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

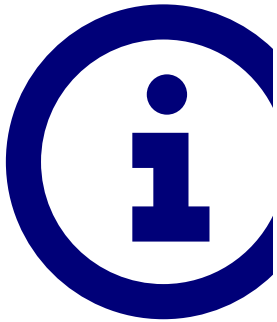
Christian Rubén Molina Caza

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

Seguridad Empresarial

Universitat Oberta de Catalunya

Índice



01

Marco Metodológico

En la actualidad, la “información” se ha constituido en el activo más importante y valioso que posee cualquier organización ya sea del ámbito público o privado.

Contexto y Justificación

01

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 prevenir amenazas futuras y detectar proactivamente aquellas amenazas existentes.

02

El CACES 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.

03

Este trabajo se enfocará en los puntos principales que el CACES debe tomar en cuenta para poder establecer los procesos de un 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.

Objetivos

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.

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

Planificación

0 %	20 %	40 %	60 %	80 %	100 %
Entrega 1 – Plan de trabajo	Entrega 2	Entrega 3	Entrega 4 – Memoria final	Entrega 5 – Presentación en vídeo	Defensa del TFM

02

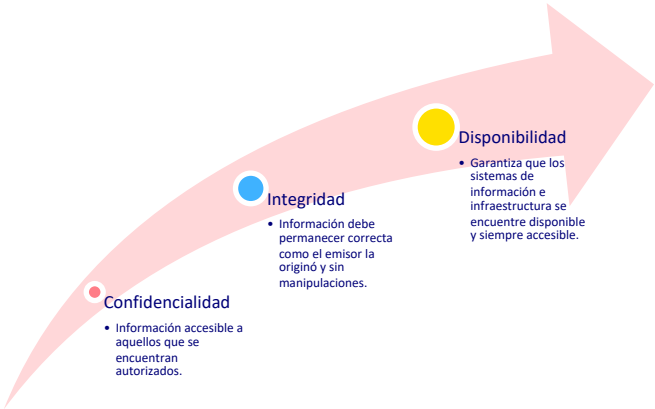
Marco Teórico

Es necesario conocer aquellos conceptos primordiales que requerimos sobre la seguridad de la información y su relación con el funcionamiento y gestión de un SOC.

Seguridad de la Información

Objetivos

- ✓ Minimizar y gestionar los riesgos, así como identificar las posibles amenazas a la seguridad de la información de la organización.
- ✓ Garantizar el uso adecuado de los bienes y recursos con los cuales la organización desempeña sus actividades diarias.
- ✓ 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.
- ✓ Cumplir con el marco legal vigente, referente al sector en el cual se desenvuelve la organización.



Centro de Operaciones de Seguridad

Definición

Al referirnos a un 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 SOC se encarga 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.

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

Estándares y Normativa

ISO

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

NIST

Promueve la innovación y la competitividad industrial a nivel de programas de laboratorio que incluyen ciencia y tecnología ingeniería, tecnología de la información.

ITIL

Proporciona asesoramiento sobre la provisión de servicios de TI de calidad y de los procesos, funciones y demás capacidades necesarias para darles apoyo basado en el ciclo de vida del servicio.

COBIT

Ayuda a las organizaciones a minimizar los perfiles de riesgos, mediante la administración adecuada de la seguridad basado en mejores prácticas para la protección de la información.

MITRE

Sin fines de lucro proporciona sistemas de ingeniería, investigación, desarrollo y soporte en información tecnológica que opera con recursos federales.

EGSI

Necesidad de gestionar la seguridad de la información acorde a la evolución normativa y tecnológica; ya que actualmente los riesgos muestran continuos cambios, que tienen efectos considerables en la sociedad.

03

Situación actual del CACES

Regular, coordinar y planificar los procesos participativos de acompañamiento, evaluación, acreditación y cualificación para garantizar el desarrollo de una cultura de la calidad.

Análisis Situacional

Función

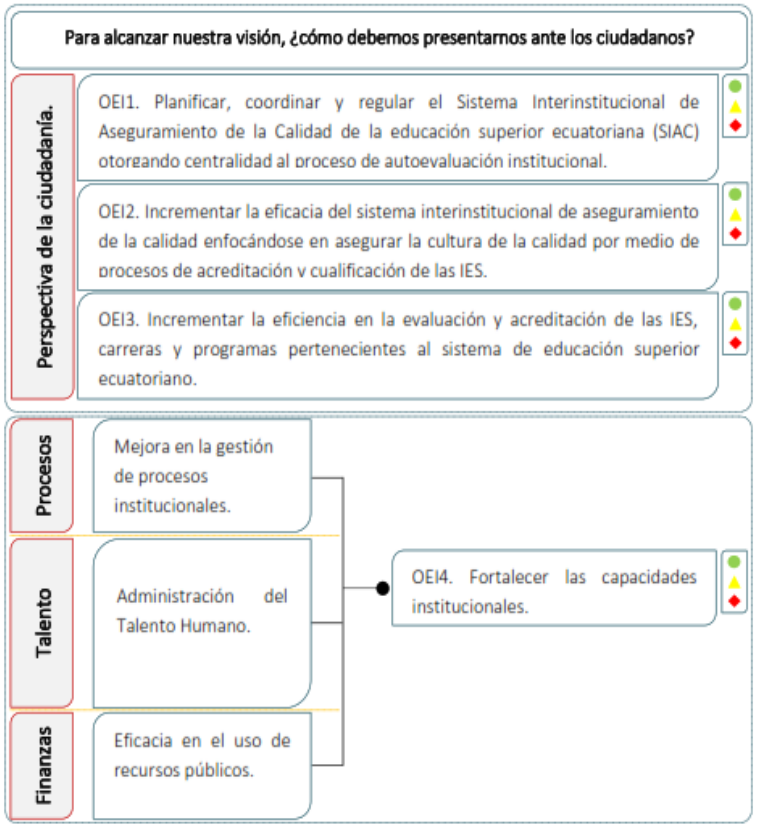
La regulación, planificación, coordinación del Sistema de Aseguramiento de la Calidad de la Educación Superior.

Política de Calidad

- Generar procesos transparentes, articulados y eficientes que guíen los sistemas internos y promuevan la cultura de calidad en las IES.

Política de Seguridad de la Información

- 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.



Infraestructura Tecnológica

Procesamiento

Comprende toda la infraestructura ligada a servidores físicos, servidores virtuales y almacenamiento. Al momento el CACES 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.

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.

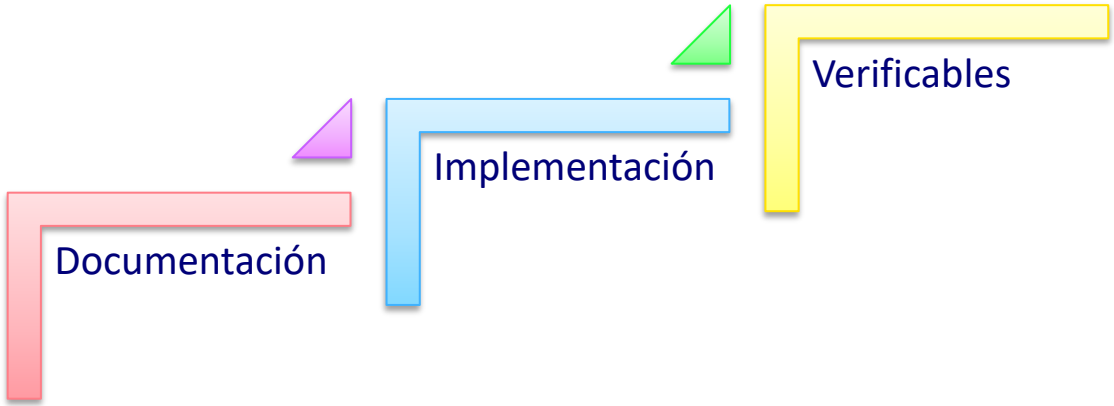
Aplicaciones

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

Nivel de Madurez

Elementos

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.



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.

04

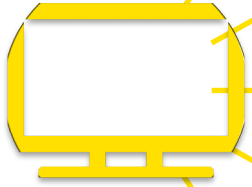
Propuesta de implantación

El SOC constituye una plataforma integral que tiene el propósito de diseñar, implementar y ejecutar procesos de detección y reacción ante posibles incidentes de seguridad.

Talento Humano

01

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).

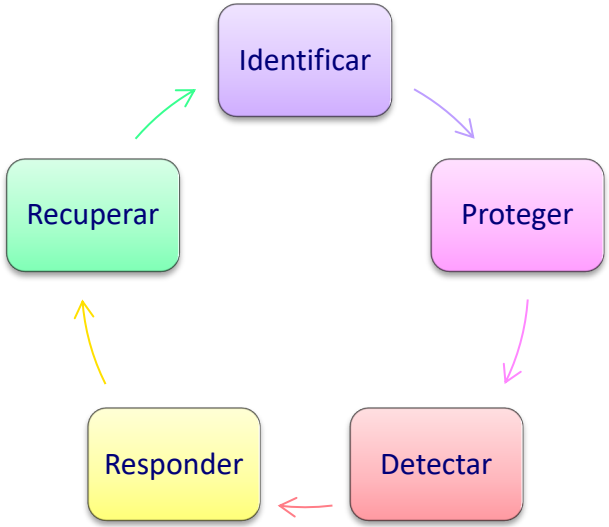


- **Director de la Seguridad de la Información** — Responsable de definir toda la postura de seguridad de la institución. Planea estrategias, programas, políticas y procedimientos.
- **Jefe de Centro de Operaciones de Seguridad** — Responsable de diseñar, contratar y/o construir procesos relacionados con la seguridad de la información.
- **Especialista de Seguridad** — Responsable de realizar pruebas complejas de penetración y análisis de vulnerabilidades.
- **Ingeniero de Seguridad** — Responsable de construir arquitecturas de seguridad e ingeniería de seguridad de sistemas.
- **Analistas de Seguridad** — Responsables de detectar. Investigar y responder ante los incidentes de seguridad que se presenten.

Procesos

02

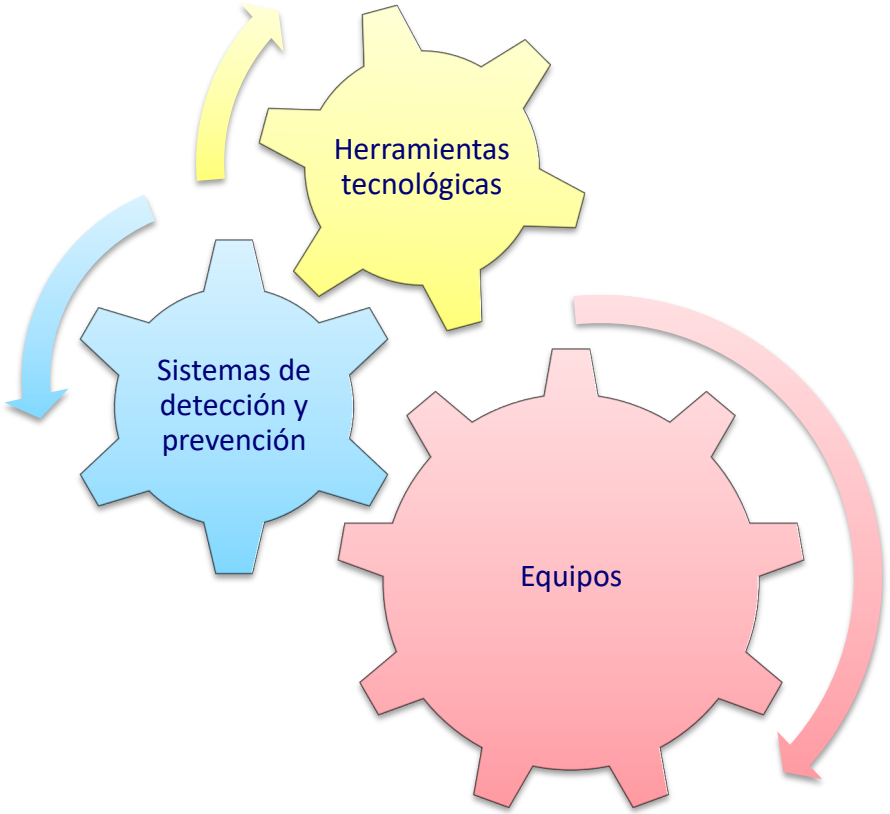
El conjunto de normas ISO 9000 indica que las organizaciones alcanzan los resultados deseados de manera más eficiente, cuando las actividades y los recursos son gestionados como procesos. En este sentido el SOC necesita documentar y comunicar procesos efectivamente e implementar mecanismos de control que permitan retroalimentación cuando surjan mejoras.



Tecnología

03

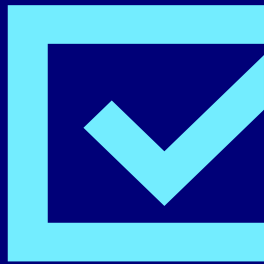
Se encuentra enfocada a las herramientas y recursos informáticos que se utilizarán para el desarrollo de las actividades diarias relacionadas con la gestión de incidentes de seguridad. Un SOC debe encontrarse equipado con una suite de productos tecnológicos que provean la visibilidad adecuada hacia el entorno que contribuya a la postura de seguridad de la información de la organización.



05

Conclusiones

Evidenciar la real importancia que en la actualidad tiene, para las organizaciones, un Centro de Operaciones de Seguridad (SOC) para el monitoreo en tiempo real las actividades.



Generales

01

Se lograron identificar aquellos aspectos primarios y secundarios que deben ser necesariamente considerados en el diseño de un SOC y las operaciones de seguridad, sobre las que pueden ser definidas las funciones y actividades a desempeñar dentro del SOC del CACES, así como, una visión general de todas aquellas herramientas que podrían ser utilizadas.

02

El diseño 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.

03

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.

Desarrollo del TFM

01

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.

02

Otro de los inconvenientes que hemos encontrado es la integración de los módulos requeridos, ya que de manera generalizada 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.

03

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.

Trabajos Futuros

01

- ✓ 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 para garantizar que la información se encuentra debidamente protegida y resguardada.

02

- ✓ 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.

03

- ✓ Extender el presente estudio aportando métricas más precisas que permitan establecer la operación exitosa del diseño y 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.

Gracias
Thank you
Gràcies