacional de Telecomunicaciones.

3.5.2. RED

Comprende toda la infraestructura que permite la interconectividad de los diferentes sistemas dentro y fuera de las instalaciones. Esta arquitectura está soportada por los equipos de red cableada, red inalámbrica y los sistemas de monitoreo y gestión de red. Adicionalmente, cuenta con el servicio de red gubernamental, Internet de banda ancha y seguridad perimetral. La arquitectura tecnológica es la base fundamental que soporta las arquitecturas de aplicaciones, datos, procesos y gobierno electrónico.

La infraestructura de red es el conjunto de elementos que se utilizan para el intercambio de información y el envío de datos de un lugar a otro. La infraestructura de red del Consejo de Aseguramiento de la Calidad de la Educación Superior está compuesta de cableado estructurado, equipos de red, equipos inalámbricos, equipos de seguridad informática, servidores y conexiones de internet.

El Consejo de Aseguramiento de la Calidad de la Educación Superior dispone de 346 puntos de red que cubren el 100% de las instalaciones físicas y dispone de una red basada en capas o niveles que se detallan a continuación:

a) **Capa de Core:** Los equipos de esta capa concentran todo el tráfico del CACES y permiten que el tráfico del usuario circule a toda la capacidad de la red. Los equipos implementados en esta capa son de la marca Allied Telesys.
b) **Capa de Distribución:** Permite que los usuarios del CACES tengan un acceso libre de tráfico no requerido. Esto se realiza a través de un control en el tráfico que circula por el CACES. Los equipos implementados en esta capa son de la marca Allied Telesys.
c) **Capa de Acceso:** Permite a los usuarios finales acceder a los servicios del CACES basados en una clasificación de tráfico por tipo de usuario. Esta clasificación es:
   - ✓ Autoridades.
   - ✓ Funcionarios.
   - ✓ Invitados.

Estas 3 capas forman la infraestructura de red Cableada que es el sustento de todos los servicios Institucionales hasta la fecha (Internet, GIIES, Red Inalámbrica, Correo electrónico Institucional, Web Institucional, Repositorio Institucional, etc.).

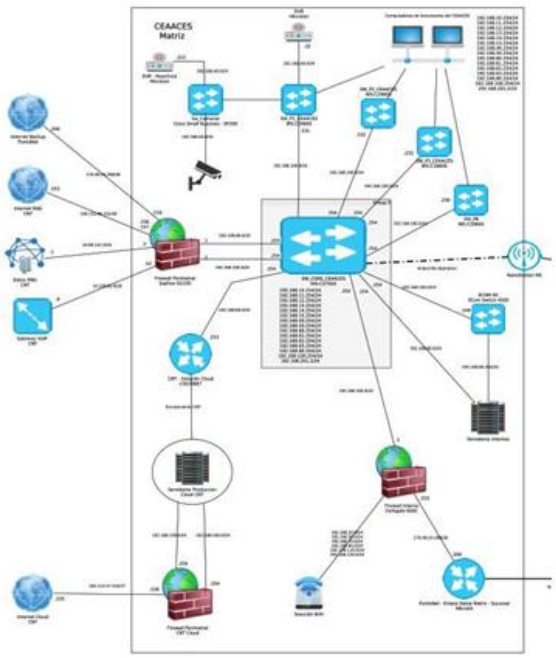

Ilustración 10. Diagrama de topología de red del Consejo de Aseguramiento de la Calidad de la Educación Superior

La infraestructura de red del Consejo de Aseguramiento de la Calidad de la Educación Superior además cuenta con equipos de seguridad y equipos de red inalámbrica.

a) **Equipos de seguridad:** Son equipos que brindan seguridad a nivel de red, desde el medio externo (Internet) hacia el CACES y viceversa.
b) **Equipos de red inalámbrica:** Los equipos inalámbricos (Access Point) permiten la conexión de dispositivos móviles como laptops, celulares inteligentes, tabletas, etc. del usuario final hacia la infraestructura de la Institución mediante conexiones inalámbricas.

Adicionalmente, cuenta con el servicio de red gubernamental, Internet de banda ancha y seguridad perimetral. La infraestructura tecnológica es la base fundamental que soporta las arquitecturas de aplicaciones, datos, procesos y finalmente gobierno electrónico.

3.5.3. APLICACIONES Y SISTEMAS

Actualmente, existen en producción dos versiones del sistema GIIES, cada uno con su respectiva arquitectura, las cuales se detallan a continuación:

- Arquitectura No. 1: La arquitectura consta de dos servidores, uno con el servidor de aplicaciones Tomcat, donde se despliegan los componentes web .war; y el segundo servidor contiene dos servidores de aplicaciones Jboss, donde se despliegan los componentes con la lógica del negocio .jar y estos a su vez, se comunican con el servidor de base de datos.

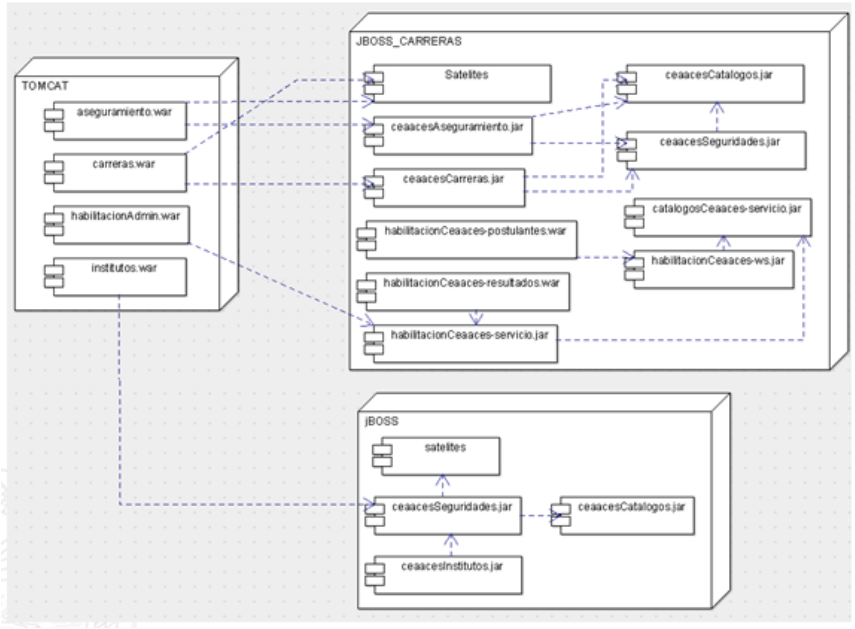

Ilustración 11. Diagrama No. 1 de arquitectura de sistemas del Consejo de Aseguramiento de la Calidad de la Educación Superior

- Arquitectura No. 2: La arquitectura está compuesta por un servidor de aplicaciones Wildfly, donde se despliegan los componentes web. war y la lógica del negocio .jar, dicho servidor se comunica con el servidor de base de datos.

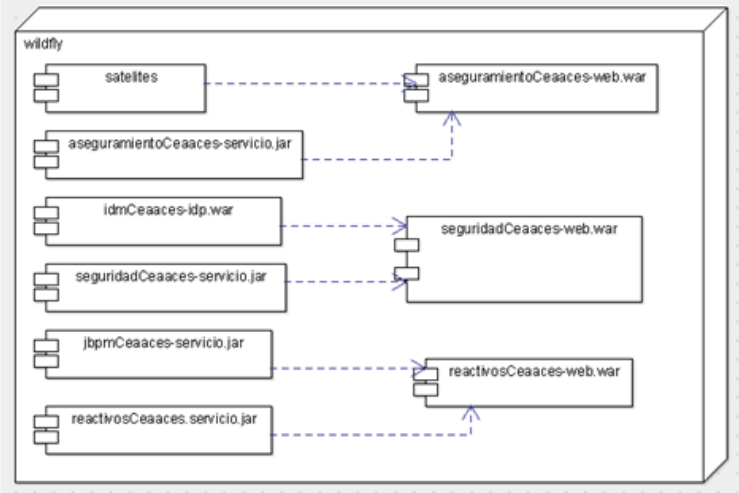

Ilustración 12. Diagrama No. 2 de arquitectura de sistemas del Consejo de Aseguramiento de la Calidad de la Educación Superior

- Arquitectura No. 3: La arquitectura está compuesta por un servidor de aplicaciones Apache, donde se despliegan los componentes web y los microservicios, dicho servidor se comunica con el servidor de base de datos.

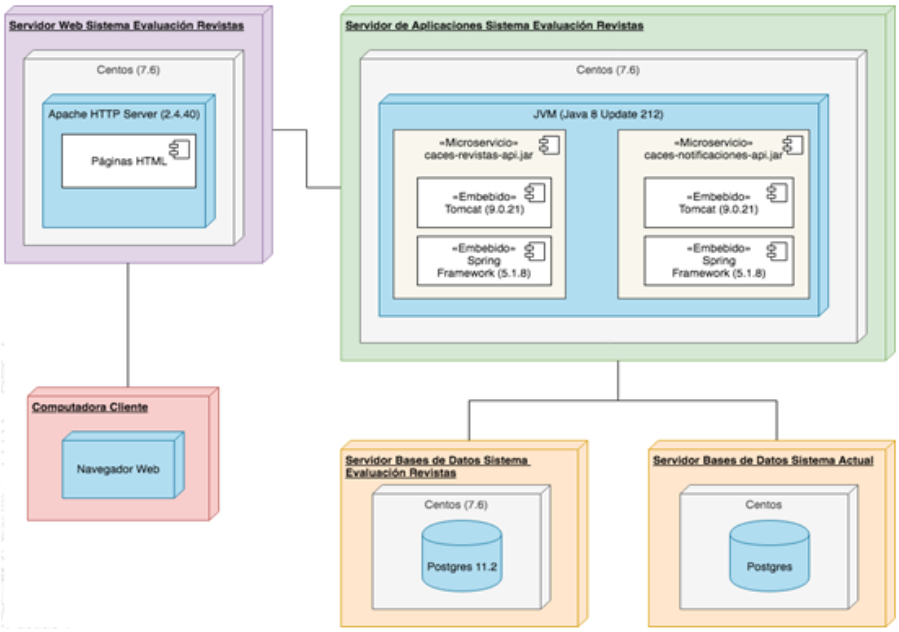

Ilustración 13. Diagrama No. 3 de arquitectura de sistemas del Consejo de Aseguramiento de la Calidad de la Educación Superior

En función de la información proporcionada en las ilustraciones anteriores debe indicarse que la Unidad de Tecnologías de la Información del Consejo de Aseguramiento de la Calidad de la Educación Superior es custodia de la información existente, así como la generadora de cambios en virtud de los requerimientos funcionales que cada una de las áreas requirentes de la Institución solicite en función de los procesos institucionales que se estén llevando a cabo.

La administración funcional de los sistemas informáticos corresponde a cada una de las unidades administrativas y son estas las instancias generadoras de cambios a las aplicaciones existentes o de nuevas aplicaciones informáticas según las necesidades propias de cada una.

En la actualidad el Consejo de Aseguramiento de la Calidad de la Educación Superior se

encuentra en un proceso de rediseño de la gestión y arquitectura tecnológica en respuesta a las vulnerabilidades identificadas y para robustecer los procesos agregadores de valor (Evaluación Institucional y Examen de Habilitación para el Ejercicio Profesional en línea).

3.6. NIVEL DE MADUREZ INSTITUCIONAL EN CUANTO A LA SEGURIDAD DE LA INFORMACIÓN

Con fecha 19 de septiembre de 2013 se emitió el Acuerdo Ministerial No. 166, publicado en el Registro Oficial No. 88 del 25 de septiembre de 2013, el cual dispone la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en todas las entidades de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva (APCID).

En este sentido se ha realizado una breve evaluación del EGSI en base al cumplimiento de la implementación y al tiempo en el que se ha implementado el mismo. La evaluación refiere a la documentación, implementación y los verificables que evidencien que la implementación del EGSI se mantiene de manera eficaz, eficiente y efectiva con el objetivo de asegurar la información crítica de la entidad además de estar en conformidad con los requisitos de la familia de normas ISO/IEC 27000, legales y los del EGSI establecidos en el acuerdo 166.
Se ha constatado el estado de la implementación del Esquema Gubernamental de Seguridad de la Información – EGSI – para lo cual se seleccionaron 30 controles de acuerdo con los hitos planteados por la institución, los mismos que fueron definidos aleatoriamente.

La calificación de los controles se basó en tres parámetros los cuales se mencionan a continuación:

a) **Documentación:** Normas, políticas, procedimientos, etc., formalmente establecidos.
b) **Implementación:** La aplicación de lo establecido en la documentación.
c) **Verificables:** Informes, diagramas de red, reportes, correos electrónicos, etc.

3.6.1. ELEMENTOS DE CONTROL INTERNO EVALUADOS

Se ha evaluado la capacidad que el Consejo de Aseguramiento de la Calidad de la Educación Superior ha tenido en la implementación del Esquema Gubernamental de Seguridad de la Información para de esta forma poder asegurar el cumplimiento de los requisitos establecidos en la norma.

No.	HITO	PROCESO Y/O ACTIVIDAD
1	2.5.1	Elaborar y aprobar los acuerdos de confidencialidad y de no divulgación de información conforme la Constitución, las leyes, las necesidades de protección de información de la institución y el EGSI.
2	3.1.3.2	Software de servicio, mantenimiento o administración de: gabinetes de servidores de cuchilla, servidores (estantería/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento (NAS, SAN), telefonía, sistemas (de UPS, grupo electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), etc.
3	3.3.2	Reglamentar el acceso y uso de la Internet y sus aplicaciones/servicios.
4	5.5.1	Código de uso equipos de grabación, cámaras, equipos de vídeo y audio, dispositivos móviles, etc., implementado.
5	4.4.1	Explicar y definir las funciones y las responsabilidades respecto a la seguridad de la información, antes de otorgar el acceso a la información, contraseñas o sistemas de información sensibles.
6	5.8.1	Tener un sistema de suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios y equipos que soportan las operaciones críticas de los servicios informáticos de la institución.

No.	HITO	PROCESO Y/O ACTIVIDAD
7	5.9.1	Disponer de documentación, diseños/planos y la distribución de conexiones de: datos alámbricos/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc.
8	6.6.3	Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado.
9	6.12.1	Los responsables del área de Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos para el resguardo y contención de la información.
10	6.12.3	Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo con los requisitos del negocio de la institución.
11	6.30.1	Revisar los registros de fallas o errores del sistema.
12	7.4.1	Establecer un proceso formal para la asignación y cambio de contraseñas.
13	7.16.1	Usuarios autorizados autenticados, de acuerdo con la política de control de acceso de la institución, que deberá estar documentada, definida y socializada.
14	7.17.1	Rastrear utilizando los identificadores de usuario y evidenciar las actividades de las personas responsables de administraciones críticas de la institución.
15	9.1.1	Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.
16	2.2.1.3	Definir y mantener la política y normas institucionales particulares en materia de seguridad de la información y gestionar la aprobación y puesta en vigencia por parte de la máxima autoridad de la institución, así como el cumplimiento por parte de los funcionarios de la institución.
17	2.2.1.4	Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
18	2.2.1.8	Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.
19	2.2.1.9	Promover la difusión y apoyo a la seguridad de la información dentro de la institución.
20	4.5.1	Socializar y capacitar de forma periódica y oportuna sobre las normas y los procedimientos para la seguridad, las responsabilidades legales y los controles de la institución, así como en la capacitación del uso correcto de los servicios de información.
21	5.1.2	Definir y documentar claramente los perímetros de seguridad (barreras, paredes, puertas de acceso controladas con tarjeta, etc.), con una ubicación y fortaleza adecuadas.
22	5.1.5	Disponer de un sistema de vigilancia mediante el uso de circuitos cerrados de televisión.
23	9.1.3	Establecer un punto de contacto (Oficial de Seguridad de la Información) para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto sea conocido en toda la institución, siempre esté disponible y puede suministrar respuesta oportuna y adecuada.

No.	HITO	PROCESO Y/O ACTIVIDAD
24	9.2.2.1	Cuando un empleado, contratista o usuario contratado por un proveedor detecte una vulnerabilidad o debilidad en un equipo, sistema o servicio deberá ejecutar las siguientes acciones: ✓ Notificar a su jefe inmediato y este al Oficial de Seguridad de la Información de la debilidad o vulnerabilidad detectada.
25	9.2.2.2	Registrar la fecha, hora, apellidos y nombres del funcionario que detectó la debilidad o vulnerabilidad, descripción de la debilidad, descripción de posibles incidentes de seguridad que pudieran ocurrir producto de esta debilidad. El responsable de llevar este reporte denominado "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el Oficial de Seguridad de la Información.
26	9.3.1	Además de la bitácora de registro de incidentes y el reporte de vulnerabilidades de la seguridad de la información, el monitoreo de los sistemas, las alertas y las vulnerabilidades, se debería establecer y ejecutar un procedimiento para la gestión de incidentes.
27	9.3.4	Planificar e implementar acciones correctivas para evitar la recurrencia del incidente.
28	9.3.6	El Oficial de Seguridad de la Información, emitirá un reporte a los jefes de las áreas afectadas por el incidente.
29	9.4.1	La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debe utilizar para identificar los incidentes recurrentes o de alto impacto.
30	9.4.2	Determinar el número de incidentes por tipo, el número de incidentes graves, el tiempo medio de resolución de incidentes.

Tabla 1. Elementos de control evaluados en el Consejo de Aseguramiento de la Calidad de la Educación Superior

3.6.2. HALLAZGOS

3.6.2.1. HALLAZGOS DE EVALUACIÓN AL PERSONAL

De la prueba realizada a los funcionarios del Consejo de Aseguramiento de la Calidad de la Educación Superior, se pudo obtener los siguientes resultados:

- ✓ A nivel de conocimiento de la Política de Seguridad de la Información, el 61,84% de los funcionarios no conocen de la misma, por lo cual se recomienda realizar socializaciones para mantener informado al personal.
- ✓ Existe un porcentaje del 72,37% de los funcionarios que aún no tiene conocimiento de que se trata el Esquema Gubernamental de Seguridad de la Información (EGSI) y cuál es su alcance, es necesario difundir comunicados a fin de concientizar la obligatoriedad del cumplimiento de la implementación del EGSI en todas las instituciones de la APCID.
- ✓ Es recomendable que los funcionarios públicos que laboran en una institución conozcan el mapa de procesos de su institución, el 56.58% de los funcionarios que respondieron la encuesta expresó no tener conocimiento de este, además de no existir información al respecto.
- ✓ Un porcentaje del 65,79% de los funcionarios afirmó que no recibe información acerca de la importancia de la Seguridad de la Información dentro de la Institución. Se debe mantener la emisión permanente de correos informativos respecto a la seguridad de la información, brindar charlas informativas, campañas de concientización y demás.

- ✓ El proceso de notificar incidentes de seguridad para el 48,68% de los funcionarios aún no está claro o no lo conocen, por lo que se recomienda socializar de manera permanente.
- ✓ Un porcentaje del 68,42% de los funcionarios no conocen al Oficial de Seguridad y sus funciones, mediante un plan de difusión informar el nombre del Oficial de Seguridad con una fotografía, indicando sus funciones, resaltando la importancia de esta figura dentro de la institución.
- ✓ Existe un 64,47% de funcionarios que aún no tiene claro el nivel de seguridad que con el que se debe manejar la información entregada, es importante que cada funcionario esté consciente de la criticidad de la información que opera cada área.
- ✓ El 78,95% de los funcionarios no conocen dónde encontrar la política, procedimientos o normas de la institución, es imprescindible almacenar la información en un repositorio digital de fácil acceso, se deberá difundir la ubicación exacta para que sea de conocimiento y uso frecuente.

3.6.2.2. HALLAZGOS DE LOS CONTROLES

HITO	DESCRIPCIÓN	HALLAZGO	RECOMENDACIÓN
3.1.3.2	Software de servicio, mantenimiento o administración de: gabinetes de servidores de cuchilla, servidores (estantería/rack, torre, virtuales), sistema de redes de datos, sistemas de almacenamiento (NAS, SAN), telefonía, sistemas (de UPS, grupo electrógeno, de aire acondicionado, automático de extinción de incendios, de circuito cerrado de televisión), etc.	El inventario proporcionado por la Unidad de Tecnologías de la Información no concuerda con lo que físicamente tiene la institución.	Mantener actualizado el o los inventarios.
5.8.1	Tener un sistema de suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios y equipos que soportan las operaciones críticas de los servicios informáticos de la institución.	Se cuenta con un UPS de 6 KVA, no muestran evidencias del último mantenimiento realizado.	Realizar mantenimientos del UPS o al menos contar con un instructivo en donde se indique que servicios se prenden o se apagan en orden cronológico.
5.9.1	Disponer de documentación, diseños/planos y la distribución de conexiones de: datos alámbricos/inalámbricas (locales y remotas), voz, eléctricas polarizadas, etc.	No se tiene disponible el registro de los diseños/planos de los puntos eléctricos, voz, datos. Edificios arrendados. En el informe de cumplimiento mencionan la elaboración de un procedimiento que no se lo ejecutó.	Elaborar los diseños o planos de lo solicitado en el hito.
6.6.3	Revisar y verificar los registros y pruebas de auditoría de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionados con el servicio prestado.	Se realizó 2 auditorías con Telconet y la Escuela Politécnica Nacional, en la cual se evidenció el nivel de madurez en seguridad de la información en la institución basados en la norma ISO/IEC 27000. Se generó recomendaciones, las cuales se procedió a la implementación de varias de ellas. A partir de la fecha de realización de las auditorías la institución no ha realizado intervenciones.	Al menos anualmente se deben realizar este tipo de auditorías. Si no hay el presupuesto se puede solicitar a la Secretaría Nacional de Inteligencia.
6.12.1	Los responsables del área de	Se tiene la política actualizada en	El hito indica que la información que se

HITO	DESCRIPCIÓN	HALLAZGO	RECOMENDACIÓN
	Tecnologías de la Información, Oficial de Seguridad de la Información junto con el propietario de la información, determinarán los procedimientos para el resguardo y contención de la información.	donde se menciona el procedimiento de respaldos, coordinando con la unidad de negocio y tecnologías de la información, pero no mencionan al oficial de seguridad de la información. La bitácora de respaldos no concuerda con lo que menciona la política.	va a respaldar debe estar en conocimiento de los tres entes, Jefe de Unidad de Gestión Tecnológica, dueño de la información y oficial de seguridad de la información, en base a esto se debe realizar este hito.
6.12.3	Definir la extensión (completo/diferencial) y la frecuencia de los respaldos, de acuerdo con los requisitos del negocio de la institución.	Se tiene la política actualizada en donde se menciona el procedimiento de respaldos, coordinando con la unidad de negocio y tecnologías de la información, pero no mencionan al oficial de seguridad de la información. La bitácora de respaldos no concuerda con lo que menciona la política.	Contar con bitácoras de los registros que efectivamente se está sacando el respaldo.
6.30.1	Revisar los registros de fallas o errores del sistema.	Se lo realiza a través del sistema MANTIS para la validación y corrección de errores de funcionalidad del aplicativo GIIES y SIIES.	No se pudo evidenciar los registros de las fallas o errores recurrentes o que han ocurrido.
7.16.1	Usuarios autorizados autenticados, de acuerdo con la política de control de acceso de la institución, que deberá estar documentada, definida y socializada.	Se cuentan con un "Manual para el Proceso de Gestión de Acceso la Red " en el cual se menciona *"(…) La implementación de este control lo realiza a través del Active Directory y el acceso a Internet a través del Firewall Palo Alto"*. De igual manera se maneja un formato de "Solicitud de Creación de Usuarios", que utilizan las Instituciones de Educación Superior para requerir acceso a los sistemas informáticos institucionales.	Actualizar y socializar la política.
7.17.1	Rastrear utilizando los identificadores de usuario y evidenciar las actividades de las personas responsables de administraciones críticas de la institución.	Se lo realizan bajo demanda, a través de la base de datos (logs), no se cuenta con un módulo de auditoría en el sistema GIIES.	Establecer directrices periódicas en la que se revise las actividades que realizan los administradores de la información crítica de la institución. Si la institución cuenta con software desarrollado debería contar con un módulo de auditoría.
9.1.1	Instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información.	Se cuenta con un "Procedimiento para la Gestión de Incidentes" elaborado que no está actualizado. Formalmente no se ha difundido por lo que no se está implementando, siguiendo el debido proceso, al contrario, lo realizan como buenas prácticas.	Difundir y actualizar el procedimiento, que esté al alcance de todos los usuarios y saber qué acciones se debe tomar en caso de suscitarse un incidente de seguridad
2.2.1.3	Definir y mantener la política y normas institucionales particulares en materia de seguridad de la información y gestionar la aprobación y puesta en vigencia por parte de la máxima autoridad de la institución, así como el	Se emitió la RESOLUCIÓN No. 081-P-CEAACES-2014. No se ha socializado, las evidencias de capacitación en cuanto al contenido de la Resolución se lo realizaban en las inducciones.	Socializar periódicamente.

HITO	DESCRIPCIÓN	HALLAZGO	RECOMENDACIÓN
	cumplimiento por parte de los funcionarios de la institución.		
2.2.1.4	Monitorear cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.	El monitoreo se lo ha venido realizando a través de una "Evaluación y Plan de Tratamiento del Riesgo".	Realizar esta actividad periódicamente.
2.2.1.8	Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.	Elaboración de Banco de Preguntas en el GIIES, existe recomendaciones para este servicio. El proceso "Elaboración de Exámenes" se encuentra en etapa de evaluación y aprobación.	Continuar con esta buena práctica e implementar los controles necesarios para seguridad.
4.5.1	Socializar y capacitar de forma periódica y oportuna sobre las normas y los procedimientos para la seguridad, las responsabilidades legales y los controles de la institución, así como en la capacitación del uso correcto de los servicios de información.	Se cuenta con el material y fotografías con reportes de asistencia a capacitaciones. En la actualidad ya no se realizan las inducciones relacionadas con seguridad de la información.	Actualmente no se cumple con el hito. Se deben tomar acciones para el cumplimiento de este hito.
5.1.2	Definir y documentar claramente los perímetros de seguridad (barreras, paredes, puertas de acceso controladas con tarjeta, etc.), con una ubicación y fortaleza adecuadas.	Se definió los perímetros de seguridad, se tiene implementado accesos a través de biométricos, guardias en el acceso principal, sensores de movimiento nocturno en el perímetro de las instalaciones.	Elaborar el documento de cómo se encuentra la institución en la actualidad que sea la evidencia de que lo están implementando de acuerdo con la documentación.
5.1.5	Disponer de un sistema de vigilancia mediante el uso de circuitos cerrados de televisión.	Se cuenta con circuito cerrado que es monitoreado por los guardias y los respaldos de las grabaciones son ejecutados por la Unidad de Tecnologías de la Información con una petición formal.	No hay documentación de cómo está ubicado el sistema de vigilancia y como se está monitoreando la cual debe ser elaborada.
9.1.3	Establecer un punto de contacto (Oficial de Seguridad de la Información) para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto sea conocido en toda la institución, siempre esté disponible y puede suministrar respuesta oportuna y adecuada.	No se ha socializado el "Informe de Incidente de Seguridad".	Socializar con los funcionarios el punto de contacto para el reporte de eventos de seguridad, esta socialización debe ser constante.
9.2.2.1	Cuando un empleado, contratista o usuario contratado por un proveedor detecte una vulnerabilidad o debilidad en un equipo, sistema o servicio deberá ejecutar las siguientes acciones: ✓ Notificar a su jefe inmediato y este al Oficial de Seguridad de la Información de la debilidad o vulnerabilidad detectada.	No se dispone de documentación para el cumplimiento de este hito.	Levantar la documentación de cómo será la notificación y socializar con los proveedores, usuarios y funcionarios.
9.2.2.2	Registrar la fecha, hora, apellidos y nombres del funcionario que detectó la	No se dispone de documentación para el cumplimiento de este hito.	Levantar el reporte en donde se contemple los datos solicitados en el

HITO	DESCRIPCIÓN	HALLAZGO	RECOMENDACIÓN
	debilidad o vulnerabilidad, descripción de la debilidad, descripción de posibles incidentes de seguridad que pudieran ocurrir producto de esta debilidad. El responsable de llevar este reporte denominado "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el Oficial de Seguridad de la Información.		hito como hora, fecha, apellidos, etc. Incluir quien es el responsable.
9.3.1	Además de la bitácora de registro de incidentes y el reporte de vulnerabilidades de la seguridad de la información, el monitoreo de los sistemas, las alertas y las vulnerabilidades, se debería establecer y ejecutar un procedimiento para la gestión de incidentes.	Se cuenta con el procedimiento y el formato de la bitácora de gestión de incidentes y no se está ejecutando.	Levantar el procedimiento en donde se incluya el monitoreo y alertas, socializar, aprobarlo y ejecutarlo.
9.3.4	Planificar e implementar acciones correctivas para evitar la recurrencia del incidente.	Se cuenta con el procedimiento y el formato de la bitácora de gestión de incidentes y no se está ejecutando.	Socializar constantemente, no sirve de nada si solo se tiene plasmado en un documento y no se lo socializa.
9.3.6	El Oficial de Seguridad de la Información, emitirá un reporte a los jefes de las áreas afectadas por el incidente.	El Oficial de Seguridad de la Información en su momento emitió el reporte "Informe de Incidentes Pishing – Correo Electrónico".	Es una buena práctica la que se estaba realizando, pero recordar que esto se debe hacer constantemente.
9.4.1	La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debe utilizar para identificar los incidentes recurrentes o de alto impacto.	Se cuenta con un "Procedimiento para la Gestión de Incidentes" elaborado que no está actualizado. Formalmente no se ha difundido y tampoco se está implementando.	No lo están implementando, se debe socializar con el área respectiva, esto permitirá realizar una base de conocimiento.
9.4.2	Determinar el número de incidentes por tipo, el número de incidentes graves, el tiempo medio de resolución de incidentes.	Se cuenta con un "Procedimiento para la Gestión de Incidentes" elaborado que no está actualizado. Formalmente no se ha difundido y tampoco se está implementando.	No lo están implementando, se recomienda clasificar los incidentes por tipo tal como se indica en el hito.

Tabla 2. Hallazgos sobre los controles aleatorios realizados en el Consejo de Aseguramiento de la Calidad de la Educación Superior

3.6.3. RESULTADO OBTENIDO

Una vez realizada la evaluación y de acuerdo con la ponderación establecida por la metodología de evaluación, el Consejo de Aseguramiento de la Calidad de la Educación Superior, sobre los controles que fueron seleccionados aleatoriamente, ha alcanzado una ponderación del 62,17% que corresponde a "Regular" por lo que como acciones inmediatas se han emitido las observaciones y hallazgos a la implementación de tal forma que puedan ser corregidas.

3.6.4. RECOMENDACIONES A LA EVALUACIÓN REALIZADA

- ✓ Es indispensable y obligatorio cumplir con el Acuerdo Ministerial 166 en la que se indica en el artículo 3 que la institución debe contar con un Oficial de Seguridad de la Información el cual se encargara de velar el cumplimiento y seguimiento de la implementación, el oficial debe recibir el apoyo de la máxima autoridad y de todas las

áreas de la institución en la correcta implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información EGSI.

- ✓ La institución debería dar estabilidad al Oficial de Seguridad de la Información con el fin de que no exista periodos en los que la institución no muestre evidencia de que no se realizó nada en cumplimiento al Esquema Gubernamental de Seguridad de la Información, particularmente en el Consejo de Aseguramiento de la Calidad de la Educación Superior no habido continuidad con el puesto del Oficial de Seguridad de la Información y por tanto existen periodos en los que no se realizaron gestiones para velar por la buena implementación del EGSI.
- ✓ Emprender una campaña de difusión tanto de las políticas de seguridad como del Esquema Gubernamental de Seguridad de la Información a todos los funcionarios del Consejo de Aseguramiento de la Calidad de la Educación Superior, con el objetivo de mantener la concientización de la importancia de la seguridad de la información dentro de la institución.
- ✓ Planificar charlas de concientización orientada a la seguridad de la información a las distintas áreas para que formen parte de la implementación del Esquema Gubernamental de Seguridad de la Información en la institución y faciliten recursos e información durante todo el proceso.
- ✓ Generar boletines sobre seguridad de la información en los cuales se detalle información referente a buenas prácticas de seguridad de la información, además de nuevos ataques informáticos o noticias de seguridad, con el fin de promover el interés en la seguridad de la información en los funcionarios y así prevenir posibles riesgos asociados al personal.
- ✓ Socializar el mapa de procesos de la institución y los procesos críticos a todos los funcionarios.
- ✓ Difundir y socializar la ubicación del repositorio en donde se encuentran almacenadas las políticas, procedimientos, normas, etc., para que los funcionarios tengan fácil y libre acceso a esta fuente de información.
- ✓ Evaluar los hitos implementados y que formaron parte de la evaluación bajo el mismo esquema que se realizó con los 30 hitos evaluados para este Trabajo de Fin de Máster, a fin de identificar e ir corrigiendo errores en la implementación del Esquema Gubernamental de Seguridad de la Información.

CAPÍTULO IV: PROPUESTA DE IMPLANTACIÓN

Un Centro de Operaciones de Seguridad (SOC) consiste en una plataforma integral que tiene el propósito de diseñar, implementar y ejecutar procesos de detección y reacción ante posibles incidentes de seguridad en las organizaciones, durante las 24 horas del día, los 7 días de la semana, los 365 días del año. Un Centro de Operaciones de Seguridad (SOC) controla de forma constante el estado de la seguridad lógica de una organización, mediante el monitoreo en tiempo real de las actividades que se realizan en los recursos tecnológicos de la misma, para evitar que las amenazas externas puedan acceder fácilmente a la red interna de la organización.

4.1. DEFINICIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Cuando nos referimos a un Centro de Operaciones de Seguridad (SOC) hacemos alusión a "un término genérico que describe ya sea una parte o el todo de una plataforma que tiene el propósito de proveer servicios de detección y de reacción a incidentes de seguridad" (Bidou, 2002).

Los Centros de Operaciones de Seguridad (SOC) proporcionan la información necesaria para que la organización se encuentre en capacidad de detectar de manera eficiente las posibles brechas de seguridad para que posteriormente puedan ser mitigadas mediante la implementación de controles, de esta manera se pueda reducir los tiempos de respuesta ante esta clase de eventos (Alien Vault, 2015).

La implementación y operación de un Centro de Operaciones de Seguridad (SOC) sin duda alguna trae beneficios a las organizaciones entre los cuales podemos mencionar:

a) **Preparación ante incidentes de seguridad:** Si una organización opera un Centro de Operaciones de Seguridad (SOC) se traslada de una postura reactiva a una de preparación, a través de un proceso bien establecido que permita un movimiento rápido y efectivo para aislar, contener y mitigar las amenazas.
b) **Reducción de riesgos para los clientes:** Un Centro de Operaciones de Seguridad (SOC) permite proteger de manera más efectiva el tráfico de información de los clientes y evitar su pérdida o manipulación, controlando mejor los servicios de seguridad.
c) **Mejora en la respuesta de seguridad:** Al mantener en operación un Centro de Operaciones de Seguridad (SOC) la organización puede contar con niveles de escalamiento a seguir, que de forma sistemática permiten analizar las razones potenciales de la anomalía en el tráfico y resolver los incidentes de manera apropiada. Con una capacidad de respuesta rápida y oportuna, se puede afrontar los incidentes de seguridad en corto tiempo, con lo cual se puede eliminar problemas potenciales en servicios críticos y procesos de negocio.
d) **Incremento de la eficiencia operacional:** Si se tienen claramente definidas reglas de seguridad y políticas, los especialistas del Centro de Operaciones de Seguridad (SOC) estarán en capacidad de identificar amenazas rápidamente y de esta forma aplicar remedios a sitios en riesgo antes de que las amenazas los alcancen.
e) **Reducción de costos:** Un Centro de Operaciones de Seguridad (SOC) tiene su razón de ser en las tecnologías, herramientas y procedimientos de seguridad, por lo que a raíz de su implementación se puede emplear de manera más eficiente a los especialistas de seguridad de tecnologías de la información sin que se vea comprometida la calidad de los entregables del SOC ya que la organización ahora se basará en los procesos y la tecnología para llevar a cabo que antes lo realizaban los expertos de seguridad.
f) **Asistencia a clientes para cumplir con regulaciones:** De manera frecuente tanto las organizaciones como sus clientes se encuentran en la obligación de cumplir con regulaciones y políticas sobre el uso, protección y privacidad de la información. En este sentido se puede hacer uso los reportes que el Centro de Operaciones de Seguridad

(SOC) genera para evidenciar el cumplimiento de las regulaciones, así como sus respectivas métricas.

Una vez que se haya podido identificar la información que posee la organización, deberemos pasar a identificar las necesidades en cuanto seguridad de la información y cuáles son aquellos aspectos relevantes con los cuales se requiere contar dentro del Centro de Operaciones de Seguridad (SOC). Para esto es importante contar con una buena estrategia de colaboración y comunicación entre todas las áreas de la organización, sus funciones, los productos de seguridad previamente utilizados y diferentes procesos y procedimientos que se mantengan vigentes en la organización.

Para esto nos enfocaremos en los aspectos principales de las operaciones de seguridad de la información que constituyen:

a) **Personas:** Se enfoca en el talento humano que estará a cargo de ejecutar los procesos del Centro de Operaciones de Seguridad (SOC) y de las competencias y conocimientos que deben tener.
b) **Procesos:** Se enfoca en el detalle de la totalidad de los procesos que ejecutará el Centro de Operaciones de Seguridad (SOC) de tal forma que se pueda detectar y prevenir incidentes relacionados con la seguridad de la información.
c) **Tecnología:** Se enfoca en las soluciones y herramientas que serán utilizadas dentro del Centro de Operaciones de Seguridad (SOC) que permiten realizar la ejecución de los procesos diarios de monitoreo y gestión de amenazas e incidentes de seguridad de la información.

En la actualidad existen dos esquemas que permitan a las organizaciones utilizar un Centro de Operaciones de Seguridad (SOC):

4.1.1. DISEÑAR E IMPLEMENTAR UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Diseñar e implementar un Centro de Operaciones de Seguridad (SOC) dentro de la organización como parte de la estructura jerárquica de la misma.

Por lo general las organizaciones que administran información sensible optan por el diseño e implementación de un Centro de Operaciones de Seguridad (SOC) dentro de su organigrama jerárquico con el propósito de disminuir el riesgo de fuga de información. Sin embargo, para poder realizar esto la organización debe tener en cuenta algunos criterios que le permitan alcanzar el propósito de forma efectiva:

- ✓ Personal interno altamente entrenado y capacitado.
- ✓ Metodología de manejo del Centro de Operaciones de Seguridad (SOC) claramente definido.
- ✓ Asignación del presupuesto adecuado que será destinado para la implementación y crecimiento del Centro de Operaciones de Seguridad (SOC).
- ✓ Clara y adecuada definición de los procesos del Centro de Operaciones de Seguridad (SOC).
- ✓ Establecer un proceso adecuado que permita integrar la respuesta a incidentes.

4.1.2. TERCERIZAR LAS FUNCIONES DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

La tercerización de las funciones del Centro de Operaciones de Seguridad (SOC) a una empresa de seguridad de la información especializada para que brinde protección a la organización constituye una forma válida de implementación utilizada, sin embargo, la organización se expone a un riesgo de seguridad al permitir que terceras personas recolecten y monitoreen los logs de los recursos de tecnologías de la información y comunicaciones de la organización. Para adoptar este tipo de implementación se deben tener definidos ciertos tipos de métricas

definidas para controlar las actividades de la organización externa:

- ✓ La organización externa debe ofrecer a la organización una interfaz virtual con información detallada sobre el servicio de seguridad que está ejecutando.
- ✓ La organización externa debe ofrecer varios puntos de vistas para la organización de las actividades que realiza.
- ✓ La organización externa debe entregar reportes periódicos de diferente tipo, como: técnicos, ejecutivos y de gestión.
- ✓ La organización externa debe gestionar de forma completa los tickets de incidencias de tal modo que se pueda registrar toda la información relacionada a ellos.
- ✓ La organización externa debe suscribir los respectivos SLA (acuerdos de niveles de servicios) y los mismos deben encontrarse claramente definidos.

4.2. PROBLEMÁTICA RELACIONADA CON UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

4.2.1. SEGURIDAD DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Podemos indicar que gran parte de los problemas que se presentan dentro de un Centro de Operaciones de Seguridad (SOC) en cuanto a la seguridad se refiere, se debe en gran medida a las fallas que existen en la implementación y desarrollo del proceso de seguridad de la información. Es así como los fallos más comunes y críticos que se suelen dar se presentan a continuación:

a) **Ausencia de políticas, normas y procedimientos:** La normativa interna de la organización establece como los recursos de tecnologías de la información y comunicaciones van a ser usados.
b) **Control de acceso:** Algunas organizaciones poseen identificaciones que no son individuales y son utilizadas por un grupo determinado de usuarios lo cual dificulta el poder identificar que usuario hizo determinada acción.
c) **No existencia de un administrador de información:** Sin duda constituye un factor importante para alcanzar el éxito en la implementación del proceso de seguridad de la información. Este rol de administrador de la información recae sobre la persona del área de negocio o del área administrativa responsable de la información quien se encargará de autorizar o denegar el acceso de los demás usuarios de la organización a determinada información.
d) **Planes de continuidad:** Estos planes de continuidad deben actualizarse de manera periódica. La realidad es que las organizaciones los elaboran una vez y no los vuelven a mirar más razón por la cual el plan de continuidad tiene que ser activo, actualizarse constantemente, probarse probado y mejorarse de forma continua.
e) **Registros de acciones realizadas:** Siempre es recomendable mantener una bitácora de tentativas de acceso, acceso, errores de identificación, errores de contraseña y modificaciones en los sistemas de la organización.
f) **Copias de seguridad:** La necesidad de la existencia de copias de seguridad radica en que en función del cumplimiento de la normativa legal que aplica y regula a cada organización se debe mantener bajo resguardo las operaciones y transacciones históricas de la organización. El procedimiento para la creación de las copias de seguridad debe actualizarse de manera permanente, así como es de vital importancia asegurarse que las copias de seguridad que se obtienen puedan ser probadas y restauradas en caso de llegar a necesitarse ante un evento adverso que comprometa la seguridad de la información.
g) **Ausencia de un responsable de seguridad de la información:** La seguridad de la información es responsabilidad de todos los miembros de la organización. Sin embargo, las organizaciones deben esforzarse por contar en su equipo con un profesional

capacitado y dedicado expresamente a las actividades inherentes al proceso de seguridad de la información.

h) **Gestión del riesgo:** Si la organización no realiza un tratamiento adecuado de la gestión y análisis de riesgos, las amenazas que existen pueden derivar en riesgos inminentes que terminen afectando la operación normal de la organización.

i) **Usuarios:** La falta de capacitación concientización de parte de las personas que conforman la organización constituyen factores determinantes en el éxito o fracaso del proceso de seguridad de la información en una organización. Cada usuario debe conocer sus responsabilidades, lo que puede y lo que no puede hacer y las sanciones que deberá enfrentar si incumple lo dispuesto.

4.2.2. OPERACIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Un Centro de Operaciones de Seguridad (SOC) exitosamente implementado se basa en la excelencia operacional, inspirada en procesos bien diseñados y ejecutados, personal capacitado y altamente motivado que se encuentra un paso adelante de aquellos factores internos o externos que pudieran comprometer la seguridad de la información de la organización. En términos generales podemos hacer alusión a que los problemas en la operación radican principalmente en lo siguiente:

a) **Niveles de Servicio:** El objetivo primordial de la gestión de niveles de servicio es definir, negociar y monitorizar la calidad de los servicios de tecnologías de la información ofrecidos por la organización. Si los servicios no se adecuan a las necesidades del cliente, la calidad de estos es deficiente o sus costes son desproporcionados, tendremos clientes insatisfechos y la organización será responsable de las consecuencias que se deriven de ello. Para la implementación del Centro de Operaciones de Seguridad (SOC), se recomienda el manejo de niveles de servicio considerando como mínimo lo siguiente:
   - ✓ Control de cambios.
   - ✓ Soporte a fallos.
   - ✓ Monitorización de actividad sospechosa.
   - ✓ Gestión de incidentes de seguridad.
   - ✓ Entrega de informes.

b) **Calidad en el servicio:** Corresponde a la manera de ser y al conjunto de características esenciales que identifican a las actividades y procedimientos de conformidad con ciertos requisitos preestablecidos por parte de la organización. Hoy en día la calidad dejó de ser una opción para las organizaciones ya que constituye un elemento fundamental para la consecución de ventajas competitivas, mayor rentabilidad y satisfacción de los clientes lo que sin duda garantizará la permanencia en el mercado y el crecimiento con mayor facilidad.

c) **Niveles de atención y respuesta:** La calidad de atención tanto a los usuarios internos como externos de la organización constituyen un proceso para la satisfacción total de los requerimientos y necesidades de estos. Es por esta razón que la Alta Dirección debe preocuparse en todo momento por mejorar la calidad del servicio que ofrecen a sus clientes, enfocándolo hacia la calidad y la mejora continua, ya que no es cuestión de elección, la imagen de la organización depende de ello.

4.2.3. VENTAJAS Y DESVENTAJAS DE UN CENTRO DE OPERACIONES DE SEGURIDAD(SOC)

Existen algunas ventajas y desventajas que pueden ser indicadas para que las organizaciones puedan tomar la decisión de adoptar un Centro de Operaciones de Seguridad (SOC) entre las cuales podríamos citar:

VENTAJAS	DESVENTAJAS
✓ Reducción de riesgos y amenazas. ✓ Mayor disponibilidad de los servicios. ✓ Identificación y prevención de vulnerabilidades. ✓ Optimizar la capacidad de respuesta operativa. ✓ Implementación de políticas y reglas claras. ✓ Centralización de los registros de datos. ✓ Mejorar la generación de informes y reportes. ✓ Mayor seguridad para los servicios y productos. ✓ Prevención, protección y eliminación de los riegos asociados con los fraudes informáticos.	✓ No es una solución global por cuanto la organización debe prestar atención a los objetivos de negocio y a aquellos elementos que resulten determinantes tras el análisis de riesgos. ✓ Es intrusivo lo cual puede afectar a activos de información críticos para la organización que pueden cambiar el comportamiento de estos. ✓ En el caso de la externalización del servicio la regulación contractual debe encontrarse claramente definida. ✓ El seguimiento a terceros prestadores de servicios con la finalidad de verificar si éstos se encuentran cumpliendo con los acuerdos firmados.

Tabla 3. Ventajas y desventajas de un Centro de Operaciones de Seguridad (SOC)

4.3. CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Las mejores prácticas para la implementación de un Centro de Operaciones de Seguridad (SOC) hacen énfasis en las consideraciones que se deben tener en cuanto a los requerimientos de negocio, así como requerimientos técnicos entre los que podemos mencionar los siguientes:

4.3.1. REQUERIMIENTOS DE NEGOCIO

a) **Reducción de riesgos:** La organización debe mitigar los riesgos antes de que las amenazas empiecen a expandirse rápidamente.
b) **Control y prevención de amenazas:** El hecho de prevenir y controlar amenazas involucra una notificación temprana de actividad sospechosa, así como la habilidad de implementar rápidamente un mecanismo de contingencia.
c) **Disminución de la carga de trabajo administrativa:** El Centro de Operaciones de Seguridad (SOC) debe encontrarse diseñado de tal manera que involucre la menor cantidad posible de injerencia humana. La meta es habilitar a unos cuantos especialistas con la mejor información, para lograr respuestas rápidas y automatizadas.
d) **Personal y responsabilidades:** El Centro de Operaciones de Seguridad (SOC) debe tener claramente definidas las responsabilidades, así como a los encargados de la ejecución de determinadas tareas específicas, así como asignar responsabilidades de respuesta y control para cada área de la organización.
e) **Niveles de escalamiento:** El Centro de Operaciones de Seguridad (SOC) debe tener definido los parámetros necesarios que ayuden a determinar de qué manera y cuando escalar los eventos de seguridad.
f) **Auditorías y soporte de cumplimiento:** Las organizaciones requieren realizar auditorías periódicas que le permitan cumplir con las regulaciones y normativa legal. En este sentido se necesita obtener acceso rápido y flexible a la información sobre amenazas e identificar y acceder a datos de control crítico.
g) **Respuesta a incidentes y recuperación:** Un Centro de Operaciones de Seguridad (SOC) adecuadamente diseñado brinda a los especialistas de seguridad la posibilidad de visualizar los incidentes que se han presentado y les proporciona las herramientas de administración de incidentes más adecuadas que los ayuden a detectar y remediar los problemas.

4.3.2. REQUERIMIENTOS TÉCNICOS

a) **Rapidez de agregación y correlación:** Una de las características más importantes en lo relacionado a la administración de la seguridad de la información constituye el hecho de estar en capacidad de suprimir aquella información repetida, validando alertas para confirmar su impacto, y priorizar las alertas más críticas.
b) **Cobertura de sistemas y dispositivos:** El Centro de Operaciones de Seguridad (SOC) debe tener la capacidad de soportar todos los dispositivos de seguridad y cubrir todo equipo y aplicaciones.
c) **Capacidad de respuesta oportuna:** El Centro de Operaciones de Seguridad debe tener la capacidad de proveer información en tiempo real proporcionando a los especialistas en seguridad los elementos necesarios para tomar acciones rápidamente.
d) **Funcionamiento:** El Centro de Operaciones de Seguridad (SOC) debe encontrarse en funcionamiento bajo el esquema 24x7x365 para proporcionar los niveles de seguridad requeridos por la organización.
e) **Soporte para ambientes federados y distribuidos:** El Centro de Operaciones de Seguridad (SOC) debe soportar vistas federativas y roles administrativos de tal forma que se pueda reportar la información desde los puntos remotos hacia el punto central. Para esto la herramienta debe basarse en roles de manera flexible que permita acoplarse a las diferentes necesidades.
f) **Capacidades forenses:** Las herramientas de administración de seguridad de la información que registran las actividades de eventos y pueden visualizar estos datos, habilitan a los administradores para aprender lecciones valiosas y a mitigar los riesgos.
g) **Integración entre SOC y NOC:** El Centro de Operaciones de Seguridad (SOC) convive junto con el Centro de Operaciones de Red (NOC). De manera conjunta ambas herramientas proveen una vista de red y seguridad a lo largo de la organización, que maximiza sus niveles de eficiencia.
h) **Talento Humano:** El personal del Centro de Operaciones de Seguridad (SOC) que sin duda alguna constituye personal altamente capacitado y experimentado en seguridad de la información no debe ser utilizado en labores de monitoreo de bajo nivel y se debe eliminar la dependencia de personal clave. El Centro de Operaciones de Seguridad (SOC) debe ser operado en capas, con la capa 1 recibiendo alertas y solucionando problemas a bajo nivel, y con las capas 2 y 3 manejando alertas y problemas más complejos.

En este contexto y para que las actividades descritas en los literales anteriores pueden ser ejecutadas de manera eficiente, la organización debe contar con un área dedicada a la seguridad de la información que permita llevar un control continuo y exhaustivo de las actividades que realizan los diferentes recursos con la finalidad de detectar comportamientos sospechosos que puedan incidir en una brecha de seguridad a través de un proceso efectivo de respuesta ante los incidentes que se hayan presentado.

4.4. FUNCIONES DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Desde el inicio debemos diseñar de manera correcta las funciones a realizarse dentro del Centro de Operaciones de Seguridad (SOC), para lo cual a continuación, describiremos algunos aspectos que constituyen la base de funcionamiento de un Centro de Operaciones de Seguridad (SOC).

4.4.1. FUNCIONES PRIMARIAS

Las funciones primarias hacen referencia a aquellos aspectos básicos que todos los Centros de Operaciones de Seguridad (SOC) deben poder realizar para poder ser considerados como tal.

4.4.1.1. RECOLECCIÓN DE LOGS

Esta funcionalidad consiste en la centralización que debe existir sobre la recolección de los logs

de diferentes tipos de actividades que se realicen en los recursos de tecnologías de la información y comunicaciones.

CAPACIDAD ALTA	CAPACIDAD BAJA
La recolección de logs en la organización permite garantizar el registro de casi la totalidad de eventos que se lleguen a presentar.	Se realiza el mejor esfuerzo por parte de la organización para poder recolectar la mayor cantidad de eventos posibles.

Tabla 4. Capacidades en cuanto a recolección de logs

4.4.1.2. RETENCIÓN Y ALMACENAMIENTO DE LOGS

La retención y el almacenamiento de los logs se considera una funcionalidad básica para los Centros de Operaciones de Seguridad (SOC), por cuanto los logs recolectados contienen información importante acerca de los eventos específicos que pueden ser utilizados en un análisis futuro.

En ocasiones esta funcionalidad se deriva del cumplimiento de parte de las organizaciones sobre resoluciones legales y gubernamentales por lo que se hace necesario contar con una capacidad de retención y almacenamiento alto para cumplir con la regulación sobre la recuperación y no-repudio.

CAPACIDAD ALTA	CAPACIDAD BAJA
Un Centro de Operaciones de Seguridad (SOC) con capacidad alta de retención y almacenamiento no tiene restricciones en cuanto a tiempo y almacenamiento.	Un Centro de Operaciones de Seguridad (SOC) con una capacidad baja de retención y almacenamiento tendrá restricciones en cuanto a tiempo y almacenamiento.

Tabla 5. Capacidades en cuanto a retención y almacenamiento de logs

4.4.1.3. ANÁLISIS DE LOGS

Este aspecto concierne a la habilidad que el personal del equipo de seguridad del Centro de Operaciones de Seguridad (SOC) debe poseer para que se encuentre en capacidad de analizar e interpretar datos obtenidos de los logs y poder presentar los resultados del análisis de una forma entendible, haciendo uso de las métricas adecuadas.

CAPACIDAD ALTA	CAPACIDAD BAJA
Una alta capacidad de análisis de logs ofrece como resultado del análisis, métricas y dashboard de una amplia gama de formato y tipos de dispositivos.	Una baja capacidad de análisis de logs presenta datos en crudo con un limitado tipo de formatos y dispositivos para los resultados.

Tabla 6. Capacidades en cuanto a análisis de logs

4.4.1.4. MONITOREO DE AMBIENTES PARA EVENTOS DE SEGURIDAD

Este aspecto hace referencia al monitoreo que realizará el Centro de Operaciones de Seguridad (SOC) para detectar posibles eventos de seguridad.

CAPACIDAD ALTA	CAPACIDAD BAJA
El Centro de Operaciones de Seguridad (SOC) realiza el monitoreo 24x7 con lo que se garantiza los tiempos de respuesta.	El Centro de Operaciones de Seguridad (SOC) limita la funcionalidad del monitoreo al horario de oficina sin garantizar un tiempo reducido de respuesta.

Tabla 7. Capacidades en cuanto a monitoreo de ambientes

4.4.1.5. DIVERSIDAD DE DISPOSITIVOS INTEGRADOS

Hace referencia a la diversidad en cuanto a dispositivos y proveedores que pueden ser integrados y administrados por el Centro de Operaciones de Seguridad (SOC).

CAPACIDAD ALTA	CAPACIDAD BAJA
No posee restricciones en cuanto a tipos de dispositivos y proveedores que se pueden integrar y monitorear, así como mayor capacidad de interpretación y entendimiento de las vulnerabilidades y amenazas contra esos dispositivos.	Monitorea una cantidad limitada de tipos de dispositivos y proveedores lo que imposibilita la interpretación de los diferentes tipos de vulnerabilidades contra esos dispositivos.

Tabla 8. Capacidades en cuanto a dispositivos integrados

4.4.1.6. CORRELACIÓN DE EVENTOS Y FLUJOS DE TRABAJO

Se refiere a la capacidad para correlacionar eventos de diferentes tipos de dispositivos y fabricantes, como también comenzar flujos de trabajo en respuesta a las reglas de correlación que se activan.

CAPACIDAD ALTA	CAPACIDAD BAJA
El Centro de Operaciones de Seguridad (SOC) tiene la capacidad de ofrecer un servicio complejo y amplio de correlación de eventos con reglas automáticas integrada en sistemas de herramientas de flujo de trabajo, para dar seguimiento.	El Centro de Operaciones de Seguridad (SOC) abarca únicamente lo básico con reglas de correlación manuales y no cuenta con la habilidad de generar flujos de trabajo.

Tabla 9. Capacidades en cuanto a correlación de eventos

4.4.1.7. MANEJO DE INCIDENTES

Este aspecto abarca la habilidad del SOC de responder, gestionar y escalar incidentes de seguridad que se puedan presentar.

CAPACIDAD ALTA	CAPACIDAD BAJA
El Centro de Operaciones de Seguridad (SOC) cuenta con una alta capacidad en el manejo de incidentes y escalamiento automatizado e integrado a un sistema empresarial completo de gestión de incidentes.	El Centro de Operaciones de Seguridad (SOC) con capacidad baja únicamente está en capacidad de ofrecer la función de generar, responder y escalar los incidentes de forma manual.

Tabla 10. Capacidades en cuanto a manejo de incidentes

4.4.1.8. RESPUESTA ANTE AMENAZAS

Abarca las funciones de detección de amenazas en tiempo real, así como la identificación de vulnerabilidades potenciales en los sistemas o dispositivos que deberán ser mitigados de manera proactiva.

CAPACIDAD ALTA	CAPACIDAD BAJA
El Centro de Operaciones de Seguridad (SOC) dispone de una fuente amplia de investigación sobre amenazas y vulnerabilidades de forma automatizada y con suscripción a múltiples proveedores externos.	El Centro de Operaciones de Seguridad (SOC) no se encuentra en la capacidad de realizar investigación interna y retroalimentación en cuanto a amenazas externas.

Tabla 11. Capacidades en cuanto a respuesta ante amenazas

4.4.1.9. IDENTIFICACIÓN DE AMENAZAS

Se refiere a la capacidad del Centro de Operaciones de Seguridad (SOC) para identificar amenazas y vulnerabilidades en tiempo real o también con fines de investigación.

CAPACIDAD ALTA	CAPACIDAD BAJA
El Centro de Operaciones de Seguridad (SOC) dispone de la capacidad de investigación y consultas en tiempo real de sus sistemas integrados para la gestión de amenazas.	El Centro de Operaciones de Seguridad (SOC) tiene una limitada capacidad para identificar amenazas y vulnerabilidades.

Tabla 12. Capacidades en cuanto a identificación de amenazas

4.4.1.10. REPORTERÍA

Se refiere a la capacidad de generación de distintos tipos de reportes de seguridad ajustados a las necesidades de los interesados de la organización.

CAPACIDAD ALTA	CAPACIDAD BAJA
El Centro de Operaciones de Seguridad (SOC) puede ofrecer reportes de acuerdo con lo solicitado, mediante el análisis de distintas plataformas y en una gran variedad de formatos.	El Centro de Operaciones de Seguridad (SOC) tiene limitaciones en cuanto a reportes que no son personalizables, predefinidos en cuanto a formatos y de plataformas limitadas.

Tabla 13. Capacidades en cuanto a reportería

4.4.2. FUNCIONES SECUNDARIAS

Las funciones secundarias de un Centro de Operaciones de Seguridad (SOC) hacen referencia a un enfoque más especializado y específico entre los que podemos citar los siguientes:

- ✓ Análisis de malware.
- ✓ Análisis y escaneo de vulnerabilidades.
- ✓ Manejo de dispositivos de seguridad.
- ✓ Certificación de identidad y recertificación.
- ✓ Pruebas de penetración.
- ✓ Integración con controles de seguridad física.

Las funciones secundarias tienen una alta probabilidad de ir cambiando en el transcurso del tiempo, en el sentido de que pueden llegar a crearse más aspectos o eliminar aquellos que puedan considerarse como innecesarios.

La diferencia importante versus las funciones primarias es que estas con el tiempo se van perfeccionando, pero no cambian en su totalidad por cuanto representan la base lo que constituye el Centro de Operaciones de Seguridad (SOC).

4.5. DISEÑO DEL MODELO PROPUESTO PARA EL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

El modelo propuesto para la implementación del Centro de Operaciones de Seguridad (SOC) lo hemos basado en el modelo de mejora continua PDCA (Plan, Do, Check, Act) el cual se encuentra alineado a lo que establece la norma ISO/IEC 27001. Hay que resaltar que la adopción de este modelo constituye una decisión de tipo estratégico para la organización, cuyo diseño e implementación se encontrara influenciado por las necesidades, objetivos, requerimientos de seguridad, procesos empleados y el tamaño y estructura de ésta esperando que estos vayan siendo actualizados a lo largo del tiempo.

Si bien es cierto el modelo PDCA es ampliamente utilizado por la norma ISO, éste se halla construido sobre una base que no necesariamente va a ser de aplicación o cumplimiento por

parte de todas las organizaciones, especialmente cuando las mismas no han incursionado en los procesos relacionados con el cumplimiento de la normativa ISO.

El modelo que proponemos deberá ser perfeccionado y modificado en el futuro por cuanto el Consejo de Aseguramiento de la Calidad de la Educación Superior se debe ajustar a los constantes cambios que surgirán como sistema dinámico.

La particularidad del modelo que presentamos a continuación reside en su aspecto operativo y pseudo práctico, puesto que se incluye la estructuración, formación e implementación acorde a las fases que se han establecido a continuación:

- ✓ Fase de Análisis.
- ✓ Fase de Identificación.
- ✓ Fase de Aplicación.
- ✓ Fase de Mejora Continua.

De forma macro las fases establecidas hacen referencia a un conjunto de actividades que es necesario realizar con el objetivo de elaborar y aplicar de manera adecuada el modelo propuesto.

4.5.1. FASE DE ANÁLISIS

En esta fase del modelo el Consejo de Aseguramiento de la Calidad de la Educación Superior deberá realizar un análisis costo beneficio que le permita determinar si es económicamente viable la implementación del modelo propuesto.

Para esto se deberán realizar como mínimo las actividades descritas a continuación:

- ✓ Seleccionar al menos tres (3) proveedores externos, en el mercado ecuatoriano, que brinden servicios relacionados con Centros de Operaciones de Seguridad (SOC).
- ✓ Solicitar información a los proveedores escogidos acerca de los servicios que ofertan.
- ✓ Solicitar información de costos y niveles de servicio ofertados por los proveedores.
- ✓ Realizar una tabla comparativa de costo beneficio a partir de la información proporcionada por parte de los proveedores.
- ✓ Si el resultado del análisis determina que el costo proporcionado por el proveedor es mayor a las expectativas que tenía la Institución, entonces se procede al desarrollo del modelo de forma interna.

4.5.1.1. DEFINICIÓN DE ALCANCE Y LÍMITES DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

El alcance y límites del Centro de Operaciones de Seguridad (SOC) se encontrará determinado por el giro de negocio, su ubicación, activos y tecnología. Los puntos que deben ser considerados provienen del levantamiento de la información obtenida por parte del Consejo de Aseguramiento de la Calidad de la Educación Superior entre los que se destacan:

- ✓ Identificar los principales servicios que presta la Institución.
- ✓ Jerarquizar los servicios entregados por la Institución.
- ✓ Validar si existe un inventario de la infraestructura actual con el cual cuenta la Institución.
- ✓ Mencionar los principales problemas de seguridad de la información que han sido detectados dentro de la Institución.
- ✓ De los servicios identificados cual es el servicio que desea monitorear inicialmente.

4.5.1.2. UBICACIÓN Y TIPO DE CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PROPUESTO

El Centro de Operaciones de Seguridad (SOC) debe disponer de espacio físico independiente en instalaciones seguras. El Consejo de Aseguramiento de la Calidad de la Educación Superior deberá disponer de una locación distinta para el SOC, así como el hardware y software

necesario.

Para esto, el Consejo de Aseguramiento de la Calidad de la Educación Superior definirá la ubicación física del Centro de Operaciones de Seguridad (SOC), tomando en consideración la localización geográfica dentro de la República del Ecuador que provea el menor porcentaje de inseguridad y riesgo calculado.

4.5.1.3. DEFINICIÓN DE ACTIVOS

Para iniciar el análisis de la información del Consejo de Aseguramiento de la Calidad de la Educación Superior, de manera preliminar, se definirán los activos tecnológicos con los que cuenta actualmente y con ello se procede a calcular el nivel de riesgo de estos.

4.5.1.4. ANÁLISIS Y EVALUACIÓN DE RIESGO

- ✓ Identificar y desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables.
- ✓ Identificar las amenazas para los activos previamente identificados.
- ✓ Identificar las vulnerabilidades que podrían ser explotadas por las amenazas.
- ✓ Identificar los impactos que pueden tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.
- ✓ Calcular el impacto sobre la Institución que podría resultar de una falla en la seguridad de la información, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.
- ✓ Calcular la probabilidad realista de que ocurra dicha falla en función de las amenazas y vulnerabilidades prevalecientes, los impactos asociados con estos activos, y los controles implementados actualmente.
- ✓ Calcular los niveles de riesgo de tal forma que se pueda determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido.
- ✓ Identificar y evaluar las opciones para el tratamiento de los riesgos.

4.5.2. FASE DE IDENTIFICACIÓN

En esta fase del modelo el Consejo de Aseguramiento de la Calidad de la Educación Superior deberá profundizar en conocer a ciencia cierta los antecedentes, reglas de negocio y necesidades de la Institución, razonando y entendiendo cada unidad administrativa que la conforma y su interrelación entre las mismas. Esto ayudará a documentar en detalle el giro de negocio y la trazabilidad de todos sus procesos.

La fase de identificación se concentra en el manejo de los incidentes de manera ágil, sin embargo, para muchas organizaciones el proceso de identificar y evaluar con precisión los posibles incidentes es difícil, debido a que es necesario determinar si el incidente ha ocurrido y de ser así identificar el tipo, la extensión y magnitud del problema. Se deben tomar en consideración ciertos factores tales como:

- ✓ Un incidente puede detectarse por medio de varios mecanismos, asimismo, se pueden identificar de manera manual mediante el reporte de problemas por parte de los usuarios de la institución.
- ✓ Debe considerarse que en ocasiones el volumen de posibles incidentes puede llegar a ser alto.
- ✓ Se hace indispensable que el personal tenga los conocimientos y la experiencia necesaria para poder realizar un análisis adecuado de la información relacionada con el incidente.

La fase de análisis utilizada diferentes metodologías relacionadas con la gestión de incidentes. El objetivo principal es poder establecer un proceso de respuesta ante incidentes óptimo para

que la institución se encuentre preparada ante la manifestación de estos, pero también se enfoca en la prevención de incidentes de seguridad por medio del aseguramiento de los sistemas, redes, aplicaciones, entre otros activos informáticos de la institución.

4.5.2.1. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

Para el establecimiento de un procedimiento ágil y dinámico relacionado con la gestión y respuesta ante incidentes de seguridad de la información se hace necesario establecer algunos factores de importancia que deben ser utilizados durante el manejo de un incidente, entre los cuales podemos citar los siguientes:

4.5.2.2. PREVENCIÓN DE INCIDENTES

El Consejo de Aseguramiento de la Calidad de la Educación Superior debe realizar un proceso de aseguramiento de sus principales activos informáticos. Aunque el personal que conforma el Centro de Operaciones de Seguridad (SOC) no es el responsable de realizar los aseguramientos de las diferentes plataformas, por su lado si son responsables por definir, verificar, comunicar y sugerir varias prácticas de seguridad que pueden ser utilizadas en el proceso de aseguramiento.

4.5.2.3. PROCESO DE ANÁLISIS DE INCIDENTES

El Consejo de Aseguramiento de la Calidad de la Educación Superior debe centrar sus esfuerzos en contar con personal altamente capacitado y experimentado en el campo de seguridad de la información con el propósito de que el proceso de análisis de incidentes sea realizado de manera eficiente y no se comentan errores costosos, para esto el equipo de trabajo debe actuar rápidamente analizando cada incidente siguiendo un proceso predefinido y documentado en cada paso que se realice. Para ayudar a que el proceso de análisis sea más efectivo y ágil se podría realizar las siguientes actividades:

- ✓ Perfilar sistemas y redes.
- ✓ Tener conocimiento del comportamiento normal.
- ✓ Crear una política de retención de información.
- ✓ Realizar correlación de eventos.
- ✓ Mantener el reloj de todos los hosts sincronizado.
- ✓ Utilizar motores de busque de internet.
- ✓ Ejecutar sniffers o recolectar datos adicionales.
- ✓ Filtrar datos.
- ✓ Buscar asistencia de otros.

4.5.2.4. DOCUMENTACIÓN EN LA GESTIÓN DEL INCIDENTE

Una actividad importante constituye la documentación de todos los pasos dados desde la detección hasta la solución final. Cada documento relacionado debe ser registrado y firmado por el responsable del análisis. Este tipo de documentación podría ser útil en caso de ser necesario realizar un proceso legal.

Para que el personal del Centro de Operaciones de Seguridad (SOC) pueda mantener información sobre el estado y actividades realizadas durante la gestión del incidente es común que se utiliza herramientas automatizadas para gestionar los tickets de incidentes, sin embargo, considerar que en estos sistemas se pueda almacenar como mínimo la siguiente información:

- ✓ El estado actual del incidente.
- ✓ Resumen de las actividades del incidente.
- ✓ Señales e indicadores relacionados con el incidente.
- ✓ Acciones ejecutadas por el responsable de la gestión del incidente.
- ✓ Cadena de custodia de las evidencias, en caso de ser aplicable.
- ✓ Evaluación de impacto del incidente.

- ✓ Lista de evidencia recolectada durante la gestión.
- ✓ Comentarios de los responsables de la gestión.
- ✓ Próximas tareas por realizarse para la solución del incidente.

Un punto importante para tener siempre en consideración que toda la información debe ser registrada con la hora y fecha de tal forma que se pueda evaluar que la gestión del incidente fue realizada de manera oportuna y eficaz.

4.5.2.5. PRIORIZACIÓN DE INCIDENTES

Para que el proceso de gestión de incidentes sea eficaz se debe priorizar los incidentes de manera correcta, debido a que no es recomendable gestionar los incidentes de acuerdo con cómo se registren. Para poder realizar este proceso de priorización se puede considerar los siguientes factores:

a) **Impacto funcional del incidente:** Se refiere al impacto que tendría el incidente en las funciones del negocio, es necesario que los responsables de la gestión evalúen este factor para poder priorizar el incidente, tomando en cuenta el impacto actual a las funciones del negocio y el impacto que conllevaría no poder solucionar el incidente rápidamente.
b) **Impacto del incidente sobre la información:** Los responsables de la gestión del incidente necesitan evaluar el impacto en la filtración de la información que puede haber causado el incidente de esta manera ver el nivel de afectación con los clientes, empleados o hasta el mismo negocio en caso de haber sido comprometida información crítica para la organización.
c) **Recuperación del incidente:** El tamaño del incidente y los tipos de recursos afectados determinará la cantidad de tiempo y esfuerzo que se deberá emplear para recuperarse del incidente. El personal del Centro de Operaciones de Seguridad (SOC) debe considerar al momento de priorizar el esfuerzo necesario que se necesitará para que la organización se recupere del incidente y compararlas cuidadosamente contra el costo la recuperación.

4.5.2.6. NOTIFICACIÓN DE INCIDENTES

Como actividad final después del análisis y priorización del incidente, es necesario comunicarlo a todo el personal involucrado e interesado para que cada uno pueda realizar su rol durante la gestión del incidente. Dentro de las políticas de respuesta a incidentes la institución se necesita definir los lineamientos para la notificación de los incidentes como por ejemplo la información mínima a notificar, a quien será necesario notificar y tiempos para notificar.

El personal a quien se notificará y el medio que se utilice para notificar la información del incidente pueden variar de acuerdo con cada organización y sus necesidades.

4.5.3. FASE DE APLICACIÓN

En esta fase del modelo el Consejo de Aseguramiento de la Calidad de la Educación Superior deberá definir los controles propuestos para mitigar los riesgos, políticas y procedimientos que apoyan a regular los procesos de seguridad y los elementos de creación para el Centro de Operaciones de Seguridad (SOC).

4.5.3.1. DEFINICIÓN DE POLÍTICAS Y PROCEDIMIENTOS PARA EL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Se definen en términos de las características del negocio, la institución, su ubicación, activos y tecnología que permita:

- ✓ Incluir un marco referencial que defina sus objetivos y establezca un sentido de dirección general y principios para la acción con relación a la seguridad de la información.
- ✓ Tomar en cuenta los requerimientos operativos, legales y las obligaciones de la seguridad de la información.
- ✓ Establecer el criterio con el que se evaluará el riesgo aprobado por la máxima autoridad de la Institución.

4.5.3.2. CONTROLES PROPUESTOS

Se deben seleccionar los controles para cumplir con los requerimientos identificados por el proceso de tratamiento del riesgo, así como las políticas y procedimientos aplicables. Esta selección toma en cuenta el criterio para aceptar los riegos y a su vez mitigarlos. Las acciones posibles incluyen:

- ✓ Aplicar los controles apropiados adecuados a los activos y nivel de riesgo calculado.
- ✓ Aceptar los riesgos de manera consiente y objetiva, siempre que los mismos satisfagan de forma clara las políticas y el criterio de aceptación del riesgo de la Institución.

4.5.3.3. CONTENCIÓN DE INCIDENTES

Se debe tener definido de manera clara el proceso de contención que servirá a la institución a impedir que los incidentes terminen causando daños mayores a la operatividad de la institución. Si bien es cierto determinados incidentes no necesariamente van a requerir de un proceso de contención es recomendable que el Consejo de Aseguramiento de la Calidad de la Educación Superior cuente con una estrategia de contención de incidentes que ayude en la toma de decisiones en el sentido de volverla más sencilla al encontrarse la estrategia alineada a las necesidades y recursos que la institución maneja.

La contención de incidentes se encontrará definida en función del tipo de incidente que se está gestionando, por lo que resulta de utilidad que se diseñen diferentes estrategias de contención que vayan de la mano con la tipología de incidentes de mayor relevancia. Algo que no se debe olvidar es la generación de la documentación suficiente que ayude a que la toma de decisiones sea ágil, adecuada y acertada. Se recomienda que el diseño de la estrategia contemple al menos la siguiente información, la cual podrá variar en función de la experiencia que posee el personal del Centro de Operaciones de Seguridad (SOC):

- ✓ Daño potencial del incidente hacia los activos de la institución.
- ✓ Necesidad de preservación de evidencias.
- ✓ Disponibilidad de los servicios.
- ✓ Tiempos y recursos necesarios para poder aplicar la estrategia de contención.
- ✓ Nivel de efectividad al aplicar la estrategia de contención.
- ✓ Duración del proceso de solución.

Es importante señalar que no todos los incidentes van a poder ser contenidos, en ocasiones pueden llegar a presentarse incidentes que al momento de aplicar una estrategia de contención se puede terminar originando más daño que el mismo incidente por lo que el personal del Centro de Operaciones de Seguridad (SOC) analizará en primera instancia la factibilidad de aplicar una estrategia de contención al incidente presentado.

4.5.3.4. RECOLECCIÓN DE EVIDENCIA DE INCIDENTES PRESENTADOS

En la resolución de un incidente siempre se hace necesario recolectar la evidencia que sea requerida con el propósito de descubrir de manera precisa la causa raíz del problema. Además, constituye un factor de suma importancia si la institución debe presentar los descargos correspondientes ante procesos legales que podría afrontar como resultado del incidente presentado.

Bajo esta premisa la institución deberá contar con un procedimiento para la recolección, manejo y preservación de las evidencias ya sea en formato físico o digital. Debe determinar de forma clara los formularios a ser empleados, los responsables de cada actividad y la cadena de custodia que permitan controlar que personas manejaron la evidencia y las diferentes áreas donde se las resguardo.

En la actualidad tenemos diversos procedimientos ya establecidos para el manejo de evidencia entre los cuales se pueden citar los siguientes:

a) **Norma ISO/IEC 27037:** Esta norma realiza una división en cuanto al proceso de adquisición de evidencia clasificándola en distintos tipos como adquisición de evidencia de dispositivos prendidos, apagados, dispositivos críticos, dispositivos de almacenamiento, entre otros.
b) **NIST SP 800-86:** Constituye una guía de referencia para la integración de técnicas forenses en la gestión de incidentes la cual provee información para poder establecer un proceso forense dentro de una organización.

En función de la normativa que el Consejo de Aseguramiento de la Calidad de la Educación Superior decida aplicar para el diseño del procedimiento de manejo de evidencia, se podrá crear un log detallado para todas las evidencias que hayan sido recolectadas.

4.5.3.5. ERRADICACIÓN Y RECUPERACIÓN DEL INCIDENTE

El Consejo de Aseguramiento de la Calidad de la Educación Superior puede definir un proceso de erradicación de incidentes de forma particular por cada incidente o uno general para toda la institución. Algo importante que se debe considerar es que durante la ejecución del proceso de erradicación de incidentes se identifiquen todos aquellos hosts que hayan resultado afectados para poder erradicarlos y de esta manera evitar que componentes del incidente permanezcan y vuelvan a generar nuevos incidentes.

Por su parte el proceso de recuperación de incidentes deberá enfocarse al restablecimiento de las operaciones a los niveles normales de funcionamiento e ir remediando las vulnerabilidades que se hayan descubierto de tal forma que se prevenga que incidentes similares se susciten nuevamente a futuro. Entre las actividades más comunes para la recuperación de incidentes mencionamos las siguientes:

- ✓ Realizar restauraciones de respaldos, restaurar equipos desde cero con configuraciones de seguridad predefinidas, instalar parches, cambiar contraseñas, etc.
- ✓ Monitorear sistemas o redes críticas afectadas después de un incidente, ya que con frecuencia suelen ser el primer blanco para un próximo ataque.
- ✓ El Centro de Operaciones de Seguridad (SOC) debe definir tareas a corto, mediano y largo plazo que ayuden en la recuperación del funcionamiento normal de los servicios de la institución y prevenir incidentes futuros.
- ✓ Las tareas deben ser plenamente gestionadas y monitoreadas para que la institución se pueda recuperar totalmente del incidente ocurrido.

4.5.4. FASE DE MEJORA CONTINUA

En esta fase del modelo el Consejo de Aseguramiento de la Calidad de la Educación Superior deberá diseñar las políticas y procedimientos para prevenir la fuga de información, así como la revisión continua de los procesos del Centro de Operaciones de Seguridad (SOC).

Generalmente este aspecto en algunas organizaciones es omitido, pero también es de vital importancia ya que la institución se debe enfocar en el aprendizaje y mejoramiento continuo de los procesos. Después de que se haya presentado algún evento que afectó la seguridad de la información de la institución es importante que el equipo que forma parte del Centro de Operaciones de Seguridad (SOC) se tome el tiempo necesario para analizar y definir las lecciones

aprendidas en el incidente, en especial los que son considerados como incidentes con un nivel de afectación alto, ya que resulta muy útil para el mejoramiento de las medidas de seguridad y el proceso de gestión de incidentes dentro de la institución.

4.5.4.1. CICLO DE VIDA DE LA INFORMACIÓN

En este punto se deben diseñar políticas y procedimientos a implementar respecto al ciclo de vida de la información (creación, uso y destrucción) dentro de la Institución.

Para que la institución tenga un manejo adecuado de las lecciones aprendidas de cada incidente se recomienda hacer uso de herramientas automatizadas que permitan el acceso a esta información de una forma más ágil y organizada.

4.5.4.2. REVISIÓN CONTINUA DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Ejecutar procedimientos de revisión para:

- ✓ Detectar prontamente los errores en los resultados del procesamiento de tickets.
- ✓ Identificar prontamente los incidentes de seguridad fallidos y exitosos.
- ✓ Permitir al Comité de Seguridad de la Información determinar si las actividades de seguridad delegadas a las personas o implementadas mediante la tecnología de información se están realizando como se esperaba.
- ✓ Ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad mediante el uso de indicadores; y determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.
- ✓ Realizar revisiones regulares de la efectividad del Centro de Operaciones de Seguridad (SOC) tomando en cuenta los resultados de auditorías de seguridad, incidentes, mediciones, sugerencias y retroalimentación de todas las partes interesadas.
- ✓ Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
- ✓ Revisar las evaluaciones del riesgo a intervalos planeados y revisar el nivel de riesgo residual y riesgo aceptable identificado, tomando en cuenta los cambios en:
  - ➢ La institución.
  - ➢ Tecnología.
  - ➢ Objetivos y procesos comerciales.
  - ➢ Amenazas identificadas.
  - ➢ Efectividad de los controles implementados.
  - ➢ Eventos externos, como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social.
- ✓ Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del Centro de Operaciones de Seguridad (SOC).

La información obtenida de la gestión del incidente servirá para poder investigar las características que conlleven a la identificación de vulnerabilidades y amenazas de seguridad que pudieran presentarse de manera sistemática. Asimismo, constituye un insumo a utilizar en la evaluación y tratamiento de riesgos que sirva de guía para la selección e implementación de controles de seguridad necesarios para evitar nuevos incidentes.

4.5.4.3. CUMPLIMIENTO DE INDICADORES Y AUDITORÍAS INTERNAS

Otro aspecto importante en el que puede ser utilizada la información proveniente de los registros del Centro de Operaciones de Seguridad (SOC) tiene que ver con la posibilidad de verificar si los indicadores de desempeño tanto del personal de respuesta ante incidentes como de los procesos organizacionales en su conjunto se están cumpliendo conforme lo establecido. Algunas métricas que pueden ser utilizadas las describimos a continuación:

a) **Número de incidentes gestionados en un período de tiempo:** Este indicador ayuda a la institución a conocer la cantidad de trabajo que el Centro de Operaciones de Seguridad (SOC) debe emplear en la gestión de cada uno de los incidentes. Este tipo de indicador debe emplearse en función de la categorización y complejidad de cada incidente.

b) **Tiempo de gestión por incidente:** Este indicador puede ser dinámico ya que existen diferentes formas de poder establecer una tipología de medición de este, como, por ejemplo:
   - ✓ Cantidad total de tiempo trabajado en el incidente.
   - ✓ Tiempo transcurrido desde el inicio del incidente hasta el descubrimiento.
   - ✓ Tiempo transcurrido desde la evaluación inicial de impacto hasta cada etapa del manejo del incidente.
   - ✓ Tiempo que se tomó el equipo de respuesta en responder el reporte inicial del incidente.
   - ✓ Tiempo que tomó en reportar el incidente a la administración o a entidades externas.

c) **Evaluación de objetivos de cada incidente:** Este indicador determina que tan efectivas resultaron las acciones tomadas en cuanto a:
   - ✓ Revisión de logs, formularios, reportes u otra información del incidente para establecer políticas y procedimientos de respuesta del incidente.
   - ✓ Identificar cuáles fueron los indicadores de los incidentes almacenados para determinar el nivel efectividad de registro de identificación de este.
   - ✓ Determinar si el incidente causaría daño antes de ser detectado.
   - ✓ Determinar si la causa del incidente fue detectada, el vector de ataque, vulnerabilidades explotadas, etc.
   - ✓ Determinar si es un incidente recurrente.
   - ✓ Cálculo estimado del daño económico potencial que puede causar cada incidente.
   - ✓ Medir la diferencia entre la evaluación de impacto inicial y la evaluación de impacto final.

INDICADOR	DESCRIPCIÓN	FÓRMULA	FRECUENCIA
Cantidad de incidentes.	Cantidad total de los incidentes registrados en el período evaluado, divididos según su categoría.	$No.\,total\ de\ incidentes$	Mensual.
Incidentes repetidos.	Porcentaje de incidentes repetidos en el periodo evaluado.	$\%IncidentesRepetidos = \left(\frac{No.\,IncidentesRepetidos}{No.\,TotalIncidentes}\right) x100$	Trimestral
Incidentes solucionados.	Porcentaje de incidentes que fueron solucionados o cerrados durante el periodo evaluado.	$\%IncidentesSolucionados = \left(\frac{No.\,IncidentesSolucionados}{No.\,TotalIncidentes}\right) x100$	Mensual.
Incidentes críticos solucionados.	Porcentaje de incidentes que son considerados como críticos que fueron solucionados o cerrados durante el periodo evaluado.	$\%IncidentesSolucionadosCríticos = \left(\frac{No.\,Inc.\,Soluc.\,Críticos}{No.\,TotalIncidentes}\right) x100$	Mensual.
Incidentes pendientes.	Porcentaje de incidentes pendientes de solucionar durante el periodo de tiempo evaluado. Sin importar la fecha de registro del incidente.	$\%IncidentesPendientes = \left(\frac{No.\,IncidentesPendientes}{No.\,TotalIncidentes}\right) x100$	Mensual.

INDICADOR	DESCRIPCIÓN	FÓRMULA	FRECUENCIA
Incidentes críticos pendientes.	Porcentaje de incidentes considerados como críticos pendientes de solucionar durante el periodo de tiempo evaluado. Sin importar la fecha de registro del incidente.	$\%IncidentesPendientesCríticos = \left(\frac{No.Inc.Pend.Críticos}{No.TotalIncidentes}\right)x100$	Mensual.
Tiempo promedio de resolución.	Tiempo promedio de resolución de los incidentes solucionados en el periodo de tiempo evaluado.	$TiempoPromedio = \frac{\sum TiempoResol.Inc.Solucionados}{No.IncidentesSolucionados}$	Mensual.

Tabla 14. Definición de métricas base para el Centro de Operaciones de Seguridad (SOC)

El Consejo de Aseguramiento de la Calidad de la Educación Superior debe realizar auditorías de manera periódica sobre los procesos que lleva a cabo el Centro de Operaciones de Seguridad (SOC) que permitan identificar problemas o deficiencias que necesiten ser corregidas. Las auditorías internas y/o externas deberían centrarse en la revisión como mínimo de lo que se detalla a continuación:

- ✓ Políticas, procedimientos, planes relacionados con la respuesta ante incidentes.
- ✓ Herramientas y recursos que se utilizan durante la gestión del incidente.
- ✓ Modelo y estructura del equipo de respuesta.
- ✓ Educación y entrenamiento sobre el manejo de incidentes.
- ✓ Documentación y reportes de incidentes.
- ✓ Las medidas o métricas utilizadas para evaluar la efectividad del proceso.

4.6. IMPLEMENTACIÓN DEL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

4.6.1. TALENTO HUMANO PARA EL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

El talento humano es uno de los factores clave en la implementación de un Centro de Operaciones de Seguridad (SOC). El Consejo de Aseguramiento de la Calidad de la Educación Superior debe tener claramente definidos los perfiles y cargos que serán incorporados en la estructura orgánica funcional como parte del Centro de Operaciones de Seguridad (SOC).

Un error común que cometen las organizaciones al momento de implementar un proceso de respuesta a incidentes, cuando no se ha implementado un Centro de Operaciones de Seguridad (SOC), consiste en hacer uso del talento humano interno existente para que realicen la gestión de incidentes, sin embargo, no se encuentran dedicado exclusivamente a este proceso de seguridad además que no poseen el conocimiento y experiencia necesarios para desempeñar estas actividades.

En virtud de lo expuesto, la selección de talento humano es un paso fundamental incluso antes de pasar a la adquisición de herramientas de seguridad ya que en primea instancia se requiere contar con personal competente que pueda administrar las herramientas, debido a que son ellos los que las entenderán y usarán a diario, sin dejar de lado que todos los procesos de seguridad de la información que la institución ejecute sean realizados correcta y efectivamente.

Para que el Consejo de Aseguramiento de la Calidad de la Educación Superior pueda definir de manera correcta este requerimiento debe tener en cuenta lo que se detalla a continuación:

- ✓ Los roles o cargos que se utilizarán dentro del Centro de Operaciones de Seguridad (SOC).
- ✓ Las responsabilidades de cada rol que tendrán que definirse.
- ✓ Cantidad de personas que integraran el equipo de trabajo del Centro de Operaciones de Seguridad (SOC).

- ✓ El conjunto de habilidades que se busca.

Un Centro de Operaciones de Seguridad (SOC) debe constituirse como un área independiente del resto de áreas administrativas dentro del Consejo de Aseguramiento de la Calidad de la Educación Superior. Esto se debe a que esta área será la encargada de monitorear y supervisar las actividades de todas las áreas de institución. Desde el punto de vista de la estructura orgánica lo podemos definir bajo el siguiente esquema:

Ilustración 14. Estructura orgánica propuesta para el Centro de Operaciones de Seguridad (SOC)

En esta propuesta de implementación a continuación se describen roles que podrían utilizarse en el Consejo de Aseguramiento de la Calidad de la Educación Superior como aquellos roles más comúnmente utilizados en la actualidad dentro de un Centro de Operaciones de Seguridad (SOC).

4.6.1.1. DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN

El rol del Director de Seguridad de la Información dentro del Consejo de Aseguramiento de la Calidad de la Educación Superior constituye la autoridad máxima en cuanto a seguridad de la información. Esta persona es la responsable de definir toda la postura de seguridad de la institución. Sus actividades se encuentran enfocadas a planear estrategias, programas, políticas y procedimientos para proteger los activos de la organización. Dependiendo del organigrama institucional el CISO debe reportar directamente a la Máxima Autoridad de la institución, por lo cual es él quien transmite las necesidades e intereses del equipo de seguridad a la alta dirección de la institución. Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

RESPONSABILIDADES	CONOCIMIENTOS
✓ Supervisa el programa completo de seguridad. ✓ Desarrolla estrategias generales de seguridad. ✓ Comunica la importancia de la seguridad al equipo ejecutivo de la organización. ✓ Alinea los objetivos de la organización con los de seguridad. ✓ Supervisa los requerimientos de cumplimiento de diferentes entidades certificadoras. ✓ Define el plan de continuidad de negocio. ✓ Desarrolla el plan para evitar la pérdida de información y prevención de fraude. ✓ Administración del presupuesto para gastos de seguridad.	✓ Habilidad para manejar personal. ✓ Tener conocimientos técnicos. ✓ Comprender las implicaciones del negocio. ✓ Tener una extensa experiencia en seguridad y/o manejo de operaciones de tecnologías de la información. ✓ Administración de sistemas operativos como Linux, Windows, Mac, etc. ✓ Conocimientos en lenguajes de programación, como Python, Ruby, PHP, C#, Java, entre otros. ✓ Capacidad para investigar y llegar a la causa raíz de los incidentes. ✓ Trabajo bajo presión.

RESPONSABILIDADES	CONOCIMIENTOS
✓ Maneja asuntos de privacidad.	✓ Habilidades de hacker de sombrero blanco. ✓ Conocimientos o certificaciones de seguridad de la información.

Tabla 15. Rol del Director de Seguridad de la Información

4.6.1.2. JEFE DE CENTRO DE OPERACIONES DE SEGURIDAD (CSO)

Dentro de un Centro de Operaciones de Seguridad (SOC) esta persona se encarga de liderar el Centro de Operaciones de Seguridad (SOC) y al equipo de seguridad que trabaja junto a él. Además, debe tener una visión clara al momento de diseñar, contratar y/o construir procesos relacionados con la seguridad de la información. La persona que desempeñe este rol debe tener una experiencia significativa con el manejo de equipos de seguridad y tener la habilidad de proveer tanto orientación técnica como supervisión de tipo gerencial. Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

RESPONSABILIDADES	CONOCIMIENTOS
✓ Supervisar todas las actividades del Centro de Operaciones de Seguridad (SOC). ✓ Proveer visión y estrategia para el equipo de trabajo, procesos y tecnología. ✓ Contratar personal de seguridad y supervisar crecimiento profesional. ✓ Definir alertas y manejar procedimientos. ✓ Desarrollo de planes de respuesta ante incidentes. ✓ Desarrollo programa de manejo de vulnerabilidades. ✓ Analizar y optimizar flujos de trabajo incluyendo la automatización de estos. ✓ Comunicar necesidades de seguridad a las áreas interesadas de la organización. ✓ Manejo de presupuesto para gastos de seguridad. ✓ Desarrollo y ejecución de planes de comunicación de crisis al CISO y otros interesados. ✓ Generar reportes para ayudar a la auditoría de procesos. ✓ Definir métricas para medir el rendimiento de un Centro de Operaciones de Seguridad (SOC).	✓ Fuerte habilidad de liderazgo. ✓ Habilidades de comunicación con diferentes niveles jerárquicos. ✓ Administración de sistemas operativos como Linux, Windows, Mac, etc. ✓ Conocimientos en lenguajes de programación, como Python, Ruby, PHP, C#, Java, entre otros. ✓ Capacidad para investigar y llegar a la causa raíz de los incidentes. ✓ Trabajo bajo presión. ✓ Habilidades de hacker de sombrero blanco. ✓ Conocimientos o certificaciones de seguridad de la información.

Tabla 16. Rol del Jefe del Centro de Operaciones de Seguridad (SOC)

4.6.1.3. ESPECIALISTA DE SEGURIDAD

Dentro de un Centro de Operaciones de Seguridad (SOC) los especialistas de seguridad realizan pruebas complejas de penetración y análisis de vulnerabilidades y utilizar herramientas relacionadas con estas actividades. Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

RESPONSABILIDADES	CONOCIMIENTOS
✓ Ejecutar escaneos de vulnerabilidad en los activos informáticos de la organización de forma periódica.	✓ Utilizar herramientas para visualización de data. ✓ Experiencia en uso de herramientas para escaneo de vulnerabilidades y pruebas de penetración.

RESPONSABILIDADES	CONOCIMIENTOS
✓ Realizar pruebas de penetración a las redes de la organización de forma periódica y detectar puntos vulnerables. ✓ Generar informes de las pruebas de seguridad que se realicen. ✓ Utilizando inteligencia en amenazas, identificar amenazas ocultas que no se hayan identificado en revisiones generales. ✓ Pruebas de penetración en sistemas de producción para validar la resiliencia e identificar puntos débiles a mitigar. ✓ Recomendar la optimización de herramientas de monitoreo de seguridad basadas en la identificación de amenazas.	✓ Administración de sistemas operativos como Linux, Windows, Mac, etc. ✓ Conocimientos en lenguajes de programación, como Python, Ruby, PHP, C#, Java, entre otros. ✓ Capacidad para investigar y llegar a la causa raíz de los incidentes. ✓ Trabajo bajo presión. ✓ Habilidades de hacker de sombrero blanco. ✓ Conocimientos o certificaciones de seguridad de la información.

Tabla 17. Rol del Especialista de Seguridad

4.6.1.4. INGENIERO DE SEGURIDAD

Dentro de un Centro de Operaciones de Seguridad (SOC) los ingenieros de seguridad centran sus actividades en la construcción de arquitecturas de seguridad e ingeniería en seguridad de sistemas, sin dejar de lado la documentación de requerimientos, procedimientos y protocolos de las arquitecturas y herramientas de seguridad que implementen. De manera frecuente coordinan acciones con el equipo de desarrollo para poder crear soluciones seguras y certificar puestas en producción de los sistemas. Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

RESPONSABILIDADES	CONOCIMIENTOS
✓ Crear requerimientos de seguridad para los sistemas y documentación de estos. ✓ Definir y documentar procedimientos y protocolos de seguridad que se utilicen dentro de la organización. ✓ Configuración y soporte de la infraestructura de seguridad de la institución. ✓ Implementar herramientas de seguridad y dar soporte a las mismas. ✓ Recomendar mejoras de herramientas de seguridad. ✓ Crear, probar y/o implementar planes de recuperación ante desastres de redes de telecomunicaciones. ✓ Automatización de procesos entre herramientas de seguridad. ✓ Comunicación de incidentes de seguridad a las áreas interesadas de la organización. ✓ Reportar aseguramientos y recomendaciones de mejora a otras áreas.	✓ Conocimientos en diferentes tipos de herramientas de seguridad. ✓ Conocimientos en arquitectura de seguridad. ✓ Conocimientos en seguridad de telecomunicaciones y plataformas de tecnologías de la información. ✓ Habilidad analítica y agilidad en generación de reportes y métricas. ✓ Administración de sistemas operativos como Linux, Windows, Mac, etc. ✓ Conocimientos en lenguajes de programación, como Python, Ruby, PHP, C#, Java, entre otros. ✓ Capacidad para investigar y llegar a la causa raíz de los incidentes. ✓ Trabajo bajo presión. ✓ Habilidades de hacker de sombrero blanco. ✓ Conocimientos o certificaciones de seguridad de la información.

Tabla 18. Rol del Ingeniero de Seguridad

4.6.1.5. ANALISTAS DE SEGURIDAD

Dentro de un Centro de Operaciones de Seguridad (SOC) los analistas de seguridad son los encargados de detectar, investigar y responder ante los incidentes de seguridad que se presenten, también del monitoreo y administración de las herramientas relacionadas con estas actividades. De forma general estos cargos tienen horarios rotativos para poder ofrecer el

servicio de monitoreo 24x7.

4.6.1.5.1. ANALISTA DE SEGURIDAD SENIOR

Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

RESPONSABILIDADES	CONOCIMIENTOS
✓ Revisar y analizar tickets de atención para incidentes de seguridad. ✓ Poner en práctica métodos de inteligencia en amenazas emergentes para poder detectar sistemas afectados y el alcance del ataque. ✓ Planificar e implementar medidas de seguridad. ✓ Realizar verificaciones de riesgos de seguridad y testear procesamiento de data de los sistemas de información. ✓ Capacitar a personal técnico en procedimientos de seguridad de la información y redes.	✓ Administración de sistemas operativos como Linux, Windows, Mac, etc. ✓ Conocimientos en lenguajes de programación, como Python, Ruby, PHP, C#, Java, entre otros. ✓ Capacidad para investigar y llegar a la causa raíz de los incidentes. ✓ Trabajo bajo presión. ✓ Habilidades de hacker de sombrero blanco. ✓ Conocimientos o certificaciones de seguridad de la información.

Tabla 19. Rol del Analista de Seguridad Senior

4.6.1.5.2. ANALISTA DE SEGURIDAD JUNIOR

Entre las responsabilidades y conjunto de habilidades, se nombra las siguientes:

RESPONSABILIDADES	CONOCIMIENTOS
✓ Monitoreo y priorización de alertas. ✓ Creación de alertas de monitoreo. ✓ Creación de tickets de atención para incidentes de seguridad. ✓ Manejo y configuración de herramientas de seguridad y monitoreo. ✓ Investigación y respuesta ante incidentes de seguridad.	✓ Administración de sistemas operativos como Linux, Windows, Mac, etc. ✓ Conocimientos en lenguajes de programación, como Python, Ruby, PHP, C#, Java, entre otros. ✓ Conocimientos o certificaciones de seguridad de la información.

Tabla 20. Rol del Analista de Seguridad Junior

4.6.2. PROCESOS PARA EL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

El segundo factor de importancia para un Centro de Operaciones de Seguridad tiene relación con el diseño y definición de procesos para la detección y gestión de los incidentes de seguridad de la información de tal manera que se puedan estandarizar todas las actividades que se realizan en la institución y de esta manera evitar que aquellas tareas que son consideradas claves terminen siendo excluidas por la falta de un trabajo estructurado y documentado.

El enfoque basado en procesos según lo establece el conjunto de normas ISO 9000 indica que las organizaciones alcanzan los resultados deseados de manera más eficiente cuando las actividades y los recursos son gestionados como procesos. Cuando se definen los procesos adecuadamente la institución estará en capacidad de obtener los resultados deseados siempre que haya considerado lo siguiente:

- ✓ Se han definido las actividades y responsabilidades que integran el proceso.
- ✓ Se han identificado las relaciones con otros procesos.
- ✓ Se realiza análisis y mediciones de los resultados para verificar la capacidad y eficacia del proceso.
- ✓ Se centran en los recursos y métodos que permitan la mejora del proceso.

El Consejo de Aseguramiento de la Calidad de la Educación Superior debe tener procesos bien

definidos. En este sentido el Centro de Operaciones de Seguridad (SOC) necesita documentar y comunicar procesos efectivamente e implementar mecanismos de control de cambios para poder actualizar rápidamente los procesos cuando surjan oportunidades de mejora.

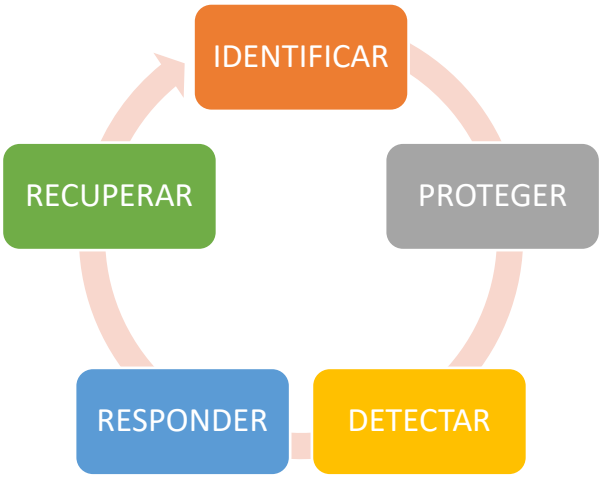

Ilustración 15. Marco de ciberseguridad del NIST

De igual manera un Centro de Operaciones de Seguridad (SOC) requiere la creación de procesos con la suficiente amplitud y profundidad que permita atender adecuadamente el universo de posibles escenarios de incidente y proveer guía detallada para la respuesta. El Centro de Operaciones de Seguridad (SOC) necesitará definir e implementar estos procesos en colaboración con las áreas administrativas relacionadas. Para ello, se definen las principales recomendaciones de implementación y gestión del SOC, entre las que se pueden mencionar las siguientes:

- ✓ Definición de hardware y software mínimo requerido.
- ✓ Establecimiento de tiempos de atención y niveles de servicio.
- ✓ Definición de herramientas de monitoreo (SIEM).
- ✓ Definición de la estructura funcional del Centro de Operaciones de Seguridad (SOC).
- ✓ Implementar niveles de escalación que permitan distribuir las actividades a realizar.
- ✓ Implementar los procedimientos capaces de permitir una pronta detección y respuesta a incidentes de seguridad.

Los procesos pueden definirse en esquemas de ciclos repetitivos que pasen por los diferentes niveles de atención que se encuentren establecidos dentro del Centro de Operaciones de Seguridad (SOC). Esto sumado a la correcta utilización del flujo de trabajo para la gestión de incidentes ayudará a la institución a que los recursos invertidos sean utilizados eficientemente.

4.6.2.1. PROCESOS

Los procesos se encuentran orientados a optimizar la interacción de las personas y las tecnologías en las operaciones de seguridad de la información, basándose en inteligencia, con lo cual se pretende lograr una reducción en el tiempo promedio de resolución de incidentes. Como mínimo el Consejo de Aseguramiento de la Calidad de la Educación Superior deberá disponer de los procesos que se indican a continuación:

a) **Proceso de resolución:** Este proceso comprende el proceso de gestión de incidentes y de gestión de problemas.
b) **Proceso de gestión de incidentes:** Este proceso tiene como objetivo resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz

posible. Su enfoque radica en la restauración del servicio sin buscar y analizar las causas que lo ocasionaron.

c) **Proceso de gestión de problemas:** Este proceso ayuda a la gestión de incidentes informando sobre errores conocidos y posibles soluciones. Su enfoque radica en la investigación y análisis de las causas originadas por una alteración de los servicios de tecnologías de la información. Este proceso es reactivo cuando realizamos el análisis de los incidentes ocurridos a fin de determinar su causa y proponer soluciones; y, proactivo cuando se realiza monitoreo de la infraestructura de tecnologías de la información a fin de prevenir incidentes.

4.6.2.2. PROCEDIMIENTOS

Los procedimientos son aquellas actividades organizadas que se deben seguir para llegar a la ejecución de determinado proceso. Se detallan a continuación los procedimientos mínimos que el Consejo de Aseguramiento de la Calidad de la Educación Superior debería establecer:

a) **Procedimiento de gestión de incidentes:** Este procedimiento tiene como objetivo resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible. El procedimiento tiene como disparador las solicitudes generadas por parte de los usuarios a través de correo electrónico, eventos reportados de mesa de ayuda o eventos reportados por la plataforma de correlación de eventos SIEM. Se debe evaluar si se trata de un evento falso positivo o de un incidente. Los eventos deben ser solucionados por el analista de seguridad y los incidentes deben ser escalados al ingeniero de seguridad para que en conjunto con el personal del Centro de Operaciones de Seguridad (SOC) deben garantizar la continuidad del servicio.

b) **Procedimiento de gestión de problemas:** Este procedimiento tiene como objetivo analizar la causa y solucionar los incidentes mayores y problemas sobre los servicios de tecnologías de la información para garantizar la continuidad del servicio minimizando el impacto a los usuarios. El procedimiento tiene como disparador la identificación y registro de un problema y finaliza con el cierre de este.

4.6.2.3. MATRIZ DE RIESGOS

Para el Consejo de Aseguramiento de la Calidad de la Educación Superior debe constituir de importancia el contar con herramientas y metodologías que garanticen la correcta evaluación de los riesgos a los cuales pueden encontrarse sometidos los procesos e identificar los procedimientos de control mediante los cuales se puede medir el desempeño del entorno organizacional.

Para que se pueda identificar los eventos y/o incidentes que van a ser monitoreados por el Centro de Operaciones de Seguridad (SOC) será necesario definir una estrategia a partir del análisis de riesgos mediante el cual se logre:

- ✓ Determinar qué es necesario proteger.
- ✓ Determinar cuál es la infraestructura tecnológica que se trata de proteger.
- ✓ Identificar las amenazas y la probabilidad de ocurrencia.
- ✓ Identificar e implementar los controles requeridos para proteger los activos de información y reducir el riesgo.
- ✓ Revisar continuamente el proceso cada vez que se detecte una nueva vulnerabilidad.

4.6.2.3.1. ANÁLISIS DEL RIESGO

El objetivo del análisis de riesgos es el de establecer una valoración y priorización de los riesgos con base en la información levantada, con el fin de clasificar los riesgos y proveer información para establecer el nivel de riesgo y las acciones que se van a implementar en la institución.

a) **Criterios de probabilidad:** La probabilidad hace referencia a la posibilidad de que suceda el evento (situación, suceso o acontecimiento) en un periodo determinado y para su calificación se tienen en cuenta los valores establecidos.
b) **Criterios de impacto:** El impacto se analiza a partir de las consecuencias que puede ocasionar la materialización de la amenaza identificada y para su calificación se tienen en cuenta los criterios relacionados.

Una vez definidos los criterios de probabilidad e impacto, se identifican los activos de información a ser protegidos y se registran las amenazas y vulnerabilidades asociadas a fin de determinar el nivel de riesgo antes de controles.

4.6.2.3.2. ACTIVOS DE INFORMACIÓN QUE REPORTAN AL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

Considerando que el Centro de Operaciones de Seguridad (SOC) es el área encargada de la ejecución del proceso de resolución de incidentes y problemas se debe realizar la identificación de los activos de información a proteger en el Consejo de Aseguramiento de la Calidad de la Educación Superior entre los cuales tenemos:

a) **Físico (Hardware):** Son aquellos activos que tienen relación con los servidores, estaciones de trabajo, computadoras personales, portátiles, soportes magnéticos y ópticos, medios removibles, redes de diferente tipo, líneas de comunicación, módems, firewalls, switches, routers entre otros.
b) **Software:** Son aquellos activos que tienen relación con los códigos fuentes, programas ejecutables, utilitarios, de diagnósticos, de comunicaciones, sistemas operativos entre otros.
c) **Servicios:** Son aquellos activos relacionados con los servicios de computación y comunicación, servicios de energía y acondicionamiento de aire.
d) **Activos Físicos:** Son aquellos activos relacionados con las edificaciones y/o locaciones donde se encuentran ubicados los activos de información, tipos de construcción y estructura, puntos de acceso, visibilidad desde el exterior entre otras.
e) **Personas:** Son aquellos activos relacionados con los usuarios, operadores, proveedores, programadores, personal de mantenimiento, entre otros.
f) **Información:** Son aquellos activos relacionados con las bases de datos, archivos de datos, contratos y acuerdos, materiales de capacitación, procedimientos operacionales y de soporte, acuerdo de contingencia, información de auditoría entre otras.

4.6.2.3.3. VALORACIÓN DE LOS RIESGOS

La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo (Muy Alto, Alto, Medio, Bajo) con los resultados de la evaluación de los controles existentes para cada riesgo. Esto debe realizarse con el propósito de definir un nuevo nivel de riesgo lo cual permitirá establecer prioridades para su manejo.

4.6.2.3.4. TRATAMIENTO DEL RIESGO

Después de obtener los niveles de riesgo para cada activo de información se deben definir si estos son aceptables o no. Para el caso de que estos no hayan sido definidos, se deberá establecer el mecanismo para el tratamiento de estos. Se requiere seleccionar y aplicar medidas que sean adecuadas para manejar o modificar el riesgo, para lo cual se tienen las siguientes opciones:

a) **Evitar el riesgo:** Son las acciones encaminadas a prevenir la materialización del riesgo. Se logra cuando los procesos generan cambios sustanciales para el mejoramiento, rediseño o eliminación, que son resultado de unos adecuados controles y acciones emprendidas.

b) **Reducir el riesgo:** Son las acciones encaminadas a disminuir la probabilidad (medidas de prevención) o el impacto (medidas de protección). Si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles, se consigue mediante la optimización de los procedimientos y la implementación de controles.
c) **Compartir el riesgo:** Son las acciones encaminadas a buscar respaldo y compartir con otro parte del riesgo, reduce su efecto a través del traspaso de las pérdidas a otros procesos o dependencias.
d) **Transferir el riesgo:** Son las acciones encaminadas a eliminar el riesgo mediante el cambio de responsabilidad o carga por las pérdidas a otra entidad, mediante legislación, contrato, convenios u otros medios.
e) **Asumir un riesgo:** Luego de que el riesgo ha sido reducido transferido puede quedar un riesgo residual que se mantiene, en este caso el responsable del proceso simplemente acepta la pérdida residual probable.
f) **Planes de contingencia:** Constituye parte importante del plan de manejo de riesgos y contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de dar continuidad a los objetivos de la institución.

Una vez que se haya logrado definir la opción de tratamiento del riesgo (evitar, reducir, compartir, transferir, asumir) se deben establecer nuevos controles que permitan eliminar las causas del riesgo.

4.6.3. TECNOLOGÍA PARA EL CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

El tercer factor de relevancia para un Centro de Operaciones de Seguridad (SOC) constituye la tecnología la cual se encuentra enfocada a las herramientas y recursos informáticos que se utilizarán para el desarrollo de las actividades diarias relacionadas con la gestión de incidentes de seguridad.

A menudo las organizaciones realizan un esfuerzo importante en aras de desplegar tecnologías de la información y comunicaciones con la finalidad de atender los temas críticos relacionados con la seguridad de la información. Algo que generalmente ocurre en las organizaciones es que los proyectos de tecnologías de la información y comunicaciones normalmente son medidos por el éxito en la implementación más que por el valor que la tecnología le termina aportando a la organización.

Si la organización requiere obtener el mayor valor de las soluciones tecnológicas implementadas deberá coordinar también los esfuerzos a través de iniciativas estratégicas que establezcan la gobernanza apropiada, procesos, entrenamiento y concientización.

Un Centro de Operaciones de Seguridad (SOC) debe encontrarse equipado con una suite de productos tecnológicos que provean la visibilidad adecuada hacia el entorno que contribuya a la postura de seguridad de la información de la organización. Una vez que hemos seleccionado la tecnología correcta, el Centro de Operaciones de Seguridad (SOC) necesita asignar un equipo de seguridad debidamente calificado que pueda identificar exactamente cuáles son las herramientas adecuadas para la realización de sus actividades. Este equipo será responsable de evaluar los requerimientos de integración del sistema, evaluar la interoperabilidad con la infraestructura existente y realizar demostraciones y pruebas de las soluciones.

Entre las herramientas requeridas podemos hacer uso de aquellas destinadas a la detección y prevención de intrusiones, soluciones SIEM, herramientas de administración de amenazas y vulnerabilidades, tecnologías de filtrado, herramientas de prevención de pérdida de datos, soluciones de inspección de tráfico y plataformas de análisis de datos y reportes.

4.6.3.1. FIREWALL

Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall. Los firewalls de red son dispositivos o sistemas que controlan el flujo de tráfico entre redes que emplean diferentes posturas de seguridad (Microsoft, 2016).

Un firewall nos es de utilidad en el sentido que impide que personas externas hackers o software malintencionado obtengan acceso a los equipos de la organización a través de una red o de Internet. También nos ayuda a impedir que el equipo envíe software malintencionado a otros equipos dentro de la red de datos de la organización.

4.6.3.2. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)

La detección de intrusos hace referencia al proceso que consiste en monitorear los eventos ocurridos en un sistema de cómputo o red y analizarlos en busca de señales de posibles incidentes, los cuales son violaciones o inminentes amenazas de violación de políticas de seguridad de cómputo, políticas de uso aceptable o prácticas de seguridad estándar (González, 2013).

Conceptualmente un sistema de detección de Intrusos (IDS) automatiza el proceso de detección de intrusos. Una vez que se detecta actividad maliciosa, el IDS envía mensajes de alerta a una consola central de monitoreo de modo que la acción pueda ser tomada por el administrador de la red. Las alertas son enviadas en forma de mensajes de syslog o alertas vía correo electrónico.

Los IDS se encuentran disponibles en el mercado como dispositivos basados en hardware, así como en agentes o sensores basados en software. Un IDS provee las siguientes ventajas para un administrador de la red:

- ✓ Exponer las vulnerabilidades de seguridad presentes en la red.
- ✓ Proveer monitoreo y alertas 24x7, liberando de esta forma tiempo y recursos para el administrador de la red.
- ✓ Proveer registros para análisis forense de ataques e intrusiones.

4.6.3.3. SISTEMA DE PREVENCIÓN DE INSTRUSOS (IPS)

Al referirnos a un sistema de prevención de intrusos hacemos mención del software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad constituye otro tipo de control de acceso, más cercano a las tecnologías de firewall.

Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos.

4.6.3.4. SERVIDORES

Cuando mencionamos un servidor nos referimos a una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora (hardware). La ventaja de montar un servidor en computadoras dedicadas es la seguridad.

Los servidores operan a través de una arquitectura cliente – servidor. Los servidores en si son programas de computadora en ejecución que atienden las peticiones de otros programas, los clientes. Por lo tanto, el servidor realiza otras tareas para beneficio de los clientes. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red, pero también pueden acceder a él a través de la computadora donde está funcionando o a través del Internet.

En el mercado existen diferentes tipos de servidores por lo que a continuación describiremos los más comunes:

a) **Plataformas de Servidor:** Usado comúnmente como sinónimo de sistema operativo, la plataforma es el hardware o software subyacentes para un sistema, es decir, el motor que dirige el servidor.
b) **Servidores de Aplicaciones:** Designados a veces como un tipo de middleware (software que conecta dos aplicaciones), los servidores de aplicaciones ocupan una gran parte del territorio entre los servidores de bases de datos y el usuario, y a menudo los interconectan.
c) **Servidores FTP:** Uno de los servicios más antiguos de Internet que permite mover uno o más archivos con seguridad entre distintos computadores proporcionando seguridad y organización de los archivos, así como control de la transferencia. Servidores de Correo: Su implementación es tan crucial como los servidores web, los servidores de correo mueven y almacenan el correo electrónico a través de las redes corporativas LAN y WAN y sin dudad a través de Internet.
d) **Servidores Proxy:** Los servidores proxy se sitúan entre un programa del cliente (típicamente un navegador) y un servidor externo (típicamente otro servidor web) para filtrar peticiones, mejorar el funcionamiento y compartir conexiones.
e) **Servidores Telnet:** Un servidor telnet permite a los usuarios entrar en un computador remoto y realizar tareas como si estuviera trabajando directamente en ese computador.
f) **Servidores Web:** Un servidor web sirve contenido estático a un navegador, carga un archivo y lo sirve a través de la red al navegador de un usuario. Este intercambio es mediado por el navegador y el servidor que hablan el uno con el otro mediante HTTP.

4.6.3.5. HERRAMIENTAS TECNÓLOGICAS DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC)

A continuación, haremos una descripción breve de las herramientas que resulten útiles para el personal de un Centro de Operaciones de Seguridad (SOC) para el desarrollo de las actividades.

4.6.3.5.1. SIEM ADMINISTRACIÓN Y ANÁLISIS DE LOGS

Los logs se consideran como la fuente de información de mayor relevancia por lo cual es necesario que el Consejo de Aseguramiento de la Calidad de la Educación Superior cuente con herramientas que ayuden a recolectar, centralizar e interpretar el contenido para que de esta forma la acción de correlacionar eventos se vuelva más sencilla de ejecutar.

Las herramientas SIEM (Security Information and Event Management) ayudan en la administración de logs y en el mercado difieren según el costo y la funcionalidad de estas. En la actualidad las herramientas más utilizadas son las siguientes:

- ✓ Splunk Enterprise Security (ES).
- ✓ LogRhythm SIEM.
- ✓ AlienVault Unified Security Management (USM).
- ✓ Micro Focus ArcSight.
- ✓ Micro Focus Sentinel Enterprise.
- ✓ McAfee Enterprise Security Manager (ESM).
- ✓ Trustwave SIEM Enterprise and Log Management Enterprise.
- ✓ IBM Security QRadar.
- ✓ RSA NetWitness Suite.
- ✓ SolarWinds Log & Event Manager.

4.6.3.5.2. SISTEMAS DE DETECCIÓN DE INTRUSOS

Este tipo de herramientas a menudo interactúan con firmas conocidas de ataques o líneas base

que ayudan a identificar el comportamiento sospechoso lo cual deriva en la generación de alertas que posteriormente deberá ser revisada por el equipo de seguridad.

Los sistemas de detección de intrusos se encuentran basados en hosts los cuales monitorean servidores y en red los cuales monitorean toda la red de datos. En la actualidad las herramientas más utilizadas son las siguientes:

- ✓ McAfee NSP.
- ✓ Trend Micro TippingPoint.
- ✓ Hillstone NIPS.
- ✓ Darktrace Enterprise Immune System.
- ✓ NSFocus NGIPS.
- ✓ H3C SecBlade IPS.
- ✓ Huawei NIP.
- ✓ Entrust IoTrust Identity and Data Security.
- ✓ Cisco Firepower NGIPS.
- ✓ Snort.
- ✓ Suricata.
- ✓ BroIDS.
- ✓ OSSEC.

4.6.3.5.3. ANALIZADOR DE FLUJO DE RED

Estas herramientas pueden monitorear el tráfico actual de una red, de esta manera se podría hacer verificaciones de amenazas específicas o protocolos utilizados en la red. En la actualidad las herramientas más utilizadas son las siguientes:

- ✓ Ntop.
- ✓ NfSen.
- ✓ Nfdump.

4.6.3.5.4. ESCÁNERES DE VULNERABILIDADES

Estas herramientas permiten encontrar los puntos débiles de una plataforma para que puedan ser remediados y evitar que posibles amenazas se materialicen. De igual forma pueden ser utilizadas para aplicar parches de seguridad en ciertos recursos, además sirven como guía para la solución de ciertos tipos de vulnerabilidades. En la actualidad las herramientas más utilizadas son las siguientes:

- ✓ Comodo HackerProof.
- ✓ OpenVAS.
- ✓ Nexpose Community.
- ✓ Nikto.
- ✓ Tripwire IP360.
- ✓ Aircrack.
- ✓ Wireshark.
- ✓ Nessus Professional.
- ✓ Retina CS Community.
- ✓ Microsoft Baseline Security Analyzer (MBSA).

4.6.3.5.5. MONITOREO DE DISPONIBILIDAD

Estas herramientas se enfocan en monitorear la disponibilidad de un servicio o aplicación, debido a que una de las primeras señales de un incidente es el mal funcionamiento de un recurso. este tipo de herramientas ayudan a identificar más rápido un problema. En la actualidad una de las herramientas más utilizadas es la siguiente:

- ✓ Nagios.

4.6.3.5.6. WEB PROXY

El web proxy es útil en la gestión de incidentes debido a que registran las conexiones que se han realizado, de esta manera se puede obtener más información sobre el ataque. En la actualidad las herramientas más utilizadas son las siguientes:

- ✓ Forcepoint Web Security.
- ✓ McAfee Web Protection.
- ✓ Barracuda Web Filter.
- ✓ TitanHQ WebTitan.
- ✓ FortiCache.
- ✓ EdgeWave St. Bernard.
- ✓ M86 Web Content Filtering.
- ✓ Squid Proxy.
- ✓ IPFire.

4.6.3.5.7. INVENTARIO DE ACTIVOS

Para que se puedan priorizar los eventos e incidentes se hace necesario que los responsables de la gestión de seguridad tengan el conocimiento certero y a detalle de los activos más críticos dentro de la institución. Para la consecución de esto se necesita un proceso de identificación y evaluación de los activos que se posee, por lo que contar con una herramienta en la que se pueda registrar los activos de la institución, el dueño del activo y el nivel de criticidad se constituyen en factores que ayudan a priorizar de manera correcta los eventos. En la actualidad las herramientas más utilizadas son las siguientes:

- ✓ Freshservice.
- ✓ ManageEngine ServiceDesk.
- ✓ ServiceNow Asset Management.
- ✓ Infor EAM.
- ✓ Lansweeper.
- ✓ BelManage.
- ✓ Samanage.
- ✓ ChangeGear.
- ✓ Asset Track.
- ✓ OCS Inventory.

4.6.3.5.8. INTELIGENCIA DE AMENAZAS

Las herramientas de inteligencia de amenazas proveen una visión global sobre las amenazas actuales como indicadores de compromiso, direcciones IP con mala reputación, dominios, hash de archivos, entre otros. Esto ayudaría a comprender a la institución los comportamientos que pueden estar afectando a sus propias redes.

Las plataformas de inteligencia de amenazas pueden incorporar una o varias fuentes de datos y someterlos a un análisis detallado para poder aislar patrones inusuales en los sistemas y extraer otros datos valiosos. En la actualidad las herramientas más utilizadas son las siguientes:

- ✓ IBM XForce Exchange.
- ✓ Anomali ThreatStream.
- ✓ Palo Alto Network AutoFocus.
- ✓ RSA NetWitness Suite.
- ✓ LogRhythm Threat Lifecycle Management (TLM) Platform.
- ✓ FireEye iSIGHT Threat Intelligence.
- ✓ LookingGlass Cyber Solutions.

- ✓ AlienVault Unifed Security Management (USM).

4.6.3.5.9. HERRAMIENTAS FORENSES PARA CAPTURA DE INFORMACIÓN Y RESPUESTA DE INCIDENTES

Este tipo de herramientas engloba todas las actividades forenses para poder identificar, preservar, recuperar, analizar y presentar evidencias y hechos sobre la información de la organización. Estas herramientas se encuentran diseñadas para poder crear un log de auditoría de todas las acciones realizadas y por ende también poseen la funcionalidad de cadena de custodia para el manejo de las evidencias. En la actualidad las herramientas más utilizadas son las siguientes:

- ✓ Sans Sift (SANS Invetigative Forensic Toolkit).
- ✓ CrowdStrike CrowdResponse.
- ✓ Volatility.
- ✓ The Sleuth Kit.
- ✓ FTK Imager.
- ✓ Caine.
- ✓ ExifTool.
- ✓ Free Hex Editor Neo.
- ✓ Bulk Extractor.
- ✓ PlainSight.
- ✓ LastActivity View.

4.6.3.5.10. HERRAMIENTAS DE RESPALDOS Y RECUPERACIÓN DE SISTEMAS

Estas herramientas se enfocan en realizar actividades de restauración de respaldos, aplicación de parches, restauración de servicios y aplicaciones, para poder volver a la funcionalidad normal después de la contención del incidente. En la actualidad las herramientas más utilizadas son las siguientes:

- ✓ Veeam Backup & Replication.
- ✓ Rubrik.
- ✓ IBM Spectrum Protect.
- ✓ Acronis Backup.
- ✓ Cohesity.
- ✓ Zero Virtual Replication.
- ✓ Veritas NetBackup.
- ✓ Micro Focus Data Protector.
- ✓ Reduxio.
- ✓ Commvault.

En resumen, si bien es cierto las herramientas técnicas son importantes, el despliegue de nuevas tecnologías simplemente porque a la organización le parece o le agrada al final del día puede terminar siendo costoso y poco efectivo. En este sentido los planes de tecnología ligados al Centro de Operaciones de Seguridad (SOC) deben siempre tomar en cuenta lo que al momento se encuentra disponible en la organización y que satisfaga las necesidades primordiales para de manera posterior mejorar y ampliar las capacidades actuales a través del despliegue de herramientas y tecnologías complementarias.

Cuando nos referimos al personal y los procesos estos suelen ser más complejos de alinear con un método de seguridad de la información basado en inteligencia que la tecnología en sí. Esto se debe a que el desarrollo, pruebas y nuevos procedimientos para la administración y respuesta a los incidentes de seguridad requiere de conocimientos especializados y tiempo. Así mismo existe una curva de aprendizaje a ser tomada en cuenta en la que el personal de operaciones de seguridad de la información llegue a conocer en detalle los procesos de negocio críticos de la

organización para plantear las estrategias óptimas para la defensa ante posibles ataques.

Es así como la manera en la que podamos realizar una optimización del personal, los procesos y la tecnología será diferente para cada Centro de Operaciones de Seguridad (SOC), ya que depende de las condiciones y necesidades únicas establecidas en cada organización.

CAPÍTULO V: CONCLUSIONES

5.1. CONCLUSIONES

En este Trabajo de Fin de Máster (TFM) se ha podido evidenciar la real importancia que en la actualidad tiene, para las organizaciones, un Centro de Operaciones de Seguridad (SOC) por cuanto nos permite controlar constantemente el estado de la seguridad lógica, monitorear en tiempo real las actividades que se realizan sobre los recursos tecnológicos del Consejo de Aseguramiento de la Calidad de la Educación Superior, así como las actividades que efectúan los usuarios encargados de la gestión y administración de los recursos y dispositivos de seguridad con el objetivo de prevenir que las amenazas externas accedan a la red interna de la Institución.

El hecho de no disponer de un estándar o norma que trate de manera exclusiva sobre las funciones o actividades que deben ser desarrolladas por el Centro de Operaciones de Seguridad (SOC), nos llevó a que realicemos el Trabajo de Fin de Máster (TFM) sobre la base de las buenas prácticas que han servido de referente en la actualidad. Se pudieron identificar aquellos aspectos primarios y secundarios que deben ser necesariamente considerados en el diseño de un Centro de Operaciones de Seguridad (SOC) y las operaciones de seguridad sobre las que pueden ser definidas las funciones y actividades a desempeñar dentro del Centro de Operaciones de Seguridad (SOC) del Consejo de Aseguramiento de la Calidad de la Educación Superior así como una visión general de todas aquellas herramientas que podrían ser utilizadas, sin descuidar en ningún momento uno de los aspectos más relevantes que constituye la gestión de respuesta ante incidentes de seguridad.

Un aspecto concluyente a destacar es que para la realización del Trabajo de Fin de Máster (TFM) y poder contextualizarlo dentro de la realidad ecuatoriana el hecho relevante fue la necesidad de profundizar en aquellos requisitos de seguridad solicitados por los entes de control (Ministerio de Telecomunicaciones y de la Sociedad de la Información, Contraloría General del Estado) del sector de la educación superior del Ecuador, a través de los cuales se pudo ir validando que existen diferentes actividades y controles que deben ser gestionados por un área independiente y especializada con personal capacitado y experiencia en gestión de seguridad de la información, como lo constituye un Centro de Operaciones de Seguridad (SOC). Se realizó una comparativa de determinados controles en cuanto a los requisitos de seguridad impuestos por los entes de control versus el estándar internacional ISO/IEC 27000, concluyendo que el Consejo de Aseguramiento de la Calidad de la Educación Superior aún tiene mucho trabajo que realizar para cubrir la totalidad de dominios del estándar y poder estar perfectamente alineado con una adecuada implementación de Sistema de Gestión de la Seguridad de la Información.

Para el Consejo de Aseguramiento de la Calidad de la Educación Superior el diseño aquí planteado constituye el primer hito que permita proteger los servicios críticos de la Institución. En este sentido, su posterior implementación debe identificar e integrar identificar las interrelaciones existentes entre las diferentes áreas de la organización de tal forma que se puedan identificar los impactos directos e indirectos que afecten la normal operación. Es así como la realidad actual de la mayoría de las organizaciones evidencia que, ante la presencia de un incidente de seguridad de la información que tenga afectación sobre alguno de los servicios críticos de la misma, no se cuente con los protocolos de respuesta adecuados que permitan a la organización saber cómo actuar para mitigar los riesgos presentados.

En la realidad se convierte en una situación poco probable que podamos llegar a implementar un Centro de Operaciones de Seguridad (SOC) que se encuentre en la capacidad de impedir la totalidad de las amenazas a las que el Consejo de Aseguramiento de la Calidad de la Educación Superior puede verse expuesto. Sin embargo, un punto de partida importante es el tener el diseño conceptual del Centro de Operaciones de Seguridad (SOC) que establezca procedimientos formales definidos sobre la base de las buenas prácticas, normas y estándares

aceptados internacionalmente; que posea para su operación con personal altamente especializado y capacitado en gestión de la seguridad de la información; y, sobre todo que llegue a implementar las mejores herramientas tecnológicas de seguridad que ayuden al Consejo de Aseguramiento de la Calidad de la Educación Superior a prevenir, identificar, controlar y monitorear posibles amenazas de seguridad; de tal forma que se puedan anticipar diferentes tipos de incidentes que se pudiesen llegar a presentar, identificar brechas de seguridad para tomar acciones mitigantes y sobre todo responder de forma ágil y efectiva ante los incidentes que se hayan suscitado.

5.2. DESARROLLO DEL TRABAJO DE FIN DE MÁSTER

En términos generales podemos mencionar con satisfacción absoluta que, pese a los inconvenientes presentados, en un año atípico y lleno de complejidades y obstáculos de toda índole, experimentados nivel mundial, se ha podido cumplir a cabalidad con la planificación que fuese definida inicialmente para la realización del Trabajo de Fin de Máster (TFM). Sin duda uno de los inconvenientes principales para la implementación del proyecto recae sobre la diversidad en cuanto a la información que existe al respecto, pero sobre manera a la poca información de implementaciones reales de Centros de Operaciones de Seguridad (SOC) en organizaciones similares al Consejo de Aseguramiento de la Calidad de la Educación Superior.

Es así como durante la ejecución del Trabajo de Fin de Máster (TFM) se llegó a comprender que era más provechoso el hecho de partir de la situación actual para de esta manera poder establecer las funciones, diseño e implementación, desde el punto de vista referencial, de un Centro de Operaciones de Seguridad (SOC) que mejor se adapte a las necesidades reales del Consejo de Aseguramiento de la Calidad de la Educación Superior.

Otro de los inconvenientes que hemos encontrado para la implementación del Centro de Operaciones de Seguridad (SOC) es la posibilidad de integración de los módulos requeridos para el normal funcionamiento de este, ya que de manera generalizada estos módulos funcionan de manera independiente y autónoma, a la vez que deben cumplir y no descuidar los requerimientos de disponibilidad, integridad y seguridad de los datos y sus medios de transmisión. Sin duda alguna, éste se constituye como uno de los mayores desafíos al implementar y operar un Centro de Operaciones de Seguridad (SOC) y es sobre lo que actualmente está llevando mayor tiempo y dedicación a investigaciones que permitan profundizar en este tema.

Sin embargo, una de las mayores dificultades es el nivel de detalle y desagregación con el que se puede presentar la información, pero hemos intentado presentar un modelo lo más cercano a la realidad del Consejo de Aseguramiento de la Calidad de la Educación Superior sin que esto signifique que se hubiese podido generar mucho más en cuanto a los niveles de detalle relacionados con el diseño. Es por esta razón que hemos hecho mención únicamente a las funciones principales que el Consejo de Aseguramiento de la Calidad de la Educación Superior ha de implementar. Debe indicarse también que aún quedan muchos aspectos que deben ser definidos al momento de la definición del diseño real (personas, procesos, tecnología). Los aspectos más detallados acerca de estos aspectos no han sido tratados a profundidad ya que los consideramos deberán ser tratados de manera posterior al modelado que en este Trabajo de Fin de Máster (TFM) hemos querido presentar.

Finalmente y con motivación se puede mencionar que uno de los inconvenientes que se han logrado sortear con el desarrollo del Trabajo de Fin de Máster (TFM) es que se ha podido crear conciencia en el Consejo de Aseguramiento de la Calidad de la Educación Superior sobre la necesidad de encaminar esfuerzos que ayuden a la integración, estandarización y uso de mejores prácticas a nivel mundial que permitan que el Centro de Operaciones de Seguridad (SOC) cumpla de manera eficaz con su función además de ayudar a cumplir con normativa legal y regulatoria vigente establecida en el Esquema Gubernamental de Seguridad de la Información.

5.3. TRABAJOS FUTUROS

Tal como se ha venido indicando, este Trabajo de Fin de Máster (TFM) ha planteado un diseño inicial para su posterior implementación real de un Centro de Operaciones de Seguridad (SOC) en el Consejo de Aseguramiento de la Calidad de la Educación Superior. Al no existir un estándar mundialmente aceptado en el que se precisen los detalles necesarios para la implementación en un entorno organizacional de educación superior hemos omitido algunos detalles de tal modo que hemos obtenido un modelo flexible que puede ser adaptado a diferentes organizaciones.

De este modo, en próximos trabajos se podría relatar la experiencia de la implementación real de este diseño en el Consejo de Aseguramiento de la Calidad de la Educación Superior, en el cual se expongan las distintas fases ejecutadas, así como las conclusiones y lecciones aprendidas durante este proceso. No obstante, al tratarse del Centro de Operaciones de Seguridad (SOC) de un proceso que involucra varias aristas tanto organizacionales como procedimentales, alguien podría considerar temas en concreto referentes a:

- ✓ Diseñar una política de seguridad de la información con la finalidad de asegurar el compromiso de toda la organización, desde la alta dirección hasta cualquier servidor.
- ✓ Diseñar estrategias de formación y de capacitación permanente en el ámbito de la seguridad de la información con carácter de obligatorio para todos los servidores y funcionarios del Consejo de Aseguramiento de la Calidad de la Educación Superior para garantizar que la información se encuentra debidamente protegida y resguardada.
- ✓ Diseñar el Centro de Operaciones de Seguridad (SOC) a partir de los procesos específicos establecidos en la versión más reciente de ITIL.
- ✓ Establecer una organización de roles para operar un Centro de Operaciones de Seguridad (SOC) en función del presente diseño y las mejores prácticas que aporten valor agregado en lo que se refiere a su aplicación e implementación en las Instituciones de Educación Superior en el Ecuador.
- ✓ Extender el presente estudio aportando métricas más precisas que permitan establecer si se tiene una operación exitosa del diseño o a su vez de la plataforma implementada del Centro de Operaciones de Seguridad (SOC) que permitan evaluar el cumplimiento de regulaciones.
- ✓ Diseñar el Centro de Operaciones de Seguridad (SOC) con mayor precisión y detalle basado en las mejores prácticas y su integración con otras normas y estándares como ISO y COBIT.

REFERENCIAS BIBLIOGRÁFICAS

Cisco Systems. (2015). Security Operations Center. Building, Operating, and Mantaining Your SOC. Indianapolis, Indiana, Estados Unidos: Cisco Press.

Comisión Europea. (5 de Julio de 2016). The Directive on security of network and information systems. Recuperado el Julio 18 de 2017, de ec.europa.eu: https://ec.europa.eu/digitalsingle-market/en/network-and-information-security-nis-directive

Electric Power Research Institute. (2013). Guidelines for Planning an Integrated Security Operations Center. Recuperado el 1 de Septiembre de 2016, de Metering.com: https://www.metering.com/wp-content/uploads/2014/02/EPRI-Planning-ISOCreport.pdf

EY. (Octubre de 2014). Security Operations Centers - helping you get ahead of cybercrime. Obtenido de Security Operations Centers - helping you get ahead of cybercrime: http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helpingyou-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-getahead-of-cybercrime.pdf

IBM Corporation. (Diciembre de 2013). Strategy considerations for building a security operations center. Obtenido de IBM Global Technology Services: https://www356.ibm.com/partnerworld/wps/servlet/download/DownloadServlet?id=OULVYbVhue7iPCA$cnt&attachmentName=SEW03033USEN_02.pdf&token=MTUxMzEwMzA2NjQwMg==&locale=en_ALL_ZZ

International Organization for Standardization. (2012). ISO/IEC 27032:2012 - Guidelines for cybersecurity. Geneva: International Organization for Standardization.

International Organization for Standardization. (2013). ISO/IEC 27002:2013 Code of practice for information security controls. Ginebra, Suiza: ISO.

McAfee. (2013). Creating and Mantaining a SOC. The details behind successful security operations centers. Obtenido de McAfee.com: http://www.mcafee.com/de/resources/white-papers/foundstone/wp-creatingmaintaining-soc.pdf

MITRE Corporation. (2014). Ten strategies of a world-class Cybersecurity Operations Center. Estados Unidos: MITRE Corporate.

SANS Institute. (Mayo de 2015). Building a World-Class Security Operations Center: A Roadmap. Recuperado el 1 de Septiembre de 2016, de SANS Institute Reading Room: https://www.sans.org/reading-room/whitepapers/analyst/building-world-classsecurity-operations-center-roadmap-35907

Tenable. (2017). 2017 Global Cybersecurity Assurance Report Card. Recuperado el 9 de Julio de 2017, de Tenable.com: https://www.tenable.com/lp/2017-global-cybersecurityassurance-report-card/