Universidad Nacional de Ingeniería

Facultad de Ciencias y Sistemas

Maestría en Gestión de la Seguridad de la Información

Ciclo Académico 2013-2015

Informe Final de Tesis para Optar al Título de Máster en Gestión de la Seguridad de la Información.

Propuesta de diseño e implementación de un Centro de Operaciones de Seguridad (SOC) y un Centro de Repuesta a Incidencias (CSIRT) para la Universidad de Ingeniería"

"Implementación de un caso de estudio aplicado usando herramientas Opensource"

Autor: Javier Antonio Garcia Velasquez

Tutor: Msc Reynaldo Castaño

Managua, Marzo 2016

Dedicatoria

A Dios y a la Virgen María

Por haberme dado la oportunidad de cumplir este sueño y las fuerzas necesarias para poder concluirlo satisfactoriamente y demostrarme en todo momento que están a mi lado.

A Nohelia y Ericka

Cuyo Amor, Cariño y Comprensión son los motores que me impulsan a seguir luchando cada día.

A Mis Padres

Francisco Javier Garcia Romano (qepd) cuyo amor y apoyo incondicional me ha permitido aprender a enfrentar la vida y mirar siempre hacia adelante, Infinitas Gracias.

Lesbia Mercedes Velasquez Rivera, quien a pesar de las dificultades que ha vivido siempre ha estado a mi lado con sus oraciones para darme palabras de ánimo, Infinitas Gracias.

A Mis Hermanos

Esnayre Martin Laínez Velasquez

Lissette Mercedes Garcia Velasquez

Jorge Alberto Garcia Velasquez

Eduardo Miguel Garcia Dávila

Ethel Marina Garcia Dávila

Cuyas palabras de ánimo y apoyo incondicional fueron fundamentales para culminar satisfactoriamente estos estudios.

Agradecimientos

A mi Asesor Principal Msc Reynaldo Castaño

Por haberme dado la oportunidad de desarrollar este tema y haberme brindado el conocimiento, sugerencias y recomendaciones necesarias para poder culminarlo satisfactoriamente.

A SPC Internacional

Empresa para la cual laboro y que me ha brindado el apoyo económico para el desarrollo y culminación de los estudios de maestría.

Resumen del Tema

En Nicaragua al igual que en el mundo entero el Internet ha crecido de una manera desmesurada y se ha convertido en el más poderoso medio de comunicación disponible. Esta situación ha facilitado que la información que se genera desde o hacia las empresas u organizaciones fluya por este medio. Hoy en día el internet es barato y de fácil acceso, por lo que es difícil encontrar una Empresa u Organización que no cuente con Internet para el apoyo de sus procesos y operación Diaria.

A pesar del uso globalizado, las tecnologías sobre las que Internet basa su funcionamiento son inseguras. Muchas Empresas u Organizaciones implementan la seguridad de Internet de manera limitada o de manera inadecuada. Es precisamente la combinación de la vasta información disponible, con la dificultad que existe para protegerla adecuadamente lo que hace que todos los sistemas que utilicen Internet, sean blancos fáciles para un posible ataque de seguridad.

En el presente estudio se muestra una propuesta de diseño de un Centro de Monitoreo de Seguridad (SOC, Security Operation Center, por sus siglas en Inglés) y de un Equipo de Repuestas a Incidencias de Seguridad (CSIRT, Computer Security Incident Response Team) para la Universidad Nacional de Ingeniería, como entidades relacionadas que contribuyen a aminorar los tiempos de respuesta ante un incidente de seguridad.

Con la intención de demostrar el funcionamiento de ambas entidades se desarrolló un caso de estudio utilizando una Institución ficticia denominada Seguros y Mas, SyM. El caso consistió en un primer momento en la realización de un ataque (dirigido por un hacker) a un servidor Windows 2008 Server afectado por la vulnerabilidad ms09_050. Mediante esta vulnerabilidad se pudo implantar un Malware (específicamente el RAT[1] Apocalypse), realizar una denegación de servicio y un ataque de fuerza bruta. En un segundo momento y a lo interno de la Institución se utilizaron las herramientas Open Source tales como: Alienvault OSSIM como sistema de administración de eventos de seguridad (SIEM), RTIR como sistema de administración de casos o incidentes de seguridad y MEDIAWIKI como sistema de colaboración, para poder cubrir el ciclo del incidente de seguridad, desde su descubrimiento , manejo, hasta la resolución y cierre.

Palabras Claves *– Incidencia, Seguridad, Repuesta, Monitoreo, Ataque, SOC, CSIRT, UNI, OSSIM, RTIR , MEDIAWIKI*

[1] Remote Administration Tool

Tabla de Contenido

Índice de Ilustraciones

Capítulo 1: Introducción

1.1 Introducción

Desde la década de los 90 el uso de las TIC - especialmente el uso de Internet - en Nicaragua ha venido creciendo a una velocidad impresionante a tal punto que hoy en día ha dejado de ser un lujo para convertirse en una necesidad. La información ha pasado a ser, para toda empresa u organización, un activo de mucha importancia a tal punto que el negocio en sí, depende en gran parte de esta para poder subsistir.Se debe recordar que Internet es una red abierta e insegura por naturaleza y por lo tanto está plagada de amenazas.

Para contrarrestar esta inseguridad, muchas organizaciones que tienen presencia en Internet usualmente utilizan mecanismos y tecnologías ampliamente desarrolladas que detectan, corrigen y mejoran la seguridad de la información (Firewall, IDS, Antivirus). A pesar de estos mecanismos, es difícil poder afirmar que la información, está 100 % protegida, muchas veces porque no se cuentan con el personal capacitado o simplemente no existen un proceso de monitoreo y repuesta oportuna.

Dado lo antes expuesto es necesario disponer de mecanismos adicionales que ayuden a las empresas u organizaciones comprobar que su información está realmente protegida ante las amenazas globales existentes.

En Nicaragua los mecanismos de seguridad tanto de las instituciones de gobierno como de la empresa privada son manejados de manera independiente, cada instancia se encarga de salvaguardar sus recursos y sus propios sistemas, en caso de que alguna de estas entidades experimente un ataque o incidencia de seguridad no la dan a conocer al público e inclusive muchas de estas ni siquiera cuentan con personal especializado que sepan manejar situaciones de este tipo.

Es debido a lo antes expuesto, que en el presente documento se propone diseñar e implementar un [2]SOC y un CSIRT como entidades con tareas interrelacionas entre sí, para la Universidad Nacional de Ingeniería (UNI). Esta propuesta puede haber sido desarrollada en cualquier entidad pública o privada, inclusive en otra universidad, sin embargo la UNI representa una institución educativa pionera en temas de tecnología, miembro de la comisión nacional de Ciencia y Tecnología, Rectora del Proyecto TIC[3] que atiende las nuevas demandas del desarrollo tecnológico de la sociedad Nicaragüense y es la primera universidad poseedora de un nodo de Internet Sección: UNI (2016).

Este nodo es el que se conoce hoy en día como NIC.NI que en 1988 delego IANA[4] ahora ICANN [5] para responsabilizarse de la operación estable, confiable y redundante de la base de datos autorizada y única llamada Sistema de Nombres de Dominios .NI, que indexa los nombres de dominios que terminan con .NI a los números IP (Protocolo de Internet, IP) que identifican a cada computadora que los hospedan dentro y fuera del país.

El NIC.NI es miembro actual de LACNIC[6] – Una de las 5 existentes a nivel mundial, que tiene como uno de los puntos relevantes de su misión “El Fortalecimiento constante de una Internet Segura, estable, abierta y en un continuo crecimiento". Adicionalmente el LACNIC presta servicios de Reporte de incidentes de Seguridad, Intermediación, y Publicación de Advertencias de Seguridad. LACNIC. (2016).

[2] SOC: Security Operation Center / CSIRT:Computer Security Incident Response Team
[3] Tecnologías de Información y Comunicación
[4] Internet Assigned Numbers Authority.
[5] Internet Corporation For Assigned Names and Numbers
[6] Latin America & Caribbean Network Information Centre

Por todos los puntos antes mencionados la UNI representa la entidad educativa idónea para convertirse en un referente en administración de la seguridad de la información a nivel de nacional, y que mejor forma, que hacerlo a través de la creación de un SOC y un CSIRT. En un primer momento desarrollado a nivel interno de la UNI, pero con un poco más de madurez podrá convertirse en la Entidad que ayuden a las Instituciones de Gobierno y Empresas Privada de Nicaragua a poder monitorear, analizar y reaccionar ante amenazas de seguridad.

Este estudio sirve para que tanto las autoridades civiles y gubernamentales puedan coordinarse y retomar la propuesta acá planteada y poderlo llevar a cabo, garantizando de esa manera la protección de uno de los componentes más críticos de toda organización: La Información.

1.2 Antecedentes

a) En Nicaragua

A nivel de país: Nicaragua se conoce muy poco sobre el tema de estudio, tanto a Nivel Gobierno y empresas privadas.

1. SOC: A grandes rasgos se menciona que los ISP locales, cuentan con un SOC para ayudar a reducir las incidencias de seguridad propias de la entidad.

2. CSIRT: Hace algunos años se manejaba una iniciativa entre algunas instituciones de Gobierno para la formación de un CSIRT sin embargo hasta donde se sabe no se logró concretar ningún avance. A través de investigaciones realizadas recientemente, se conoció de la existencia del proyecto AMPARO (una iniciativa del LACNIC) a través del cual se pretende fortalecer la capacidad regional de atención a incidentes de

seguridad en América Latina y el Caribe, sin embargo Nicaragua aún no forma parte de ese proyecto.

b) A nivel Global

A nivel internacional si existen mayor cantidad de investigaciones y documentos relacionados con el tema que se propone estudiar. Estos documentos van desde documentos oficiales desarrollados por algunos centros de investigación de algunas universales hasta publicaciones de organismos no gubernamentales.

1. SOC : Se debe de estar claro que en el caso de los SOC es una iniciativa que generalmente está más orientada a que cada Institución, Empresa u Organización la defina, de acuerdo a sus requerimientos de monitoreo de amenazas o incidentes de seguridad a las que estén expuestas.

2. CSIRT: El primer CSIRT del mundo se creó en el año 1989. Para el año 1990 se creó el FIRST (Forum of Incident Response and Security Teams). A este organismo está adscritos una cantidad de CSIRT a nivel mundial principalmente en Europa. Sin embargo también se conoce de la existencia de otras experiencias de CSIRT a nivel de Latino América como por ejemplo Argentina, Brasil, Chile por mencionar algunos.

1.3 Definición Problemática

El Internet, es sin dudas un medio de comunicación imprescindible en las organizaciones y empresas a nivel mundial y específicamente en Nicaragua, donde se ha observado a través de los últimos años la dependencia a esta tecnología. Antes, el flujo de información entre instituciones de gobierno por ejemplo se realizaban de manera manual hoy en día todo se ha orientado hacia la automatización utilizando como medio Internet.

Pero Internet por su misma naturaleza es un medio inseguro y todas aquellas instituciones que tengan participación de una u otra forma en este

medio, estarán expuestas a amenazas y vulnerabilidades que cada día se vuelven más complejas. En su gran mayoría el personal de TI de cada institución sabe que como mínimo se debe de tener protección a nivel de Hardware a través de Cortafuegos (Firewall), Sistemas de Prevención de Intrusos (IPS/IDS), pero muchas veces a pesar de la existencia de estos equipos la seguridad se ve comprometida.

Un caso muy particular y que sirve de ejemplo para ilustrar, es el ocurrido en Febrero del 2014 en donde el sitio web de una institución de gobierno “La Gaceta” fue “hackeada” por un grupo denominado “Fantasmas Argelinos”, en aquel momento no se pudo obtener mayor información al respecto y al parecer los encargados de administrar el sitio se limitaron a volver a cargar el sitio web original, sin novedad adicional.

¿Qué hubiera ocurrido, o que repercusión hubiera tenido si en vez de simplemente hacer un cambio de la página principal del sitio de la Gaceta, los atacantes hubieran podido irrumpir en los sistemas de la institución y haber robado algún tipo de información confidencial. Este caso fue públicamente conocido porque se realizó un reportaje en varios periódicos locales, sin embargo esto no es un caso aislado, existen sitios en Internet en donde se pueden obtener información sobre los sitios que han sido “Hackeados” por país y es sorprendente observar como existen varios sitios conocidos de Nicaragua que se encuentran en esas listas. De algo si se puede estar seguro, en el caso de que una institución de gobierno o privada se vea comprometida con una incidencia de seguridad, difícilmente lo harán público y acá es donde surge la principal justificación para la realización del estudio que se pretende desarrollar. *¿Están preparadas las instituciones para detectar a tiempo una amenaza de seguridad? ¿Saben cómo reaccionar? ¿A quién llamar? ¿Tienen el personal experto que pudiera ayudarles?.* Sorprendentemente la mayoría de las repuestas a estas preguntas es NO , basado en eso el presente estudio pretende desarrollar una propuesta para el diseño de un SOC y un CSIRT que

permita poder llenar el vacío que existe por la ausencia de mecanismos de visibilidad a incidentes y repuesta a los mismos.

1.4 Hipótesis

La creación de un SOC y un CSIRT para la UNI ayudará a conocer si la institución está siendo objeto de ataques informáticos, que a la vez permita contar con un equipo profesional capaz de restaurar servicios y fortalecer la seguridad de la infraestructura de TI.

1.5 Justificación

Según el informe de Incidentes de Seguridad publicado por ESET (2015) a nivel de Latinoamérica se observan algunos datos alarmantes para Nicaragua en términos de seguridad.

a) El 50 % de las empresas nicaragüenses sufrieron un incidente relacionado con infecciones de códigos maliciosos. El mayor a nivel de Centro América y México. Seguido por Guatemala con el 42 %.
b) El 56 % de las empresas nicaragüenses sufrieron un incidente relacionado con acceso indebido a aplicaciones y/o bases de datos.
c) El 12 % de las empresas nicaragüenses sufrieron un incidente relacionado con explotación de vulnerabilidades.

Los datos antes expuestos están justificados por la inexistencia de una entidad que cuente con mecanismos y personal experto que esté preparada a nivel nacional para monitorear las infraestructuras de seguridad , tanto a nivel de gobierno como empresa privada , y provea capacidades de detección , análisis y repuesta a incidentes de seguridad.

El aporte más significativo que se busca con este estudio es poder desarrollar una propuesta de creación de un SOC y un CSIRT para la Universidad Nacional de Ingeniería. Mediante el SOC la UNI dispondrá de las herramientas necesarias para poder monitorear en tiempo real los eventos de seguridad relevantes de su infraestructura de TI así como personal altamente calificado que de repuesta a esos incidentes de seguridad que se puedan dar.

1.6 Alcances

A través de esta propuesta se pretende dar a conocer los pasos necesarios para el diseño, creación y puesta en marcha de manera tropicalizada de un SOC y un CSIRT. Las generaciones de SOC han venido cambiando a lo largo de los años, tiempo en el cual se han venido incorporando nuevos servicios. Para el caso específico de la UNI únicamente se tomaran en cuenta los servicios de Monitoreo de Alertas y Repuesta a Incidentes de Seguridad.

Indudablemente que llevar a cabo este estudio beneficia indirectamente a las instituciones públicas y privadas que en algún momento quieran participar, ya que al ser implementado en la UNI se contará con dos entidades (SOC y CSIRT) que dispongan del personal, experiencia y mecanismos formales para ayudar a proteger el recurso más valioso del cual todas las instituciones dependen: La Información.

Esta propuesta será desarrollado a nivel interno de la UNI, sin embargo se pretende, que los resultados obtenidos sirvan para concientizar a las autoridades gubernamentales y civiles sobre el uso inherente de internet en nuestros días, su naturaleza insegura, y como consecuencia la necesidad imperativa de contar con entidades especializadas para el monitoreo, análisis y repuesta a incidentes de seguridad.

Es necesario cambiar la mentalidad de las organizaciones de ocultar la información sobre incidencias de seguridad por pena o desconocimiento. El problema de las incidencias de seguridad es de todos y se debe abordar de manera conjunta.

1.7 Objetivos

a) Objetivo General

- ✓ Realizar una propuesta de diseño e implementación de un Centro de Operaciones de Seguridad y un Centro de Repuesta a Incidencias de Seguridad, para la Universidad Nacional de Ingeniería.

b) Objetivos Específicos

1. Definir el tipo de SOC a implementar en la UNI.
2. Enumerar los procesos, personas y tecnologías involucrados en la implementación del SOC de la UNI.
3. Enumerar los servicios que prestará el CSIRT de la UNI.
4. Mostrar la relación que tiene el SOC y el CISRT como entidades complementarias.
5. Demostrar la Implementación y operación de un SOC y un CSIRT utilizando herramientas Open Source.

Capítulo 2: Marco Teórico

2.1 Seguridad de la Información

Según el módulo 1 de la “Academia Latinoamericana de Seguridad “ Microsoft (2005) La seguridad de la información tiene como propósito proteger la información registrada, independientemente del lugar en que se localice : impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que la conocen.

Hoy en día, la seguridad de la información es fundamental para la operación de la mayoría de los negocios, sin importar que sean organizaciones pequeñas o corporaciones multinacionales. En tiempos recientes la implementación de redes de área amplia y la instalación de equipos de computadoras en las áreas de oficinas ha traído la tecnología de la información a casi cada área de trabajo. Doddrell (1996)

El resultado, es una dependencia creciente en la confidencialidad, integridad y disponibilidad de la información almacenada y procesada en los sistemas de cada una de las organizaciones. Doddrell (1996)

Cualquier sistema de seguridad que una organización desee utilizar para garantizar la protección de su información debe garantizar estos tres aspectos a) Confidencialidad : a través del cual se garantizara que el acceso a la información ha de ser permitido únicamente a aquellos elementos o personas autorizadas, b) Integridad : a través de la cual se garantiza que la información solo puede ser modificada por aquellos elementos o personas que han sido autorizadas y de una manera controlada y por ultimo c) Disponibilidad : indica que la información tiene que permanecer accesible a todos aquellos elementos o personas autorizadas. Fitzgerald (1995)

Existe una serie de razones básicas por la que una organización requiere de protección cuando está conectada al Internet o a cualquier otra red externa. Doddrell (1996)

- Internet es una red abierta que carece de seguridad.
- La seguridad de redes externas no puede ser garantizada, ya que también se pueden ver comprometidas.
- La mayoría de los sistemas operativos de los servidores en Internet tienen medidas inefectivas de seguridad.
- Existen una gran cantidad de usuarios en Internet, lo que significa que existen por lo tanto mayores fuentes de abuso.
- Usuarios socialmente irresponsables, competidores deshonestos, trabajadores y ex trabajadores inconformes quienes tienen acceso a Internet y pueden comprometer la seguridad si existe algún tipo de vulnerabilidad en el sistema de seguridad de la organización para la cual trabaja.

2.2 Ataques más Rápidos y Complejos

Según el reporte de Investigación de Brechas de Seguridad 2015 publicado por la compañía VERIZON, el 60 % de las brechas de seguridad que una empresa experimenta hoy en día ocurre en un periodo aproximado de un minuto, sin embargo el periodo de descubrimiento de las mismas varía y va desde algunos meses hasta años.

Con la facilidad que ofrece Internet para compartir información, hoy en día es factible encontrar desde códigos muy sencillos que pueden ser utilizados por los llamados Script Kiddies[7] hasta ataques muy sofisticados que muchas veces

[7] Se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender.

inclusive las herramientas de seguridad actuales no son capaces de detectar. De ahí que las brechas de seguridad en hoy día no son un tema de Si la empresa será atacada sino más bien ¿Cuando?

Es por eso que las organizaciones deben de contar con mecanismos o infraestructuras que sirvan para poder detectar estas amenazas o brechas de seguridad en el menor tiempo posible que les permita poder reaccionar adecuadamente. El SOC y un CSIRT con parte de las infraestructuras y personal experto disponibles para estos fines.

2.3 Centro de Operaciones de Seguridad (SOC-Security Operation Center)

Como lo menciona Nathans (2015) , un centro de Operación es un cuarto o ambiente equipado con varias pantallas colocadas en semi-circulo , con varios agentes los cuales, poseen equipos de cómputo independientes, cuya tarea fundamental es la del monitoreo de procesos o información crítica de una organización.

Dentro de los más relevantes que se pueden mencionar están: NOC (Network Operation Center) enfocado principalmente en el monitoreo de equipos de comunicación y telefonía. EOC (Emergency Operation Center) dedicado a dar repuestas ante una crisis natural especifica cuando esta se presente y finalmente el ***SOC (Security Operation Center)*** que no es más que un centro de trabajo destinado a dar un servicio de seguridad gestionada externalizado a una serie de clientes.

Un SOC debe reducir tanto la duración como el impacto de los incidentes de seguridad que puedan explotar, denegar, degradar o destruir los sistemas que las empresas requieren para el funcionamiento normal de su negocio. Nathans (2015)

Un SOC monitorea y administra amenazas potenciales, las analiza, determina el riesgo y luego recomienda o ejecuta algún tipo de acción de remediación para proteger a la empresa, todo esto realizado de una manera efectiva, eficiente y medible. Nathans (2015)

2.3.1 Generaciones de SOC

A través de los años el SOC ha venido evolucionando en cuanto a los componentes y servicios que ofrece. Esta transformación se debe al cambiante escenario de amenazas que se ha experimentado. Muniz, Alfardan, Mcintyre (2015).

a) Primera Generación :

- Monitoreo de Dispositivos
- Retención y Recolección de Logs
- Cobertura Limitada de Dispositivos
- Reacción lenta a incidentes de Seguridad

b) Segunda Generación : (Incluye los de la Primera Generación)

- Correlación de Eventos
- Recolección de Logs de Sistema y Red
- Administración de Casos

c) Tercera Generación : (Incluye los de la Primera y Segunda Generación)

- Administración de Vulnerabilidades
- Repuesta a Incidentes

d) Cuarta Generación : (Incluye los de la Primera y Segunda y Tercera Generación)

- Correlación de Datos
- Análisis de Seguridad de Big Data
- Servicios de Inteligencia de Amenazas
- Servicios de Seguridad de la Nube
- Investigación Digital
- Análisis de Flujo de Red

2.3.2 Procesos, Personas y Tecnologías

La creación de un SOC no es una actividad trivial, por lo tanto requiere la inversión en Procesos, Personas y Tecnologías. Splunk-Buiding-a-SOC (2016)

Procesos: Se requiere el modelado de Amenazas. Este es un proceso donde el personal de Seguridad de TI y de Negocio recolecta información para determinar las principales amenazas, priorizarlas, modelarlas y luego determinar cómo detectarlas y remediarlas.

Una parte crítica de cualquier SOC es el proceso de repuesta de alertas e incidentes y para ellos la mayoría de los SOC utilizan una metodología multi-capa. Las alertas se generan a través de varias fuentes incluidas soluciones SIEMs[8] y son dirigidas a la primera capa en donde se les hace una revisión inicial. Si esta capa no puede resolver el incidente, se escala a capas subsiguientes en donde existe personal más calificado y que cuenta con herramientas de repuesta a incidentes

[8] Security Information and Event Management

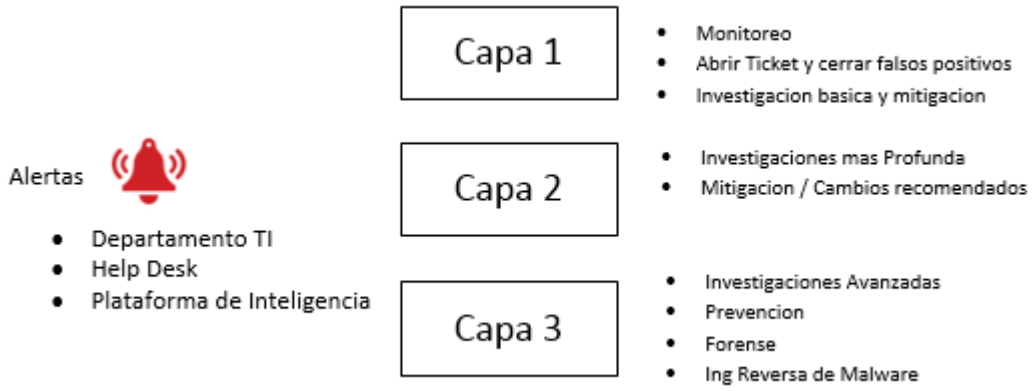


Ilustración 1 Metodología Multicapa de un SOC

Personas: Un SOC requiere una diversidad de personal, cada uno con diferentes habilidades, calificaciones, y personalidades. También es necesario que se establezca una ruta de cursos de entrenamientos así como de promoción de tal forma que los analistas puedan avanzar a través de los diferentes niveles dentro del SOC.

Tecnología: Un SOC debe de contar con una plataforma de inteligencia de seguridad que tenga la capacidad de indexar todos los datos de los dispositivos y archivos de logs de fuentes de seguridad y no seguridad en tiempo real. Esta plataforma debe de ser amigable para su fácil uso y flexible para ser personalizada.

2.3.3 Recolección de Datos

Una de las tareas fundamentales de un SOC es el Análisis y Recolección de Datos (Tarea que habitualmente se realiza apoyándose en un SIEM) . Antes de realizar cualquier análisis es necesario recolectar datos o información que sea relevante la cual puede ser obtenida de diferentes fuentes. Entre los datos que tienen especial interés tenemos registros de eventos, paquetes de red y

flujos de red, los cuales de forma directa e indirecta pueden contribuir a la detección de incidentes de seguridad. Muniz, Nadhem,Mcintyre (2015).

Entre los protocolos utilizados para la recolección de datos tenemos:

a) Protocolo Syslog : A como se define en IETF RFC 5424, provee un formato de mensaje que permite que cierta información de los fabricantes sea proveída de una manera estructurada, además de establecer el mecanismo a través del cual se dará la notificación de mensajes desde un cliente syslog (origen) hacia un destino syslog (collector o reenviador). El protocolo Syslog soporta tres roles específicos :

- Origen: Genera contenido de Syslog en un mensaje.
- Recolector: Recolecta mensajes de Syslog.
- Reenviador: Reenvía mensajes, desde un origen a otros reenviadores y los envía a los recolectores u otros reenviadores.

b) Flujos de Red

Toda la información o datos de una organización son transportados a través de dispositivos físicos o virtuales (conmutadores, enrutadores), lo cual representa una oportunidad para poder tener una visibilidad y conciencia sobre el tráfico y sus patrones de uso.

A través del protocolo IPFIX[9] RFC 7011 , que define la exportación de información de flujo IP unidireccional se puede tener visibilidad de información que puede llevar a la identificación de una amenaza de seguridad como un Malware.

[9] IP Flow Information Export

Una de los beneficios de utilizar herramientas de seguridad basadas en flujos es que se puede detectar comportamientos anómalos que no necesariamente están vinculados a una firma reconocida de un ataque. Adicionalmente mediante este tipo de herramientas se habilita toda la red como un sensor en comparación a la visibilidad restringida que pueden tener algunos productos específicos de seguridad como IPS[10] y Cortafuegos (Firewall).

2.3.4 Normalización de Datos

Una vez obtenida la información de las diferentes fuentes a través de los diferentes protocolos, es necesario analizarla (compilarla) y normalizarla. El análisis se refiere al proceso de tomar información en bruto y colocarla o clasificarla de acuerdo a diferentes campos de un esquema predefinido. La normalización se refiere al proceso de permitir que eventos similares obtenidos de diferentes orígenes sean almacenados de manera uniforme para ser utilizados posteriormente. Muniz, Nadhem y Mcintyre (2015).

2.3.5 Análisis de Seguridad

El análisis de seguridad se refiere al proceso de investigar los datos obtenidos con el propósito de descubrir amenazas conocidas y desconocidas. La Correlación de eventos es la forma más común utilizada para el análisis de datos de seguridad. La correlación de eventos de seguridad se refiere a proceso de crear un contexto (o ambiente) dentro del cual se observan relaciones entre eventos desiguales recibidos de distintos orígenes con el propósito de identificar y reportar amenazas posibles. Muniz, Nadhem,Mcintyre (2015).

2.3.6 Administración de Vulnerabilidades

[10] Intrusion Prevention System

Según Muniz, Nadhem y Mcintyre (2015) la Administración de Vulnerabilidades se refiere al proceso de descubrir, confirmar, clasificar, priorizar , asignar , remediar y rastrear vulnerabilidades. Las vulnerabilidades pueden ser percibidas como una debilidad en las personas, procesos y tecnologías. Desde el punto de vista de un SOC la administración de vulnerabilidades se enfoca en debilidades técnicas conocidas generalmente presente en software y firmware.

El elemento más importante dentro de la administración de vulnerabilidades es ser lo suficientemente rápido en la protección de los activos vulnerables antes que una posible debilidad sea explotada. Esto se realiza aplicando de manera continua una serie de pasos para identificar, evaluar, y remediar el riesgo asociado con la vulnerabilidad. Existen varios modelos que pueden ser tomados como referencia para administración de vulnerabilidades, uno de ellos es el de SANS (Organización de los Estado Unidos dedicada a la investigación cooperativa y educación en seguridad informática) quien establece los siguientes pasos dentro de su modelo:

- ✓ Inventario de Activos
- ✓ Administración de la Información
- ✓ Evaluación del Riesgo
- ✓ Evaluación de Vulnerabilidades
- ✓ Elaboración de Reportes y Remediación
- ✓ Repuesta

2.3.7 Inteligencia de Amenazas

De acuerdo con Gartner la Inteligencia de Amenazas consiste en evidencia basada en conocimiento, contexto, mecanismos, indicadores sobre una amenaza existente o emergente a los activos que se puede utilizar para la

toma de decisiones del individuo responsable de esa amenaza. Según Forrrester el propósito principal de la Inteligencia de Amenazas es la de informar a los tomadores de decisiones de acuerdo a los riesgos e implicaciones asociadas con las amenazas.

Desde el punto de vista de un SOC es importante porque a través de la Inteligencia de Amenazas se puede extender la concientización de seguridad más allá de los límites internos de una organización al consumir inteligencia de otras fuentes presentes en Internet sobre posibles amenazas que pudieren afectar a la organización.

2.3.8 Metodología de Creación de un SOC

Para la creación del SOC de la UNI se utilizara la metodología propuesta por Muniz,Nadhem y Gary (2015) . Esta metodología contempla 4 Fases:

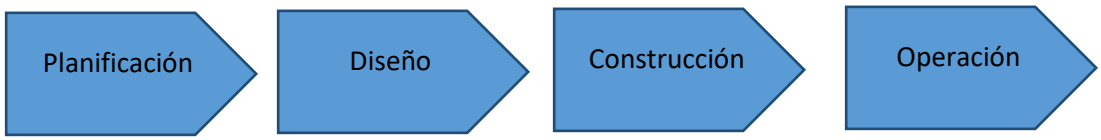


Ilustración 2 Metodología de Creación de un SOC

Planificación: En esta etapa se realiza una evaluación de las metas tanto a nivel de TI como a nivel de Organización de la UNI, las capacidades actuales en cuanto a personas, procesos y tecnología existentes en el contexto de un SOC, así como los requerimientos para su creación.

Diseño: Esta etapa se toman en cuenta todos aquellos elementos que definen la manera como operara el SOC tales como el alcance, modelo de operación así como los servicios que brindara.

Construcción: Una vez que se tiene un diseño definido, es necesario definir los elementos puntuales de la tecnología que será utilizada para la operación del SOC.

Operación: En esta etapa se define la manera cómo interactúan y se relacionan las personas, procesos y la tecnología que hacen que el funcionamiento del SOC sea efectivo.

2.4 Equipo de Repuesta a Incidencias de Seguridad Informáticas (CSIRT)

Como menciona Killcrece (2003) cuando ocurre un ataque de seguridad a una organización, se ha detectado una brecha de seguridad u otro tipo de incidentes de seguridad, es crítico para esa organización disponer de un mecanismo rápido y efectivo de repuesta. Una forma para abordar este problema es mediante la creación de un equipo de repuesta a incidencias de seguridad informáticas (CSIRT por sus siglas en ingles).

Cuando un incidente ocurre, el objetivo principal de un CSIRT es controlar y minimizar cualquier daño, preservar la evidencia, proveer procedimientos de recuperación rápidos y eficientes, prevenir eventos similares futuros y conocer a profundidad la amenaza que afecto la organización. El proceso a través del cual un CSRIT ejecuta todas esas tareas es conocido como manejo de incidentes, según la división CERT (Computer Emergency Readiness Team) del Instituto de Ingeniería de Software de la Universidad Carnegie Mellon cada organización debe de definir lo que representa un incidente para ella, sin embargo de forma general podemos mencionar como ejemplos de incidentes las siguientes actividades :

- ✓ Intentos de acceso o autorizados a sistemas y datos informáticos.
- ✓ Interrupción no solicitada o denegación de servicios.

- ✓ Uso no autorizado de un sistema para el procesamiento o almacenamiento de datos.
- ✓ Cambios a los sistemas de hardware, firmware, o las características de un software sin el consentimiento de su creador.

El manejo de incidentes incluye tres funciones:

Reporte del incidente: Esta función le permite al CSIRT servir como punto centralizado de contactos para reportar incidentes locales. Esto permite que todos los reportes de incidentes sean recolectados en un mismo lugar donde la información pueda ser revisada y correlacionada. Esta información puede ser utilizada para determinar tendencias - patrones de actividad de intrusos y recomendar estrategias preventivas.

Análisis del incidente: Esta función permite analizar profundamente un reporte de incidencia o actividad para determinar el ámbito, prioridad y amenaza del incidente al mismo tiempo que estrategias de mitigación y repuesta.

Repuesta al incidente : La respuesta a (los) incidentes se puede dar de diferentes formas, un CSIRT puede enviar recomendaciones para la recuperación , prevención o contención a los administradores de los sistemas o redes ubicados dentro de la organización , quienes llevan a cabo las recomendaciones, o se puede dar el caso que el mismo CSIRT lleva a cabo las recomendaciones por su propia cuenta.

2.4.1 ¿Qué se protege con un CSIRT ?

Un equipo de respuesta debe de tener como objetivo proteger infraestructuras críticas de la información, en base al segmento de servicio al que esté destinado así deberá de ser su alcance para cubrir requerimientos de

protección sobre los servicios que brinda. El CSIRT debe de brindar servicios de seguridad a las infraestructuras críticas de su segmento básicamente.

Las infraestructuras críticas en un país están distribuidas en grandes sectores, los cuales pueden ser: Gobierno (En todos sus ámbitos: Agricultura, Energia, Transporte,Salud), Telecomunicaciones, Banca , enfocadas en los distintos infraestructuras de información como son : Internet, Software, Hardware.

2.4.2 ¿Tipos de CSIRT ?

De acuerdo al sitio WEB del CERT[11], (www.cert.org) los CSIRT pueden establecerse en diferentes tamaños, formas y jurisdicciones, existen algunos que pueden estar a cargo de un país, otros pueden funcionar de manera regional, otros pueden ser establecidos en una universidad o inclusive algunos pueden brindar sus servicios de manera comercial a los clientes que lo soliciten.

A continuación se muestran algunas de los tipos de CSIRT que se pueden encontrar:

Internos: proveen servicios de manejo de incidentes a su organización matriz, por ejemplo para un Banco, una Universidad o una Agencia Gubernamental.
Nacionales: proveen servicios de manejo de incidentes a un país.
Centros de Coordinación: coordina y facilita el manejo de incidentes entre varios CSIRT.
Centros de Análisis: enfocados en la sintonización de los datos provenientes de varios orígenes para determinar tendencias y patrones en la actividad de incidentes.
Proveedores de Repuesta a incidentes: proveen servicios de manejo de incidentes a otras organizaciones por una cantidad específica.

[11] Computer Emergency Readiness Team

Capítulo 3: Desarrollo y Justificación

3.1 Creación de un SOC

3.1.1 Fase de Planificación

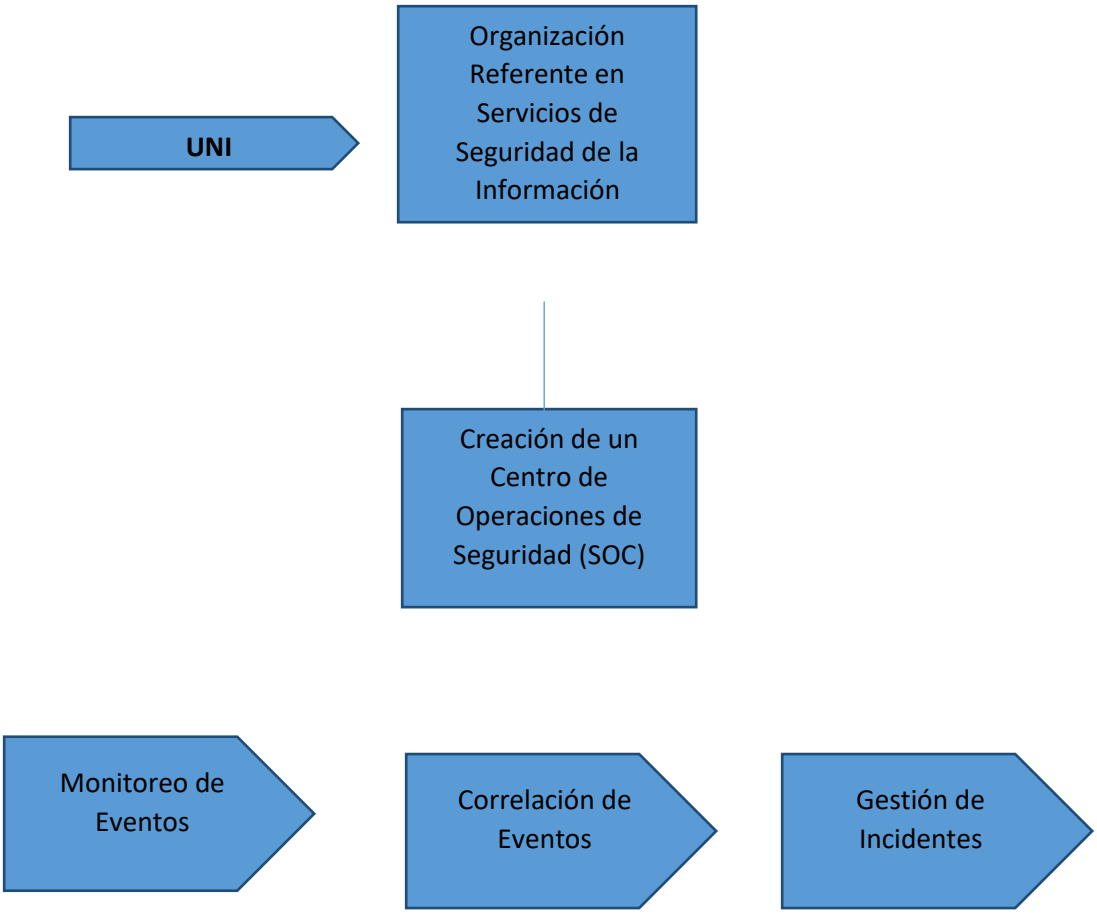
a) Identificación de metas de TI y Organización

Mediante entrevistas re-alizadas a ciertos funcionarios de la UNI se pudo obtener la siguiente lista de metas tanto a nivel de TI como a nivel de Organización:

- Ofrecer servicios de TI alineados a los procesos de negocios de manera ágil y segura.
- Uso adecuado de aplicaciones, información y soluciones tecnológicas.
- Compromiso de la Dirección ejecutiva para la toma de decisiones.
- Disponibilidad de información útil y confiable para la toma de decisiones.
- Disponer de personal de TI y del Negocio Competente y Motivado.
- Convertirse en la primera organización referente en servicios de seguridad de la información.
- Monitoreo del flujo e intercambio de información de los diferentes procesos.
- Correlacionar eventos de seguridad.
- Disponer de mecanismos de repuestas antes incidentes de seguridad.

Tomando como punto de partida la meta Organizacional de la UNI en convertirse en una Organización Referente en Servicios de Seguridad se puede alinearla con la creación de un SOC que permita monitorear

eventos de seguridad, correlacionarlos y establecer mecanismos de repuesta a incidentes.



b) Evaluación de Capacidades

Para la creación del SOC fue necesario evaluar las capacidades con las que disponía la UNI en cuanto a personas, procesos y tecnologías.

Personas: Los elementos evaluados en este punto fueron:

- Gobierno: No existe un SOC definido en este momento, por lo que no existe ningún tipo de administración del mismo.
- Estructura: Únicamente existe una estructura en cuanto a TI y no asociada a ningún SOC.

- Experiencia en SOC: La UNI no cuenta con ningún tipo de experiencia en el uso de un SOC.

- Entrenamiento y Certificación: El personal de la UNI no cuenta con ningún entrenamiento asociado al uso y administración de un SOC.

Procesos: Los procesos son los habilitadores entre la tecnología y las personas. Se refieren a la manera como los incidentes de seguridad y las vulnerabilidades son administradas. Los elementos evaluados en este punto fueron:

- Reporte de Incidentes, Análisis de Incidentes, Cierre de Incidentes, Descubrimiento y Resolución de Vulnerabilidades. La UNI no cuenta con experiencia para ninguno de estos elementos.

Tecnologías: Se refiere a todos aquellos aspectos a nivel tecnológico que soportan la operación del SOC. Los elementos evaluados fueron:

- Infraestructura de Red: La UNI dispone de una infraestructura de red que sirve como soporte para todos los procesos y aplicaciones de TI.

- Herramientas de recolección, correlación y análisis de Datos: La UNI no dispone de ninguna herramienta de este tipo.

- Monitoreo: No se dispone de herramientas de monitoreo.

- Sistemas de Control: La UNI dispone de controles de seguridad básicos como son los Cortafuegos.
- Administración de Logs : La UNI no dispone de herramientas de almacenamiento de logs.

- Evaluación y Seguimiento de Vulnerabilidades: No se dispone de una herramienta que provea la evaluación y seguimiento de Vulnerabilidades.

- Colaboración: No se dispone de mecanismos o herramientas que permitan poder dar a conocer incidencias de seguridad a nivel interno o externo de la UNI para que sirvan de base de conocimiento para eventos futuros.

Como se puede observar al hacer la evaluación, la UNI no contaba con la mayoría de los elementos necesarios para la creación de un SOC, por lo que se tomó esa premisa como punto de partida para la creación del mismo.

c) Estrategia del SOC

Una vez realizada la evaluación de las capacidades de la UNI, fue necesario definir una Estrategia para la creación del SOC, en el cual se abordaron los siguientes elementos:

- Personal Involucrado
    - Líder Estrategia del SOC: Rol desarrollado por el Director del SOC.
    - Tomadores de Decisiones Estrategia del SOC: Este rol fue llevado a cabo por el Director de TI de la UNI, quien es el autorizado para tomar decisiones ante cualquier requerimiento que se presente.
    - Influyentes o Personal de apoyo en la Estrategia del SOC: Este rol fue llevado a cabo por los diferentes jefes de los departamentos de TI de la UNI, tales como sistemas, bases de datos, infraestructura y comunicaciones.

- Misión del SOC: El SOC Monitorea la postura de seguridad de redes, sistemas, y aplicaciones de TI, con el objetivo de detectar y reaccionar a los incidentes de seguridad que puedan impactar la operación de la Universidad Nacional de Ingeniería.

- Alcance: El alcance del SOC está limitado a todas las infraestructuras de TI de aquellas ubicaciones (Recintos) donde se cuente con sistemas de información críticos para la operación de la UNI. El SOC estará ubicado en el recinto central.

- Modelo de Operación: Existen diferentes formas en las que un SOC puede operar: desarrollo local o tercerizado. Dado que la UNI no cuenta con ninguna experiencia, se pretende implementar un desarrollo local con el objetivo de construir las capacidades y experiencia de su personal.

- Servicios del SOC : Los servicios que el SOC brindara son :

    - Monitoreo de Sistemas, Aplicaciones y Redes las 24 horas del día.
    - Recolección y correlación de eventos de las distintas fuentes establecidas.
    - Manejo de Incidentes de Seguridad a través de un CSIRT.

3.1.2 Fase de Diseño

SOC como desarrollo local: El SOC de la UNI se desarrollará en las instalaciones de la UNI Central, para ello es necesario tomar en cuenta los siguientes elementos:

a) Facilidades: El lugar físico donde se desarrollara el SOC debe de brindar las comodidades para:

- Sala de Monitoreo para alojar al menos 4 espacios de trabajos (incluidos equipos de cómputo y comunicación-teléfono), equipadas con Aire Acondicionado y Dos Pantallas en Alta Definición de al Menos 48”.

- Oficina para el Administrador del SOC equipada con una computadora para gestiones administrativas , teléfono , Aire Acondicionado y Una Pantalla en Alta Definición de al Menos 42”. Esta Oficina debe de tener acceso visual a la Sala de Monitoreo y Acceso Físico tanto a la Sala de Conferencia como a la Sala de Monitoreo.

- Sala de Conferencia equipada con el mobiliario necesario para poder realizar reuniones con personal tanto interno como externo, Aire

Acondicionado, Pizarra Acrílica y una Pantalla en Alta Definición de al Menos 42”.

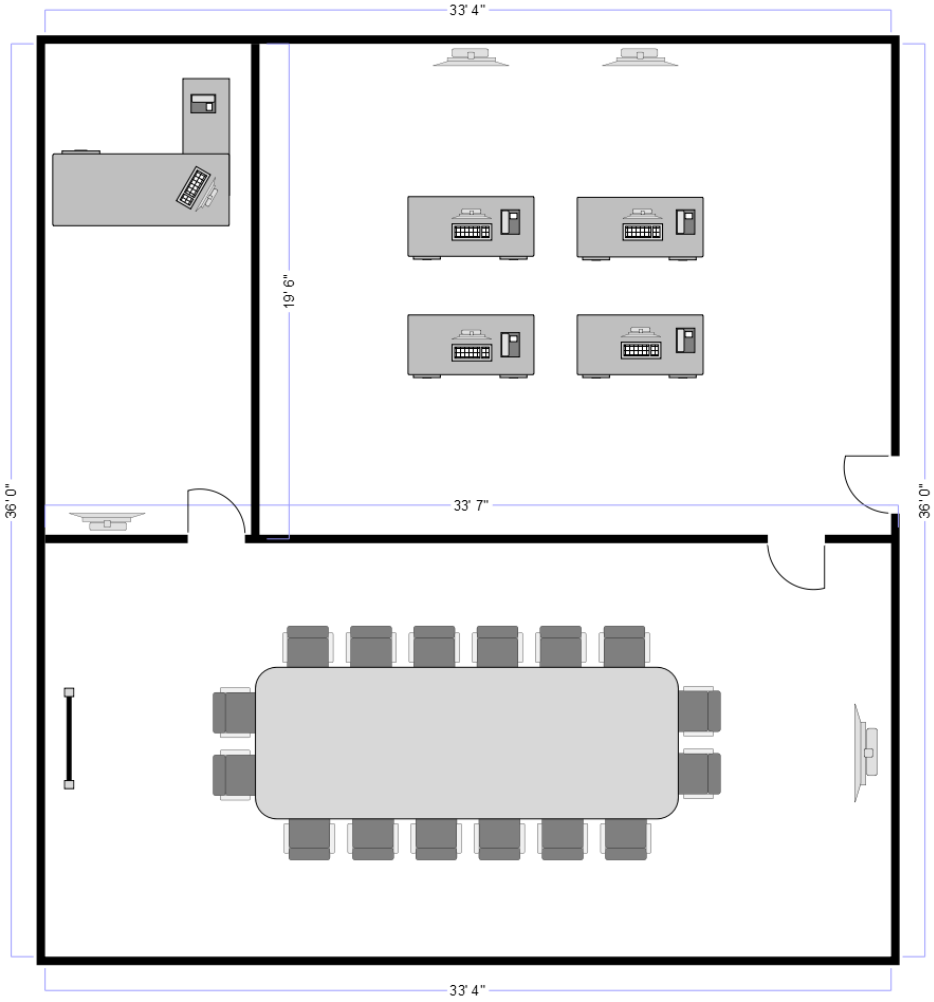


Ilustración 3 Adecuaciones Físicas SOC

b) Seguridad Física: El acceso a la Sala de Monitoreo debe de estar restringido solamente al personal autorizado. Se debe de llevar una bitácora de registros de acceso controlado. Se debe de instalar un Sistema de Cámaras de Monitoreo (Con grabación continua) de Circuito Cerrado. Dada la sensibilidad de la información que el SOC manejara se debe de instalar material a prueba de sonidos para evitar que la información que se discuta a lo interno del SOC puedan filtrarse.

c) Herramientas para los Analistas del SOC: Como se puede ver en el diagrama propuesto se están considerando 4 espacios de trabajos los cuales serán ocupados por los Analistas del SOC/CSIRT. Cada uno de ellos dispondrá de un escritorio equipado con una Computadora de Escritorio con dos Monitores LCD de al menos 22" , uno para la administración de las herramientas de monitoreo y el otro para las tareas administrativas , un teléfono con salida local e Internacional.

d) Infraestructura Activa

Una vez definido el espacio físico donde operara el SOC es necesario incorporar los elementos tecnológicos que soporten su operación, entre los cuales tenemos Infraestructura de RED, Mecanismos de Seguridad, Sistemas Operativos, Almacenamiento, Colaboración, Servicios de Administración de Casos, Herramientas de Recolección, Correlación y Análisis de Datos.

Infraestructura de Red

Actualmente la UNI dispone de una Infraestructura de RED, compuesta por un Enrutador de Perímetro, Cortafuego Perimetral, Conmutador de Núcleo (segmentada en diferentes VLANS[12] y diferentes conmutadores de acceso (donde se encuentran operando las computadoras de los usuarios).

Dentro de los Segmentos de VLANS con que se disponen, tenemos: Usuarios, Aplicaciones Internas, Aplicaciones Externas, Administración. Por efectos de seguridad para la creación del SOC, se agregara una nueva VLAN o segmento independiente donde residan todas las herramientas de monitoreo y a la cual solamente los analistas del SOC/CSIRT tendrán

[12] Virtual Local Área Network

acceso. A continuación se muestra el diagrama actual de red con la incorporación del nuevo segmento para el SOC:

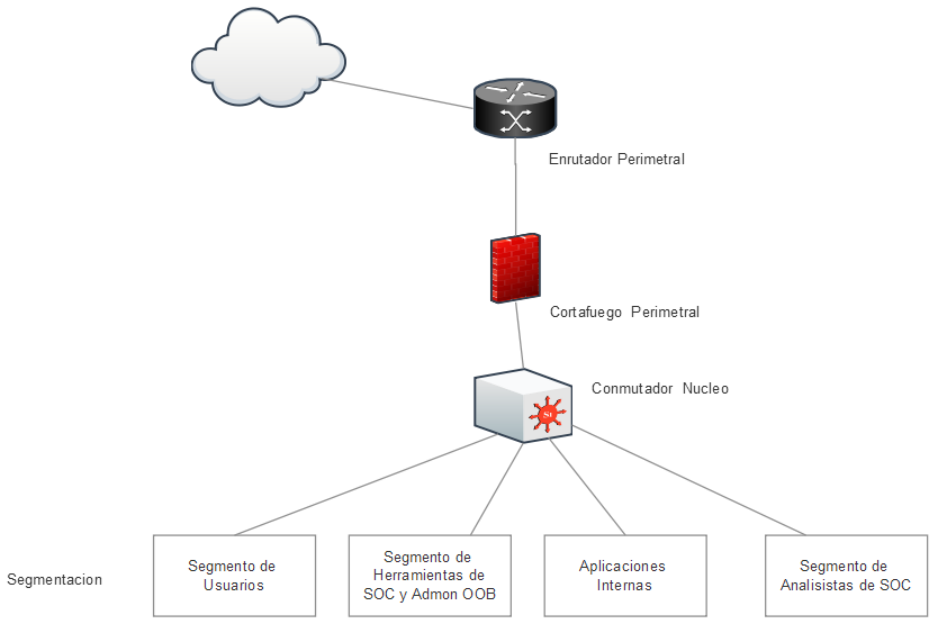


Ilustración 4 Diagrama de Infraestructura de Red

Seguridad

- Segmentación en Zonas: Como buena práctica de seguridad se debe de configurar 3 Zonas de Seguridad en el cortafuego (Inside, Outside, DMZ) de acuerdo a los servicios que ofrecen.

- Monitoreo de Equipos usando una Red de Administración Outband : Todos los equipos que vayan a ser monitoreados utilizaran un segmento de red independiente que a su vez servirá para la administración de los mismos (OOB), para evitar que usuarios no autorizados tengan acceso a información confidencial.

- Control de Acceso a los Equipos utilizando tecnología AAA : La autenticación, autorización y la contabilidad (o registro de actividad) de

los usuarios será realizado a través de un servidor AAA utilizando el protocolo RADIUS

- Listas de Control de Acceso: Para controlar el acceso de los usuarios no autorizados, se configuraran Listas de Control de Acceso en el equipo conmutador núcleo, de tal forma que solamente los usuarios Analistas y las herramientas del SOC tengan acceso a los equipos y a su administración.

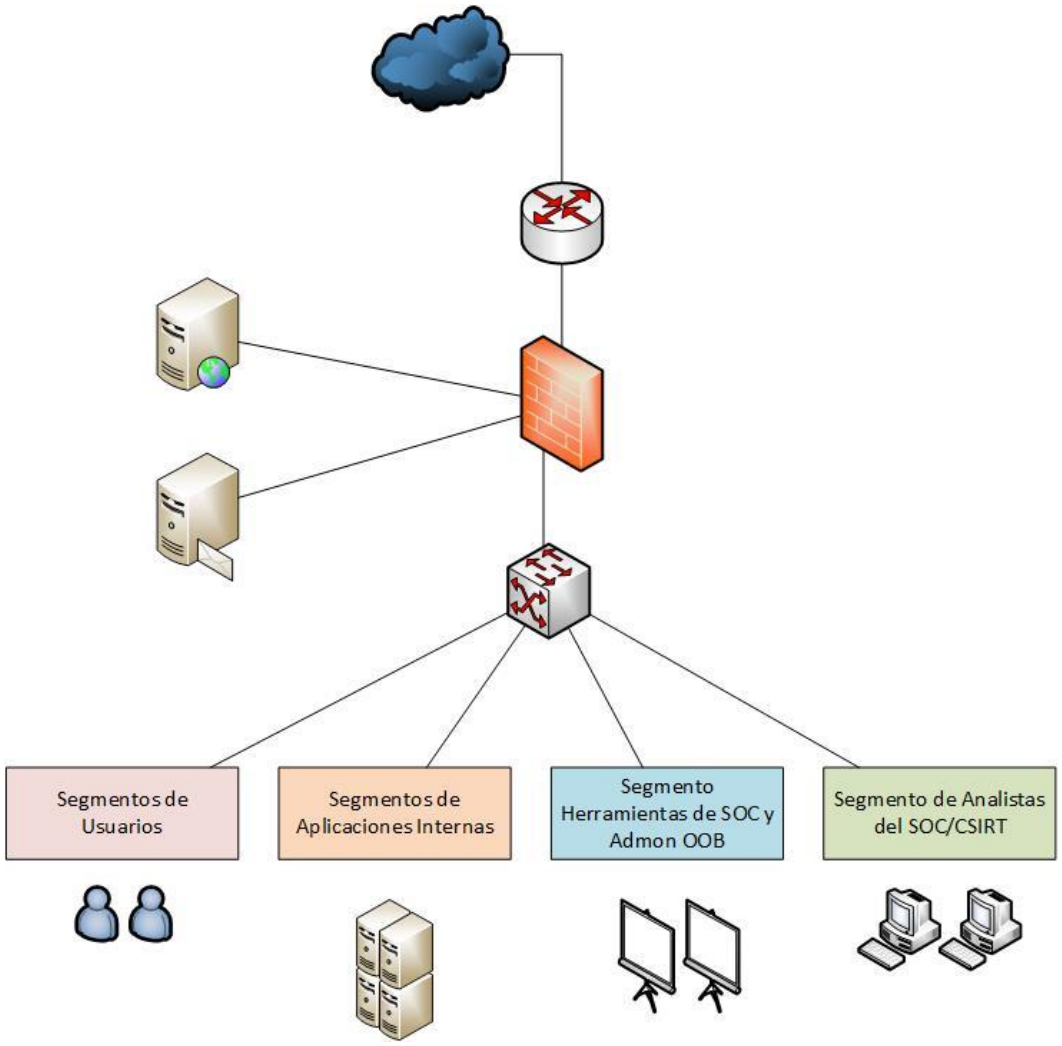


Ilustración 5 Diagrama Infraestructura SOC/CSIRT

Sistemas Operativos

El tipo de Sistema Operativo que se vaya a utilizar estará en dependencia de la herramienta que se utilice, muchas veces existen versiones de la misma herramienta tanto para Windows como para Linux.

Almacenamiento:

Para el adecuado funcionamiento del SOC es necesario poder recolectar, procesar y almacenar toda la información generada por los dispositivos que se estén monitoreando. Es preciso contar con sistemas de almacenamiento adecuados que garanticen que la información estará disponible para su debido análisis.

Colaboración:

La correlación, el análisis de la información generada por los dispositivos monitoreados y las repuestas a posibles incidentes de seguridad genera una base de conocimientos muy útil que puede ser utilizada para resolver casos futuros. En el caso del SOC para la UNI se utilizara como herramienta de colaboración, la herramienta MEDIAWIKI.

Sistemas de Administración de Tickets :

Si la recolección, correlación, y análisis de la información generada por los equipos Monitoreados permite descubrir una incidencia de seguridad, es necesario contar con personal que pueda dar respuesta a esa incidencia mediante un sistema de administración de incidencias que permita poder

administrar todo su ciclo de vida. En el caso del SOC para la UNI se utilizara la herramienta RTIR.

e) Generación y Recolección de Eventos de Seguridad

Uno de los elementos más importantes en el monitoreo de dispositivos es la generación de eventos. Cada dispositivo presente en una infraestructura de TI en su mayoría tiene capacidad para poder generar eventos ante situaciones específicas. Toda esta información generada, debe de ser recolectada y analizada para poder obtener información que lleve a descubrir un incidente de seguridad. La herramienta que se utilizara para este fin será un SIEM que no es más que una combinación de un administrador de información de seguridad (SIM) – cuyo propósito es la de digerir grandes cantidades de información de logs y facilitar la búsqueda en los datos recolectados- y un administrador de eventos de seguridad (SEM) – cuya meta es la de consolidar y correlacionar grandes cantidades datos de eventos de tal forma que un administrador pueda priorizar eventos y reaccionar de manera adecuada. Para el caso del SOC de la UNI se utilizara el SIEM: ALLIENVAULT

Network Time Protocol (NTP): Los logs generados por los equipos deben de mostrar el tiempo real en que algún evento ocurrió, con el objetivo que se pueda correlacionar la información y que sea de utilidad para los Analistas del SOC a fin de poder determinar la respuesta a la incidencia presentada de manera rápida y eficiente. Para lograr este objetivo todos los dispositivos que vayan a ser monitoreados, deben de ser configurados a través de NTP con un servidor de tiempo.

f) Administración de Vulnerabilidades

En toda infraestructura de TI donde existan sistemas o proceso que apoyen la operación de una Organización, existe el riesgo de que de que estos sean

vulnerable a ataques de personas maliciosas (Hacker). La UNI no es la excepción ya que poseen una serie de sistemas de información de los cuales depende para realizar sus operaciones diarias.

Una tarea fundamental del SOC es la de identificar y remediar cualquier vulnerabilidad que puedan tener sus sistemas antes que sean explotadas por un hacker. A medida que las infraestructuras crecen se requieren más sistemas o más procesos y por lo tanto existen más vulnerabilidades, eso significa que el proceso de identificación y remediación es un proceso continuo que requiere de un **Sistema de gestión de Vulnerabilidades**, el cual no es más que un proceso cíclico de identificación, clasificación, remediación y mitigación de vulnerabilidades.

Servicios para la identificación de Vulnerabilidades.

Existen muchos servicios utilizados para identificar vulnerabilidades como por ejemplo: pruebas de penetración, evaluación de vulnerabilidades, evaluación de configuración, evaluación de cumplimientos y auditoria. Para el caso del SOC de la UNI, únicamente se utilizara el servicio de evaluación de vulnerabilidades.

Herramientas a Utilizar

La evaluación de vulnerabilidades – mediante la cual se obtiene una lista de vulnerabilidades que se utilizan para calcular el riesgo que representan al negocio y verificar la existencia de controles- se realizara utilizando las siguientes herramientas:

a) NMAP: Herramienta de Código Abierto utilizado para descubrimiento e inventario de redes, auditorias de seguridad.

b) Kali Linux: Herramienta de Código Abierto utilizadas para pruebas de penetración y diagnósticos forenses.

c) Openvas : Herramienta gratuita utilizada para identificación de vulnerabilidades y administración de vulnerabilidades.

g) Personas

Dentro del diseño del SOC de la UNI es importante definir el personal que estará a cargo de operarlo. Para ello se tomara como punto de partida los servicios que el SOC ofrecerá.

- *Servicio de Monitoreo*

Descripción: A través del Servicio de Monitoreo del SOC se pretende que el personal a cargo pueda observar eventos generados por los diferentes equipos en las herramientas de monitoreo como el SIEM basado en reglas predefinidas con el objetivo de detectar incidentes de seguridad y escalarlos al personal adecuado para su adecuada repuesta y remediación.

Beneficios: Minimizar la interrupción de los servicios de TI y el impacto cuando un sistema sea comprometido, debido a la rápida identificación de incidentes de seguridad su adecuado escalamiento y pronta repuesta.

Componentes del Servicio: El servicio de Monitoreo incluye los siguientes SubServicios

- ✓ Monitoreo de Eventos de Seguridad
- ✓ Manejo de Alertas y Tickets
- ✓ Escalamiento de Incidentes

Cobertura del Servicio: El servicio que ofrecerá el SOC de la UNI tendrá una cobertura de 24x7

Gestión y Responsabilidad del Servicio: El servicio será gestionado por el Administrador de Monitoreo de Seguridad del SOC y será su responsabilidad velar por el buen funcionamiento del mismo.

Niveles de Servicio: El servicio dispondrá de dos niveles de Servicio, el nivel 1 que estará a cargo de un Analista Junior , quien podrá escalar cualquier evento o incidencia que no pueda manejar al nivel 2 que estará a cargo de un Analista Senior. Estos a su vez reportaran al Administrador de Monitoreo de Seguridad del SOC.

- *Roles Requeridos*

Director del SOC: Es la persona encargada de Liderar la Operación del SOC y encargado de comunicación con las diferentes autoridades de la Universidad.

Administrador de Monitoreo de Seguridad: Es la persona encargada del Servicio de Monitoreo de Seguridad, le reporta al Director del SOC.

Analista de Monitoreo N1: Es un analista Junior que está a cargo del monitoreo de los eventos de seguridad y la información de correlación. Se

encarga de darle seguimiento al ciclo de vida de una incidencia encontrada, desde la apertura de un ticket (para el equipo CSIRT), seguimiento hasta el cierre de la misma.

Analista de Monitoreo N2: Es un analista Senior que está a cargo del monitoreo de los eventos de seguridad y la información de correlación de forma similar al N1 sin embargo tiene poder de tomar decisiones en casos especiales que lo requiera y que el N1 no pueda hacerlo.

Ilustración 6 Organigrama SOC - UNI

h) Procesos y Procedimientos

Una vez que se haya definido la estructura del personal que estará a cargo de la Operación del SOC, es necesario identificar y definir los Procesos y Procedimientos que se llevaran a cabo.

- Procesos

1. Administración de Eventos: está enfocado en el monitoreo de eventos que ocurren a través en la infraestructura de TI. Se incluyen los eventos bajo condiciones normales, condiciones esperadas y todo tipo de excepciones que involucre escalamiento. Se recolectan y analizan información de eventos para identificar incidencias potenciales que puedan comprometer los servicios.

   Procedimiento 1 – ***Monitoreo de Eventos***: El Analista Junior N1 estará a cargo del monitoreo de eventos de seguridad de la Infraestructura de la UNI, mediante la herramienta de monitoreo SIEM. En caso de que se detecte una incidencia de seguridad este utilizara la herramienta RTIR para abrir un ticket de incidencia y poderlo escalar al equipo de repuesta a Incidencias – CSIRT.

   Procedimiento 2 – ***Alertas Recurrentes:*** Ciertos eventos de seguridad pueden generar alertas recurrentes que no necesariamente significan un incidente de seguridad (Falso Positivo), el Analista Junior N1 debe identificar las alertas Recurrentes, analizarlas y tomar las medidas necesarias para que no se vuelvan a generar.

   Procedimiento 3 – ***Administración de Casos:*** El Analista Senior N2 estará encargado de todo el ciclo de vida de casos por incidentes de seguridad que se hayan (creación, actualización, cierre) generado.

   Procedimiento 4 – ***Base de Conocimiento:*** Una vez que el incidente de seguridad sea resuelto por el CSIRT, el Analista Senior N2 se encargara

de alimentar la herramienta de colaboración MEDIAWIKI para documentar el caso.

2. Administración de Incidencias: Como una de sus funciones principales el SOC debe de detectar y responder a los incidentes de seguridad que se presenten con el objetivo de ayudar a identificarlos y tomar acciones de la manera más rápida posible. Este proceso en el caso del SOC de la UNI será llevado a cabo por el CSIRT bajo la coordinación del Director del SOC. Debido a la estructura lógica del presente estudio los procedimientos de operación del CSIRT serán abordados en la sección correspondiente.

3. Administración de Problemas: Una vez identificado un incidente de seguridad, es de mucha relevancia investigar cual fue la causa de origen y bajo qué condiciones se dio, de tal forma que se puedan identificar defectos ya sea en los equipos o en las configuraciones. Dado que los incidentes de seguridad son escalados para ser abordados por el CSIRT, la investigación de las causas de los incidentes de seguridad también son abordados por el mismo equipo, por lo que los procedimientos asociados con este proceso también serán abordados en la sección correspondiente.

3.1.3 Fase de Construcción

a) Infraestructura de Red

- Se utilizara un equipo Capa 3 / 2 marca Cisco Modelo 3750G como conmutador Principal para la segmentación de red LAN.
- Se utilizaran 3 equipos Capa 2 marca Cisco Modelo 2960x como conmutadores de Acceso de los Usuarios y Equipos.
- Se utilizaran las siguientes VLANS y segmentos de red:

Segmento	Vlan	Red	Gateway
Red Usuarios	10	192.168.10.0/24	192.168.10.1
Aplicaciones y Servidores Internos	20	192.168.20.0/24	192.168.20.1
Analistas SOC	30	192.168.30.0/24	192.168.30.1
Herramientas SOC y Admon de Equipos	40	192.168.40.0/24	192.168.40.1

- Direccionamiento de Servicios y Equipos Relevantes

Servidor	Dirección IP
Servidor ISE AAA	192.168.40.10
SIEM	192.168.40.11
Sistema de Gestión de Tickets = RTIR	192.168.40.12
Sistema de Base de Conocimiento - Colaboración = MEDIAWIKI	192.168.40.13

b) Seguridad

- Se utilizara un equipo Cortafuego Perimetral marca Cisco Modelo 5525X
- Se utilizaran las siguientes tres Zonas de seguridad con sus respectivos segmentos :

Segmento	Red	Gateway	Nivel de Seguridad
Inside (Segmentos Internos Protegidos)	192.168.200.0/30	192.168.200.1	100
Outside (Segmento Externo Publico)	165.98.100.0/29	165.98.100.1	0
DMZ (Segmento de Servidores Públicos)	192.168.50.0/24	192.168.50.1	50

- Se utilizara un Sistema de Prevención de Intrusos (IPS) para analizar todos los segmentos de seguridad definidos.

- Toda la navegación a Internet de los usuarios deberá de hacerse a través de un WEB Proxy

- Para los Conmutadores y Enrutadores :

    - Se utilizaran Reglas de Control de Acceso para restringir el acceso de los segmentos no autorizados a la red de Administración de Equipos, Herramientas de SOC y Red de Analistas de SOC.

- La Autenticación, Autorización y Accountability de los equipos será realizada utilizando el Servidor AAA de la marca Cisco corriendo sobre plataforma virtualizada y con la siguiente parámetros:

  Grupo Primario de AAA : Tacacs+
  Grupo Secundario de AAA (en caso de que no responda el primario): Local
  Dirección IP del Servidor AAA : 192.168.40.10

- Los puertos de los conmutadores deben de ser configurados con parámetros de seguridad para permitir que se conecten solamente los equipos que autorizados , de forma similar también se debe de establecer una política de violación (Proteger, Restringir o Apagar) en el caso de que haya un intento de acceso no autorizado.

  Equipos Máximo permitidos en un puerto de un conmutador: 1
  Política de Violación en caso de acceso no autorizado: Shutdown

c) Sistemas

El SOC estará a cargo de monitorear no solo los dispositivos de red, sino también los equipos de los usuarios así como los servidores (tanto internos como externos) de la infraestructura de TI de la UNI.

- Sistemas Operativos

Como es conocido existen muchos sistemas operativos que pueden ser utilizados para los equipos de cómputo de los usuarios. Dado el grado de madurez en el mercado y compatibilidad se recomienda la utilización del Windows 7. Para el caso de la Administración centralizada de los equipo y usuarios, se recomienda la utilización de Windows Server 2012.

- Endurecimiento de Equipos de Usuarios

    - Para garantizar un nivel de seguridad adecuado en los equipos de usuarios, se deben de tomar en cuenta los siguientes elementos:
    - Deshabilitar todos los servicios innecesarios.
    - Aplicar los permisos adecuados a archivos, servicios, equipos de usuarios y eventos de registros.
    - Aplicar parches de manera automatizada.
    - Utilizar Antivirus.
    - Utilizar Políticas de Restricción de Software.

- Detección de Incidentes en Equipos de Usuarios

Además de los elementos planteados en el punto anterior, en los equipos de los usuarios se debe de utilizar sistemas que tengan capacidad de detectar amenazas avanzadas persistentes (APT).

d) Colaboración

El SOC de la UNI brindara dos servicios específicos, monitoreo y repuesta a incidentes de seguridad. Para este propósito se utilizara un sistema de Telefonía IP que permita de manera unificada poder realizar llamada tanto de voz como de video, esto como complemento a los servicios de colaboración ya establecidos (MEDIAWIKI – para la base de conocimiento de incidentes de seguridad y la herramienta de seguimiento a casos RTIR).

e) Infraestructura Final del SOC

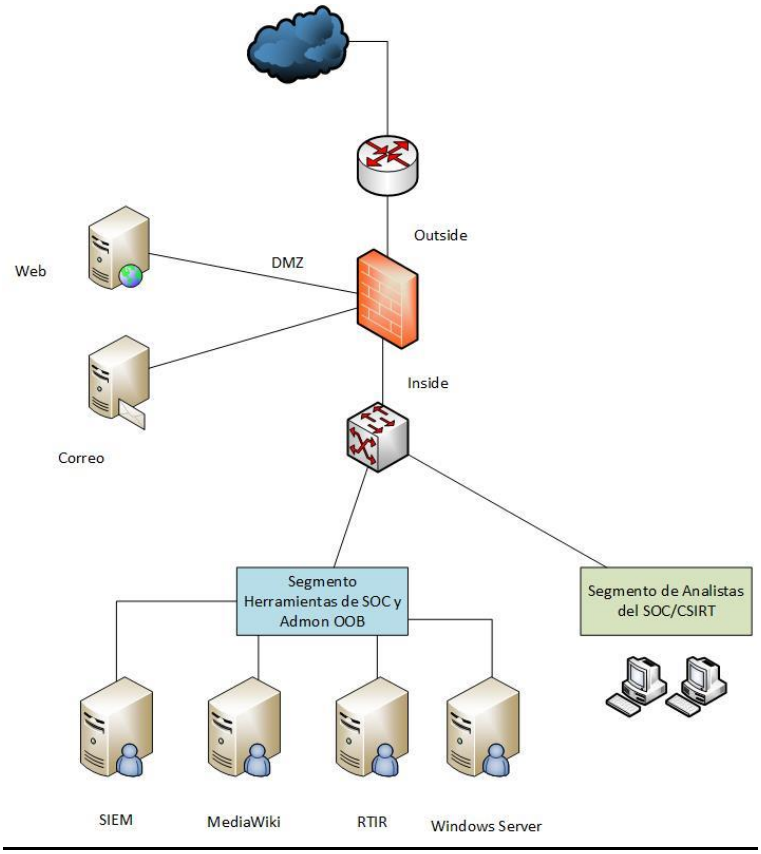


Ilustración 7 Diagrama de Red / Herramientas SOC - CSIRT

3.1.4 Fase de Operación

En esta última fase de la Creación del SOC se procederá a detallar los procedimientos que involucran el proceso de *Administración de Eventos*

Procedimiento 1 – ***Monitoreo de Eventos***

Los dispositivos de Red, Seguridad, Usuarios y Servidores de la Infraestructura de TI de la UNI estarán configurados para enviar todos los eventos que generen al SIEM. Este a su vez además de recolectarlos se encargara de correlacionarlos a través de reglas predefinidas que permiten la automatización en el descubrimiento de incidentes de seguridad. Cuando esto

ocurre el SIEM crea un alerta y envía un correo de notificación al correo compartido de los Analistas del SOC. La alerta de Seguridad también puede ser notificada por los mismos usuarios a los Analistas del SOC a través de correo electrónico, teléfono, mensajería instantánea.

Procedimiento 2 – ***Alertas Recurrentes y Clasificación***

Una vez que el Analista del SOC, que se encuentre de turno, recibe la notificación de la alerta realiza las siguientes actividades:

- Ingresar al SIEM y revisar todo tipo de alertas y eventos asociados.
- Recopilar mayor información sobre la alerta tales como: Flujo de Tráfico, Direcciones IP Origen y Destino, Usuarios asociados, bitácoras de acceso tanto lógico como físico, sistemas afectados. En caso de que dentro de la recopilación de información se viere involucrado un usuario especifico, el Analista del SOC deberá contactarlo por teléfono para indagar sobre la alerta presentada.
- El paso anterior le permitirá al Analista determinar la clasificación de la alerta, la cual puede ser clasificada como baja = nivel 0 y como alta = nivel 1.
- En el caso de que una alerta sea clasificada como bajo = 0, el Analista tendrá la capacidad de poder resolverla y documentarla a través de la herramienta de Colaboración MEDIAWIKI.
- Las alertas clasificadas como baja, habitualmente resultan por equipos mal configurados o alarmas recurrentes que no representan una real amenaza para la infraestructura de TI.

Procedimiento 3 – ***Administración de Casos***

- Si el analista del SOC determina (después de la recopilación y análisis de la información) que la alerta debe ser clasificada como alta = 1. Este debe de hacer uso del Sistema de Administración de Incidentes y generar un reporte de incidente. Este reporte de incidente debe de llevar adjunto toda la información recopilada por el Analista del SOC y debe ser escalada o notificada mediante correo electrónico y llamada telefónica al equipo de guardia del CSIRT.

Procedimiento 4 – ***Base de Conocimiento y Seguimiento***

- Una vez que el Analista del SOC haya creado un reporte de incidencia y lo escalo al equipo de guardia del CSIRT, debe de darle seguimiento continuo y realizar informes de estado enviados por correo electrónico cada una hora al administrador del servicio de monitoreo. Al mismo tiempo deberá alimentar la base de conocimiento a través de la herramienta MEDIAWIKI.

El siguiente Diagrama de Flujo muestra el proceso de Administración de Eventos:

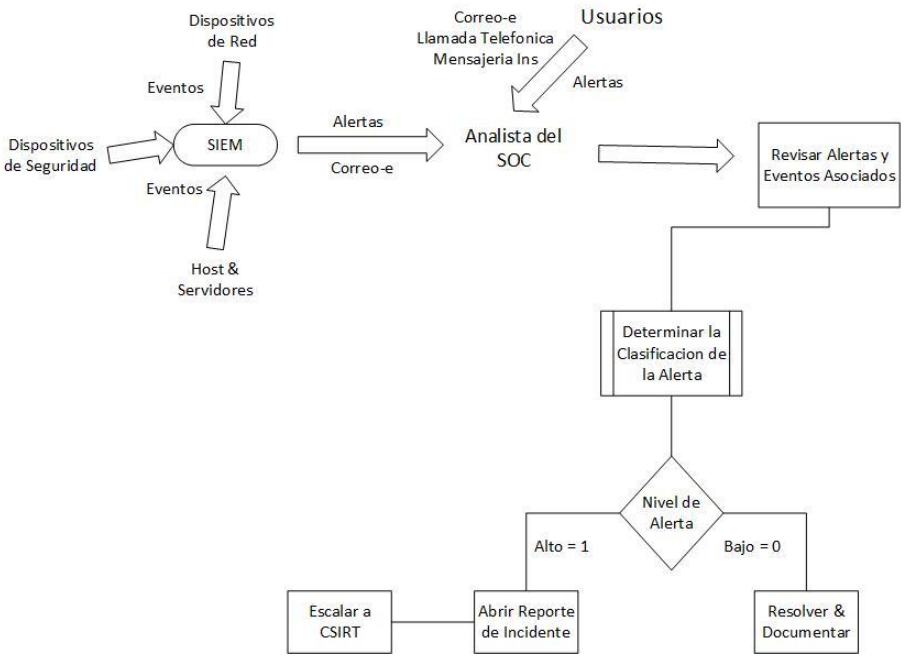


Ilustración 8 Diagrama de Flujo Administración Eventos

3.2 Creación de un CSIRT

El presente estudio no solo abarca la creación de un SOC (cuyo servicio principal es la de monitoreo de alertas), sino que también incluye la creación de un CSIRT quien es el encargado de dar repuesta a los incidentes de seguridad detectados.

El mundo de hoy es un mundo cambiante en el que los incidentes de seguridad son altamente dinámicos, no existe por lo tanto una metodología específica para la creación de un CSIRT, ya que dependerá de los requerimientos y el ambiente en el cual operara. Para la creación del CSIRT de la UNI se tomara como referencia el Libro de Trabajo para la creación de un CSIRT por West-Brown, Stikvoort, Kossakowski, Killcrece, Ruefle , Zajicek (2003), el cual propone un proceso de 3 etapas:

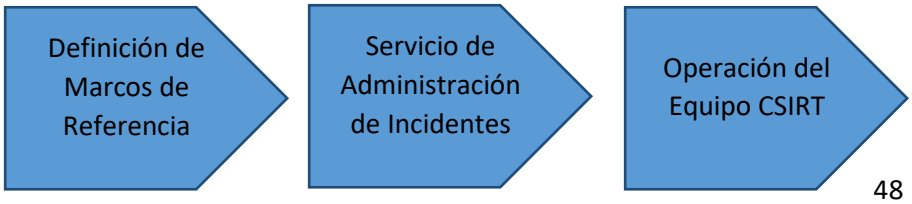


Ilustración 9 Etapas de Creación de un CSIRT

A continuación se muestra el desarrollo de cada una de ellas:

3.2.1 Definición de Marcos de Referencia

a) Bases

- *Misión del CSIRT*

Mejorar la seguridad de la infraestructura de TI de la UNI y minimizar el impacto que resulte de los ataques e incidentes de seguridad.

- *Circunscripción*

Hace referencia a la comunidad de usuarios a la que el CSIRT ofrece sus servicios. El CSIRT de la UNI tiene como usuario meta, para brindar sus servicios, al Recinto Principal.

El nivel de Autoridad entre el CSIRT y su comunidad de usuarios es **Completa**: Lo que significa que los miembros del CSIRT tienen la autoridad para tomar cualquier acción o decisión en nombre de los usuarios.

- *Ubicación dentro de la UNI*

El CSIRT de la UNI estará y formara parte del Centro de Operaciones de Seguridad de la UNI (SOC). Tanto el SOC como el CSIRT están conformados por equipos independientes con tareas limitadas pero relacionadas entre sí.

- *Relación con Otros Equipos*

EL CSIRT estará directamente relacionado con el equipo de Analistas del SOC, son los dos equipos en conjuntos los que brindan la protección de seguridad a la infraestructura de TI de la UNI. El equipo SOC encargados del monitoreo, análisis y clasificación de las alarmas y el CSIRT quien son los encargados de responder ante un eventual incidente de seguridad.

b) Servicios

Existen varios servicios que un CSIRT puede ofrecer, sin embargo para el caso específico de la UNI, únicamente brindara servicios de carácter reactivo dentro de los que podemos mencionar:

- Administración y Repuesta a Incidentes, el cual incluye :
    - Análisis de Incidentes.
    - Repuesta de Incidentes en Sitio.
    - Soporte a Repuesta a Incidentes.
    - Coordinación de Repuesta a Incidentes.

c) Flujo de Información

El CSIRT ejecuta una serie de actividades a lo interno y a lo externo que deben de ser coordinadas adecuadamente para que el flujo de información se realice de manera correcta y no se desperdicien recursos valiosos.

Los reportes de incidentes creados por el equipo de analistas del SOC de la UNI, son enviados a un correo compartido del CSIRT. El o los miembros del CSIRT que se encuentren de turno serán los encargados de recibir el reporte de incidencia, analizarlo y abrir un caso si lo amerita.

Una vez abierto el caso, se hace una investigación más profunda y de requerirlo se notifica el Administrador del CSIRT quien estará a cargo de

establecer las coordinaciones necesarias tanto a lo interno, con los subequipos (forense) o lo externo con otras entidades relacionadas.

3.2.2 Servicio de Administración y Repuesta a Incidentes

3.2.2.1 Descripción de los Servicios

En el punto anterior se mencionó que el equipo CSIRT de la UNI brindara un servicio reactivo. En esta sección se hará una descripción detallada de los mismos.

Análisis de Incidentes

A través de este servicio se pretende identificar el alcance del incidente, el daño causado, su naturaleza y las estrategias de repuesta disponibles para su resolución. EL CSIRT puede hacer uso de dos subservicios para este análisis:

1. Recolección de evidencia Forense: recolección, preservación, documentación y análisis de evidencia de un sistema o equipo comprometido que ayuden a determinar los cambios al sistema y asistan en la reconstrucción de hechos previos al incidente.

2. Rastreo: seguir las huellas del intruso o identificar los sistemas al cual el sistema tuvo acceso.

Repuesta de Incidentes en Sitio

El CSIRT provee asistencia directa en sitio, para ayudar a sus usuarios a recuperarse de un incidente. Físicamente analiza y procede a la recuperación y reparación de los sistemas afectados. EL CSIRT realiza esta actividad ya sea a través de un equipo local que se encuentre en las instalaciones del SOC, o en caso de no estar presente a la hora del incidente hacerse presente a la

brevedad posible. Este servicio aplicara cuando por alguna razón no pueda ser resuelto mediante teléfono o correo.

Soporte a Repuesta a Incidentes

El CSIRT asiste a la víctima a recuperarse del incidente o ataque a través de correo o teléfono. Provee asistencia técnica en la interpretación de los datos recolectados, proveyendo guías sobre estrategias de mitigación y recuperación. Este servicio no incluye asistencia en sitio y más bien se realiza de manera remota de tal forma que el personal en sitio pudiera realizar la recuperación por su propia cuenta.

Coordinación de Repuesta a Incidentes

El CSIRT coordina las acciones o comunicaciones que se realicen con otras entidades a la hora de un incidente de seguridad. Entre las entidades tenemos, la propia víctima, servicios de Monitoreo de Alarmas (ubicado dentro de la UNI-SOC), servicios de inteligencia externos, otros CISRT. La coordinación no incluye acciones de repuesta a incidentes, más bien se trata de poder brindarle la suficiente información a las entidades externas a través de una comunicación fluida para que de alguna forma puedan contribuir a la resolución del incidente.

3.2.2.2 Objetivos

- Proveer un punto único de contacto para la atención, prevención y respuesta a incidentes de seguridad de la UNI.
- Proveer un servicio de calidad para la protección de las Infraestructuras Criticas de TI de la UNI.

- Promover las políticas que generen buenas prácticas en materia de seguridad de la información en la UNI.

- Promover la concientización a los usuarios de la UNI en materia de seguridad de la información.

3.2.2.3 Alcance y Profundidad de los Servicios

El servicio de Administración y Repuesta a incidente será llevado a cabo a lo interno de la UNI por miembros del equipo CSIRT conformados por 4 personas, el administrador, dos analistas de incidentes y un analista forense.

El CSIRT formara parte del SOC de la UNI como equipo independiente y a cargo administrador del CSIRT quien además estará a cargo de la coordinación con otras entidades que participan en el proceso. Debajo del Administrador estarán los analistas quien son los encargados directos de atender los reportes de incidencias abiertos por los analistas del SOC, son adicionalmente los que darán apertura a los casos y trabajaran de manera conjunta con los otros analistas para la resolución de los casos.

Debido a la alta especialización técnica requerida por los miembros del CSIRT, su puesta en marcha incluirá una seria de capacitaciones previas que los prepare para poder hacer frente a los incidentes que le sean reportados.

3.2.2.4 Disponibilidad

El servicio que brinde el CSIRT estará disponible para todos los usuarios de la UNI, en un horario de dos turnos (mañana y noche) durante los 7 días de la semana. El servicio será provisto una vez que se reciba un reporte de incidente a través del correo centralizado del servicio.

3.2.2.5 Aseguramiento de la Calidad

Con el objetivo de asegurar la calidad en el proceso de la administración y repuesta a cualquier incidente presentado, el equipo CSIRT debe dar una repuesta, al usuario del servicio , inicial de aceptación y verificación del reporte de incidencia en un tiempo comprendido entre 15 y 30 minutos.

Cada 60 minutos el analista a cargo deberá de bridar mediante la herramienta de seguimiento a casos una retroalimentación sobre el estado o avance del caso, de tal forma que todos los involucrados estén al corriente.

3.2.2.6 Interacciones y Divulgación de la Información

Como se planteó en secciones anteriores, las alertas pueden venir de los equipos que están siendo monitoreados e inclusive de parte de los mismos usuarios. Una vez que los analistas del SOC determinan (con los análisis realizados) que hay necesidad de abrir un reporte de incidencia, toda la información recopilada hasta ese momento (correos, archivos, enlaces) son incluidos como parte del reporte que luego será utilizado para realizar mayores análisis y estudios por el equipo CSIRT.

3.2.2.7 Relaciones con Otros Servicios

Como ya se planteó en secciones anteriores el CSIRT forma parte del SOC de la UNI como equipo independiente, pero relacionado con el equipo de analistas del SOC.

3.2.2.8 Funciones de los Servicios

A continuación se muestran un diagrama con las funciones de los servicios que el CSIRT ofrecerá a los usuarios de la UNI.

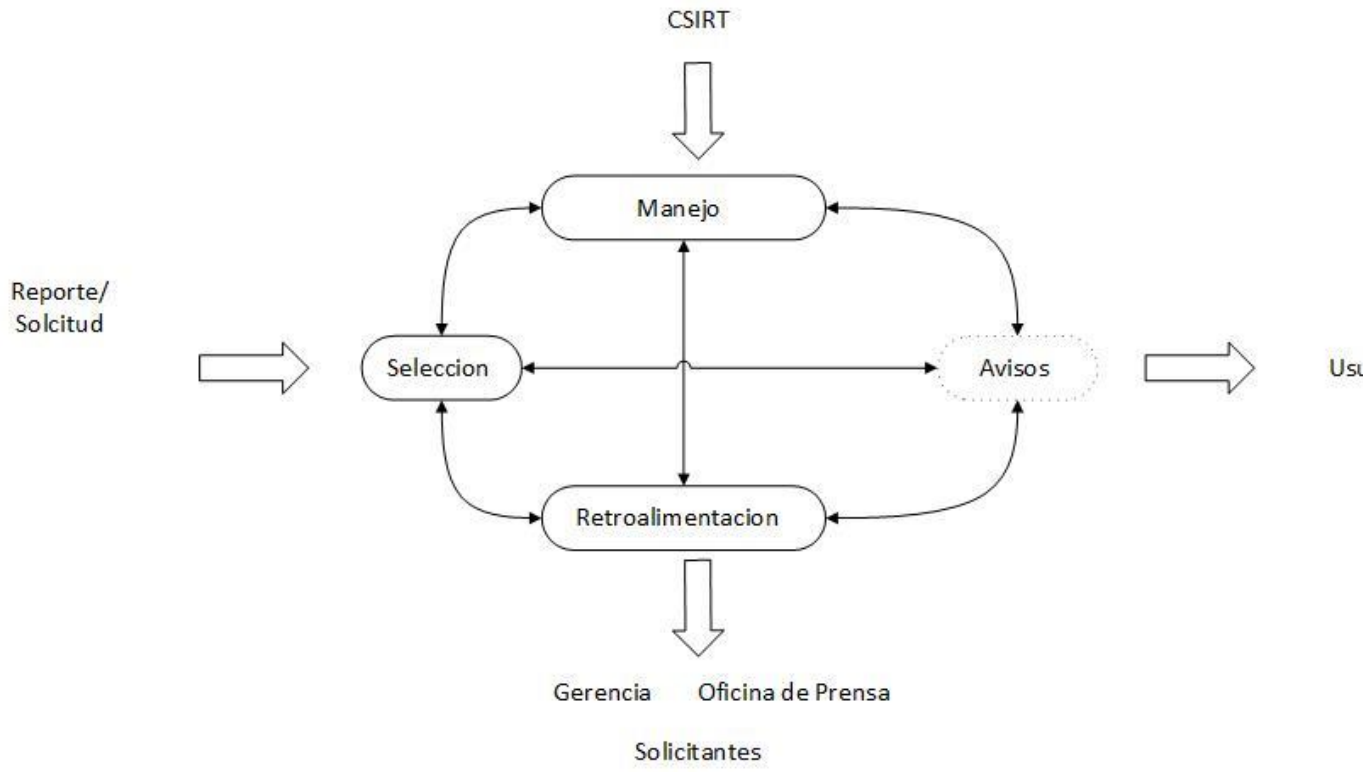


Ilustración 10 Funciones de Servicios de CSIRT

a) <u>Selección / Recepción</u>

Esta es la función a través de la cual se reciben los reportes de incidentes, el cual es canalizado a través de un punto único de contacto independientemente del origen. Para el caso específico será un correo electrónico único (compartido) que permitirá el manejo y distribución de los reportes.

El administrador del Servicio de Manejo a Incidentes dará a conocer a los analistas del SOC toda la información de contacto del equipo y la disponibilidad de los mismos (calendario).

El procedimiento a Seguir para reportar un reporte de incidente es el siguiente:

- Una vez que se ha determinado por parte de los analistas de monitoreo del SOC que una alerta no representa un falso positivo , que no puedo ser resuelto por ellos y que requiere de análisis más profundo, se procede a abrir un reporte de incidencia y se escala vía electrónica al correo compartido del equipo CSIRT.

- Se contacta al analista de turno del equipo CSIRT y se le notifica el reporte de incidencia.

- El reporte de incidencia debe incluir toda la documentación de soporte que respalde los hallazgos y condiciones encontradas hasta ese momento por los analistas del SOC.

- El analista de turno del equipo CSIRT debe de notificar el recibido del reporte de incidente.

Basada en la información que se reciba, esta puede ser:

- Clasificada: Para determinar el tipo de incidente que se está presentando.

- Priorizada: Basado en el impacto que pueda tener en el funcionamiento normal de la UNI.

- Rastreada: Debe determinarse si el reporte de incidente está asociado a uno ya existente, o a uno completamente nuevo. En este último caso se le debe asignar una prioridad inicial en el sistema de manejo de incidentes.

- Escalada: Si el analista de CSIRT determina que requiere de un servicio más especializado (por ejemplo Forense), puede notificárselo al administrador del servicio de CSIRT para que se realicen las coordinaciones necesarias para el escalamiento.

- Cuando el equipo de analistas del CSIRT comienza a trabajar sobre un reporte de incidente y determina que este requiere análisis a profundidad, procede a abrir un caso de incidente, el cual a su vez sirve para darle seguimiento, poder escalar a otros especialistas y para poderlo documentar, de tal forma que sirve como base de conocimiento para casos futuros.

- La apertura de casos de incidentes, son controlados en el sistema de administración de incidentes y se les debe asignar un numero de caso con el siguiente formato AAMMDD-IS/UNI#; Ano, Mes, Día-Incidente de Seguridad/Universidad de Ingenieria#Numero . El número será entero e iniciara desde el 1 hasta 999999 de manera secuencial.

b) Manejo

Esta es la función a través de la cual se provee repuesta y soporte a los incidentes de reporte recibidos, en este caso, de los analistas de monitoreo del SOC.

Para realizar esta función se debe contar por lo menos con los siguientes atributos:

- Punto de Recepción de Reportes: Los reportes de incidencia serán recibidos utilizando las mismas facilidades de correo electrónico (centralizado) establecidas para el SOC de la UNI.

- Análisis: Se contemplan todos los análisis técnicos necesarios para poder dar una respuesta satisfactoria sobre el incidente.

- Notificación: Se notifica la repuesta o información de recuperación del incidente.

Ilustración 11 Ciclo de Vida del Manejo de un Incidente

El ciclo de vida del Manejo de un incidente es un proceso cíclico que inicia cuando el equipo de analistas del CSIRT abre un caso, este a su vez puede pasar por varios estados o etapas, - análisis, obtención de información, asistencia técnica, coordinación y repuesta, de manera cíclica hasta que el caso es cerrado cuando ninguna de las partes involucradas en el incidente reportan nueva información, debido en la gran mayoría de los casos a las repuestas oportunas de parte del CSIRT.

Análisis de Incidentes

Constituye el rol o la actividad principal dentro del ciclo de vida del Manejo de Incidentes, ya que permite poder tomar las decisiones y/o coordinaciones necesarias. El análisis que llevara a cabo el CSIRT de la UNI tendrá como objetivo principal analizar cualquier evidencia dejadas por actividades de los intrusos tales : como virus, trojanos, log files etc; análisis de los ambientes de los programas en los cual se generó el incidente y análisis de una red de confianza del incidente.

Para poder realizar un análisis de incidentes adecuados se tomara en cuenta los siguientes elementos

Visión Global : Se debe obtener toda la información detallada de todos los mecanismos posibles (estudios de casos, tendencias, base de conocimiento), con el objetivo de poder mejorar los tiempos de repuesta de futuros incidentes.

Análisis a Profundidad

Una vez que el analista del CSIRT tiene acceso al reporte de incidente, procede a realizar una investigación más profunda.

El nivel de profundidad de análisis que realizara sobre un incidente de seguridad estará en dependencia de factores como: capacidades técnicas, severidad del incidente, si es un incidente nuevo o previamente conocido.

Las actividades mínimas a realizar de parte del equipo CSIRT son:

- Análisis de Archivos de Logs : Generados por todas las plataformas tanto de hardware como de software que estén siendo monitoreados. A través de estos se pretende lograr obtener información acerca de cuándo y de donde accedieron los usuarios, que tipo de protocolo utilizaron para ingresar (Telnet, SSH,rlogin) e información acerca de flujo de correos electrónicos. Los dos elementos más importantes que se deben de garantizar con los archivos de logs son : Las marcas de tiempo, las cuales deben de ser lo más precisa posible, hecho que se logra mediante la utilización de servidores NTP y el Origen de los archivos de logs para identificar el equipo correcto.

- Análisis de Archivos Sospechosos: Todos los archivos (ejecutables , texto, etc) que sean considerados sospechosos pueden haber sido dejados por los intrusos como parte del incidente de seguridad, por lo tanto estos deben de ser analizados con mucho cuidado y en un ambiente aislado de tal forma que no se corra riesgo de afectar a otros usuarios en caso de que la sospecha sea afirmativa.

- Análisis del Ambiente de Software: Este tipo de análisis debe de ser realizado en coordinación con el anterior, para poder determinar sobre que programas o software el archivo sospechoso tiene algún tipo de afectación.

- Análisis de conexiones Relacionadas: Habitualmente los atacantes llevan a cabo un incidente de seguridad a través de diferentes redes y conexiones relacionadas con el objetivo de que no puedan ser identificados. Si se logra obtener el centro u origen de esas conexiones se podrá identificar el origen del incidente.

c) Avisos

Es a través de la función de aviso que el CSIRT puede dar a conocer los resultados (de diferentes formas) sobre las investigaciones que ha realizado para dar respuesta a los incidentes de seguridad. Esta función será realizada por el administrador del Servicio de CSIRT.

- Tipos de Avisos: El CSIRT de la UNI brindara los siguientes

Aviso Simple: Se sabe que ocurrió un incidente de seguridad, pero no se tiene información a profundidad. Se dará a conocer a los usuarios mediante las vías correspondientes.

Alertas: Se incluye información completa sobre ataques reciente y nuevas vulnerabilidades que pudieran afectar a los sistemas críticos.

Mensajes Consultivos: Se incluye información a mediano y largo plazo a cerca de problemas y soluciones con el objetivo de crear conciencia y ayudar a evitar incidentes.

FYI (Para su información): Son similares que los mensajes consultivos pero con menos especificaciones técnicas y con una audiencia más amplia. En este tipo de avisos se incluirán guias y procedimientos para evitar futuros incidentes.

Medios y Frecuencia de Publicación: Indistintamente del tipo de aviso que el CSIRT genere, estos serán enviados a los usuarios a través de listas de correo electrónico y de forma similar serán publicados en la página web oficial del CSIRT.

A quien va dirigido: Se deben de establecer un sistema de clasificación de los avisos (basados en los contenidos) a fin de poder enviarlos a los usuarios correspondientes.

- Ciclo de Vida de los Avisos :

Inicio: En esta etapa se debe de determinar el tipo de aviso, el tipo de contenido y la audiencia meta tomando en cuenta los siguientes parámetros: Estilo y Formato con que será escrito y canales de distribución.

Prioridad: En esta se determinara la prioridad con que serán publicados y enviados los anuncios. Cualquier anuncio que se realice debe de ser priorizado de manera interna.

Desarrollo: En esta etapa se realizara una descripción general y técnica del aviso. Se utilizaran modelos pre-establecidos de acuerdo al tipo de aviso que se vaya a generar.

Preparación Final: Antes de generar el aviso definitivo se deberá de realizar una revisión final del contenido y definir el formato de presentación.

Distribución: Una vez establecido el formato final del anuncio se procederá a distribuirlo utilizando los mecanismos previamente definidos.

d) Retroalimentación

La retroalimentación del estatus y desarrollo de la investigación que se lleve a cabo sobre un incidente de seguridad garantizara que el CSIRT de la UNI ofrezca un mejor servicio y permita clarificar cualquier duda que pudieran tener los usuarios.

El CSIRT de la UNI publicara los avances que se vayan teniendo sobre los incidentes de seguridad través de la plataforma de Base de Conocimiento. Adicionalmente estará anuente a contestar cualquier tipo de duda que tengan los usuarios como las autoridades de la UNI.

e) Manejo de Información

Para realizar su función adecuadamente el CSIRT depende de la información, esta debe de ser recolectada y manejada de forma adecuada utilizando el sistema de seguimiento de incidentes de seguridad. Se debe de considerar los siguientes elementos en el manejo de la misma:

- Recolección de la Información: La información que le llegue al CSIRT para su análisis puede ser recolectada de manera automática, a través del sistema de monitoreo de la infraestructura de TI, o de forma manual a través de la recopilación de reportes técnicos, análisis, noticias, evidencias etc.

- Verificación de Información: La información obtenida debe de ser verificada antes de que sea utilizada como soporte o evidencia de un caso, al menos debe de verificarse: su origen, su contenido, y el medio de distribución.

- Categorización de la Información: La información obtenida será clasificada de la siguiente manera: Información Privada / Información Pública; Información Urgente / No Urgente.

- Almacenamiento de La Información: La información de manera almacenada en dispositivos que permitan acceder a grandes cantidades de información de manera segura.

3.2.3 Operación del Equipo CSIRT

Una vez abordado a detalle las funciones que contempla el servicio de administración de repuesta a incidentes, es necesario plantear todos los elementos operativos que el CSIRT de la UNI necesitara para desarrollar su función.

3.2.3.1 Elementos Básicos de Operación

a) Organigrama

b) Horarios de Trabajo

Los horarios de trabajo del CSIRT de la UNI serán:

Horario Normal: de 8 am a 6 pm
Turnos: de 6 pm a 8 am

c) Equipos de Comunicación

El equipo CSIRT dispondrá de un teléfono en sitio con autorización de llamadas locales, celulares e internacionales. Tanto el administrador del Servicio de CSIRT como el analista forense dispondrán de teléfonos móviles que permita ubicarlos de manera rápida cuando se requiera coordinación con entidades expertas o externas.

d) Correo Electrónico

El equipo CSIRT dispondrá de un correo electrónico centralizado utilizado para la recepción de los reportes de incidentes de parte del equipo de analistas del SOC. De forma similar este correo será utilizado para cualquier comunicación o proceso de escalamiento que se requiera.

e) Acceso a Internet

Cada analista del CSIRT dispondrá de acceso a Internet para poder realizar cualquier consulta e investigaciones adicionales que se requiera.

f) Segmentación / Dirección IP / Dominio

El equipo CSIRT tendrá sus oficinas operativas dentro de las instalaciones del SOC de la UNI. De manera similar a como el equipo de SOC utiliza un segmento de red independiente, de esa misma forma también el equipo CISRT utilizara un segmento independiente dentro de la infraestructura de red de la UNI.

Para efectos de identificación, al equipo CSIRT de la UNI se le asignara un subdominio del dominio principal de la UNI, con la siguiente estructura: ***CSIRT.uni.edu.ni.***

g) Seguridad de Red & Host

Dado que la infraestructura de cómputo con la que trabajara el CSIRT de la UNI estará en las instalaciones del SOC, la seguridad tanto en red como en host serán las mismas establecidas para los equipos de cómputo del SOC,

esto incluye Cortafuegos perimetral, Listas de Control de Acceso, Políticas de AAA.

3.2.3.2 Políticas Fundamentales

a) Código de Conducta

Todos los miembros del equipo CSIRT estarán regidos por el código de conducta CSIRT-UNI. A través del cual se provee guías básicas de la manera como deben de reaccionar los miembros ante diversas situaciones que se presenten, así como las interacciones que deben de realizar tanto a lo interno como externo del equipo.

1. Ser amable y diplomático con todos los usuarios que soliciten información general o sobre un incidente en específico.
2. Evitar la arrogancia.
3. Enfocarse en el trabajo que se realiza para evitar desaciertos.
4. Demostrar curiosidad sobre cualquier incidente reportado demostrando sigilo y precaución.
5. No crea en nadie sin antes haber verificado la información con los procedimientos adecuados.

b) Categorización de la Información

La información que maneje el CSIRT de la UNI utilizara el siguiente esquema de clasificación:

- ✓ Clasificada Total: Para uso exclusivo dentro del equipo CSIRT.

- ✓ Clasificada Parcial: Para un intercambio de información con los demás miembros del equipo basado en la necesidad de conocimiento.
- ✓ Socio Externo: Para intercambio con entidades externas al equipo CSIRT.
- ✓ Pública: Información Pública

c) Revelación de la Información

Toda la información que se genera a partir de una alerta o incidente de seguridad se convierte en información crítica para la UNI. A través del establecimiento de una política de revelación de información se garantizara que la información generada sea manejada y revelada adecuadamente y no se filtre bajo ninguna circunstancia.

Para la revelación de la información se consideran tres criterios:

Propósito: La información puede ser revelada por el equipo CSIRT siempre y cuando exista un propósito definido, el cual será analizado y aprobado por el administrador del Servicio del CSIRT.

Destinatario: La información puede ser revelada por el equipo CSIRT en dependencia del destinatario, el cual puede ser , miembros del mismo equipo, autoridades superiores, usuarios. Obviamente se debe tener claro del tipo de información que se revelara de acuerdo a la clasificación de la misma.

En caso de que la información necesite ser diseminada a otros miembros del equipo CSIRT o a entidades externas, este debe de ser etiquetada para que se identifique de manera clara el propósito que tiene la misma.

El tiempo en que la información será revelada dependerá de los avances que tenga el equipo CSIRT sobre el análisis del incidente. Sin embargo es importante que al menos se brinde información preliminar a los posibles usuarios afectados.

d) Políticas de Seguridad

A continuación se describen las políticas por las que estará regido el CSIRT de la UNI:

- Seguridad Física: Dado que el equipo CSIRT estará en las mismas instalaciones físicas del SOC de la UNI, contara con las mismas medidas de seguridad: entre las que se incluyen, bitácora de registros de acceso, acceso biométrico controlado, circuito cerrado de televisión.

- Plan de Respaldos y Recuperación: Todas las configuraciones y archivos ejecutables de cada uno de los sistemas que se utilicen para la operación del CSIRT, serán respaldadas semanalmente en un repositorio externo previamente establecido, a cargo del Administrador del Servicio de CSIRT. De forma similar todos los registros de eventos, alarmas, incidentes y correos que se hayan generados serán respaldados de forma diaria. En caso de un algún problema con la operación de un sistema o que se requiera tener acceso a un histórico de registros se deberá solicitar la información al Administrador del Servicio de CSIRT.

- Seguridad de Red Local: La seguridad de red Local del equipo CSIRT estará regida por las mismas condiciones de seguridad en red del SOC.

- Seguridad de Información Local : Toda la información generada o recibida como parte de una alerta, reporte de incidente o caso de incidente deberá ser clasificada y manejada con mucho sigilo y únicamente por el personal autorizado.

- Manejo de Incidentes: Una vez que se genere un reporte de incidencia por parte del equipo de analistas del SOC, estos serán escalados al equipo CSIRT para su debido manejo. Solamente el equipo CSIRT estará autorizado para poder realizar análisis a profundidad, aplicar acciones de remediación, solicitar información adicional y escalar con entidades externas (si así se requiere).

e) Políticas de Errores humanos

- En casos de que miembro cometa algún error involuntario que pudiese afectar la operación del CSIRT debe de comunicarlo a la brevedad posible a su superior inmediato.

- El superior inmediato (en este caso el administrador del servicio) debe de trabajar en conjunto con el equipo CISRT para poder contener el error de manera inmediata y evitar consecuencias posteriores.

- El próximo día hábil el administrador del servicio debe de convocar a una reunión extraordinaria para analizar las causas del error cometido con el objetivo de evitar que vuelva a ocurrir en el futuro.

- Dependiendo de la causa, se deben tomar acciones correctivas que involucren entrenamiento o educación en los procesos definidos.

- Si los errores son cometidos por el mismo miembro del CSIRT de manera repetida, se deben de tomar medidas administrativas.

3.2.3.3 Aseguramiento de la Continuidad

Existen ciertas amenazas no técnicas, sino más bien administrativas que pueden impedir el funcionamiento adecuado del equipo CSRIT a lo largo del tiempo. A continuación se muestran ciertos aspectos que ayudaran a mejorar la continuidad de las funciones del CSIRT.

- El administrador del Servicio de CSIRT debe de garantizar la cobertura de los turnos (tanto dentro como fuera de horario) con la asignación del recurso humano necesario.

- Se deben de respetar los horarios establecidos previamente para el cumplimiento de las tareas a cargo del CSIRT. En caso de que a algún miembro de CSIRT se le presente alguna situación imprevista debe de notificarlo de manera inmediata a su superior.

- En caso de que exista alguna falla en las políticas y procedimientos establecidos para el funcionamiento del CSIRT, se debe de convocar a una reunión extraordinaria para establecer las revisiones adecuadas.

- A fin de evitar situaciones de agotamiento y frustración dentro del equipo del CSIRT (que conlleve a una mala operación del mismo) es necesario garantizar: condiciones adecuadas de trabajo, complimiento programado de vacaciones y programa de incentivos.

- Se debe de establecer un programa de capacitación y educación constante que garantice que los miembros del CSIRT se sientan continuamente motivados.

- Se debe de trabajar en coordinación con el equipo de Infraestructura de TI de la UNI, para la elaboración de un plan de reemplazo de equipos eficiente, cuando estos llegaran a presentar algún problema.

- Se debe de contar con sistema de admiración del flujo de trabajo que garantice que las tareas se realicen de forma eficiente y ordenadas. Dado que las tareas principales con las que se tiene que lidiar son problemas (incidentes) de seguridad, en el sistema de administración de flujo se debe de incluir: detalle del problema, acciones tomadas, acciones subsiguientes.

3.2.3.4 Capacidad Técnicas y Profesionales del CSIRT

Las tareas desarrolladas por el CSIRT requieren no solamente de experiencia técnica de parte de sus miembros sino más bien lo ideal es una combinación de habilidades interpersonales y técnicas interrelacionadas entre sí que garanticen el buen funcionamiento del CSIRT.

A continuación se muestran las habilidades interpersonales y técnicas que debe de tener cada miembro del equipo CSIRT

- Interpersonales
  - ✓ Habilidades de buena comunicación oral y escrita.
  - ✓ Habilidad para seguir políticas y procedimientos.
  - ✓ Diplomacia para lidiar con otras entidades.
  - ✓ Ganas de aprender.
  - ✓ Habilidad para manejar el estrés y trabajar bajo presión.
  - ✓ Trabajo de equipo.
  - ✓ Integridad y confidencialidad para mantener la reputación y posición del equipo.
  - ✓ Habilidad para administrar el tiempo correctamente.
  - ✓ Capacidad de resolución de problemas.

- Técnicas Básicas

Se requieren que los miembros del equipo CSIRT tengan conocimiento básico en los siguientes elementos:

- ✓ Uso de Internet.
- ✓ Protocolos de Red (TCP, UDP, IP).
- ✓ Elementos de una Infraestructuras de Red (Conmutadores, Enrutadores).
- ✓ Aplicaciones y Servicios de Red (Correo, Web, SMTP, HTTP, FTP).
- ✓ Principios de Seguridad de la Información.
- ✓ Riesgos y Amenazas a Computadores y Redes.
- ✓ Vulnerabilidades y Ataques de Seguridad (Denegación de Servicios).
- ✓ Infraestructura de Seguridad en la Red (Cortafuegos, Detección de Intrusos).
- ✓ Seguridad de Equipos de usuario Final (Antivirus, Anti-Malware).

- Técnicas Especializadas (Opcional)

De forma adicional a las básicas se requieren de las siguientes técnicas especializadas. Estas capacidades son opcionales ya que no necesariamente los miembros del CSIRT deben de poseerlas al entrar a formar parte del equipo, estas podrán ser desarrolladas como parte del programa de educación y capacitación continua.

- ✓ Programación en más de 1 lenguaje de Computadoras.
- ✓ Administración de equipos de red y Seguridad.
- ✓ Administración de más de un Sistema Operativo.

3.2.3.5 Aspectos de Contratación de Personal

a) Contratación

Se debe de seguir un proceso de contratación de varias etapas a través del cual se identifique que el candidato tenga tanto las habilidades interpersonales como técnicas necesarias para desempeñar las funciones dentro del CSIRT de manera adecuada. A continuación se presentan las etapas requeridas:

- Pre Entrevista para verificación de documentos.
- Entrevista para evaluar las habilidades técnicas e interpersonales.
- Comprobación de Documentos y Referencias.
- Presentación técnica al candidato sobre las tareas del puesto.

a) Procedimientos de Llegada y Salida

Debido a la naturaleza sensible del CSIRT cuando se contrate a un nuevo miembro se deben de seguir los siguientes procedimientos:

Al Llegar: Cada nuevo miembro del CSIRT debe de firmas acuerdos de confiabilidad, no divulgación de información no autorizada y propiedad intelectual.

Al Salir: El superior inmediato al miembro del equipo del CSIRT que deje de laborar, debe de realizar procedimientos de finiquito enfocados especialmente en aspectos técnicos como:

- Cambio de claves (tanto personales como de sistemas).
- Revocación de Llaves tanto digitales como físicas.

- Retiro de dispositivos de seguridad y cualquier otro tipo que hayan sido asignados.
- Comunicación Oficial a todas las entidades relacionadas para garantizar que todos estén al tanto.
- Entrevista de Salida a través de la cual se le hace del conocimiento al miembro saliente los compromisos que tiene que cumplir en cuando a confidencialidad.

b) Entrenamiento

Como parte del programa de capacitación y educación continua a todos los miembros del equipo CSIRT se les brindara capacitaciones en los siguientes temas

- Educación Técnica Avanzada

  - ✓ Identificación de y Análisis de Intrusos.
  - ✓ Análisis de Incidentes.

  Administrativas

  - ✓ Entrenamiento en Políticas y Procedimientos.
  - ✓ Técnicas Organizaciones y Distribución de Trabajo.

Capítulo 4: Caso de Estudio utilizando Herramientas Open Source

4.1 Introducción

Dado que para la implementación real tanto del SOC como del CSIRT de la UNI se necesitan tanto recursos económicos, físicos, humanos como tecnológicos, los cuales no están disponibles en este momento, se desarrollará el presente caso de estudio mediante el cual se pretende demostrar cómo se lleva a cabo el proceso de monitoreo y repuesta a un incidente de seguridad por medio de un SOC y un CSIRT. Para ello se utilizará una infraestructura real de una empresa Ficticia llamada SegurosyMas pero con herramientas en su gran mayoría Open Source.

4.2 Escenario del Caso

a) Descripción de la Empresa : La Empresa SyM (Seguros y Mas) es una empresa con sede en Managua dedicada a ofrecer seguros en diferentes ramos del mercado y caracterizada por brindar un servicio al cliente de alta calidad. Dentro de los servicios ofrecidos tenemos :

- Asistencia de Pagos en Línea
- Cargos Directos
- Asistencia Pólizas
- Información Sitrack
- Siniestros
- Información General
- Estatus de Pólizas
- Coberturas
- Tipo de Cambio
- Recibos de Pago
- Asesoria Personalizada

b) Infraestructura Tecnológica: Como plataforma base para ofrecer sus servicios la empresa SyM cuenta con una infraestructura tecnológica de alto nivel que incluye tanto software como hardware. A continuación se muestra el diagrama

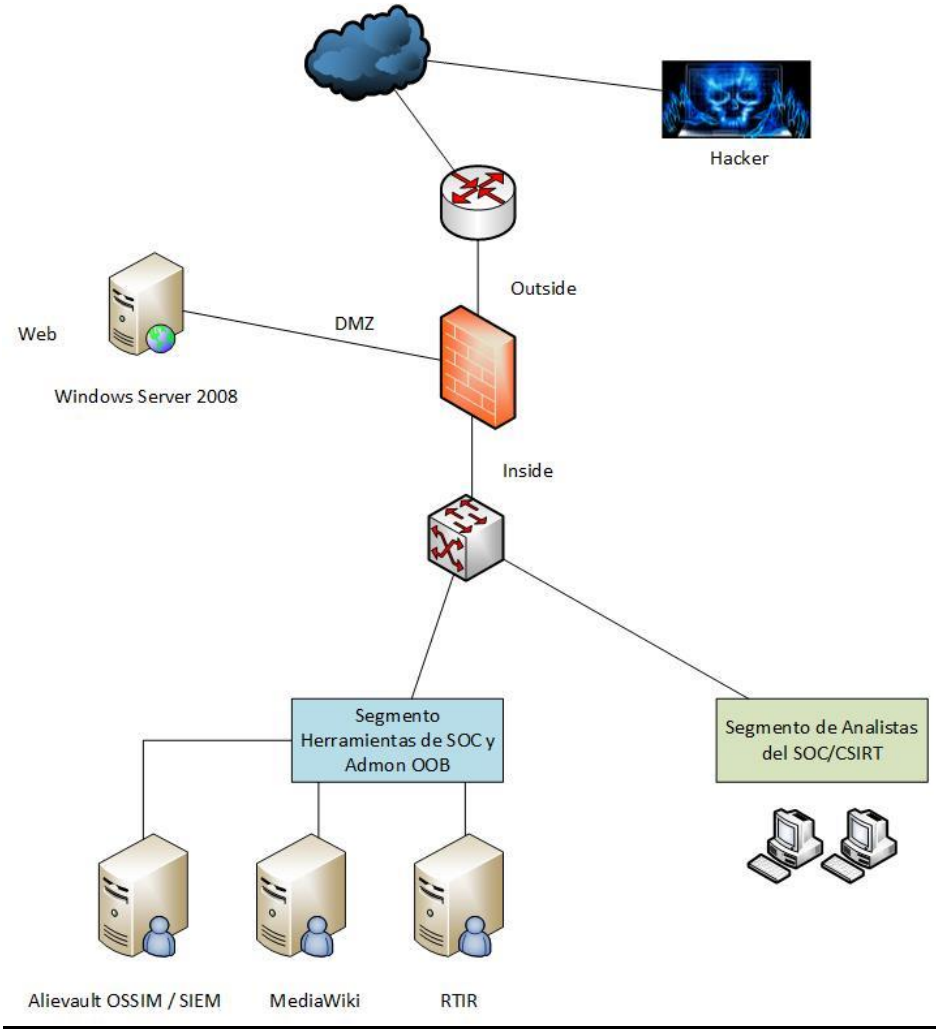


Ilustración 12 Diagrama de Caso de Estudio SyM

- Cortafuego: Dentro de la Infraestructura de SyM se cuenta con un cortafuego de seguridad cuya función principal es la de restringir el acceso desde el Internet hacia las diferentes zonas protegidas de la institución.

- Servidor Web y de Aplicaciones: Se cuenta con un servidor Windows 2008 Server donde se aloja la página web y las aplicaciones con las cuales SyM brinda sus servicios a sus clientes.

- Administrador de Eventos de Seguridad (SIEM): Alienvault OSSIM : Tanto el cortafuego como los servidores están configurados para que envíes sus logs hacia el SIEM para que sean analizados y correlacionados. Este a su vez sirve como plataforma de monitoreo para los analistas del SOC, ya que permite el envío de alarmas cuando se genera algún tipo de tráfico o evento sospechoso.

Ilustración 13 Herramienta de SIEM a utilizar - OSSIM

- Sistema de Manejo de Casos de Incidentes de Seguridad (RTIR): Sistema de Información que sirve para llevar a cabo todo el ciclo de vida de un Incidente de Seguridad. Utilizado tanto por los analistas del SOC como del CSIRT. Instalado sobre el Sistema Operativo Ubuntu 14.04

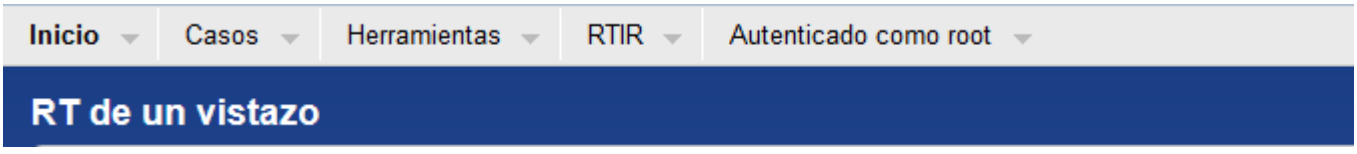


Ilustración 14 Herramienta de Administración de Incidentes a utilizar - RTIR

- Sistema de Colaboración: La herramienta MEDIAWIKI, es utilizada principalmente por el equipo CSIRT para elaborar una base de conocimiento e historial de los casos atendidos y presentados. Instalado sobre el Sistema Operativo 14.04

Ilustración 15 Herramienta de Colaboración a Utilizar - MEDIAWIKI

c) Personal

SyM cuenta con todo un departamento de TI dedicado a dar soporte a su infraestructura tecnológica. Dentro de los funcionarios más importantes de este departamento se encuentra **John López**, quien funge como Administrador de Redes y Servidores.

Dada la criticidad del negocio SyM también cuenta con Centro de Operaciones de Seguridad y un Equipo CSIRT quienes están a cargo de monitorear y dar respuesta a los incidentes de seguridad que se puedan generar dentro de la institución. **Sarah Madrigal** es la analista N1 del SOC de SyM con más de cuatros años de experiencia en el manejo de sistemas de monitoreo de seguridad de la información.

Roberto García es el analista N1 del equipo CSIRT de SyM, con vasta experiencia en repuesta a incidentes de seguridad y forense digital.

d) Simulación de Ataque

Toda institución que ofrece servicios públicos en Internet está expuesta a ser atacada. Dark Angel es un hacker como muchos en el Cyberespacio que ocupa la mayoría de sus noches para buscar sistemas que sean vulnerables en Internet. Son las 7:45 pm del 26 de Febrero de 2016 cuando **DarkAngel** termina de realizar el escaneo de un segmento de ip públicas que duro aproximadamente una hora, uno de sus resultados le llama la atención…..finalmente encontró una sistema vulnerable :

Job Name:	Scan Win 2008	Scan time:	2016-02-2
Profile:	Default - Non destructive Full and Fast scan	Generated:	2016-02-2

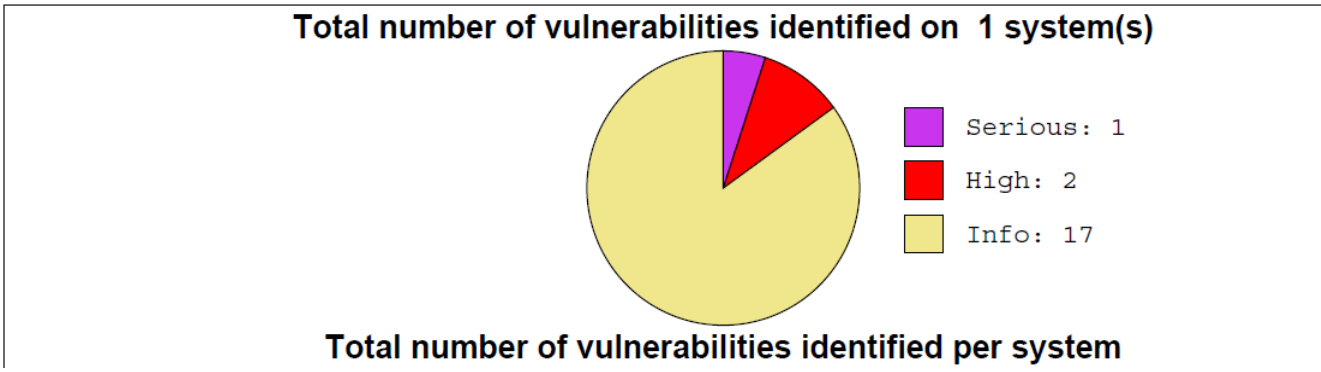


Ilustración 16 Reporte de Vulnerabilidad

Dentro de las vulnerabilidades encontradas, se da cuenta que existe una clasificada como crítica, que puede provocar una denegación de Servicios y la ejecución de código remoto. Investigando un poco más sobre la IP encontrada, descubre que pertenece a una empresa llamada SegurosyMas registrada con el dominio SyM.com y que además tiene los puertos 80, 445 y 3339 abiertos.

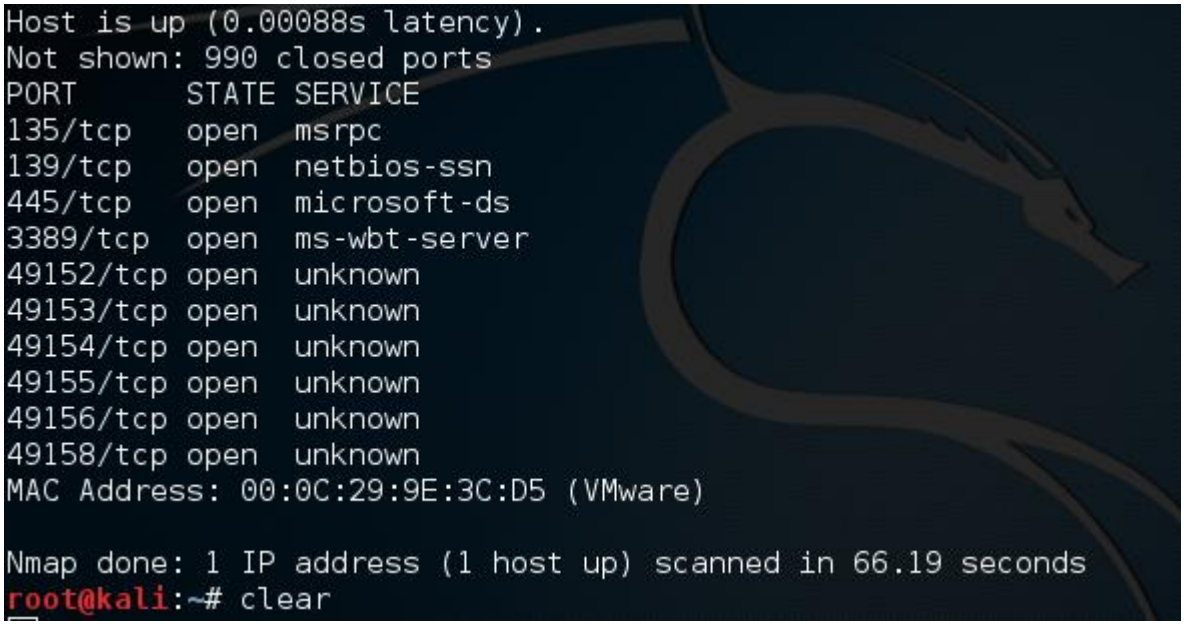


Ilustración 17 Puertos abiertos Encontrados

This host is missing a critical security update according to
Microsoft Bulletin MS09-050.
Insight:
Multiple vulnerabilities exists,
- A denial of service vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB version 2 (SMBv2) packets.
- Unauthenticated remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol software handles specially crafted SMB packets.

Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability
Risk: Serious
Application: microsoft-ds
Port: 445
Protocol: tcp
ScriptID: 900965
Impact:
An attacker can exploit this issue to execute code with SYSTEM-level
privileges
failed exploit attempts will likely cause denial-of-service
conditions.
Impact Level: System

Ilustración 18 Vulnerabilidad ms09-050

Con el objetivo de intentar acceder al equipo vulnerable, DarkAngel lanza tres tipos de ataques:

- Ataque de Fuerza Bruta : Utilizando la herramienta ***ncrack*** (incorporada en KALI LINUX) , el hacker intenta poder obtener las credenciales del sistema vulnerable aprovechando que el puerto 445 se encuentra abierto.

Ilustración 19 Ataque de Fuerza Bruta usando Kali Linux

- Denegación de Servicio

  De forma similar, también lanza un ataque de Denegación de Servicios (Dos) contra el equipo vulnerable:

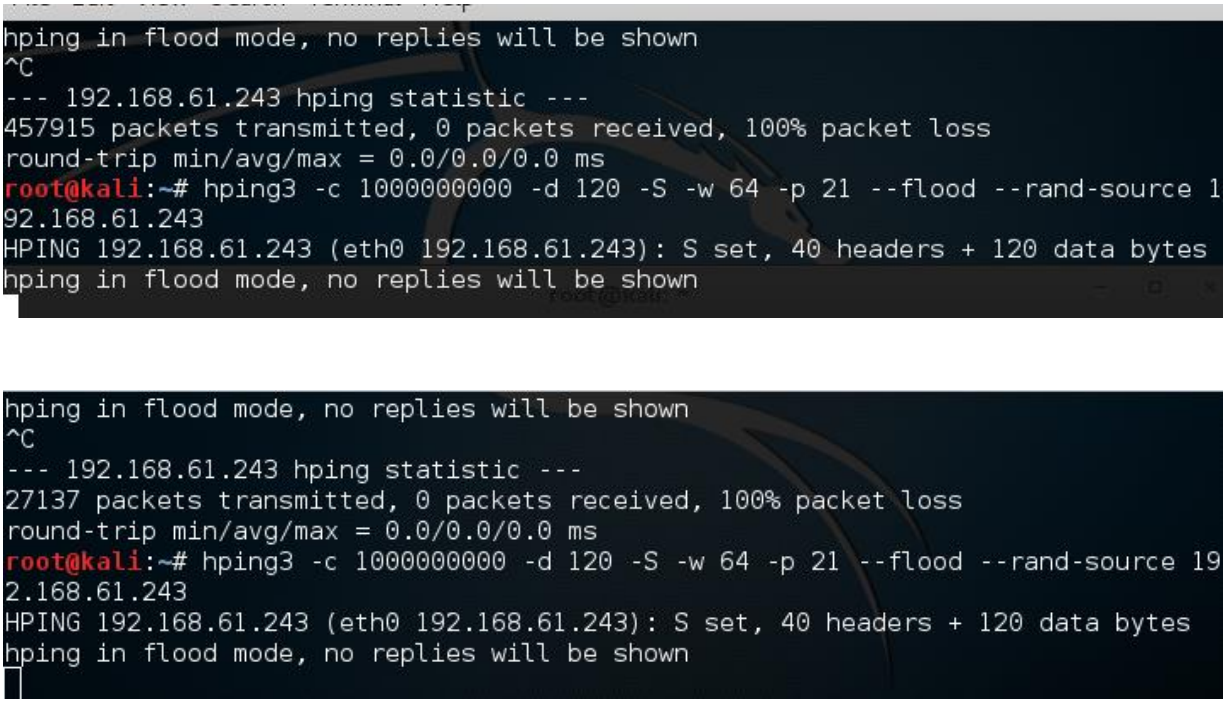


Ilustración 20 Ataque de Denegación de Servicios usando Kali Linux

- Ejecución de Código Malicioso

Aprovechando que el equipo es vulnerable a la Vulnerabilidad ms09-050 , DarkAngel crea un Archivo ejecutable con un icono y contenido falso (código malicioso MALWARE – a través de un RAT = Remote Administration Tool) como si fuera un juego de ajedrez y lo transfiere utilizando el Framework de METASPLOIT :

a) DarkAngel crea el Malware Apocalypse

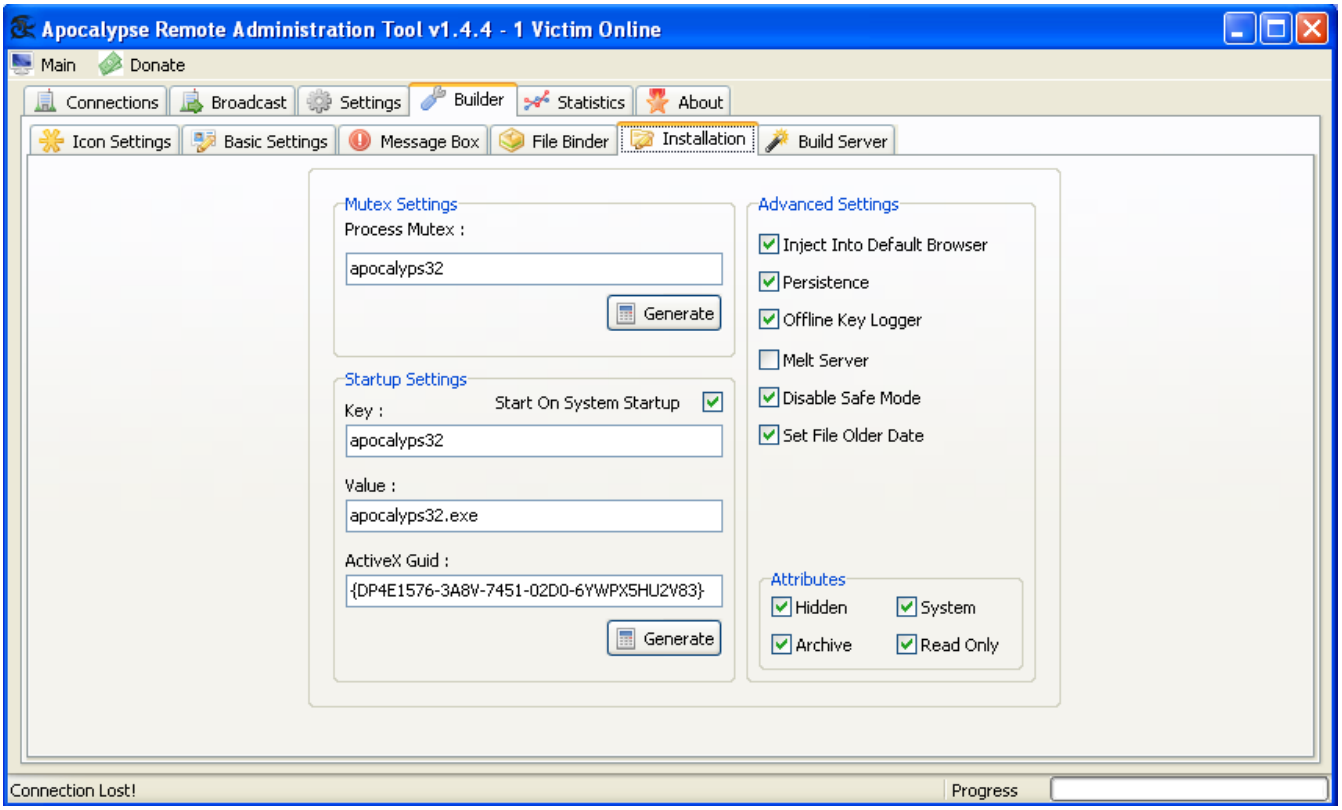


Ilustración 21 Creación de RAT Apocalypse

b) Crea un Icono y Nombre Falso

Ilustración 22 Malware Apocalypse32

c) Utilizando el Framework de Metasploit , explota la vulnerabilidad ms09-050 y logra conectarse al equipo remoto.

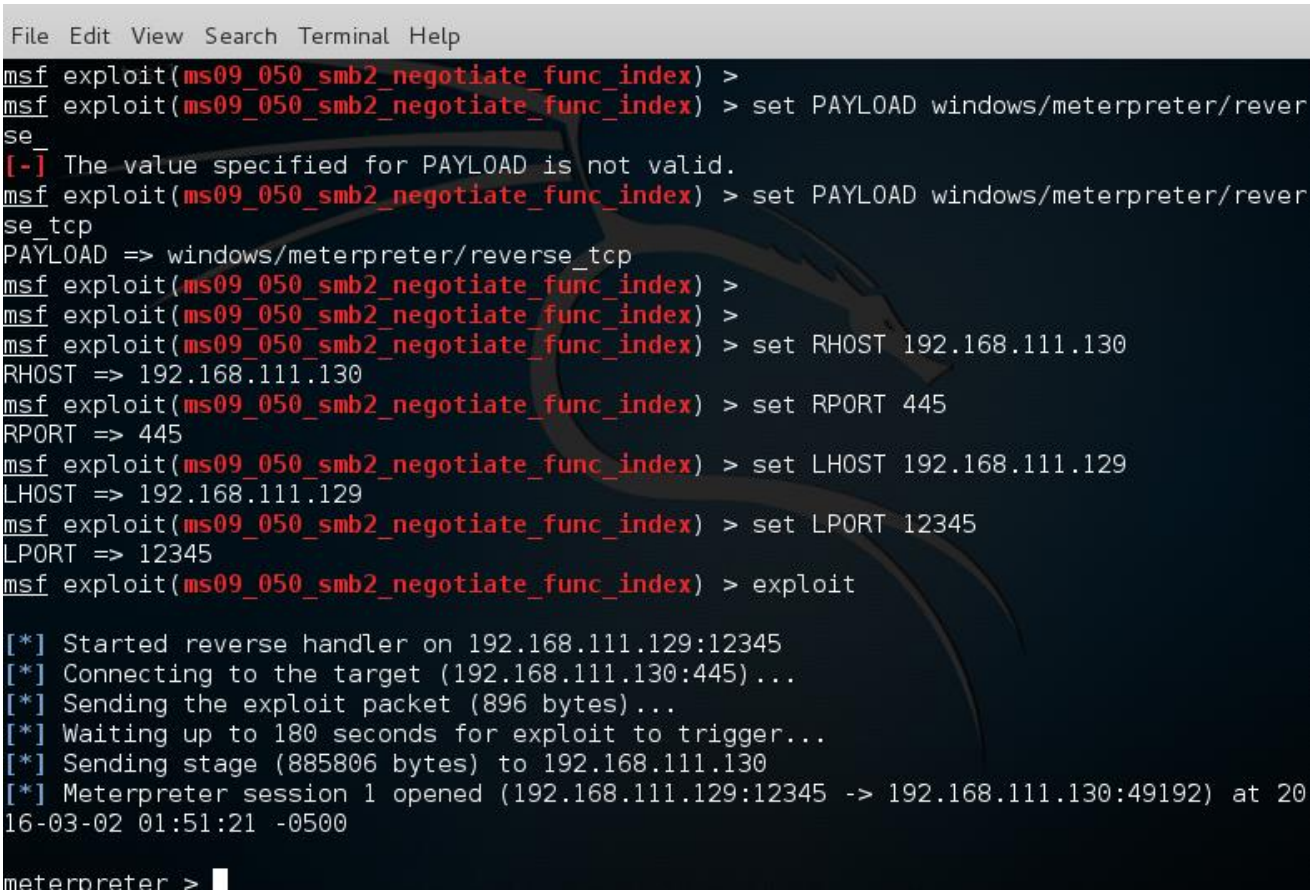


Ilustración 23 Explotación Vulnerabilidad MS09_050

d) Teniendo acceso al equipo remoto por medio del FrameWork de Metasploit transfiere el Malware Apocalypse a la carpeta Windows del equipo Vulnerable y luego la ejecuta.

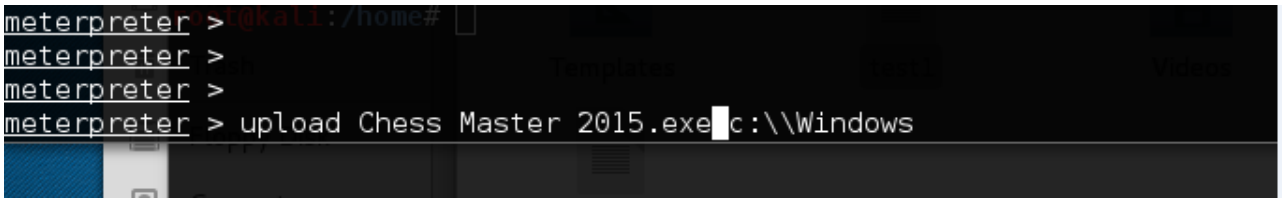


Ilustración 24 Inyección de Malware en carpeta Windows

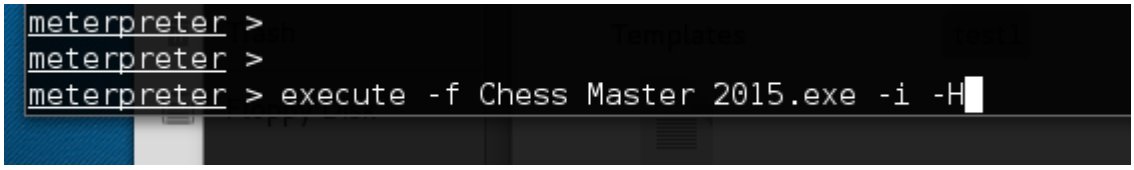


Ilustración 25 Ejecución de Malware remoto en Windows

e) El Malware Apocalype es una herramienta para administración remota, por lo tanto al ejecutarla (servidor) se establece una conexión con el cliente que está en la máquina del hacker.

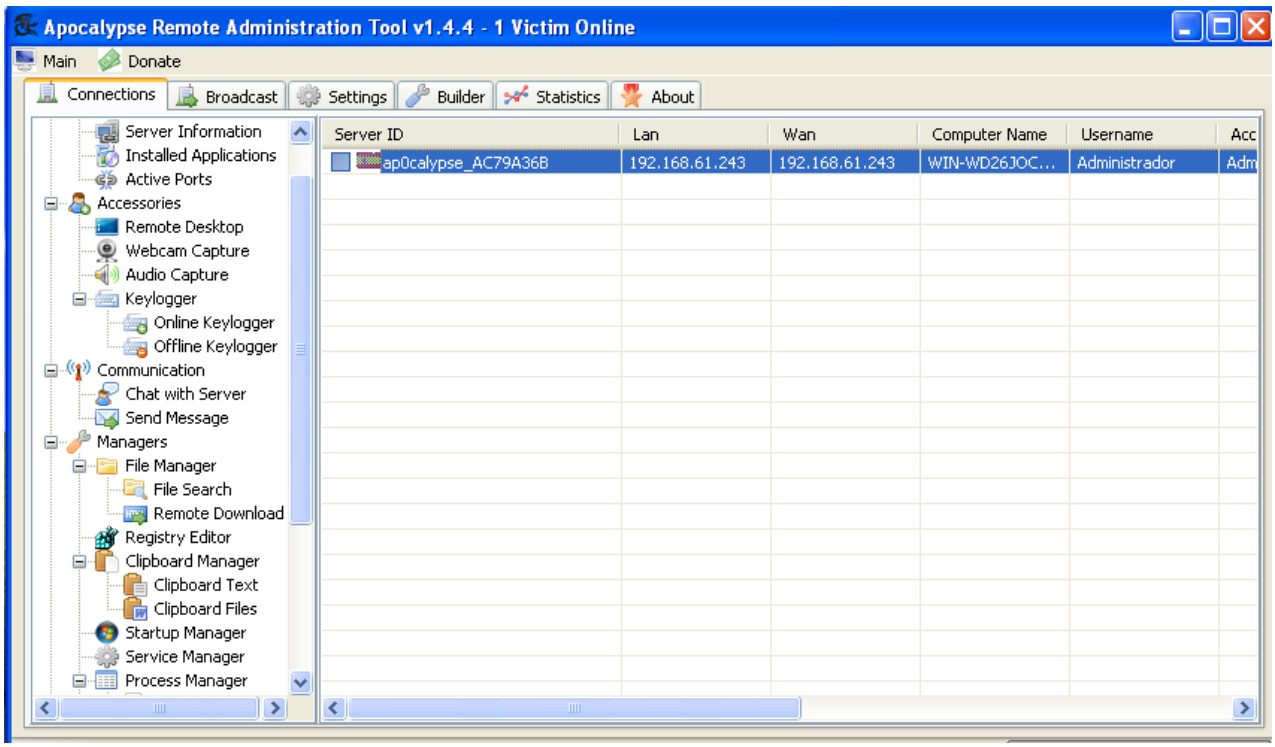


Ilustración 26 Malware Apocalypse Conectado

f) Al tener acceso remoto, el hacker puede acceder al equipo vulnerado, por lo que decide cambiar ciertos registros de ejecución del Malware y configuración de Internet Explorer.

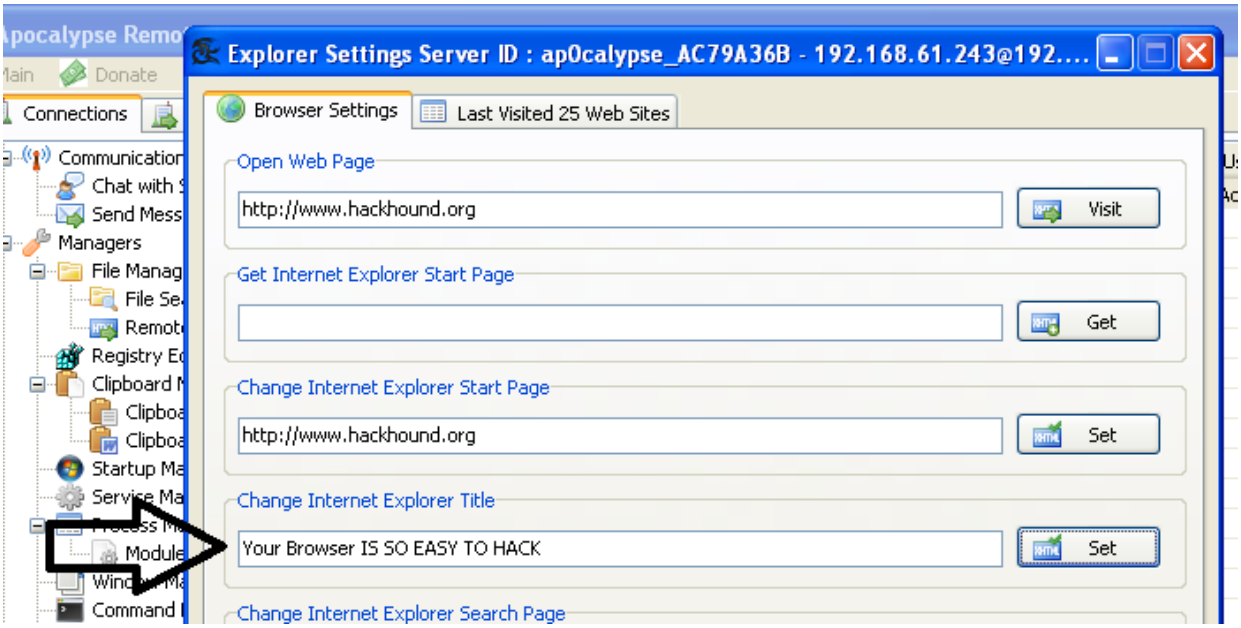


Ilustración 27 Modificación de Registros de IExplorer

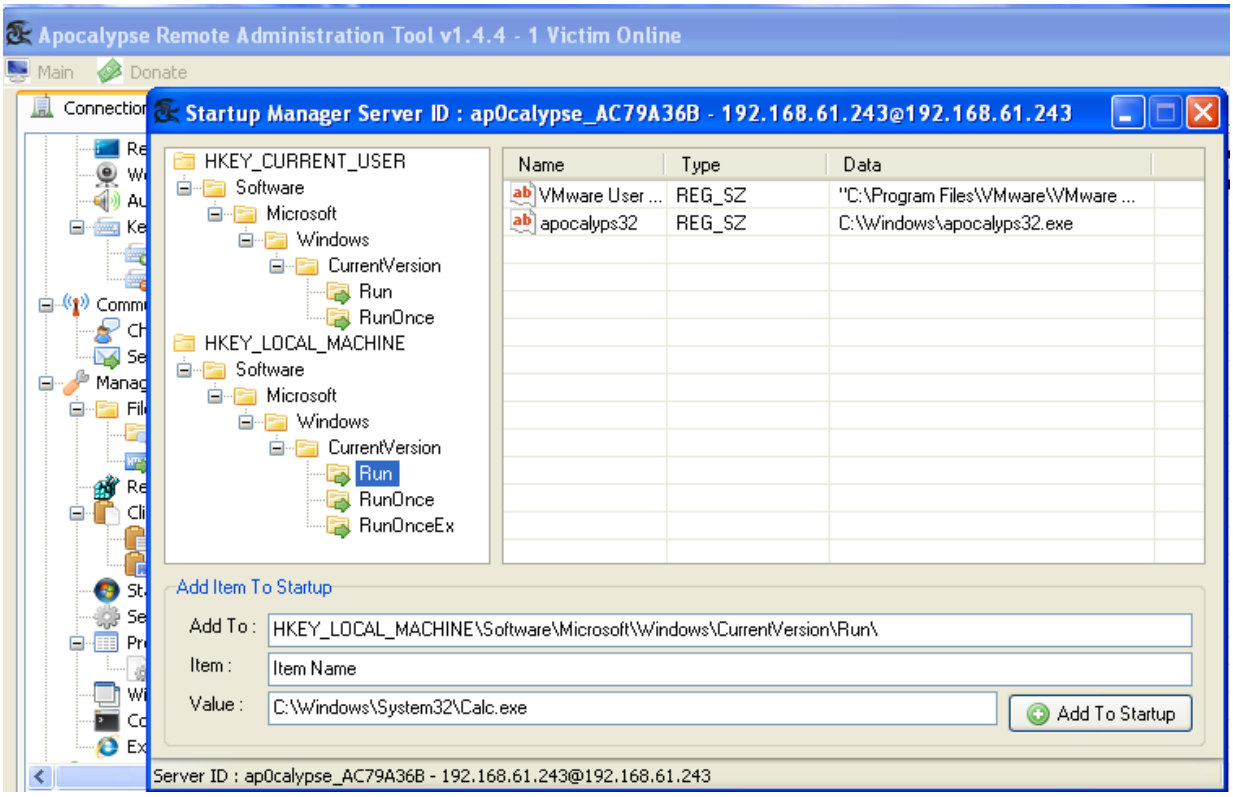


Ilustración 28 Modificación de Registros

e) Comportamiento Extraño / Alertas

El día previamente mencionado aproximadamente a las 9:00 pm, el administrador de Redes y Servidores John López decide quedarse después de las horas normales de trabajo, elaborando un informe que tiene que entregar a sus superiores al día siguiente. Como parte de sus rutinas de revisión antes de retirarse verifica la correcta operación del servidor Web y de Aplicaciones. Al ingresar al servidor nota que el desempeño del mismo está altamente degradado a tal punto que muchos de los servicios ni siquiera responden. Decide revisar la aplicación de monitoreo del mismo servidor y para su sorpresa el CPU del equipo se encuentra al 100% de utilización.

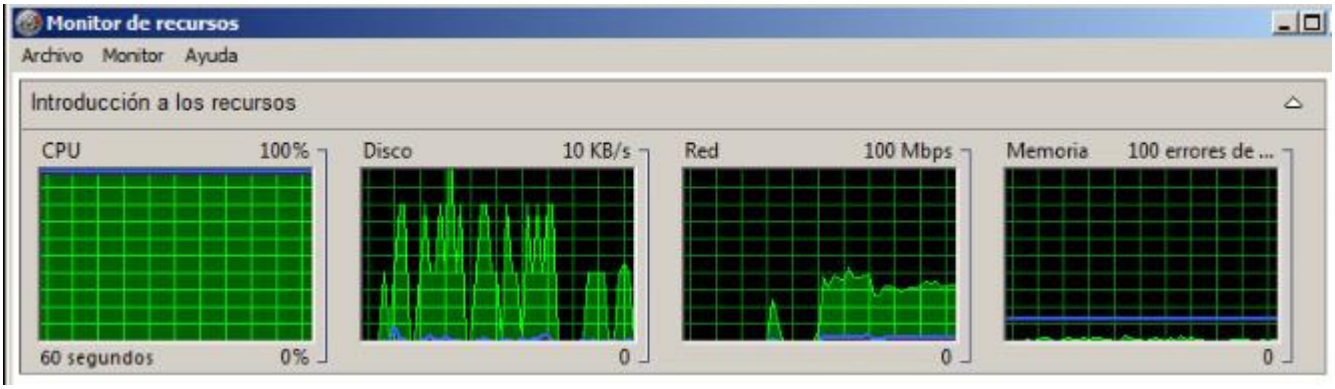


Ilustración 29 Evidencias de Ataque de DOS

Adicionalmente abre el Explorador de Internet para realizar una búsqueda sobre casos conocidos y similares al que está experimentando, solo para notar un mensaje sospechoso en la barra de título “Your Browser IS SO EASY TO HACK”

Alarmado por la situación, John decide llamar al Centro de Operaciones de Seguridad (SOC), para reportar lo sucedido, llamada que es atendida por Sara Madrigal analista de turno de monitoreo.

f) Reporte y Acciones del SOC

Al mismo tiempo que Sara está hablando con John, llega al correo del SOC: soc@SyM.com varias alertas generados por el SIEM OSSIM que indican los siguientes eventos:

De: SIEM [mailto:siem@SyM.com]
Enviado el: miércoles, 26 de febrero 2016 09:08 p.m.
Para: 'SOC@SyM.com';
Asunto: ¡!!ALERT!!! ¡!!ALERT!!! ¡!!ALERT!!! DOS Attack Attempt Detected

Alienvault NIDS: “ ET DOS Microsoft Remote DeskTop (RDP) Sync then reset 30 seconds DOS

De: SIEM [mailto:siem@SyM.com]
Enviado el: miércoles, 26 de febrero 2016 09:09 p.m.
Para: 'SOC@SyM.com';
Asunto: ¡!!ALERT!!! ¡!!ALERT!!! ¡!!ALERT!!! Brute Force Authentic action Detected

Alienvault NIDS: " Windows Authentication Attack Detectec"

Ilustración 30 Correo de Alarmas de Ataques

Sara recibe los diferentes mensajes, los observa rápidamente y decide acceder remotamente al SIEM para examinar las alertas y cualquier otro evento relacionado. Mediante las pantallas de Monitoreo Sara observa que efectivamente existen dos alertas que llaman su atención:

La primera hace referencia a un ataque de autenticación por fuerza bruta, que se dio en periodo aproximado de 7 minutos de duración.

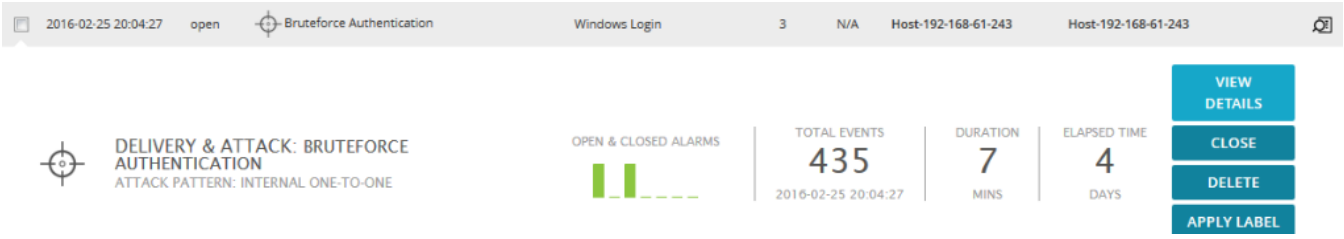


Ilustración 31 Evidencia de Ataque de Fuerza Bruta OSSIM

La segunda hace referencia a un ataque de Denegación de Servicio contra el mismo equipo.

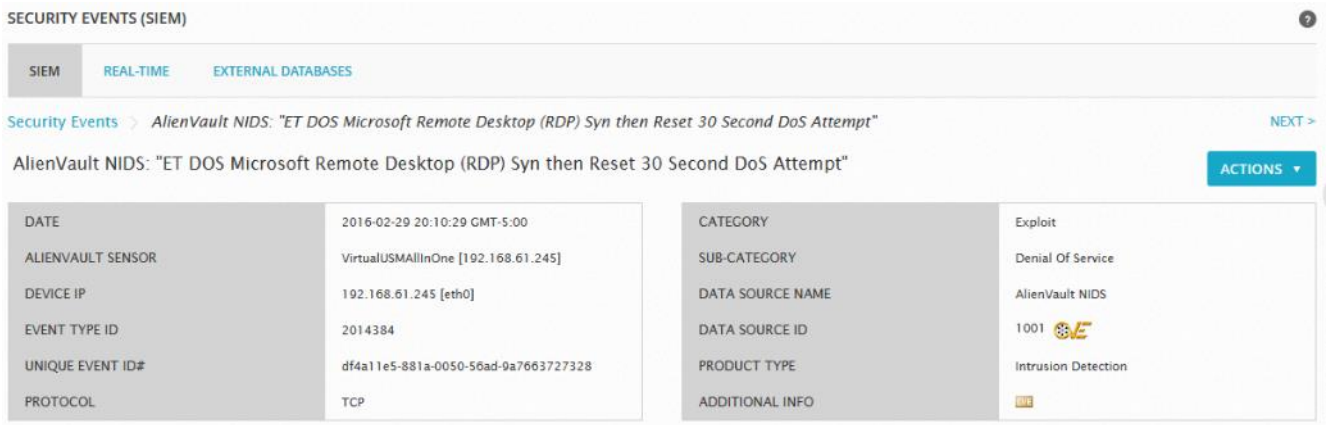


Ilustración 32 Evidencia de Ataque de DOS OSSIM

No segura de lo que estaba ocurriendo, Sara decide volver a llamar a John para asegurarse que los eventos que estaba viendo no habían sido causados por el. John sorprendido por las preguntas de Sara niega rotundamente que haya estado accediendo de forma errónea al equipo y le indica que simplemente que se encontraba realizando tareas administrativas y que de hecho le había llamado porque realizando las actividades normas de revisión del equipo había notado que el desempeño se encontraba degradado y que en el explorador de Internet había un mensaje extraño “Your Browser IS SO EASY TO HACK”

Después de revisar una serie de eventos adicionales generados y reportados al SIEM OSSIM, Sara está segura que no se trata de un Falso Positivo y considera que se debe de realizar un análisis más profundo.

1	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-02-25 20:07:21	Host-192-168-61-243	Host-192-168-61-243	N/A	6
2	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-02-25 20:07:17	Host-192-168-61-243	Host-192-168-61-243	N/A	6
3	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-02-25 20:07:17	Host-192-168-61-243	Host-192-168-61-243	N/A	6
4	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-02-25 20:07:17	Host-192-168-61-243	Host-192-168-61-243	N/A	6
5	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-02-25 20:07:17	Host-192-168-61-243	Host-192-168-61-243	N/A	6
6	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-02-25 20:07:17	Host-192-168-61-243	Host-192-168-61-243	N/A	6
7	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-02-25 20:07:17	Host-192-168-61-243	Host-192-168-61-243	N/A	6
8	AlienVault HIDS: Logon Failure - Unknown user or bad password.	0	2016-02-25 20:07:13	Host-192-168-61-243	Host-192-168-61-243	N/A	6

Ilustración 33 Registros de Ataque de Fuerza Bruta

g) Manejo del Reporte de Incidente

Sara decide abrir el sistema de manejo de incidentes RTIR[13] y abrir un incidente con el propósito de escalarlo al equipo especializado, en este caso el CSIRT.

- Sara entra al RTIR , utilizando las credenciales root/password

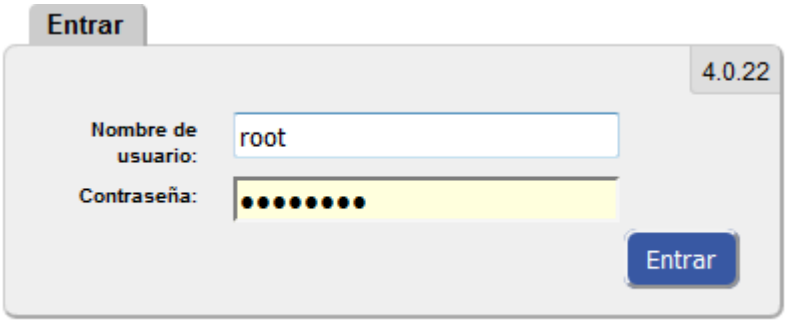


Ilustración 34 Login Sistema RTIR

- Se crea un nuevo Incidente en el cual se agrega toda la información adquirida hasta ese momento por parte de los analistas del SOC.

[13] Request Tracker for Incident Response

Ilustración 35 Creación de un nuevo incidente

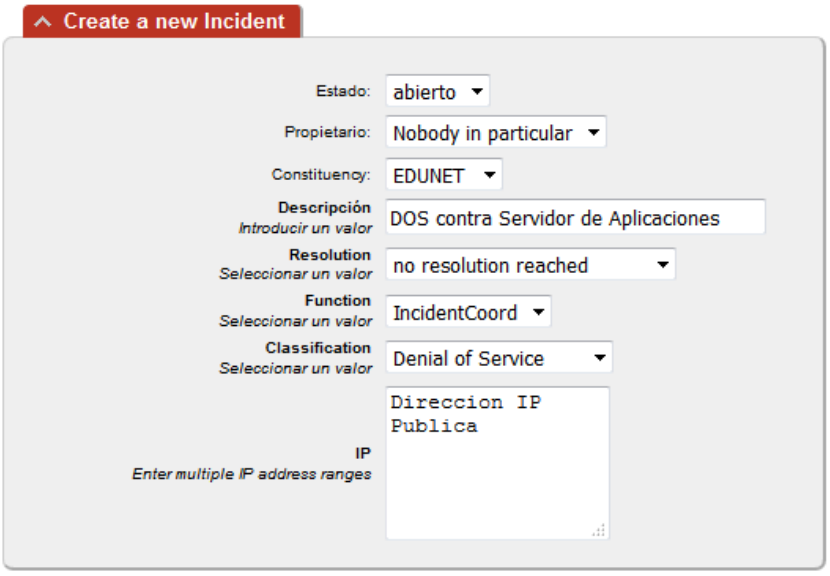


Ilustración 36 Estatus del Incidente Creado

- El nuevo incidente ha sido creado con un número consecutivo en este caso el número 1. Se permite adicionalmente alimentar el incidente con reportes adicionales, capturas, investigaciones y todos los datos relacionados con el caso.

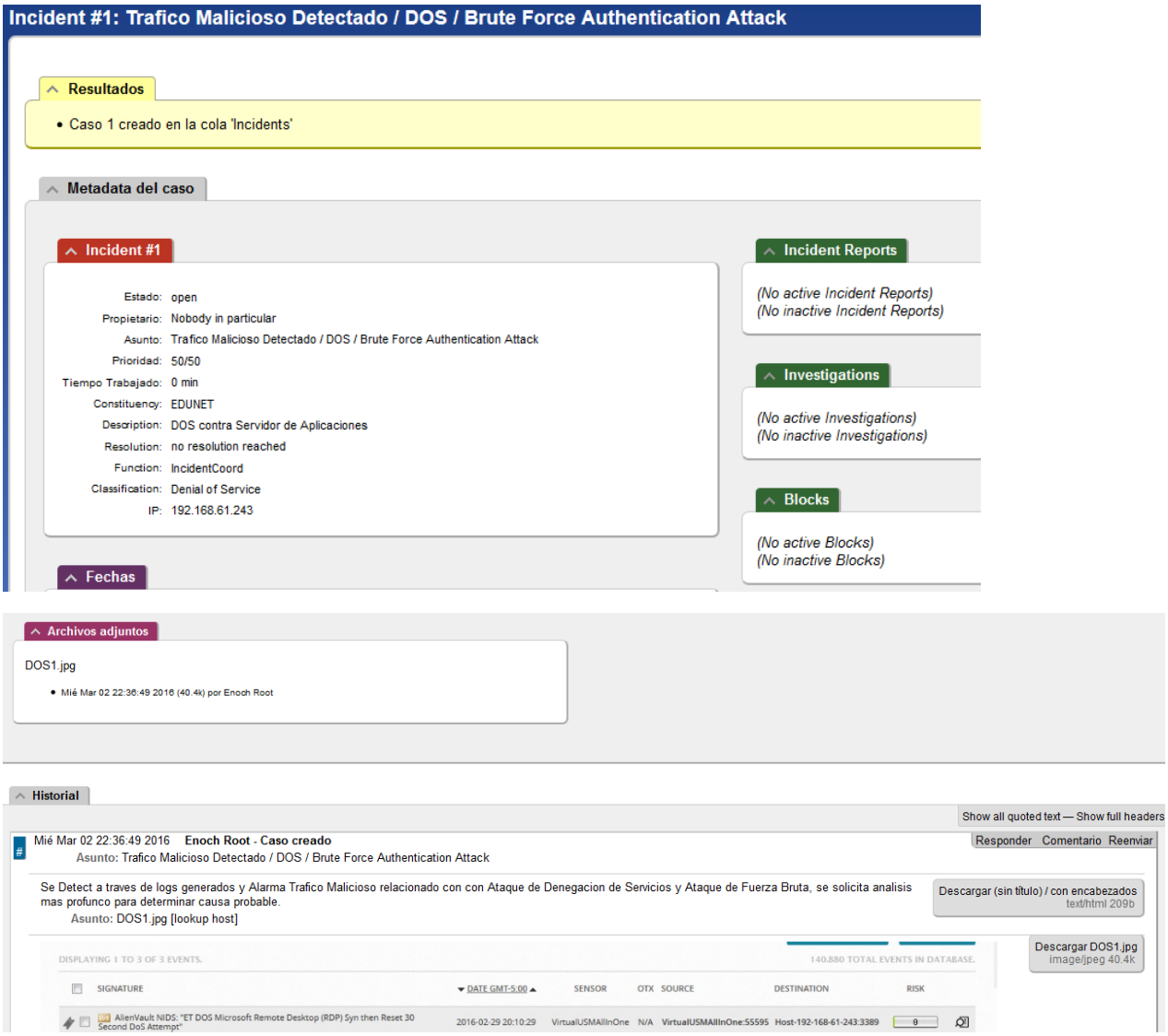


Ilustración 37 Detalles del Incidente Creado

- Se crea un reporte del incidente y se escala mediante la notificación por correo electrónico al equipo CSIRT

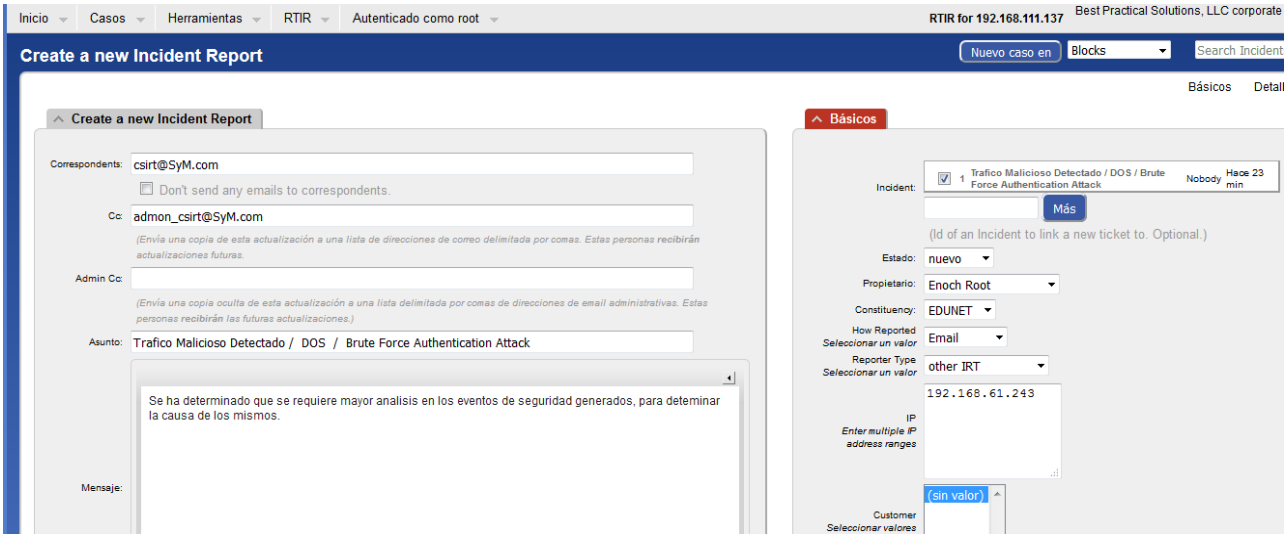


Ilustración 38 Notificación de apertura de Incidente

h) Tomado / Investigación de Reporte de Incidencia

- Roberto Garcia es el analista de turno del CSIRT quien recibe la notificación por correo del nuevo reporte de incidente.

De: RTIR [mailto:rtir@SyM.com]
Enviado el: miércoles, 26 de febrero 2016 09:30 p.m.
Para: 'csirt@SyM.com';
Asunto: Trafico Malicioso Detectado / DOS / Brute Force Authentication Attack

Se ha abierto el Reporte de Incidente # 2 Trafico Malicioso Detectado / DOS / Brute Force Authentication Attack Estado : Abierto

- Una vez notificado, entra al sistema de manejo de incidentes, toma el caso que le fue notificado y comienza el proceso de investigación.

Ilustración 39 Incidente de Seguridad Abierto

- Roberto realiza un análisis de Vulnerabilidad al equipo con problemas y de los resultados se da cuenta que está afectado con la Vulnerabilidad MS09-50, por lo que se introduce la primera línea de investigación con esa referencia:

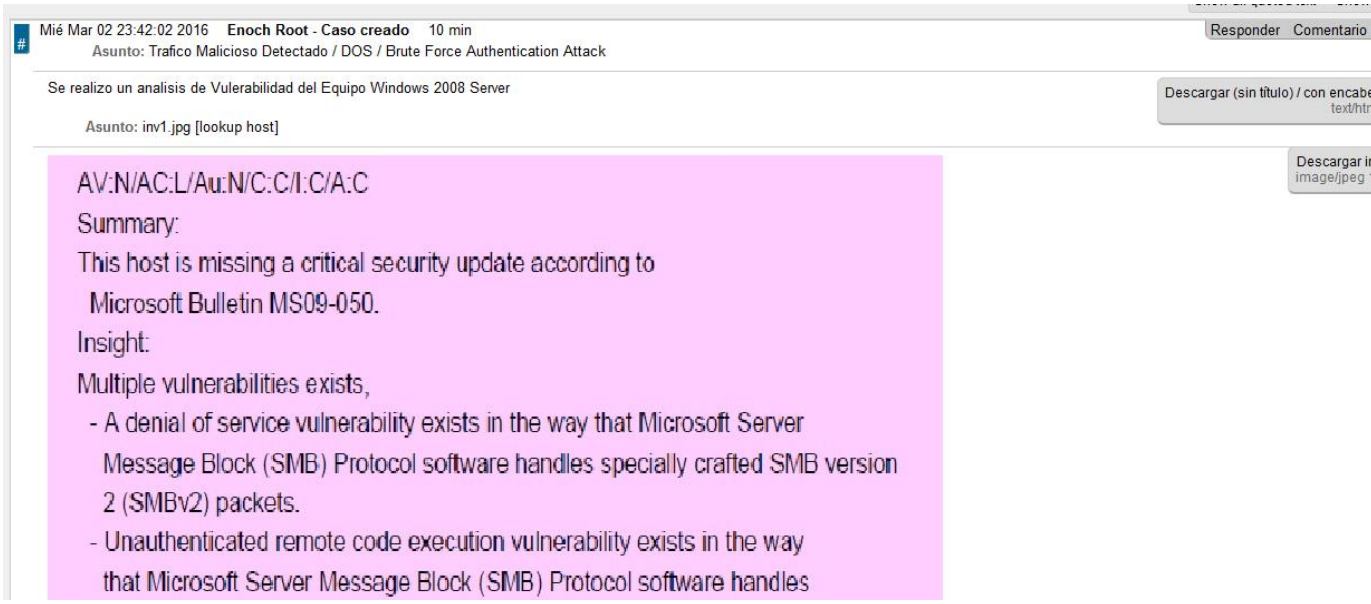


Ilustración 40 Investigación 1 = Vulnerabilidad descubierta por CSIRT

- Roberto continúa en su proceso de investigación y analiza los logs del equipo mediante el cual se logra contemplar el ataque de fuerza bruta que sufrió el equipo.

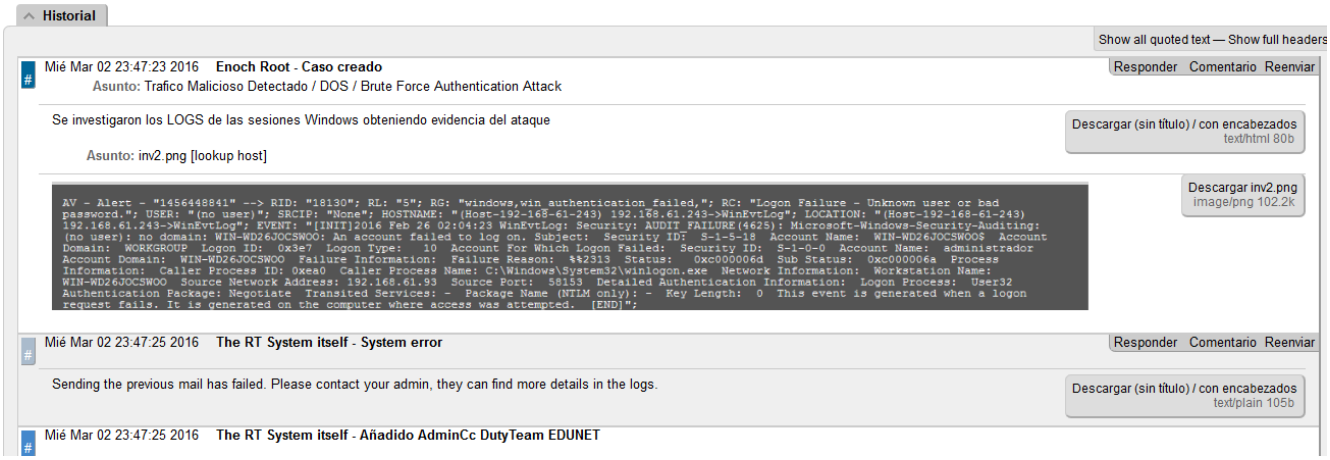


Ilustración 41 Investigación 2 = Registros de Ataque de Fuerza Bruta

- Roberto continúa en su proceso de investigación y esta vez realiza un análisis de los registros de Windows, solo para darse cuenta que existe implantado un proceso sospechoso denominado APOCALYPE32

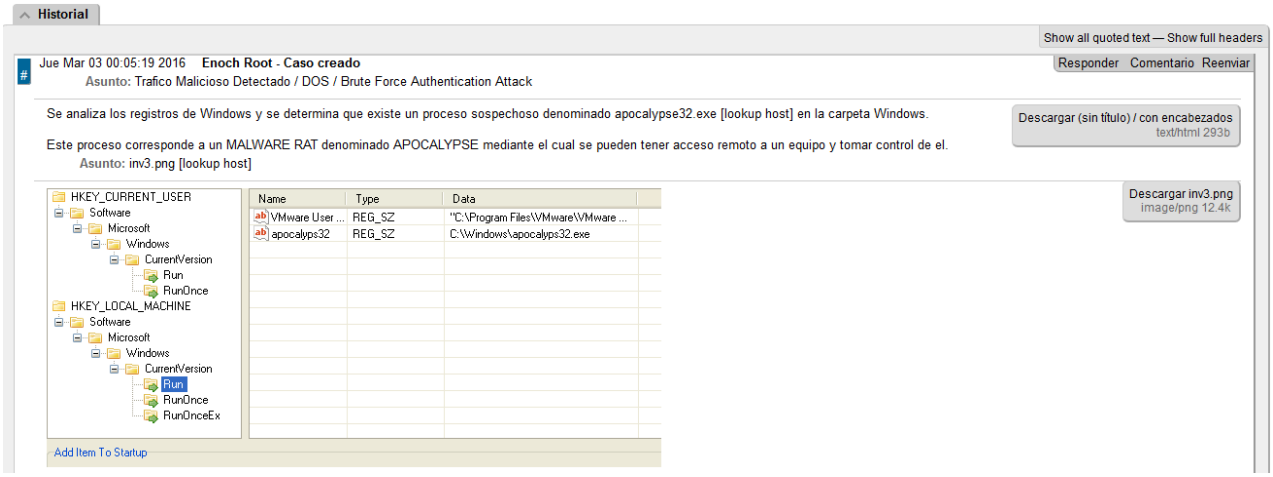


Ilustración 42 Investigación 3 = Malware por Registros

i) Medidas Correctivas y Cierre de Incidente

Luego de realizarse las diferentes investigaciones por parte de Roberto, este emite una serie de acciones y recomendaciones que deberán de ser llevadas en coordinación en este caso con John López para poder cerrar el incidente.

- Medida Correctiva 1 : Aplicar parche **WINDOWS-HOTFIX-MS09-050-7a790713-5b0b-448b-9494-46c4fadae53f** para corregir la vulnerabilidad encontrada.

- Medida Correctiva 2: Crear una Política de Fallo de Autenticación que permita poder bloquear o deshabilitar la cuenta en intentos repetitivos fallidos.

- Medida Correctiva 3 : Contar con dispositivos perimetrales que permitan protegerse de ataques de Denegación de Servicios.

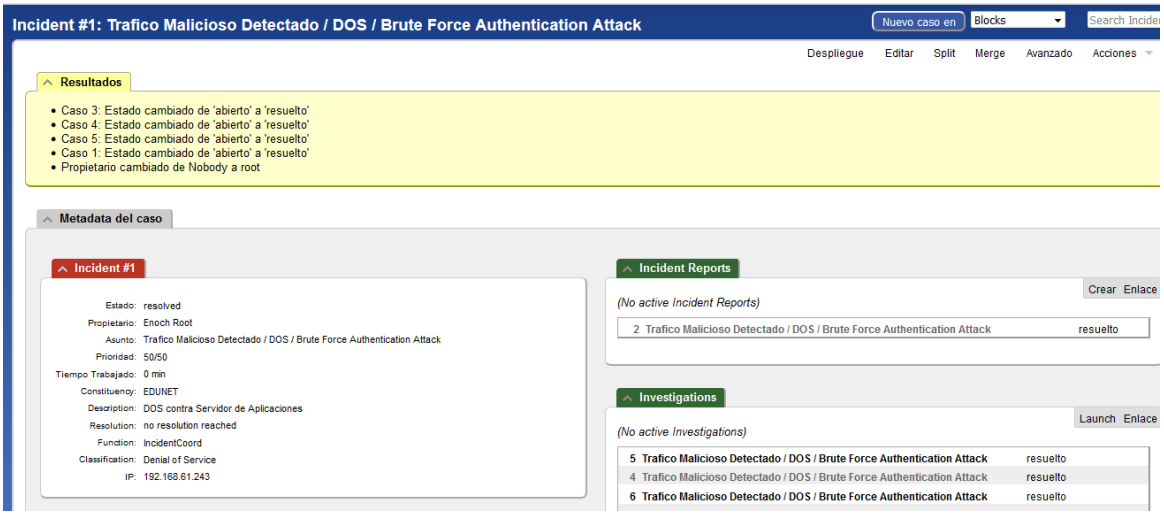


Ilustración 43 Aplicación de Medidas Correctivas - Cierre de Caso

j) Base de Conocimiento

Mediante la herramienta MEDIAWIKI el CSIRT cuenta con una base de conocimiento de incidentes que hayan resueltos en ocasiones anteriores de tal

forma que permita disminuir los tiempos de repuesta cuando se llegases a presentar en una nueva ocasión.

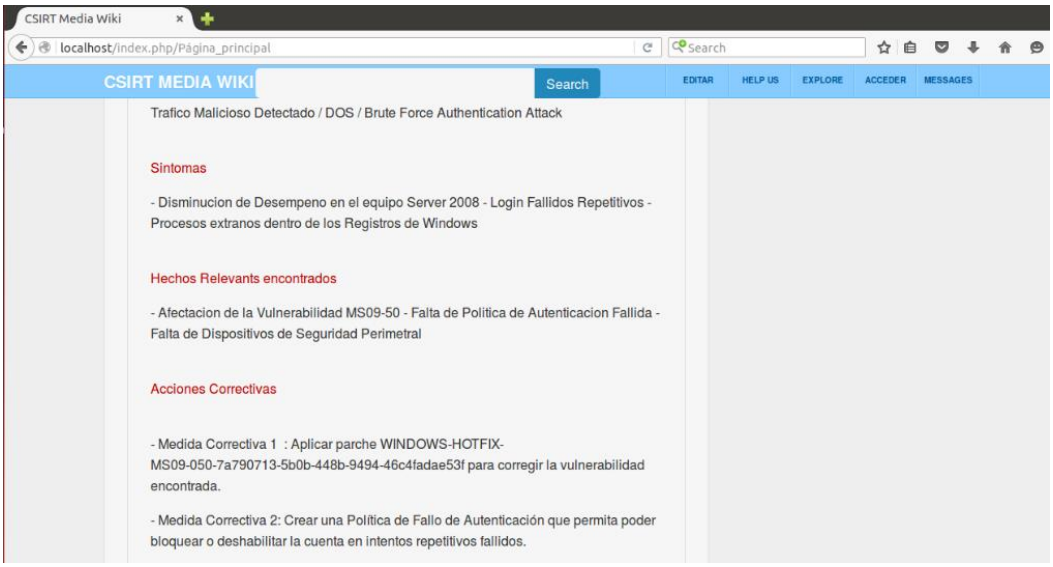


Ilustración 44 Alimentación de Sistema de Colaboración

Capítulo 5: Conclusiones y Recomendaciones

5.1 Conclusiones

- Dadas las condiciones tecnológicas actuales con que cuenta la UNI, su rol en determinas actividades y el alcance definido, se logró diseñar un SOC de tercera generación, con los servicios de monitoreo y respuesta a incidentes con la finalidad de detectar y resolver en el menor tiempo posible cualquier incidencia de seguridad que se pueda presentar.

- En la implementación del SOC de la UNI, se logró determinar los procesos, tecnologías y servicios necesarios que garantizan su operación óptima, dentro de los procesos tenemos : la detección, priorización y remediación de amenazas; como tecnologías se identificó la herramientas de correlacion de eventos a través de la cual podemos darnos cuenta cuando se presente un incidente de seguridad y finalmente se identificó las capacidades tanto técnicas como humanas que deben de tener tanto los analistas del SOC como del CSIRT.

- Una vez definido el SOC, se logró determinar que los servicios que brindara además del de monitoreo será el de repuesta a incidencias y servicios de colaboración para dar a conocer los hallazgos encontrados, el cual será llevado a cabo a través del Equipo CSIRT.

- Mediante el desarrollo de este trabajo, se logró determinar la relación existente entre el SOC y el CSIRT, como instancias relacionadas y necesarias para la respuesta efectiva y oportuna a incidentes de seguridad.

- A través del caso de estudio se demostró que es posible la implementación de un SOC, empleando tecnología y herramientas Open Source, con la calidad y eficiencia de herramientas comerciales.

5.2 Recomendaciones

- Dado que este estudio estuvo limitado a desarrollar solamente las funciones de monitoreo y repuesta a incidencias como tareas fundamentales de un SOC/CSRIT, se recomienda incluir en un futuro la función de Inteligencia de amenazas la cual permitirá no solamente consumir información de fuentes globales sino también contribuir a la misma.

- Se recomienda la creación de una página WEB especialmente para el SOC de la UNI, que a su vez esté integrada con la herramienta de colaboración MEDIAWIKI para dar a conocer los incidentes de seguridad más relevantes.

- Dado que el elemento humano muchas veces representa una amenaza más peligrosa que inclusive la misma tecnología, se recomienda que el SOC de la UNI realice programas de concientización en seguridad de la información al personal interno y público en general.

Anexos

a) Instalación de la Herramienta MEDIAWIKI en UBUNTU 14.04

Se debe de disponer de una instalación de LAMP (Linux, Apache, MySql,PHP) previamente.

- Modulos Iniciales

- De PHP5, GD, Intl

```
sudo apt-get install php5-intl

sudo apt-get install php5-gd

sudo apt-get install texlive

sudo apt-get install php5-xcache

sudo service apache2 restart
```

- Descarga de MEDIAWIKI

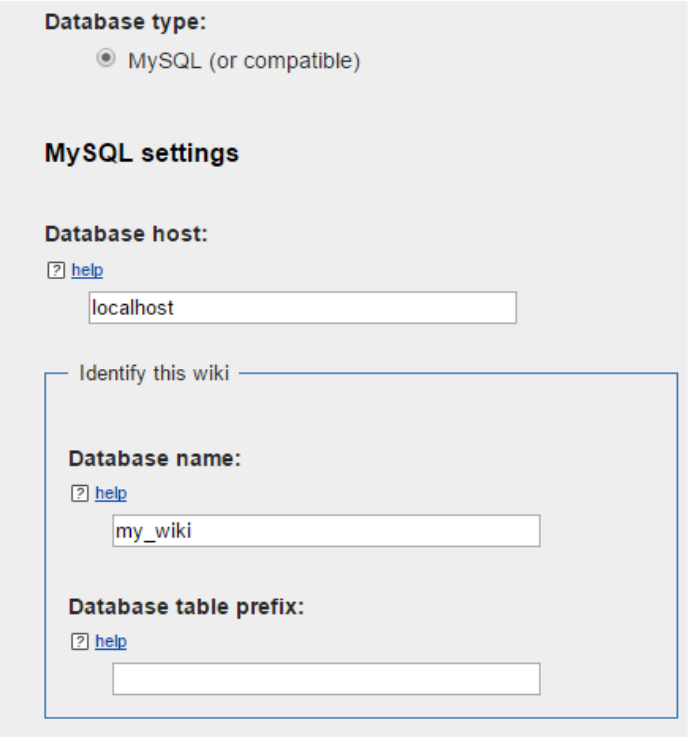
```
curl -O http://releases.wikimedia.org/mediawiki/1.24/mediawiki-
1.24.1.tar.gz

tar xvzf mediawiki-*.tar.gz

sudo mv mediawiki-1.24.1/* /var/www/html
```

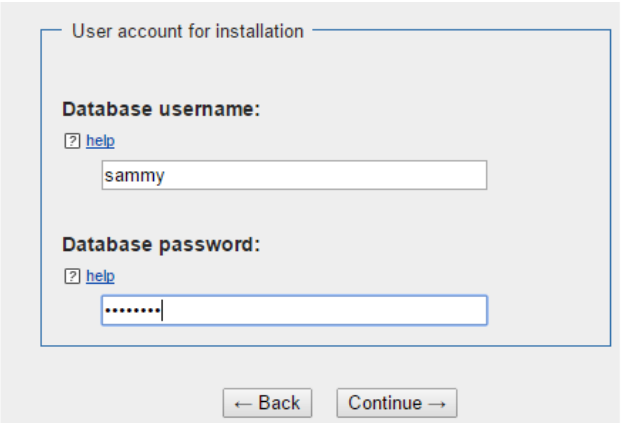
- Creacion de la Base de Datos

```
mysql -u root -p
```

```
CREATE DATABASE my_wiki;
GRANT INDEX, CREATE, SELECT, INSERT, UPDATE, DELETE, ALTER, LOCK TABLES
ON my_wiki.* TO 'sammy'@'localhost' IDENTIFIED BY 'password';


FLUSH PRIVILEGES;


exit


Bye
```

- Configuración de MEDIAWIKI





b) Instalación de la Herramienta RTIR ver 4.0.22 en UBUNTU 14.04

La instalación incluye el sistema principal llamado Request Tracker y el módulo Incident Response.

Request Tracker

- Configuración de la Base de Datos

```
# apt-get install mysql-server mysql-client libmysqlclient-dev
```

- Configuración del Servidor Web CGI

```
# apt-get install make apache2 libapache2-mod-fcgid libssl-dev libyaml-
perl libgd-dev libgd-gd2-perl libgraphviz-perl
```

- Configurar las dependencias de PERL

```
# apt-get install libwww-perl libcss-squish-perl libmodule-versions-
report-perl libcatalyst-plugin-log-dispatch-perl libregexp-common-perl
```

```
libuniversal-require-perl libtext-wrapper-perl  libtext-password-
pronounceable-perl libtime-modules-perl liblist-moreutils-perl
libscalar-util-numeric-perl libdatetime-locale-perl libtext-template-
perl libhtml-scrubber-perl libcache-simple-timedexpiry-perl
liblocale-maketext-lexicon-perl libdigest-whirlpool-perl libregexp-
common-net-cidr-perl libtext-quoted-perl libmime-tools-perl libdevel-
globaldestruction-perl  liblocale-maketext-lexicon-perl libregexp-
common-net-cidr-perl libdbix-searchbuilder-perl libdevel-stacktrace-
perl libhtml-rewriteattributes-perl libgnupg-interface-perl libperlio-
eol-perl libdata-ical-perl libtext-wikiformat-perl libhtml-mason-perl
libapache-session-browseable-perl libcgi-psgi-perl libhtml-mason-
psgihandler-perl  libcgi-emulate-psgi-perl libconvert-color-perl
liblocale-maketext-fuzzy-perl libhtml-quoted-perl libdatetime-perl
libnet-cidr-perl libregexp-ipv6-perl libregexp-common-email-address-
perl libipc-run3-perl  libxml-rss-perl libconfig-json-perl starlet
libgd-text-perl libgd-graph-perl
```

- Descargar y ejecutar la Configuración

```
cd /usr/src/;
wget https://download.bestpractical.com/pub/rt/release/rt-
4.0.22.tar.gz ;
wget https://download.bestpractical.com/pub//rt/release/RT-IR-
3.0.4.tar.gz ;
adduser --system --group rt;
usermod -aG rt www-data;
```

```
tar xzvf rt-4.0*.tar.gz;
cd /usr/src/rt-4.0.22
./configure --with-web-user=www-data --with-web-group=www-data --
enable-graphviz --   enable-gd
```

```
make testdeps
make install
make initialize-database
```

- Probar la Instalacion

```
/opt/rt4/sbin/rt-server --port 8080 # Default login localhost:8080 is
root/password
```

- Configuración de Vhost para correr módulo CGI Perl

```
cat /etc/apache2/sites-available/rt.conf
<VirtualHost *:8081>
        ServerAdmin webmaster@localhost
        ServerName 10.1.1.155:8081

        AddDefaultCharset UTF-8
        DocumentRoot /opt/rt4/share/html
        Alias /NoAuth/images/ /opt/rt4/share/html/NoAuth/images/
        ScriptAlias / /opt/rt4/sbin/rt-server.fcgi/
        <Location />
                Require all granted
        </Location>

        LogLevel info

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>


a2enmod fcgid
a2ensite rt

# vim /opt/rt4/etc/RT_SiteConfig.pm
...
Set( $rtname, '10.1.1.155');
Set($WebDomain, '10.1.1.155');
Set($WebPort, 8081);
...
```

- Permisos y Reinicio

```
chown www-data:www-data -R /opt/rt4/var/mason_data  # file perms need
correcting (bug)
service apache2 reload
```

Incident Response Module - Request Tracker

- Extraer Dependencias

```
cd /usr/src
tar xzvf RT-IR-3.0.4.tar.gz
```

```
cd /usr/src/RT-IR-3.0.4
```

```
apt-get install libhook-lexwrap-perl libnet-whois-ripe-perl
perl Makefile.PL    # this will show only - Parse::BooleanLogic
...missing.
make            # connects to CPAN and downloads
perl Makefile.PL    # verify that all deps are found.
```

- Instalar Modulo y Esquema DB

```
make install        # this populates /opt/rt4/local/plugins/RT-IR/
make initdb
```

Activate the RTIR extension in the /opt/rt4/etc/RT_SiteConfig.pm file:

```
...
Set(@Plugins, 'RT::IR');
...
```

Restart the Perl CGI

```
service apache2 restart
```

Bibliografía

1. Data Breach Investigations Report 2015. http://www.verizonenterprise.com/DBIR/2015/

2. Doddrell Gregory R (1996) “Information Security and the Internet” Internet Research: Electronic Networking Applications and Policy Volume 6 Number 1 1996 pp 5-9.

3. Eset. (2015). ESET Security Report LatinoAmerica. 2016, de Blog de Seguridad eliveSecurity http://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf

4. Fitzgerald Kevin J (1995) “Information Security Baselines”. Information Management and Computer Security Vol 2 No 2.

5. Killcrece Georgia, Kossakowski Klaus-Peter, Ruefle Robin, Zajicek Mark (2003). Software Engineering Institute (2003). Report CMU/SEI-2003-HB-001

6. LACNIC. (2016). Acerca de LACNIC. 09/02/2016, de LACNIC Sitio web: http://www.lacnic.net

7. The syslog protocol, http://tools.ietf.org/html/rfc5424

8. Muniz Joseph, Alfardan Nadhem , Mcintyre Gary (2015) “Security Operations Center : Buiding , Operating, and Maintaining your SOC. Ciscopress 2015.

9. Nathans David (2015) “Designing and Building a SOC” . Syngress 2015.

10. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information, http://tools.ietf.org/html/rfc7011

11. UNI. (2016). Historia de la UNI. 09/02/2016, de UNI Central Sitio Web: http://www.uni.edu.ni/Alma_Mater/Historia

12. West-Brown Moira J, Stikvoort Don, Kossakowski Klaus-Peter, Killcrece Georgia, Ruefle Robin, Zajicek Mark (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). USA: Carnegie Mellon University.