ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"IMPLEMENTACIÓN DE UN SISTEMA PARA ATENCIÓN, RESPUESTA A INCIDENTES DE SEGURIDAD PARA UN CENTRO DE OPERACIONES DE CYBERSEGURIDAD"

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

Ronald Javier Sáenz Huerta

Gisella Paola Yagual Ortiz

GUAYAQUIL – ECUADOR

2018

AGRADECIMIENTO

Primero a Dios, por guiarnos siempre y ayudarnos a tomar las mejores decisiones, a nuestras familias por el apoyo incondicional y a todos los profesionales con los que hemos compartido durante este proceso.

DEDICATORIA

A Dios, y a nuestras familias, por darnos siempre el impulso necesario para que estemos constantemente buscando lo mejor personal y profesionalmente.

TRIBUNAL DE SUSTENTACIÓN

_____

MG. Lenin Freire

DIRECTOR MSIA

_____

MG. Juan Carlos García

DIRECTOR DEL PROYECTO DE GRADUACIÓN

_____

MG. Ronny Santana E.

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

_____	_____
Ronald Javier Sáenz Huerta	Gisella Paola Yagual Ortiz
AUTOR	AUTOR

RESUMEN

Debido al gran avance de la tecnología, las empresas han ido mejorando e incluyendo a la tecnología en sus procesos y cada vez son más las que implementan plataformas virtuales para brindar facilidades a sus clientes. Para que esto sea posible es necesario el envío y recepción de información sensible por parte de los usuarios a través de la red, y con esto surgen un sinnúmero de incidentes y delitos informáticos. De aquí la necesidad de que en las empresas cada vez sea mayor la preocupación de crear o tercerizar un departamento de seguridad que detecte estos incidentes, y los trate en el menor tiempo posible, para asegurar la protección de la información de sus clientes.

Los centros de operaciones de ciberseguridad, son grandes departamentos de seguridad que cuentan con personal con experiencia, y certificado, que atienden los incidentes que reportan varios clientes. Debido al gran número de incidentes que podría recibir un centro de operaciones de ciberseguridad, es necesaria la implementación de una plataforma que permita gestionar y administrar los casos reportados.

En primer lugar, se analizan los procesos actuales de un departamento de ciberseguridad para darle atención y respuesta a los incidentes, se revisan las necesidades de los miembros del departamento, así como las quejas más comunes de los clientes. Luego, se plantea una opción que pueda servir como base para la implementación de una plataforma, sin que genere costos altos adicionales al departamento.

Se diseña una propuesta de implementación de software que incluye la personalización e instalación de la plataforma FIR (Fast Incident Response), de modo que se optimicen las tareas tradicionales de los ingenieros que atienden incidentes. Se implementa la plataforma, y se realizan las pruebas necesarias para validar que la funcionalidad cumpla con lo solicitado para satisfacer las necesidades del CSOC.

Como resultado de esta implementación, los tiempos de respuesta de los incidentes mejoraron notablemente, se evidenció la facilidad para correlacionar casos y los clientes pudieron dar mejor seguimiento a los incidentes.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍAS

IR	Incident Response
FIR	Fast Incident Response
SOC	Security Operations Center
CSOC	Cyber Security Operations Center
ECUCERT	Centro de respuesta a incidentes informáticos del Ecuador
COIP	Código Orgánico Integral Penal
CSIRT	Computer Security Incident Response Team
DOS	Denial of Service

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Los centros de operaciones de ciberseguridad, son departamentos dotados de servidores, antivirus, firewalls, sistemas de detección de incidentes, sistemas de monitoreo y demás herramientas que permiten proveer de seguridad a sus clientes, en tiempo real, las 24 horas los 7 días de la semana.

Es muy importante que una vez detectado un incidente, se atienda inmediatamente, se investigue, y se mitigue de forma inmediata, con la finalidad de reducir el riesgo del impacto en el negocio y definir los mecanismos de seguridad para evitar que un ataque del mismo tipo se vuelva a presentar. Para esto se propone la implementación de un sistema de gestión de atención y respuesta a incidentes, que permita llevar un control de los casos reportados con detalle de evidencia y toda la información necesaria de la solución que se le dio en su momento, que permita también automatizar ciertos pasos que realiza el centro de operaciones al no contar con un sistema de gestión.

Se analizan los problemas que tienen actualmente los integrantes del departamento, encargados de la atención de los incidentes, se revisan las necesidades de los clientes y se plantea la implementación de una plataforma de gestión de incidentes de software libre para evitar costos elevados para el departamento. Además, se desarrolla nuevas funcionalidades, de manera que se ajuste a los requerimientos funcionales de los miembros del departamento, para adaptarlo a la forma en que llevan los procesos de registro y clasificación de incidentes, investigación y solución de incidentes, y presentación de solución y resultados al cliente.

Además, se diseñan los casos de pruebas y se detalla el proceso de la implementación del software con los detalles técnicos requeridos, luego se realizan las pruebas respectivas y se analizan los resultados de la implementación.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedentes

En la actualidad, la tecnología está presente en casi todas las empresas y negocios del mundo, y con esto, sistemas, aplicaciones y software en general están siendo utilizados diariamente en las tareas de todos los departamentos de una organización facilitando el trabajo, mejorando procesos, y optimizando tiempos, sin embargo, así mismo, los usuarios se enfrentan a todas las amenazas a la seguridad de la información que existen, generando entre otros inconvenientes, pérdida o filtración de información, daño en el funcionamiento de equipos e invasión a la privacidad.

El creciente uso del internet a nivel mundial, implica que más personas sean susceptibles a riesgos de un ataque informático, los mismos que son de

diferentes tipos, y se clasifican dependiendo del atacante y de las vulnerabilidades que presenten los recursos atacados.

En seguridad informática la conservación de tres principios básicos es primordial para el logro efectivo de la protección de la información, éstos pueden ser considerados incluso como las tres propiedades más importantes a tener en cuenta para protegerla y resguardarla. La primera es la disponibilidad, la cual nos asegura que la información siempre esté al alcance de los usuarios. La segunda es la integridad, esto se refiere a que los datos sean consistentes y libres de alteraciones no autorizadas. La tercera es la confidencialidad, que nos asegura que la información sea mostrada sólo a los usuarios permitidos, y evitar que personas no autorizadas puedan acceder, leer, o modificar la información. Hoy en día existen un sin número de vulnerabilidades que pueden afectar a la integridad, disponibilidad y confidencialidad de la información. Muchas empresas desestiman estos problemas y no toman conciencia de que los ataques cibernéticos están a la orden del día, y que la información y sus recursos son vulnerables a ataques que podrían causar daños incluso, irreparables.

Entre las vulnerabilidades y amenazas más conocidas están los malwares, ataques DoS, spam, botnets, phishing, Ingeniería Social, hacking, man in the Middle, fraudes, sql injection, cross-site scripting, entre otros. Para evitarlas

es necesario un conjunto de medidas preventivas y reactivas que toda empresa debe considerar, entre ellas están las revisiones periódicas de las actualizaciones de sus máquinas y de los servidores, el bloqueo de puertos innecesarios para evitar que los virus puedan hacer uso de ellos, logrando de esta forma atacar o acceder a los recursos vulnerables de una empresa, la utilización de firewalls de modo que se asegure la protección a la red, servidores y los recursos de conectividad, el uso correcto de certificados digitales en todos los sitios que se expongan en Internet, así como el manejo de algoritmos de encriptación para el manejo de información sensible de la empresa. La seguridad de la información no solo comprende los datos que residen en medios electrónicos, puede estar en diferentes medios o formas por lo que además de estas medidas, son necesarias acciones de concientización, para que quienes manejan la información lo hagan de manera consciente, haciendo uso adecuado de todos los canales de transmisión.

Las consecuencias del mal manejo de la información son muy perjudiciales para las empresas, que de darse algún ataque se enfrentarían a diversos problemas como: pérdida de información, accesos no autorizados, espionaje, daño a la información, perjuicios económicos, problemas de credibilidad, de seguridad y legales.

En vista del aumento de ataques cibernéticos en los últimos años, combinado con el grado de complejidad en el tratamiento de los mismos, se han ido creando centros de operaciones de ciberseguridad, quienes cuentan con profesionales de seguridad para identificar y gestionar las amenazas, utilizando herramientas que permitan gestionar los incidentes y ofrecer soluciones en cuanto a protección de ciberseguridad a sus clientes.

El tiempo de respuesta y la oportuna atención que un centro de operaciones de ciberseguridad pueda darles a los incidentes reportados es crucial para evitar que los ataques se cristalicen. El centro de operaciones de ciberseguridad brinda el monitoreo 24/7, alerta y registra de un incidente para que sea atendido de inmediato, por este motivo existe la necesidad de una herramienta de software que permita además de almacenar la información de los incidentes de ciberseguridad que se presenten, gestionar con agilidad las actividades de atención y mitigación de estos eventos, y que al finalizar se encuentre disponible este historial para que permita que estos incidentes sean correlacionados y ayuden a resolver problemas futuros.

1.2 Descripción del Problema

Entre las actividades que tiene a cargo un centro de atención de incidentes de ciberseguridad, están las de gestionar los problemas relacionados con la

seguridad de la información de sus clientes. Para un CSOC que cuenta con al menos 10 clientes, la cantidad de incidentes que recibe de todos los servidores centralizadores que emiten las alertas de posibles eventos es considerable. De ahí la necesidad de la implementación de un software de gestión, que permita reducir en gran medida el tiempo empleado actualmente para el registro, categorización, y solución de incidentes.

Actualmente los procesos son manejados manualmente, se reciben alertas de incidentes vía correo electrónico y a partir de ese momento hasta la resolución del incidente, todo se realiza manualmente. Los tiempos de respuesta son muy altos por la dificultad para administrar y gestionar no solo el incidente, sino también la evidencia recolectada.

Desarrollar un sistema que solvente este requerimiento demanda mucho tiempo en cuanto a desarrollo, e implementación, es por eso que una alternativa sería comprar software realizado por otras empresas, pero estas alternativas son muy costosas y la posibilidad de personalización es mínima por lo que el departamento debería considerar ajustar sus procesos al software específico.

1.3 Solución Propuesta

Se determinarán los aspectos teóricos referentes a los incidentes de ciberseguridad y a la respuesta ante los mismos, así como la interacción de los centros de operaciones de ciberseguridad, ante la gestión de la respuesta de incidentes para convertirlos en requerimientos del software.

Es necesario analizar la situación actual del centro de operaciones de ciberseguridad (CSOC) basado en la gestión de respuesta de incidentes de ciberseguridad, para obtener todos los parámetros y variables que el software debe considerar entre sus opciones. Este análisis nos permitirá conocer cuáles serán las fuentes de la información para ingresar los eventos de ciberseguridad que se presenten.

Se propone la implementación del software FIR, por ser una alternativa de licencia Open Source, y que además provee el código fuente para poder ajustar el software según los requerimientos del centro de operaciones. El software FIR, es un proyecto de código abierto recomendado por un Cert de Francia llamado “CERT Societe Generale” para que sea utilizado por los CSOC como una herramienta de mejores prácticas. El software está desarrollado en Python, usando el framework Django versión 1.9, también usa

Bootstrap 3 y Ajax y d3js. Este sistema puede adaptarse a cualquier base de datos.

Se definirán los parámetros de entrada que serán incluidos en el sistema, y se definirán las herramientas que serán las fuentes de información para registrar los eventos e incidentes de ciberseguridad.

El software nos permitirá:

- Registrar las categorías de eventos.
- Registrar las fuentes de detección de los eventos.
- Registrar las líneas de negocio que son afectados.
- Registrar los actores que van atender los incidentes.
- Registrar el plan de mitigación de los incidentes.
- Registrar los incidentes y eventos de ciberseguridad.
- Cargar automáticamente los incidentes.
- Registrar los artefactos que son correlacionados entre eventos.
- Registrar tareas por medio de un módulo llamado “TO-DO List”.
- Mostrar los reportes de todos los incidentes y eventos registrados.
- Generar un reporte del incidente con su información detallada en formato HTML.

Entre los beneficios que nos brindará el nuevo software son los siguientes:

- Garantizar la fácil creación de los eventos de ciberseguridad.
- Reducir el tiempo de ingreso y categorización de los incidentes de ciberseguridad.
- Monitorear el estado de los incidentes de ciberseguridad
- Correlacionar los artefactos (ips, hosts, hashes) con otros eventos.

1.4 Objetivo General

Implementar un sistema para atención, respuesta a incidentes de seguridad para un Centro de Operaciones de Cyberseguridad.

1.5 Objetivos Específicos

- Determinar los aspectos teóricos referentes a los incidentes de ciberseguridad y a la respuesta ante los mismos, así como a la interacción de los centros de operaciones de ciberseguridad ante la gestión de la respuesta de incidentes.
- Recolectar información de la situación actual de la empresa basado en la gestión de respuesta de incidentes de ciberseguridad.
- Plantear el diseño de la propuesta de implementación del software FIR.
- Ejecutar la instalación y los casos de pruebas del software FIR.

- Analizar los resultados de las pruebas del uso del software FIR.

1.6 Metodología

Según Gordon Dankhe, los estudios son clasificados en cuatro tipos: exploratorios, descriptivos, correlacionales, explicativos. Cada tipo de estudio es muy importante, pues de ellos depende la estrategia de la investigación. Los componentes del proceso de investigación son diferentes en cada tipo de estudio, pues varían en diseño, los datos recolectados son distintos, incluso la forma de obtenerlos, el muestreo, y tratamiento de los datos difiere entre cada investigación.[1]

El presente estudio comenzará con la investigación exploratoria para conocer los tipos de incidentes de ciberseguridad, más comunes, que actualmente son manejados o atendidos por el centro de operaciones. Para esto se realizará la recopilación documental, obteniendo información de registros de los incidentes que posee el centro de soporte del último año de atención a los clientes, verificando las veces de ocurrencia, de modo que se identifiquen los 3 incidentes más frecuentes, los mismos que servirán para la definición de los casos de usos para la etapa de pruebas del software a implementar.

Luego de la consolidación de estos datos, se aplicarán entrevistas a los directivos del centro de operaciones y encuestas a todo el universo que

corresponde a los diez clientes a los que el centro brinda el servicio de monitoreo y atención de incidentes de cyberseguridad, con el fin de sustentar la Implementación de un sistema para atención y respuesta a incidentes.

La entrevista es una herramienta que nos facilita la obtención de información a través del empleo de un formulario, el cual será aplicado únicamente a los gerentes del departamento de ciberseguridad con el fin de evidenciar la necesidad de la implementación de un software de gestión de incidentes. El formulario de entrevista puede ser revisado en el anexo “A”.

Para conocer la percepción del cliente en cuanto a la gestión de incidentes que recibe por parte del CSOC, se aplicará una encuesta basada en preguntas de selección múltiple con la finalidad de obtener información relevante sobre sus necesidades. El formulario de encuesta puede ser revisado en el anexo “B”.

CAPÍTULO 2

MARCO TEÓRICO

2.1 El Internet y su infraestructura en Ecuador

En la actualidad, la mayoría de los negocios ya sean grandes corporaciones, pequeñas o medianas empresas, se ven en la necesidad de llevar su información a medios electrónicos, esto debido al volumen de datos que manejan, a la necesidad del rápido acceso a la información, o a la importancia de la disponibilidad desde cualquier lugar, mejorando los tiempos de atención a sus clientes, y facilitando la labor de sus empleados. Esto se logra gracias a un sinnúmero de servicios que la tecnología nos brinda; redes cableadas, conexiones inalámbricas, potentes servidores, equipos cada vez con mejores características, y sobre todo la gran red que hoy en día conecta al mundo, y que permite que los negocios, instituciones educativas, financieras, organizacionales, y todas las que mantienen la matriz productiva del Ecuador se mantengan conectados, el Internet.

El Internet aparece en los años 70, con el nombre de ARPANET, y nace de la necesidad de comunicación que tenían los militares de los Estados Unidos, esta gran red mantiene su desarrollo durante los años 80, cuando se utilizaba principalmente con fines académicos e investigativos. Es en los años 90 cuando las grandes corporaciones empiezan a introducirla en sus negocios con el fin de mejorar los procesos, realizar transacciones más rápidas, y proveer de correo electrónico a sus usuarios.

Esta red gigantesca logra que nos comuniquemos en milésimas de segundos, desde cualquier punto del mundo, únicamente haciendo uso de algún tipo de conexión, y esto es posible gracias a la infraestructura que hay detrás de todo esto. El viaje que realiza la información que solicitamos a través de un clic desde nuestras computadoras, no sería posible sin los cables submarinos que llevan la fibra óptica que nos permite transmitir grandes volúmenes de información.

En el Ecuador la primera institución en proveer acceso al Internet fue Ecuanex, un nodo de Internet establecido en 1991 por la Corporación Interinstitucional de Comunicación Electrónica, Intercom. En el año 1992 se estableció el segundo nodo de Internet (Ecuanet) por medio de la Corporación Ecuatoriana de información, una entidad sin fines de lucro auspiciada por el Banco del Pacífico, la ESPOL, la Universidad Católica de Guayaquil, entre

otras. Para el año 1995, los medios impresos del resto del mundo se volcaban al Internet, publicando noticias e información de interés, y en Ecuador, diario Hoy fue el primero en presentar un boletín informativo a través de un medio digital, en donde la noticia de interés del momento era el conflicto fronterizo con Perú. [2]

En el año 1999, el Ecuador, se conectó por primera vez a esta red global de fibra óptica desde Punta Carnero; la capacidad del Internet en ese momento fue de 2.5 Gbps (Gigabit por segundo).

En el 2007, el Ecuador, empezó a brindar 1.92 Tbps (Terabit por segundo), esta vez a través de la conexión desde Salinas. Aumentando notablemente la velocidad a lo largo de los últimos años, llegando en el 2016 aproximadamente a los 60000 kms, esto permitiéndole a los ecuatorianos mejorar las condiciones de acceso a Internet y que de esta forma sean cada vez más las empresas que lo usen en pro de sus procesos informáticos.[3]

En el Ecuador, el acceso a internet ha crecido considerablemente, según la Encuesta Nacional de Empleo Desempleo y Subempleo – ENEMDU (2012 - 2016), con respecto a este tema, el 36,0% de los hogares a nivel nacional tienen acceso a internet, 13,5 puntos más que hace cinco años.

En el área urbana el crecimiento es de 13,2 puntos, mientras que en la rural de 11,6 puntos.

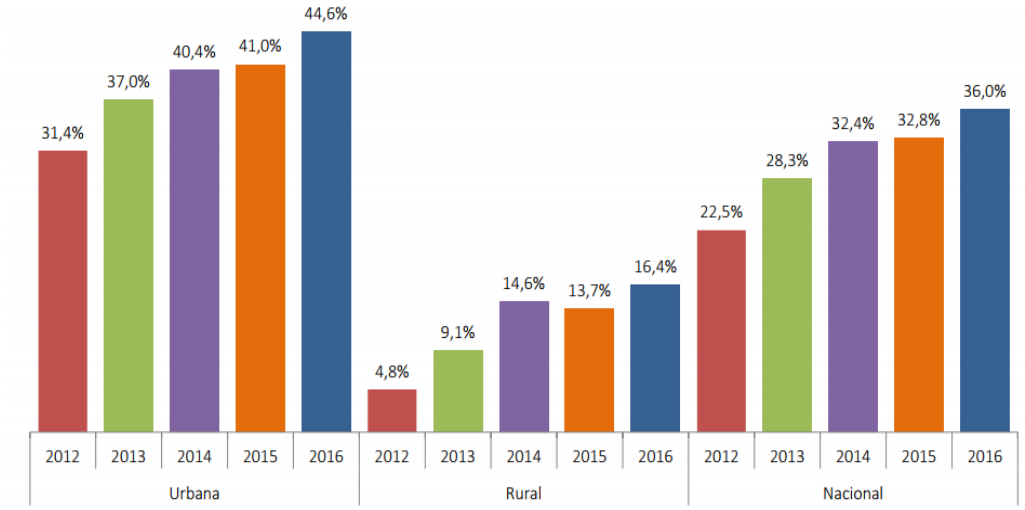


Figura 2.1 Acceso a Internet en el Ecuador según el área

La población de las zonas rurales y urbano-marginales posee aun barreras de acceso a la tecnología. Barreras que se intentan derrumbar poco a poco con programas de infocentros con acceso gratuito, estos espacios comunitarios ayudan a que el ciudadano se introduzca al conocimiento de las TIC`s. Según el Ministerio de Telecomunicaciones, los beneficiarios de este programa ascienden los 500 mil ciudadanos capacitados tanto de zonas urbanas y rurales del Ecuador.

2.2 Actualidad de la ciberseguridad en Ecuador y en América Latina.

A medida que pasa el tiempo, y con las facilidades de acceso, nos vemos inmersos en un mundo virtual, en el cual los usuarios pueden realizar muchos procesos, que antes sólo se lo podían realizar personalmente. La mayoría de empresas, negocios, instituciones financieras, e instituciones públicas han optado por facilitar los procesos de pagos en líneas, facturación electrónica, consultas de cuentas bancarias, trámites con instituciones del estado, compras en línea.

El internet y las nuevas tecnologías nos ofrecen facilidad y rapidez en los procesos, ya que pueden ser realizados desde cualquier dispositivo móvil o computadora, en cualquier momento y desde cualquier lugar.

Hay que mencionar que el Internet es una puerta abierta al acceso a información personal y al acceso a redes privadas, por tal motivo hay que promover el uso correcto, seguro y confiable de las redes informáticas.

En la actualidad, las empresas además de ofrecer sus servicios web, buscan proteger la información de sus clientes, para que no se vean envueltos en delitos cibernéticos, que cada día van en aumento.

Los ciberataques provienen de distintas partes del mundo y su objetivo puede ser cualquier sistema vulnerable.

En el Ecuador, las estadísticas referentes a ataques de ciberseguridad, presentan al sistema financiero como la principal víctima de estos delitos. Este no deja de ser un tema preocupante para la banca ecuatoriana, para quienes, con el uso de la tecnología, se enfrentan también a desafíos en la búsqueda de herramientas, métodos y procedimientos que permitan asegurar y mantener la confianza de sus clientes.

Si bien es cierto, todos los negocios pueden sufrir ataques o violaciones a la seguridad informática, las mismas plataformas del gobierno han sufrido ataques atribuidos al grupo Anonymous (El Comercio 2012), personajes públicos son víctimas de ataques a sus redes sociales (La República 2014), sin embargo, las estadísticas indican que es el sistema financiero el preferido por los atacantes. Por ejemplo, en 2014 se registró un aumento de 37% de robos a la banca virtual, 14% en tarjetas de crédito y 46% en cajeros electrónicos. [4]

En vista de todos los problemas y posibles riesgos que conllevan el uso de nuevas tecnologías, en el Ecuador se han implementado medidas para combatir a los ciberdelincuentes, por este motivo se implementó el centro de

respuesta a incidentes de informáticos llamado EcuCERT, dirigido por La Agencia de Regulación y Control de las Telecomunicaciones del Ecuador (ARCOTEL), basándose en la misión de regular y controlar la seguridad en las comunicaciones y la protección de los datos personales.

El EcuCERT está comprometido a contribuir a la seguridad de las redes de telecomunicaciones de todo el país, así como también asegurar el correcto uso de la red de Internet; para esto desarrolla productos relevantes, servicios de calidad y coopera con otros equipos de respuesta a incidentes de seguridad de la información, dentro y fuera del Ecuador. Estos equipos son conocidos como CSIRT, por sus siglas en inglés.

Uno de los propósitos del EcuCERT es el de establecer criterios generales y específicos para garantizar la seguridad de los servicios de telecomunicaciones, la información transmitida y la invulnerabilidad de la red; mediante la coordinación de la gestión de vulnerabilidades e incidentes de seguridad de la información entre el EcuCERT de la Agencia de Regulación y Control de las Telecomunicaciones, ARCOTEL, y los prestadores de servicios de telecomunicaciones del país, que han sido reportados por: su comunidad objetivo, fuentes de información, centros de respuesta a incidentes informáticos reconocidos y, propia gestión.

El EcuCERT controla además que los prestadores de servicios de telecomunicaciones adopten las mejores medidas técnicas y de gestión, con la finalidad de preservar la seguridad de las redes de telecomunicaciones de todo el país, lidera actividades de capacitación y entrenamiento sobre el buen uso de las tecnologías de la información y comunicación a las Instituciones del Estado Ecuatoriano, empresas del sector de las telecomunicaciones y ciudadanía en general.

Coopera y es el punto de contacto con otros equipos de respuesta nacionales e internacionales para la resolución de vulnerabilidades e incidentes informáticos. Además, promueve la creación de Equipos de Respuesta a Incidentes Informáticos (CSIRT) para la gestión de los incidentes de seguridad informática en el sector de las telecomunicaciones.

Impulsa la conformación de un Comité de Ciberseguridad dentro del cual se desarrollará y promoverá guías de buenas prácticas y recomendaciones en seguridad de la información. [5]

El organismo especializado en Telecomunicaciones de la Organización de las Naciones Unidas (ONU), es la Unión Internacional de las Telecomunicaciones (UIT) y está encargado entre otros de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras. Con

la finalidad de promover en todos los países, el uso de buenas prácticas de ciberseguridad, y a su vez de medir el compromiso de los países en materia de seguridad cibernética, esta entidad recopila información de varias organizaciones alrededor del mundo, de manera que logra determinar el Índice Global de Ciberseguridad (GCI) de cada país. Lo importante del GCI, es que además de que permite dar a conocer la forma en que cada nación implementa medidas de ciberseguridad, esto no solo queda a nivel nacional, sino que también permite que las medidas aplicadas en los países sirvan como punto de referencia y que las mismas trascienden a nivel global. [10]

El GCI se encuentra en un proceso de actualización constante para determinar aspectos relevantes de la seguridad de los países miembros de la ITU. La obtención del índice tiene como propósito medir los siguientes elementos:

1. Medidas jurídicas.
2. Medidas técnicas.
3. Medidas organizativas.
4. Desarrollo de capacidades.
5. Cooperación.

Para esto se elabora un cuestionario de preguntas que se envía a expertos de seguridad alrededor del mundo, 134 de los 198 países respondieron las preguntas enviadas, a los que no contestaron se les invito a validar las respuestas obtenidas, de modo que los resultados comprendan todos los países inicialmente considerados. [11]

En esta segunda edición del CGI, presentada en el 2017, el Ecuador aparece en el puesto 66 del ranking mundial de Ciberseguridad, noveno en el continente americano y sexto en Latinoamérica.

Tabla 1 Ranking mundial de ciberseguridad según CGI

Pais	Puntaje	Ranking Global
Macedonia	0.517	55
Portugal	0.508	56
Lithuania	0.504	57
South Africa	0.502	58
Ucrania	0.501	59
Iran	0.494	60
Cyprus	0.487	61
Panama	0.485	62
Argentina	0.482	63
Grecia	0.475	64
Bahrain	0.467	65
Ecuador	0.466	66
Pakistan	0.447	67
Algeria	0.432	68

Los países analizados han sido clasificados en tres grupos dentro del CGI, dependiendo de la etapa en la que se encuentra cada país según la posición obtenida, estos son: etapa de Iniciación, de maduración, y etapa de liderazgo.

Gracias a las mejoras del Código Integral Penal (COIP), y a la creación del Centro de Respuesta a Incidentes Informáticos del Ecuador (EcuCERT), el país se encuentra en etapa de maduración. En esta etapa existen 77 países, que han desarrollado compromisos complejos implementando programas e iniciativas de ciberseguridad.

Tabla 2 Países en etapa de maduración según GCI

MATURING		
Albania	Ghana	Peru
Algeria	Greece	Philippines
Argentina	Hungary	Poland
Austria	Iceland	Portugal
Azerbaijan	India	Qatar
Bahrain	Indonesia	Romania
Bangladesh	Iran (Islamic Republic of)	Rwanda
Belarus	Ireland	Saudi Arabia
Belgium	Israel	Senegal
Botswana	Italy	Serbia
Brazil	Jamaica	Slovakia
Brunei Darussalam	Kazakhstan	Slovenia
Bulgaria	Kenya	South Africa
Cameroon	Laos	Spain
Chile	Latvia	Sri Lanka
China	Lithuania	Tanzania
Colombia	Luxembourg	Thailand
Costa Rica	Malta	The Former Yugoslav Rep. of Macedonia
Côte d'Ivoire	Mexico	Tunisia
Croatia	Moldova	Turkey
Cyprus	Montenegro	Uganda
Czech Republic	Morocco	Ukraine
Dem. People's Rep. of Korea	Nigeria	United Arab Emirates
Denmark	Pakistan	Uruguay
Ecuador	Panama	Venezuela
Germany	Paraguay	

Diario el Comercio de Ecuador, expuso en su momento un artículo al respecto en el que se resalta que el país se encuentre en etapa de maduración: *"En lo que respecta a las tres categorías generales, Ecuador está en estado intermedio: no figura entre los líderes, pero tampoco está en la lista de países que se encuentran en etapas iniciales de su desarrollo."* [6]

2.3 Actualidad de la ciberseguridad en el ámbito internacional

En la actualidad, la ciberseguridad se ha hecho muy importante para las organizaciones que manejan información sensible, debido a que la interconectividad de las redes conlleva a que cualquier dispositivo pueda quedar al descubierto, desde la infraestructura crítica nacional, información privada de empresas, nuestra información personal, y hasta nuestros derechos humanos básicos pueden verse comprometidos.

Por lo tanto, alrededor del mundo se promueve que los gobiernos consideren políticas que sirvan como respaldo al crecimiento tecnológico, los accesos y la seguridad. Todo esto como un primer paso a la creación de una estrategia nacional de ciberseguridad.

La ciberdelincuencia cada día va en aumento, se maneja de la misma forma que la delincuencia común, personas que buscan hacer el mal, motivados por infinidades de razones, desde cualquier lugar del mundo, y muchas veces

utilizando máquinas que son previamente atacadas para cometer los ciberdelitos con la finalidad de no dejar huellas de la ip origen.

Por eso muchos países cuentan con un Equipo de Respuesta ante Incidencias de Seguridad a nivel nacional (CSIRT por sus siglas en inglés), y los países que lideran en el tema de ciberseguridad aportan con muchas ideas, conocimientos, experiencias y herramientas para que los países que están en etapa de maduración e iniciación puedan tener una guía para su crecimiento en ciberseguridad.

El incremento de ciberataques masivos, como también de regulaciones más restrictivas, abre las puertas al mercado de la ciberseguridad.

La Revista Líderes, menciona lo siguiente con respecto al mercado de protección informática: “Claramente es un mercado en plena expansión desde hace muchos años, y especialmente desde los últimos dos o tres”, explica Gérôme Bellois, experto en ciberseguridad del gabinete de asesoramiento Wavestone. Según un estudio del gabinete Gartner, el mercado de la protección informática (antivirus, expertos, intervención de urgencia, mantenimiento y otros rubros) aumentó en 7,9% entre 2015 y 2016 y alcanzó los USD 81 600 millones. La cifra podría llegar a los 120 000 millones en este año, frente a los USD 3 500 millones del 2004, según el gabinete

CyberSecurityVentures. La cifra se multiplicaría por 35 en 13 años. “La cibercriminalidad continúa alimentando el crecimiento del mercado”, añade el estudio. Además, estima que “los gastos mundiales” en este sector sobrepasaron el billón de dólares durante los próximos cinco años. [8]

Podemos decir que a medida que van creciendo los ciberdelitos, a la par crece el mercado de la ciberseguridad, y esto conlleva a que las empresas tengan otra perspectiva sobre la importancia de proteger los datos.

La Unión Internacional de Telecomunicaciones (UIT), en su CGI del 2017, demuestra el nivel de preparación en materia de ciberseguridad de los países del mundo. En dicho listado constan 193 países, distinguiendo a cada uno con un rango específico de compromiso para combatir los posibles ciberataques. Estos países están segmentados por región: Africa, Americas, Arab States, Asia y el Pacifico, la Comunidad de Estados Independientes, y Europa.

Este grado de compromiso se basa en cinco pilares básicos, los que a continuación se detallan:

2.3.1 Medidas jurídicas

Mide la presencia de instituciones y marcos legales respecto a ciberseguridad y cibercriminalidad.

2.3.2 Medidas técnicas

Evalúa la existencia de instituciones técnicas que puedan enfrentar amenazas de ciberseguridad e implementar acciones al respecto.

2.3.3 Medidas organizativas

Mide la existencia de instituciones de coordinación de políticas y estrategias para el desarrollo de la ciberseguridad a escala nacional.

2.3.4 Desarrollo de capacidades

Evalúa la existencia de educación, investigación y desarrollo, y programas de entrenamiento.

Evalúa la existencia de profesionales certificados e instituciones públicas que promuevan estas buenas prácticas.

2.3.5 Cooperación

Mide la existencia de redes de intercambio de información interinstitucionales y con otros países.

En el estudio de la UIT, se estableció una división general de todos los países en 3 categorías, cada pilar representa un área específica de evaluación.

- Países líderes en Ciberseguridad.
- Países que están madurando.

- Países que están en etapas iniciales del desarrollo de políticas de seguridad informática.

A continuación, un listado de los 96 países que están en etapa inicial, estos han empezado a desarrollar actividades con el fin de comprometerse con la ciberseguridad.

Tabla 3 Países en etapa de iniciación según GCI

INITIATING		
Afghanistan	Guatemala	Palau
Andorra	Guinea	State of Palestine
Angola	Guinea-Bissau	Papua New Guinea
Antigua and Barbuda	Guyana	Saint Kitts and Nevis
Armenia	Haiti	Saint Lucia
Bahamas	Honduras	Saint Vincent & the Grenadines
Barbados	Iraq	Samoa
Belize	Jordan	San Marino
Benin	Kiribati	Sao Tome and Principe
Bhutan	Kuwait	Seychelles
Bolivia (Plurinational State of)	Kyrgyzstan	Sierra Leone
Bosnia & Herzegovina	Lebanon	Solomon Islands
Burkina Faso	Lesotho	Somalia
Burundi	Liberia	South Sudan
Cambodia	Libya	Sudan
Cape Verde	Liechtenstein	Suriname
Central African Republic.	Madagascar	Swaziland
Chad	Malawi	Syrian Arab Republic
Comoros	Maldives	Tajikistan
Congo	Mali	Timor-Leste
Cuba	Marshall Islands	Togo
Democratic Republic of the Congo	Mauritania	Tonga
Djibouti	Micronesia	Trinidad and Tobago
Dominica	Monaco	Turkmenistan
Dominican Republic	Mongolia	Tuvalu
El Salvador	Mozambique	Uzbekistan
Equatorial Guinea	Myanmar	Vanuatu
Eritrea	Namibia	Vatican
Ethiopia	Nauru	Viet Nam
Fiji	Nepal (Republic of)	Yemen
Gabon	Nicaragua	Zambia
Gambia	Niger	Zimbabwe
Grenada		

Los 77 países que se encuentran en etapa de maduración, son aquellos que han desarrollado compromisos complejos, y además participan en programas e iniciativas en pro de la ciberseguridad, a continuación, el listado de los mismos.

Tabla 4 Países en etapa de maduración según GCI

MATURING		
Albania	Ghana	Peru
Algeria	Greece	Philippines
Argentina	Hungary	Poland
Austria	Iceland	Portugal
Azerbaijan	India	Qatar
Bahrain	Indonesia	Romania
Bangladesh	Iran (Islamic Republic of)	Rwanda
Belarus	Ireland	Saudi Arabia
Belgium	Israel	Senegal
Botswana	Italy	Serbia
Brazil	Jamaica	Slovakia
Brunei Darussalam	Kazakhstan	Slovenia
Bulgaria	Kenya	South Africa
Cameroon	Laos	Spain
Chile	Latvia	Sri Lanka
China	Lithuania	Tanzania
Colombia	Luxembourg	Thailand
Costa Rica	Malta	The Former Yugoslav Rep. of Macedonia
Côte d'Ivoire	Mexico	Tunisia
Croatia	Moldova	Turkey
Cyprus	Montenegro	Uganda
Czech Republic	Morocco	Ukraine
Dem. People's Rep. of Korea	Nigeria	United Arab Emirates
Denmark	Pakistan	Uruguay
Ecuador	Panama	Venezuela
Germany	Paraguay	

Existe además un grupo de 21 países, los que han demostrado alto nivel de compromiso con respecto a los cinco pilares evaluados. [10]

Tabla 5 Países líderes en ciberseguridad segun GCI

LEADING		
Australia	Japan	Oman
Canada	Korea	Russian Federation
Egypt	Malaysia	Singapore
Estonia	Mauritius	Sweden
Finland	Netherlands	Switzerland
France	New Zealand	United Kingdom
Georgia	Norway	United States

Dentro de los países líderes, el que ocupa el primer lugar es Singapur, seguido por Estados Unidos y luego por Malasia. Las seis regiones consideradas por el UIT están representadas en este listado de los 10 países con mejores políticas de ciberseguridad, por lo que el compromiso de los países para con la seguridad no depende de la situación geográfica.

2.4 Marco legal sobre ciberdelitos en el Ecuador

En el Ecuador se expidió en el 2002 la Ley de Comercio Electrónico, Firmas y Mensaje de Datos, mediante la Ley No. 67, publicada en el Registro Oficial Suplemento No. 577.

Con esta aprobación, se logra regularizar los mensajes de datos, los servicios de certificación, la firma electrónica, la contratación electrónica y telemática,

y la prestación de servicios electrónicos, mediante redes de información, que incluye el comercio electrónico y la protección que se brinda a los usuarios de estos sistemas, logrando que el riesgo prácticamente tienda a nulo para su falsificación.

El primer gran logro de esta ley fue darle el reconocimiento jurídico a los mensajes de datos de modo que puedan tener la misma validez que los documentos escritos, así su eficacia, valoración y efectos se someterán al mismo tratamiento según las leyes ya establecidas, tal como lo indica el artículo 2. [9]

El reconocimiento internacional de certificados de firma electrónica es uno de los puntos importantes que se contemplan en la ley, donde se indica que los certificados emitidos en el extranjero tienen validez legal en el Ecuador después de obtener la revalidación respectiva emitida por la CONATEL, entidad que debe comprobar la solvencia técnica de quien los emite, y el grado de fiabilidad de los certificados.

Después de obtener la revalidación, cualquier empresa o institución que haya utilizado este mecanismo, podrá demostrar ante cualquier auditoría, la autenticidad y validez de los documentos firmados electrónicamente, amparado en los artículos 15 y 51 de La Ley de Comercio Electrónico, Firmas

Electrónicas y Mensajes de Datos, en donde se establecen las siguientes características de la firma electrónica:

1. *“Ser individual y estar vinculada exclusivamente a su titular;*
2. *Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos;*
3. *Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.*
4. *Que, al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y,*
5. *Que la firma sea controlada por la persona a quien pertenece*”. [7]

Con esta ley, los usuarios pueden confiar en la utilización y validación jurídica de las firmas electrónicas para realizar sus actividades, obteniendo todos los beneficios que esto conlleva, tales como la transparencia en los procesos gubernamentales, eficiencia, posibilidad de servicios a distancia, portabilidad y agilidad.

Con la inclusión de esta ley, se reformó el COIP, estableciendo cinco nuevas figuras penales, relacionadas con las infracciones informáticas:

- Acceso no autorizado
- Falsificación Informática
- Fraudes Informáticos
- Daños Informáticos
- Violaciones al derecho a la intimidad

En agosto del 2014, luego de la aprobación del Código Orgánico Integral Penal (COIP) aparecieron, además, otros delitos como el grooming (ciber-acoso a los niños, niñas y adolescentes), y la posesión de pornografía infantil.

En su Disposición Derogatoria Novena el COIP derogó el Título V, desde el artículo 57 al artículo 64 de la Ley de Comercio Electrónico, Firmas y Mensaje de Datos y en lugar de esos artículos, incorporó varias figuras penales relacionadas con los sistemas informáticos y amplió el alcance de las infracciones informáticas ya existentes. [7]

Un artículo de los que fueron ampliados en el nuevo Código Penal se refiere a la violación a la intimidad. Debido al creciente uso de la tecnología y con esto la mejora en las comunicaciones, se ha propagado el uso de redes sociales, y la transmisión de información, es por esto que se torna necesaria

la protección a la intimidad del individuo, *"respaldando el acceso autorizado de datos personales, mensajes de texto, mensajes de voz, videos, y toda información contenida en medios informáticos, para que sea sancionado con pena privativa de libertad de uno a tres años todo aquel que se apropie, difunda, propague, o comparta información personal de un tercero"*.[9]

Así mismo se estableció la misma sanción para quienes se apropien de un bien ajeno, se transfiera bienes, o valores, en beneficio propio o de una tercera persona, utilizando medios electrónicos, alterando redes, programas, o sistemas informáticos, tal como lo especifica el artículo 190 de la Ley de Comercio Electrónico, Firmas y Mensaje de Datos. [7]

Los Artículos desde 191 hasta el 195 tipifican los delitos cometidos mediante terminales móviles. El Artículo 191 sanciona con pena privativa de la libertad de uno a tres años la reprogramación o modificación de información de identificación de equipos terminales móviles.

Existen artículos que contemplan la protección de la información, de modo que sanciona a quienes revelen o transfieran información contenida en ficheros, bases de datos o cualquier otro medio de almacenamiento, con la finalidad de beneficiar a terceros o a sí mismo. La sanción podría incrementarse a prisión de tres a cinco años si esta conducta se comete por

una o un servidor público, o empleados bancarios internos o de instituciones de la economía popular y solidaria.

Con la penalización de estos delitos informáticos se intenta brindar mayor seguridad a los usuarios, pues las cuentas bancarias y tarjetas de crédito suministradas durante una actividad de comercio electrónico, no podrán ser reveladas a terceras personas, divulgadas, interceptadas ni ser utilizadas sin algún tipo de orden judicial, para cometer ningún tipo de delito. Así mismo será penalizado quien ataque la integridad ya sea, borrando, o alterando el funcionamiento normal de los sistemas informáticos, los ataques de tipo denegación de servicios se considerarían en estos artículos.

2.5 Incidentes de ciberseguridad

Se considera incidente de ciberseguridad, por definición, cualquier suceso que afecte a los tres aspectos más importantes de los activos de información de una empresa u organización (confidencialidad, integridad o disponibilidad).

Un incidente de ciberseguridad es la violación o inminente amenaza a la violación de una política de seguridad de la información implícita o explícita.

Para los equipos de respuesta ante incidentes, es muy importante categorizar los incidentes. El valor de la categoría identifica el tipo de un incidente y su

potencial impacto. Esta categorización es muy importante en el desempeño del equipo de respuesta, debido a que ayudará en la asignación de recursos apropiados para analizar e investigar el incidente.

Un modelo de categorización según el tipo de incidentes es la que se plantea como a continuación se muestra la siguiente tabla. [12]

Tabla 6 Categoría de incidentes

No. Categoría	Nombre	Descripción
0	Pruebas	Se usa como un prueba de penetración autorizada.
1	Accesos no autorizados	Se usa cuando un individuo obtiene un acceso físico o lógico sin permisos a una red, sistema, aplicación, datos u otro recurso del cliente.
2	Denegación de Servicio (DoS)	Se usa cuando un ataque previene o deteriora con éxito la funcionalidad normal autorizada de redes, sistemas o aplicaciones al agotar sus recursos.
3	Código Malicioso	Se usa cuando se identifica la instalación de software malicioso, como un virus, un gusano, un troyano, u otra entidad maliciosa basada en código, que infecta el sistema operativo o las aplicaciones.
4	Escaneos / Sondeos / Intentos de acceso	Se usa cuando se identifica cualquier actividad que busque acceder o identificar la computadora del cliente, abrir puertos, protocolos, servicios, para un ataque futuro.
5	Investigación	Se incluye a incidentes no confirmados que son potencialmente maliciosas o anómalas que la entidad informante considera que merecen una revisión posterior.

Según esta tipificación, a continuación, se detallan algunos ejemplos sobre la categoría de los incidentes de ciberseguridad:

2.5.1 Accesos no autorizados

Se considera un acceso no autorizado, cuando un atacante accede a información a la que no esta supuesta a obtener, ejecutando alguna herramienta exploit, podría obtenerse acceso a archivos o claves de servidores. También se considera acceso no autorizado cuando un atacante luego de obtener esta información, amenaza a la víctima con divulgar información personal, a cambio de algún tipo de recompensa.

2.5.2 Denegación de Servicio (DoS)

Los ataques de este tipo se dan cuando el atacante envía paquetes elaborados al servidor de la víctima, causándole daño, de modo que éste quede inaccesible, muchas veces el atacante se hace de un grupo de muchas maquinas comprometidas para que envíen muchas peticiones ICMP (Internet Control Message Protocol) como sea posible a la red de la organización, de modo que cause saturación a la red y la misma quede inaccesible.

2.5.3 Código Malicioso

> Un gusano usa la compartición de archivos para infectar rápidamente muchas estaciones de trabajo dentro de una organización. Una organización recibe alertas de un antivirus que un nuevo virus se está expandiendo de una manera muy rápida mediante el correo electrónico.

Los niveles de severidad de los incidentes de ciberseguridad son basados en el impacto esperado y observado de un incidente. Esto se lo utiliza para priorizar el incidente, y es algo fundamental para la cantidad de recursos que deben ser asignados, así como para poder determinar el proceso de escalamiento para el seguimiento del incidente.

Los incidentes informáticos pueden ser un hecho real o puede ser sólo una sospecha que podría originar un incidente o una vulnerabilidad. Entre los incidentes más comunes están: gusanos, virus, troyanos, que afectan a una red en general, ataques SPAM (correo no deseado), ataques DoS (denegación de servicio), suplantación de identidad (phishing y spoofing), alteraciones no autorizadas de software o hardware.

El hacking también puede ser catalogado como un incidente, si es que no hay un contrato de servicios para realizar las pruebas de vulnerabilidades a los sistemas.

2.6 Respuesta a los incidentes de ciberseguridad

La detección y la respuesta de los incidentes de ciberseguridad son el núcleo de las operaciones de seguridad. Del equipo asignado para las operaciones de seguridad se espera que monitoree los activos de la organización, y reaccione a los incidentes y eventos de ciberseguridad, incluyendo detección, investigación de lo que se consideraría indicadores de compromiso.

Los indicadores de compromisos son señales de compromiso de seguridad que pueden ser detectados por procesos, tecnologías y personas.

Un tema que de vital importancia en la seguridad informática es el tiempo de respuesta del tratamiento de los incidentes, es por eso la necesidad de crear, mantener y desplegar un CSIRT efectivo. Si la respuesta ante los incidentes es efectiva y se lo realiza de la manera más rápida se puede minimizar la afectación financiera, de hardware y software a causa de un incidente de seguridad. El equipo CSIRT debe ser capaz de identificar a los causantes del incidente suscitado, de tal manera que los involucrados puedan ser perseguidos y castigados como lo estipule la ley.

La respuesta ante incidentes comienza por la primera detección de que un incidente ocurra y que esté dentro del alcance asignado al equipo de operaciones de seguridad.

Según J. Muniz, G. McIntyre, N. AlFardan, un típico proceso de manipulación de incidentes, sigue una serie de pasos que son representados como una línea de tiempo de la respuesta ante incidentes (IR), tal como se observa en la Figura 2.2.

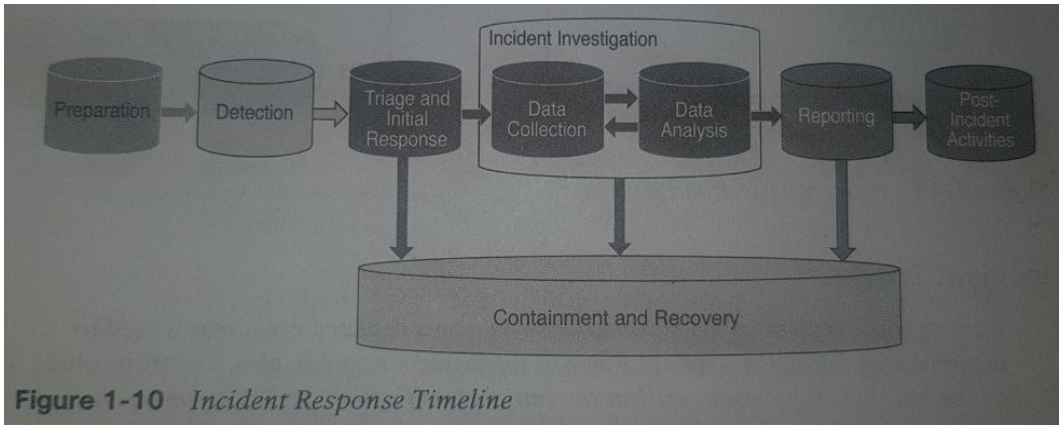


Figura 2.2 Línea de tiempo de la respuesta de incidentes

En esta línea de tiempo de la respuesta ante incidentes que se aprecia en la Figura 2.2 se detalla las siguientes fases:

2.6.1 Fase de detección de incidentes

La detección hace referencia a la fase en la cual los incidentes son observados y que son reportados por personas o por tecnología y por los procesos que gestionan la reportería.

Se debe documentar y formalizar lo siguiente, para que la detección sea efectiva:

- Identificar las fuentes, como las personas y tecnología, que serán los responsables de la detección y de reportar los incidentes de ciberseguridad.
- Identificar los diferentes canales a través del cual serán reportados los incidentes de ciberseguridad.
- Identificar los pasos que deben ser ejecutados para aceptar y procesar los incidentes de ciberseguridad.
- Identificar los requerimientos sobre las personas y tecnología, para que el proceso de detección funcione correctamente.

2.6.2 Fase de triaje de incidentes

El triaje de incidentes corresponde a la acción inicial, luego de la detección de un evento. Es usado para determinar los pasos restantes de acuerdo al plan de respuesta ante incidentes. Esta fase consiste en tres subfases: verificación, clasificación inicial y asignación.

El proceso de triaje necesita que sea desarrollado para que los incidentes sean priorizados y que puedan ser movidos a lo largo de toda la línea de tiempo de respuesta ante incidentes para que sean analizados y finalmente poder concluir de alguna manera su resolución. Este proceso envuelve la definición de los incidentes dentro de una categoría, la asignación de tareas y la aplicación del nivel de severidad, todo esto para que los incidentes puedan ser priorizados y que sean procesados según la definición de estos parámetros.

Existen algunas preguntas que deberían ser respondidas en esta fase:

- ¿El incidente está al alcance del programa?
- ¿Es un incidente nuevo, o está relacionado con algún incidente anterior?
- ¿Qué categoría debe ser asignado al incidente?
- ¿Qué nivel de severidad debe ser asignado al incidente?
- ¿Quién debe ser asignado para el análisis y la investigación del incidente?
- ¿Existe un marco de tiempo asociado para el incidente?

2.6.3 Fase de resolución de incidentes

El ciclo de vida de un incidente debe conducir a varias maneras de resolución de un incidente. Dentro de esto incluye análisis de data, propósito de la investigación, una acción propuesta o realizada anteriormente, y recuperación.

Lo más importante de esta fase es descubrir la causa raíz del incidente, para determinar el origen y poder mitigarlo, mientras se trabaja en la contención del incidente lo más pronto posible.

Durante esta fase el equipo de respuesta ante incidentes y demás equipos involucrados deben colaborar de la manera más eficiente para lograr la mejor resolución del incidente con rapidez.

La fase de análisis y la fase de investigación envuelven ciertas actividades que deben ser realizadas por el equipo de respuesta ante incidentes y los demás equipos:

- Identificar las cuentas, sistemas y activos comprometidos.
- Reconocer el impacto de los incidentes de ciberseguridad.
- Identificar de accesos no autorizados a data confidencial.
- Reconocer la cadena de eventos que han realizado los incidentes de ciberseguridad.

En esta fase, se deben tomar acciones para mitigar de la manera más rápida un incidente de ciberseguridad, para minimizar el posible daño que puede causar. Dependiendo de la severidad del incidente y de su impacto, esta fase puede ser realizada antes, durante o después de la fase de análisis.

Los pasos a seguir para contener un incidente de ciberseguridad, pueden variar dependiendo de muchos factores, como por ejemplo la naturaleza del incidente, la severidad del incidente, la criticidad del activo dentro de la organización. A continuación, se lista una serie de acciones de contención:

- Desconectar un sistema (activo) de la red.
- Mover un sistema (activo) infectado a una red en cuarentena.
- Detener los procesos o los servicios afectados.
- Deshabilitar una cuenta.
- Agregar una regla de firewall.
- Agregar una regla o una firma en un sistema de prevención ante intrusos (IPS), para detectar o bloquear un vector específico de ataque.

2.6.4 Fase de cierre de incidentes

El cierre de incidentes hace referencia a la erradicación de las vulnerabilidades que fueron descubiertas en la fase de investigación. Esto quiere decir que todos los rastros que pudo originar el incidente han sido eliminados.

En esta fase de cierre de incidentes también se incluye una etapa de verificación de los sistemas para asegurarse que los pasos y controles efectuados han sido óptimos y efectivos. También se debe verificar que los vectores de ataque no existan en los sistemas y que no sean efectivos.

Las acciones que se deben considerar en esta fase, son: la elaboración de un informe final sobre el evento, editar la clasificación del incidente, enviar notificaciones externas, y archivar la información sobre el incidente.

Algunos de los pasos que pueden ser usados para la erradicación de incidentes, puede ser los siguientes:

- Reconfiguración de los sistemas
- Reconstrucción del sistema

- Reemplazar al sistema con una imagen backup
- Parchar los sistemas
- Actualizar el software
- Borrar cuentas
- Borrar archivos

2.6.5 Fase de post-incidentes

Esta fase de post-incidentes incluye la fase de lecciones aprendidas, en la cual se debe pensar en cómo mejorar los procesos de la respuesta ante incidentes de ciberseguridad, y reflexionar sobre la actualidad de los controles de personas, procesos y tecnología.

Las actividades que se realizan en esta fase dependen de la severidad del incidente de ciberseguridad. El valioso conocimiento adquirido con los incidentes de ciberseguridad aumenta gradualmente la experiencia del equipo de ciberseguridad, lo cual puede ser usado para prevenir o mitigar futuros incidentes, de una manera proactiva, para lo cual es necesario que el equipo de ciberseguridad sea entrenado y capacitado para estos eventos, y otra forma sería de mejorar los equipos de ciberseguridad.

Analizando la línea de tiempo de la respuesta ante incidentes de ciberseguridad, el equipo de ciberseguridad debe manipular algunas tareas críticas con la finalidad de realizar la detección de incidentes para su cierre. En cada etapa de los incidentes pueden existir procesos propios, como también dependientes de otras áreas dentro de la organización. Por eso es muy importante que exista un plan bien diseñado, en el que se explique cada fase de la respuesta ante incidentes y que todo esté bien definido, documentado y al alcance de toda la organización.

Para dar respuesta ante incidentes es primordial la atención oportuna, ya que el peor momento de asignar responsabilidades, definir procedimientos y establecer estrategias de atención, es durante un ataque que se encuentra activo.

2.7 Participación de los equipos de respuesta frente a incidentes de ciberseguridad (CSOC)

Existen muchos términos que se utilizan para referenciar a un equipo experto en ciberseguridad, entre ellos se incluye los siguientes:

- Computer Security Incident Response Team (CSIRT)
- Computer Incident Response Team (CIRT)
- Computer Incident Response Center (CIRC)

- Computer Security Incident Response Center (CSIRC)
- Security Operations Center (SOC)
- Cybersecurity Operations Center (CSOC)
- Computer Emergency Response Team (CERT) [5]

Carson Zimmerman indica en su libro para referirse al SOC, como: “La práctica de la defensa contra la actividad no autorizada dentro de las redes informáticas, incluidos monitoreo, detección, análisis, y las actividades de respuesta y restauración”. [13]

CSIRT es el acrónimo más apropiado técnicamente, que debe ser usado en referencia al equipo preparado para buscar y responder ante intrusiones. Un CSIRT está compuesto principalmente por Ingenieros en Seguridad, Analistas en Seguridad, organizados para detectar, analizar, responder, reportar y prevenir incidentes de ciberseguridad.[14]

Un CSIRT puede proveer servicios a un conjunto de clientes en referencia a un conjunto limitado de usuarios, sitios, activos, redes y organizaciones. Pueden ser creados a nivel nacional por medio de instituciones públicas, como por ejemplo en Ecuador existe el ECUCERT regulada por la ARCOTEL. También pueden ser creados a nivel empresarial para atender requerimientos internos de la misma empresa, o para atender a

sus clientes que han contratado sus servicios de protección informática. Los CSIRTs a nivel de gobierno, por ejemplo, gestionan todas las incidencias de un país. Por lo regular los CSIRT evalúan de forma periódica las situaciones mediante la proactividad y si es necesario también incluye las brechas de seguridad existentes. [15]

Entre las actividades que realiza un CSOC se encuentran las siguientes:

- Proveer un medio a través del cual informar sobre los incidentes sospechosos de seguridad informática.
- Proveer asistencia en el manejo de incidentes de ciberseguridad.
- Difundir información relacionada a los incidentes.
- Analizar las ciberamenazas.
- Analizar vulnerabilidades de los activos.
- Coordinar la implementación de contramedidas.
- Realizar consultoría de la arquitectura y políticas de seguridad.
- Monitorear, detectar, y analizar las potenciales intrusiones en tiempo real, mediante tendencias históricas de fuentes de datos relevantes.
- Responder a incidentes confirmados, bajo la coordinación adecuada de recursos, y la utilización oportuna de contramedidas.

- Concientizar y reportar el estado de ciberseguridad, incidentes y tendencias de comportamientos extraños en una organización.

Entre las funciones de los miembros de un CSIRT están las siguientes:

- Gestionar o liderar el equipo de seguridad.
- Gestionar la resolución de incidentes.
- Realizar el análisis de vulnerabilidad de los activos.
- Definir el tratamiento de remediaciones de los activos.
- Brindar soporte a las plataformas de redes y de seguridad.
- Monitorear plataformas de seguridad.
- Mantenerse a la vanguardia de novedades de seguridad.

Los CSIRTs deben ofrecer servicios proactivos, antes que sólo responder ante incidencias de seguridad. Para esto los CSIRTs deben poseer personal capacitado y contar con los recursos de hardware y software esenciales para la protección de seguridad, y siempre estar a la vanguardia en los conocimientos y recomendaciones de seguridad.

2.8 Casos de éxito de implementaciones de software de respuesta ante incidentes de ciberseguridad

Para que un centro de operaciones pueda atender y proveer servicios de manera óptima con los niveles de servicios esperados y cumplir con los tiempos acordados en los contratos con los clientes, es necesario que todos los procesos de la gestión de la respuesta ante incidentes de ciberseguridad estén automatizados.

Existe un sin número de tecnologías que son requeridos por el SOC para proveer servicios de core:

- Gestión de logs de seguridad
- Información de seguridad y Gestión de eventos (SIEM)
- Gestión de casos
- Gestión de tickets
- Base de conocimientos / Wiki
- Telefonía y colaboración

Hay que recordar que las herramientas de seguridad varían de acuerdo a los servicios que cada empresa ofrece a sus clientes, porque existen muchas tecnologías como son:

- Análisis Forense
- Laboratorio de análisis de Malware
- Hardening
- Análisis de Vulnerabilidades
- Gestión de Activos

La tecnología puede ser de gran ayuda en los tiempos de respuesta ante incidentes de seguridad, debido a que al tener la data en un sistema centralizado se puede gestionar el incidente basado en incidentes previos y agilizar el proceso de investigación.

Existen muchas soluciones informáticas para la gestión de incidentes de ciberseguridad, como por ejemplo podemos mencionar las siguientes:

Tabla 7 Softwares de gestión de incidentes de cyberseguridad

Nombre Producto/Servicio	Vendedor
AlienVault USM Anywhere	AlientVault
Splunk Enterprise Security	Splunk
SIEM - McAfee	McAfee

Existen soluciones muy buenas que son pagadas, y que cumplen con las exigencias de la gestión de respuesta ante incidentes, pero el principal problema es que todas estas herramientas tienen altos costos por lo tanto demandan una fuerte cantidad de inversión financiera, lo cual hace que algunos CSOC-s desistan de utilizar estas soluciones, además estas herramientas generalmente tienen muchas opciones, con la intención de darle más funcionalidad al producto, y no se enfocan en la gestión de respuesta ante incidentes. Hoy en dia, en cuanto a software y aplicaciones en general, es muy común encontrar alternativas de código abierto, y este caso no es la excepción. Existen proyectos de código abierto, creados para ayudar a los CSOCs a administrar los incidentes de seguridad que necesitan ser atendidos por el equipo. Entre los más conocidos tenemos los siguientes:

Tabla 8 Softwares libres de gestión de incidentes de cyberseguridad

Nombre Proyecto	**Url Proyecto**
Fast Incident Response (FIR)	https://github.com/certsocietegenerale/FIR
Request Tracker (RT)	https://github.com/bestpractical/rt
TheHive	https://github.com/TheHive-Project/TheHive

Un caso de éxito es la empresa CERT Société Générale que se dedica a brindar servicios de seguridad de computadores, respuesta ante incidentes, análisis forense, análisis de malware y cibercrimen. Esta empresa comenzó a desarrollar un software propio llamado FIR en el 2013, en su búsqueda de una herramienta que los ayudará en la gestión de muchos incidentes que no podían atenderlos diariamente, esto porque la mayoría de herramientas que existían en ese año no cumplía con sus necesidades, y por tal motivo decidieron realizar un sistema propio. Este sistema los ayudó de una manera rápida y ágil, el cual se centraba sólo en la respuesta ante incidentes de ciberseguridad. En el año 2015 analizaron la idea de publicar el proyecto de manera de código abierto y lo así lo hicieron. La finalidad era ayudar a la comunidad proporcionado una herramienta muy sencilla en la gestión de incidentes de ciberseguridad, aunque también era para aprender de la comunidad que podían compartir sus flujos de trabajo y métodos y así contribuir con el proyecto.

2.9 Software FIR desarrollado por CERT de Francia (CERT SOCIETE GENERALI)

El Software FIR (Fast Incident Response), que significa Rápida Respuesta a Incidentes, es una plataforma web de administración de incidentes de ciberseguridad diseñados con agilidad y rapidez. Esta plataforma tiene una

interacción muy sencilla que permite una fácil creación, seguimiento y reportería de incidentes de ciberseguridad.

FIR es una herramienta muy necesaria para cualquier organización que necesita rastrear incidentes de ciberseguridad como pueden ser los equipos de ciberseguridad (CSIRTs, CERTs, CSOCs, SOCs, etc.).

Esta herramienta fue desarrollada por el equipo de ciberseguridad de una financiera llamada Société Générale, este equipo es llamado CERT Societe Generale (Computer Emergency Response Team), cuya misión es prevenir y ayudar a resolver los incidentes de seguridad de la información del Grupo Societe Generale. FIR fue diseñado para satisfacer las necesidades y los hábitos del equipo CERT Societe Generale, pero ellos se esforzaron para que esta plataforma fue muy genérico y adaptable posible antes de lanzarlo para que otros equipos de seguridad de todo el mundo también tengan la oportunidad de usarlo y personalizarlo como ellos les parezca mejor.

Estos son algunas de las bondades que ofrece esta plataforma de seguridad, que ayuda de una manera muy eficiente a la respuesta ante incidentes de ciberseguridad:

- Permite dar seguimiento, y administrar los incidentes de ciberseguridad.

- Provee inteligencia basado en incidentes anteriores.
- Genera reportes y estadísticas bajo demanda.
- Framework extensible.
- Basado en multi usuarios.
- Colecciona artefactos.
- Provee correlación de incidentes.
- Permite agregar información para la línea de tiempo de investigación.
- Permite editar atributos de los incidentes.
- Estadísticas generales.

FIR está desarrollado en un lenguaje de programación llamado Python, y usa un Framework Django versión 1.9. También usa el Framework Bootstrap 3 y algunos scripts de javascript como Ajax y D3js. La base de datos puede ser cualquiera que sea compatible con Django. La plataforma FIR no necesita muchos recursos tecnológicos, podría correr sin problema en una máquina virtual que tenga un 1 core, con 40GB de disco duro y 1GB de memoria RAM y que tenga instalada un sistema operativo Ubuntu 14.04

Esta plataforma es un proyecto de código abierto, avalado por GNU General Public License v3.0, eso quiere decir que cualquier persona o empresa puede descargar este proyecto, modificar el código y utilizarlo como les parezca para uso personal, comercial, o investigativo. El proyecto se encuentra alojado en GITHub y puede ser descargado del siguiente url https://github.com/certsocietegenerale/FIR, existe una comunidad para que los usuarios que utilizan esta plataforma puedan aportar con ideas y que puedan ayudar en la programación del proyecto.

CAPÍTULO 3

SITUACIÓN ACTUAL

3.1 Situación Actual del CSOC

El centro de operaciones de ciberseguridad de la empresa tiene actualmente 10 grandes clientes que han contratado los servicios de monitoreo y operaciones de ciberseguridad, es por esto que el centro cuenta con distintas herramientas de seguridad, las cuales sirven para dar protección a los clientes ofreciéndoles los siguientes servicios:

- Seguridad Perimetral
- Seguridad Antispam
- Seguridad en Aplicaciones Web (WAF)
- Protección DDoS
- Protección para equipos de usuarios finales
- Monitoreo 24/7 de CSOC

- Gestión y atención de incidentes detectados

Además, cuenta con los siguientes recursos trabajando directamente en el departamento:

- 1 Gerente del departamento
- 1 Jefe Operativo del departamento
- 6 Ingenieros especialistas en Seguridad
- 2 Ingenieros de automatización en Seguridad Informática
- 5 Ingenieros Junior para el monitoreo CSOC

3.1.1 Proceso actual de gestión de incidentes

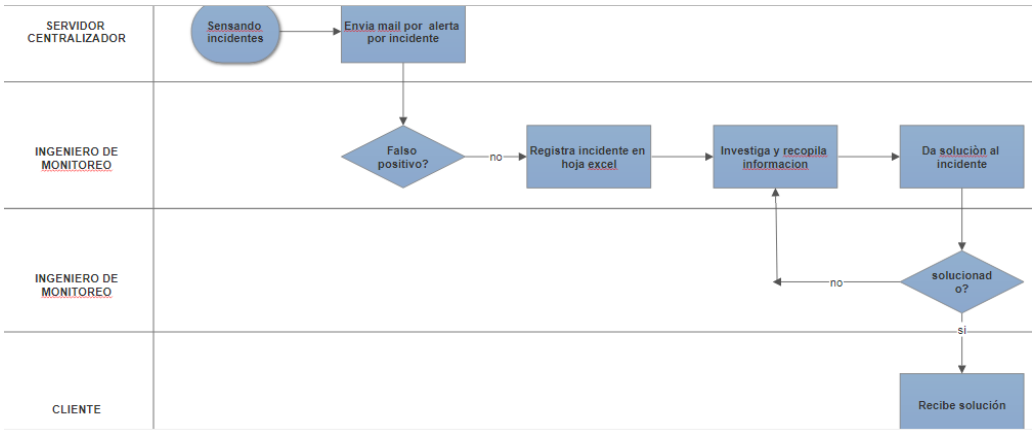


Figura 3.1 Diagrama de proceso actual de gestión

Actualmente el centro de operaciones cuenta con una plataforma que se encarga de centralizar todos los eventos generados por las distintas

aplicaciones de seguridad, la cual emite una alerta vía correo electrónico a los ingenieros de monitoreo del departamento por medio de casos de uso previamente definidos.

Una vez que el ingeniero de monitoreo recibe el correo, este lo registra en un archivo Excel compartido, en la pestaña de casos abiertos, y recopila la información del incidente en una carpeta de la red a la que todos los ingenieros tienen acceso. La alerta puede venir también directamente desde el cliente por detección de algún incidente por parte de ellos, así mismo envía, un correo y la evidencia necesaria al Jefe Operativo, quien registra el caso y ubica la evidencia en la carpeta respetiva. En este caso, el Jefe Operativo le pide a un ingeniero que se encargue de este incidente.

Se da inicio al proceso de investigación para resolver el incidente presentado, y manualmente el ingeniero revisa algunos casos para intentar encontrar si un incidente de este tipo ya ha sido resuelto antes, este proceso resulta tedioso, por lo que generalmente lo omiten y únicamente se realiza la investigación para encontrar una solución al incidente.

Existen casos que tienen un nivel de complejidad mayor, y cuando el ingeniero de monitoreo identifica un suceso de este tipo, interviene el especialista de seguridad, el cual se dirige a la carpeta que corresponde, revisa los logs y archivos, recibe los comentarios del ingeniero de monitoreo y empieza a trabajar en la solución.

Una vez identificada la causa del incidente, el ingeniero o el especialista emiten un diagnóstico, e informan de las posibles soluciones al cliente, a través de un correo electrónico. Luego de haber coordinado y recibido la respectiva autorización por parte del cliente, se procede a aplicar los mecanismos de mitigación que sean necesarios para atenuar el suceso, y se le da al cliente las recomendaciones para prevenir un ataque del mismo tipo en el futuro.

Una vez resuelto el caso, se elimina el registro de esa pestaña de Excel y se lo crea en otra pestaña donde se encuentran todos los casos cerrados.

3.1.2 Observación del proceso de la gestión de respuesta ante incidentes de ciberseguridad

Desde la creación de CSOC, cuando se contaba únicamente con tres clientes hasta la actualidad en donde existen diez clientes se ha venido

manejando este proceso. Debido al crecimiento de los clientes y de sus recursos tecnológicos, las alertas por incidentes han aumentado paralelamente, por lo que el actual proceso de gestión está causando algunas molestias, no solo a los clientes, sino también a los ingenieros y especialistas que intervienen a lo largo de la creación y cierre de un suceso. Entre ellas mencionamos las siguientes:

- No existe un software automatizado que permita gestionar los incidentes de ciberseguridad que afectan a los clientes.
- La información actual de incidentes de ciberseguridad no cuenta con una clasificación de acuerdo a su criticidad.
- Clientes se quejan de que algunas veces no se atienden los casos más graves primero.
- Clientes se quejan del tiempo de respuesta, incluso de incidentes que ellos consideran que ya se han presentado para otros servidores en unos meses atrás.
- Es muy complicado realizar una correlación de incidentes anteriores para revisar la solución que se le dio a incidentes que ya fueron resueltos y agilizar el tiempo en la respuesta.

- Las evidencias se almacenan en una carpeta compartida, sin estandarización en cuanto a los nombres, por lo que en la actualidad es difícil encontrar los archivos de un incidente específico, especialmente cuando la resolución del caso tiene que ser escalada a un especialista de seguridad.

- Realizar los reportes conlleva mucho tiempo, debido a que la información no se encuentra centralizada en un sólo sistema.

Se ha realizado el seguimiento respectivo al proceso actual de la gestión de los incidentes y se verificó que en promedio el centro de operaciones recibe 35 incidentes de los 10 clientes con los que cuenta actualmente, de estos, únicamente se logra registrar en la hoja de Excel, aproximadamente 15, y debido al tiempo que esto implica, solo se logra atender en promedio 12 incidentes por día.

3.1.3 Resultados de las entrevistas a los directivos del departamento de CSOC.

Luego de haber realizado las entrevistas a los gerentes del departamento CSOC nos indican que la realidad de los incidentes de ciberseguridad de los clientes sigue en aumento, y que la resolución de estos es vital para la protección y mejorar la calidad de servicio.

Una de las grandes debilidades que tiene el departamento es la inexistencia de una herramienta que facilite la gestión de incidentes de ciberseguridad, porque es un problema muy crítico, y esto se evidencia en las quejas de los clientes, que indican que el tiempo de respuesta es demasiado, que no pueden dar seguimiento al estado de los casos y que toda la comunicación se hace vía correo electrónico volviendo complicada la búsqueda de información por incidente.

Debido a esta debilidad, el centro de operaciones se ve afectado sobremanera en la gestión de incidentes, porque el ingreso de incidentes se vuelve lento, quita tiempo de solución y al no existir correlación con incidentes anteriores no es una ayuda para que los operadores sean eficaces.

El proceso de la gestión actualmente se lo hace de manera manual, en el cual el operador debe leer correos y llenarlos en un archivo de Excel, este proceso resulta tedioso. Muchas veces los operadores de monitoreo CSOC olvidan registrar todos los incidentes y por tal motivo existen quejas de los clientes. La categorización no existe, por tal motivo no se puede priorizar la atención. Además entregar reportes al cliente, resulta una tarea complicada pues debe hacerse de forma manual.

3.1.4 Resultados de las encuestas a los clientes actuales de servicios de monitoreo 24/7 de CSOC.

Se les consultó a los diez clientes del CSOC, sobre el servicio recibido en cuanto a la gestión de incidentes de ciberseguridad y según las respuestas obtenidas se puede decir que la satisfacción en términos generales puede mejorar, los clientes esperan reportes con mayor frecuencia, y además evidencian ciertos problemas en la gestión, como el tiempo de respuesta y la falta de priorización en la atención. A continuación, las respuestas de las preguntas realizadas.

Se preguntó a los clientes, cuanto conocen sobre los incidentes de ciberseguridad que afectan a su empresa, y según lo que respondieron podemos decir que el 70% está muy inmerso en lo que está ocurriendo en su empresa en cuanto a incidentes de ciberseguridad, mientras el otro 30% conoce poco sobre el tema.

Con respecto a las vulnerabilidades detectadas, de los 10 encuestados, el 90% indica que se han detectado vulnerabilidades en sus sistemas, si bien, este tipo de incidente no es considerado un ataque, el CSOC lo atiende como parte de la acción preventiva por la identificación de una vulnerabilidad, otro tipo de incidente relevante es el “malware”, el 70% de los encuestados admiten haber registrado incidentes de este tipo, los

siguientes más comunes, son “phishing” y “detección de equipos comprometidos”, pues ha afectado al 60% de los encuestados.

Se encuestó también sobre el nivel de satisfacción con respecto al servicio de monitoreo 24/7, para lo que el 60% de los encuestados piensan que el servicio es poco satisfactorio, e incluso existe un 10% que considera que el nivel de satisfacción es nada, solo el 30% cree que con la gestión que se realiza hasta ahora es suficiente.

Tabla 9 Nivel de satisfacción del servicio

Respuesta	Frecuencia	Porcentaje
Nada	0	10.00%
Poco	3	60.00%
Suficiente	5	30.00%
Mucho	2	0.00%
Muchisímo	0	0.00%
Total	**10**	**100.00%**

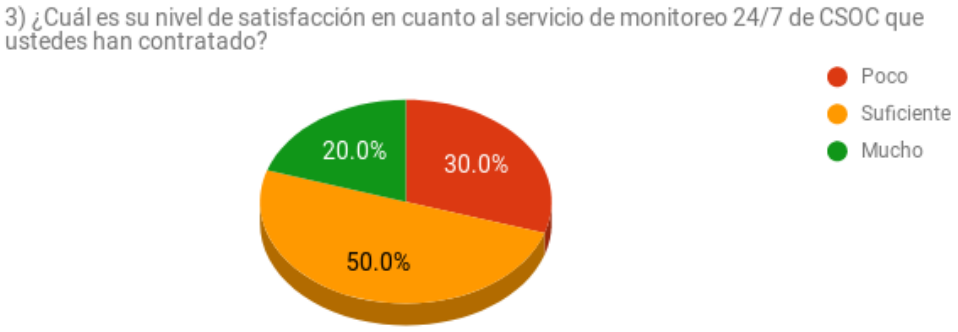


Figura 3.2 Nivel de satisfacción del servicio

Se consultó también a los clientes, sobre cuál es el nivel de satisfacción con respecto a la interacción que mantiene con el CSOC, a lo que se puede indicar que el 60% de los encuestados al menos cree que es suficiente la interacción mantenida hasta el momento.

Tabla 10 Nivel de satisfacción de la interacción con el CSOC

Respuesta	Frecuencia	Porcentaje
Nada	1	10.00%
Poco	3	30.00%
Suficiente	4	40.00%
Mucho	2	20.00%
Muchisímo	0	0.00%
Total	**10**	**100.00%**

Figura 3.3 Nivel de satisfacción de la interacción con el CSOC

En cuanto al nivel de satisfacción por la frecuencia y el contenido de los reportes recibidos por el CSOC, es preocupante que el 50% de los clientes no están complacidos con la frecuencia y el contenido de los reportes.

Tabla 11 Nivel de satisfacción en cuanto a los reportes

Respuesta	Frecuencia	Porcentaje
Nada	2	20.00%
Poco	3	30.00%
Suficiente	3	30.00%
Mucho	2	20.00%
Muchisímo	0	0.00%
Total	**10**	**100.00%**

Figura 3.4 Nivel de satisfacción en cuanto a los reportes

Se consultó a los clientes, sobre la atención prioritaria a los incidentes más críticos, a lo que el 60% de los encuestados contestó que considera que los incidentes no están siendo atendidos en orden prioritario.

Así mismo, en cuanto al tiempo de respuesta en que el CSOC atiende los casos, el 70% de los encuestados considera que no es el tiempo adecuado.

Tabla 12 Atención de incidentes prioritarios

Respuesta	Frecuencia	Porcentaje
SI	3	30.00%
NO	7	70.00%
Total	**10**	**100.00%**

Figura 3.5 Atención de incidentes prioritarios

El 70% de los encuestados piensa que la implementación de un sistema de respuestas ante incidentes por parte del CSOC ayudaría muchísimo en la gestión de atención de incidentes.

3.1.5 Análisis de servidores actuales del departamento CSOC

El departamento de centro de operaciones de ciberseguridad de la empresa cuenta actualmente con los siguientes servidores:

- 40 servidores de aplicaciones de seguridad
  - Características diversas
- 2 Servidores de aplicaciones administrativas
  - Sistema Operativo: Centos 6.5
  - Disco Duro: 120 GB
  - Memoria Ram: 8 GB
- Servidor de base de datos
  - Sistema Operativo: Centos 6.5
  - Disco Duro: 250 GB
  - Memoria Ram: 8 GB
- Servidor de logs
  - Sistema Operativo: Centos 6.5
  - Disco Duro: 2 TB

- Memoria Ram: 12 GB

- Servidor centralizador de eventos
  - Sistema Operativo: Centos 6.5
  - Disco Duro: 1 TB
  - Memoria Ram: 16 GB

Uno de los servidores de aplicaciones administrativas es utilizado actualmente, para almacenar en carpetas compartidas, la evidencia informática que resulta de las revisiones de incidentes, así mismo en este equipo se encuentra el archivo Excel en el que se registra la información de los incidentes. Todos los demás servidores son para uso de las herramientas de seguridad y monitoreo con que se trabaja actualmente en el CSOC.

3.2 Definición de parámetros a usar en el software

En la actualidad existen algunos parámetros que servirán de entrada para el uso de software, de los cuales se puede mencionar: la categoría del incidente, el nivel de severidad, y el estado del incidente.

A continuación, se muestra la categorización actual de los incidentes de seguridad que, según el análisis realizado a los casos cerrados durante el último año, resultaron con mayor relevancia:

Tabla 13 Tipos de incidentes más relevantes

Tipo Incidente	Total
Vulnerability	150
Compromise	112
Malware	85
Phishing	59
Spam	41
DoS	28
Reputation	7
Scam (web)	4

Hoy en día existe gran cantidad de incidentes de seguridad lo que hace poco eficiente el trabajo de los ingenieros sin una categorización por prioridad de la respuesta del incidente. Existe un total de 300 casos registrados en el último año, que aún no han sido atendidos. Las categorías que deberían permitir categorizar los incidentes son:

Tabla 14 Categorización de incidentes

Nivel	Descripción
Crítico	Incidentes que podrían detener las operaciones y deben ser atendidos de inmediato.
Alto	Incidentes que tienen impacto severo en las operaciones.
Medio	Incidentes que tienen un impacto significante, o tienen el potencial para tener un impacto severo en las operaciones.
Bajo	Incidentes que tienen un impacto mínimo con el potencial de impacto significativo o severo en las operaciones.

Los incidentes de seguridad, una vez que llegan al CSOC, son atendidos y pasan por diferentes estados a medida que avanzan en el proceso de resolución, en la tabla X están los posibles estados por los que puede pasar un caso.

Tabla 15 Estados del incidente

Nivel	Descripción
Pendiente	Los incidentes que llegan por parte del cliente o a través de las alertas emitidas por el servidor centralizador y se registran en la hoja Excel se consideran en este estado.
Investigación	Cuando el ingeniero empieza la investigación para dar solución al incidente.
Verificación	El ingeniero aplica la solución defensiva y envía sugerencia al cliente para prevenir un nuevo ataque del mismo tipo.
Cerrado	El ingeniero cierra el caso luego de darle solución y lo elimina de la lista de incidentes creados.

3.3 Definición de las fuentes de información para la creación de incidentes y eventos

Como se mencionó anteriormente las fuentes de información para la creación de incidentes de seguridad son principalmente las alertas que genera el servidor centralizador de eventos de seguridad. Sin embargo, no es la única fuente, existen incidentes que llegan también al CSOC, identificados por el cliente, por llamada o vía correo electrónica dependiendo de la urgencia del

caso. El gerente del CSOC, lo registra en la hoja de Excel para que sea atendido por un ingeniero.

El servidor centralizador de eventos de seguridad es alimentado por los logs que generan las diferentes herramientas de seguridad que el centro de operaciones tiene configurado para brindar el servicio de protección.

Actualmente este servidor de eventos de seguridad genera alertas que se envían mediante correo electrónico a la bandeja de correo del departamento y a los clientes.

Otra fuente de información son los ingenieros de monitoreo, que podrían detectar eventos que no son identificados por medio de las herramientas debido a que está fuera de su alcance.

CAPÍTULO 4

DISEÑO DE LA PROPUESTA

4.1 Diseño de los casos de uso de los incidentes de ciberseguridad

En este capítulo abordaremos el diseño de la propuesta, para dar solución a los problemas de gestión presentados en un centro de atención de incidentes de ciberseguridad, de tal modo que se obtengan ventajas para todos los actores del proceso, se optimicen los tiempos de respuesta y se brinde facilidades de seguimiento y acceso a reportes al cliente. Se definen los procesos que intervienen en todo el ciclo de gestión y atención de incidentes como se muestra en la Figura 4.1.

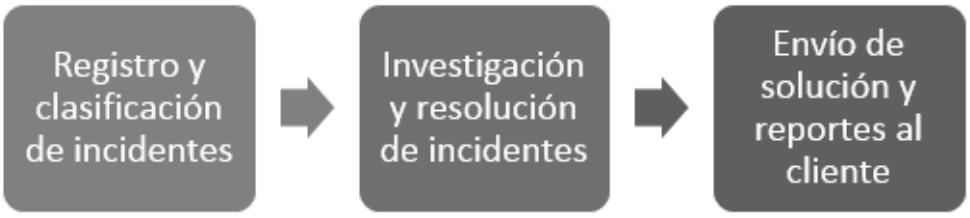


Figura 4.1 Procesos de la gestión de incidentes

En vista de las limitantes de presupuesto planteadas en la entrevista realizada a los gerentes del departamento de ciberseguridad del CSOC, y la poca oferta en cuanto a software de este tipo, contemplamos como software de gestión de incidentes, la plataforma FIR, por sus siglas en inglés, (Fast Incident Response), desarrollada por el departamento de seguridad de un banco francés, principalmente para crear, dar seguimiento y visualizar reportes de los incidentes de ciberseguridad suscitados.

Este software ha sido desarrollado bajo licencia GNU General Public License v3.0, por lo tanto, implementaremos la versión base, con ciertos ajustes realizados para satisfacer las necesidades planteadas en el capítulo anterior.

FIR está desarrollado en Python utilizando Django 1.9. Utiliza, además Bootstrap 3, y para mejorar la apariencia se han aplicado recursos Ajax y d3js. Se adapta a cualquier base de datos compatible con Django.

La versión de este software es muy genérica, uno de los principales inconvenientes es que no permite la administración de incidentes de diferentes clientes, por lo que se realizarán varios cambios en la programación para que el aplicativo cumpla con las necesidades del CSOC, las cuales son:

- Permitir que el sistema tenga una arquitectura **Multi-Tenant**, esto servirá para que soporte la información de varios clientes, y que sus usuarios sólo puedan acceder a la información asignada.
- Se cambiará el flujo de la gestión de los incidentes, con la incorporación de nuevos estados del incidente.
    - Antes sólo existían los estados: Abierto (Open) y Cerrado (Closed).
    - Ahora se añadieron los estados: Pendiente (Pending), Investigación (Investigate) y Verificación (Verification).

- En la página inicial es necesario incluir varias pestañas y modificar algunas para presentar información más detallada:

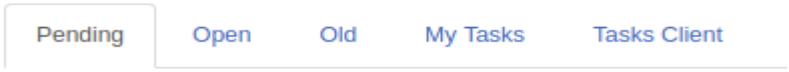


Figura 4.2 Nuevas opciones del software FIR

    - En la pestaña “Pending” se mostrarán los eventos e incidentes que tienen estado Pendiente.

- En la pestaña “Open” se mostrarán los eventos e incidentes que tienen estado Abierto, Investigación y Verificación.
- En la pestaña “My Task” se mostrarán sólo las tareas que fueron asignadas al CSOC.
- En la pestaña “Task Client” se mostrarán sólo las tareas que fueron asignadas a los clientes.

- En la página inicial se agregó una opción para filtrar de una manera más específica la información. Esta opción se llama Search & Filter.

El proceso macro a mejorar con la ayuda del software, es el de gestión de incidentes de ciberseguridad. Se mantienen las fuentes de información de la situación actual, ya que son las mismas que alimentarán el software propuesto.

4.1.1 Proceso de Registro y Clasificación de Incidente

El sistema permitirá al ingeniero de monitoreo o al cliente registrar directamente los incidentes que se presenten, ingresando información relevante como categorización, criticidad, recurso afectado, o artefactos involucrados, estos pueden ser ips, nombres de dominio, archivos, correos electrónicos y todo lo que se considere evidencia para llegar a

la solución del caso presentado. Los casos ingresados se registran con estado “Pending”.

Los ingenieros que posean el perfil respectivo para atender los incidentes podrán seleccionar el caso en el que van a trabajar y empezar la etapa de revisión, en esta instancia podrán agregar información, cambiar la categoría, la criticidad, o adjuntar nuevos artefactos, y si se tratase de un evento crítico, dar inicio a la etapa de investigación para solucionar el problema, cambiando el estado a “Investigate”.

En caso de que luego de la revisión, se identifica que el caso no es crítico, se dejará definida la criticidad y se cambiará el estado a “Open”, para que esté listo para ser investigado una vez se culmine con los casos críticos, asegurando así la atención prioritaria de incidentes.

4.1.2 Proceso de Investigación y resolución de incidente

Cuando un incidente pasa al estado “Investigate”, el ingeniero empieza a reunir y recabar toda la evidencia necesaria para llegar al problema. Entre las bondades del software está la capacidad para correlacionar artefactos, lo que ayuda mucho para buscar fácilmente si alguna de la información registrada como parte de la evidencia estuvo involucrada en un caso previamente registrado.

Las ips, direcciones de correo, nombres de dominio, y archivos son considerados artefactos, el sistema detecta el formato de estas entradas para luego correlacionar entre incidentes. En el caso de los archivos, el software obtiene el hash del mismo, para identificarlo. Si en otro incidente se llegare a subir el mismo archivo como evidencia, los hashes coincidirán, permitiendo evidenciar la correlación.

El sistema, además, ofrece acceso directo con envío de parámetros a las urls: virustotal.com y centralops.net, lo que permite identificar inmediatamente de donde proviene una ip, y analizar archivos y urls sospechosas.

4.1.3 Proceso de envío de solución e informes al cliente

Los incidentes de ciberseguridad, generalmente requieren de aplicar soluciones defensivas para reducir el impacto, y luego aplicar los mecanismos preventivos para evitar en la medida de lo posible, que un evento del mismo tipo se presente sobre el mismo recurso.

Una vez que el ingeniero detecta la raíz del problema, aplica inmediatamente la solución mitigante. Si el recurso afectado, está fuera del alcance del CSOC, se comunica al cliente sobre las acciones a tomar, el software permite ingresar tareas relacionadas al incidente y

asignarlas a un responsable que puede ser, el CSOC o el Cliente. En estas tareas, especifica las acciones preventivas además de la solución defensiva, de modo que quede registrada toda la información relevante al caso. Una vez que el cliente las revisa, las valida, y las aplica, el ingeniero puede cambiar el estado del caso a “Cerrado”.

En todo momento, el cliente puede ingresar a la plataforma y validar el estado de los incidentes, puede consultar aplicando filtros por estado, de modo que conozca en qué etapa se encuentra el incidente de su interés. El software ofrece reportes de estado del incidente, así como estadísticas del número de casos registrados en el tiempo. Además provee gráficos de incidentes por categorías, por el nivel de severidad.

4.2 Diseño de interacción del software FIR con las fuentes de información

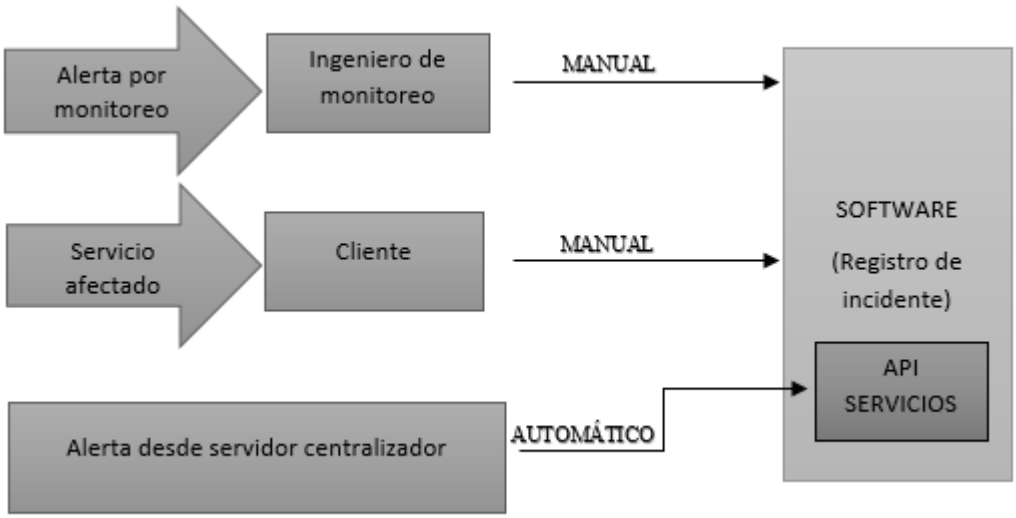


Figura 4.3 Diseño de interacción del software

Con el software, el ingreso de los incidentes de ciberseguridad se continúa realizando manualmente, pero ya no en todos los casos, el ingeniero o gerente puede continuar recibiendo por parte de las fuentes de información, la alerta y la evidencia de un suceso y registrar el incidente en la plataforma. Las alertas vía correo electrónico que genera el servidor centralizador a los empleados del CSOC, se van a registrar automáticamente como incidentes para alimentar el sistema. Esto gracias a que, con la implementación del software, se expondrán servicios, de modo que permite que una fuente de información automática alimente el sistema. Se debe considerar que es

necesaria cierta configuración en el servidor centralizador para que consuma el servicio expuesto por la plataforma FIR, y el incidente se registre automáticamente.

El servicio que expone el sistema, contempla todos los atributos como si se tratase de un ingreso manual, es decir se creará automáticamente el incidente con la información más relevante requerida que el servidor centralizador pueda ofrecer. En la etapa de revisión el ingeniero puede adicionar más información en caso de que sea necesario.

En la Figura 4.3 podemos ver un diagrama que aclara esta interacción entre el software FIR y las tres alternativas de fuentes de información existentes.

4.3 Diseño de los perfiles de usuarios a crear en el software FIR

Los perfiles de usuarios que serán asignados a los usuarios del software FIR, están definidos de acuerdo a los roles de su cargo en el departamento.

4.3.1 Perfil Administrador

Este perfil será otorgado a los gerentes del departamento, es decir, al gerente y al jefe operativo, además se otorgará este perfil a los 2 ingenieros de automatización, quienes son los administradores del software, pues son los encargados de implementar nueva funcionalidad al mismo.

Este perfil tendrá todas las opciones habilitadas, tiene autorización para ingresar, modificar y eliminar toda la información relacionada a la gestión de incidentes y eventos, de todos los clientes, además tiene acceso a las opciones de configuración de los parámetros del sistema y acceso a todos los reportes generados por la plataforma.

4.3.2 Perfil Operativo

Este perfil será otorgado a los 6 ingeniero especialistas en seguridad, y a los 5 ingenieros junior para el monitoreo CSOC.

Tendrá habilitadas las opciones que se relacionan con la gestión de incidentes y eventos, así como las opciones de estadística y reportería de todos los clientes.

4.3.3 Perfil Cliente Supervisor

Los perfiles de usuarios que serán creados para los clientes sólo podrán ver los incidentes y eventos que correspondan a su empresa.

Este perfil será asignado al cliente, con las opciones habilitadas para crear, consultar y gestionar incidentes. Además tendrá acceso a todas las estadísticas y reportes del cliente.

4.3.4 Perfil Cliente Lectura

Este perfil será otorgado al cliente solo como modo consulta, de modo que puedan revisar los reportes y estadísticas, monitorear los incidentes, revisar los comentarios, los archivos o artefactos subidos como evidencia, pero sin crear nuevos casos, ni realizar modificaciones, este perfil sólo será de lectura.

4.4 Diseño de las pruebas a realizar con el software FIR

Luego de la implementación del software FIR, se deben aplicar pruebas funcionales, de modo que se realice la verificación respectiva para asegurar que el software permite realizar el flujo de todos los procesos para la gestión de los incidentes de ciberseguridad. Además, es necesario realizar pruebas de integración para validar que los servicios que expone el software para la creación automática de incidentes sean consumidos satisfactoriamente por el servidor centralizador cuando genera una alerta.

4.4.1 Pruebas de funcionalidad

Para llevar a cabo las pruebas de funcionalidad, debemos partir de los tres procesos identificados dentro de la implementación del software FIR para la gestión de incidentes de ciberseguridad. Para esto la estrategia de pruebas se ha diseñado de modo que se defina un set de pruebas por cada uno de los procesos identificados, que permita demostrar el

correcto funcionamiento del software y que se esté considerando toda la información mínima requerida para el registro y atención de un incidente.

Los encargados de la ejecución de estas pruebas será los ingenieros de Automatización CSOC 1, y 2, con ayuda del gerente técnico serán los responsables de que estas pruebas se ejecuten satisfactoriamente.

4.4.1.1 Administración e Ingreso al sistema

El primer conjunto de pruebas corresponde a validar el funcionamiento de todas las interfaces administrativas que permiten la carga de la información básica al sistema, así como de las interfaces de acceso, y para esto debe considerarse el siguiente plan:

Tabla 16 Casos de pruebas para la administración

ID PRUEBA	DESCRIPCION	PERFILES ASOCIADOS
TEST-ADM-001	Cargar información de niveles de criticidad	Perfil Administrador
TEST-ADM-002	Cargar información de categorías de incidentes	Perfil Administrador

TEST-ADM-003	Cargar información de clientes	Perfil Administrador
TEST-ADM-004	Cargar información de los perfiles	Perfil Administrador
TEST-ADM-005	Cargar información de las fuentes de información	Perfil Administrador
TEST-ADM-006	Verificar la creación de usuarios	Perfil Administrador
TEST-ADM-007	Verificar la asociación de perfiles a usuarios	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor Perfil Cliente Lectura
TEST-ADM-008	Verificar la asociación de usuarios a empresa	Perfil Operativo Perfil Cliente Supervisor Perfil Cliente Lectura

TEST-ADM-009	Verificar el acceso al sistema	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor Perfil Cliente Lectura
TEST-ADM-010	Verificar el acceso por perfiles	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor Perfil Cliente Lectura

4.4.1.2 Proceso de Registro y Clasificación de Incidente

Luego de que se haya verificado toda la funcionalidad referente a la administración y acceso al sistema, se debe validar el

registro y clasificación de un incidente, para esto debe considerarse el siguiente plan:

Tabla 17 Casos de pruebas para Registro de Incidentes

ID PRUEBA	DESCRIPCION	PERFIL ASOCIADO
TEST-REG-001	Validar que en la pantalla de registro de incidentes se cargue correctamente toda la información básica del sistema.	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor
TEST-REG-002	Registro de un nuevo incidente validando que en la información ingresada se solicite: • Título • Categoría • Estado • Usuario • Criticidad	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor

	• Fuente de información • Descripción El estado inicial de un incidente debe ser “Pending”.	
TEST-REG-003	Validar que un usuario pueda crear únicamente incidentes de la empresa a la que está asociado.	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor Perfil Cliente Lectura
TEST-REG-004	Verificar que el campo descripción, identifique correctamente los artefactos. Los campos que deben considerarse artefactos son: • Direcciones ips • nombres de dominio	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor Perfil Cliente Lectura

	• correos electrónicos	

4.4.1.3 Proceso de Investigación y resolución de incidente

Durante la etapa de revisión de un incidente, es muy importante que los ingenieros registren las evidencias recolectadas, la plataforma debe permitir el correcto manejo de los archivos, las direcciones ips y de dominio de los incidentes, para esto deben realizarse las siguientes pruebas básicas que certifiquen que la plataforma no tendrá errores durante eta etapa del proceso de gestión de incidentes.

Tabla 18 Casos de pruebas para la solución de incidentes

ID PRUEBA	DESCRIPCION	PERFIL ASOCIADO
TEST-SOL-001	Verificar que el sistema permita agregar comentarios a un incidente previamente ingresado. Este campo	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor

	debe identificar automáticamente los artefactos: • Direcciones ips • nombres de dominio • correos electrónicos	
TEST-SOL-002	Verificar que el sistema permita agregar archivos a un incidente previamente ingresado. Este campo debe identificar automáticamente los hashes de los archivos y reconocerlos como artefactos.	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor
TEST-SOL-003	Verificar que las direcciones de dominio y las direcciones ip,	Perfil Administrador Perfil Operativo

	además de que se identifiquen como artefactos, muestren el tooltip que permite redirigir a centralops.net y automáticamente muestre la información referente a esta dirección.	Perfil Cliente Supervisor
TEST-SOL-004	Verificar que todos los archivos que se carguen al sistema, generen el hash del archivo cargado, y muestre el tooltip que permite redirigir a virustotal.com y automáticamente verificar si el hash coincide con alguna firma de un virus	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor

	reconocido por esta página.	
TEST-SOL-005	Verificar que el sistema haga correctamente la correlación de artefactos entre incidentes anteriores.	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor

4.4.1.4 Proceso de envío de solución e informes al cliente

El proceso final, pero no menos importante porque además incluye al cliente, es el de presentación de soluciones e informes al cliente. Es muy importante para que el software ayude a mejorar la satisfacción del cliente, que éste pueda tener acceso a reportes, información estadística, y conocer el estado de los incidentes en cualquier momento, simplemente accediendo a la interfaz provista por el CSOC.

Tabla 19 Casos de pruebas de los reportes del sistema

ID PRUEBA	DESCRIPCION	PERFIL ASOCIADO
TEST-REP-001	Verificar que el sistema permita cargar tareas	Perfil Administrador Perfil Operativo

	para los incidentes y que estas permitan incluir además de los ingenieros, al cliente como responsable	Perfil Cliente Supervisor
TEST-REP-002	Verificar que el sistema permita consultar los incidentes creados: • por estado • por nivel de criticidad • por categoría • por fechas	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor Perfil Cliente Lectura
TEST-REP-003	Verificar el correcto funcionamiento de los reportes estadísticos que deben permitir analizar la información por trimestre o por año de los incidentes según su criticidad, o categoría.	Perfil Administrador Perfil Operativo Perfil Cliente Supervisor Perfil Cliente Lectura

CAPÍTULO 5

DESARROLLO, IMPLEMENTACIÓN Y PRUEBAS

5.1 Arquitectura de implementación del software FIR

Para entender la arquitectura de la implementación es importante conocer el flujo de la información del proyecto. Actualmente los logs de eventos de los equipos de seguridad son enviados por el servidor centralizador, el cual es el encargado de correlacionar toda la información y según los casos de uso definidos generará alertas que serán enviados al proyecto FIR por medio del consumo de un servicio web (API), el cual estará expuesto en el servidor web. Este servicio web (API) creará automáticamente un registro de incidente en la base de datos.

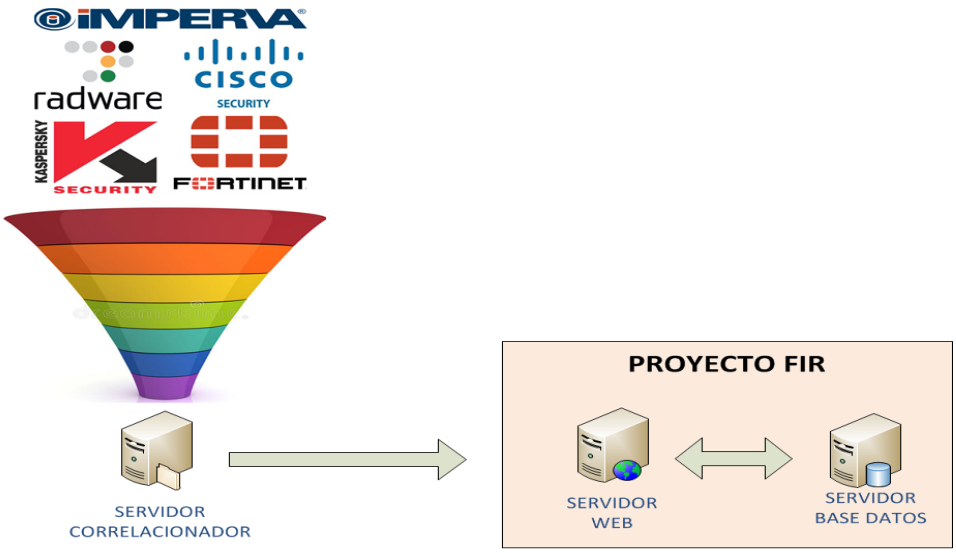


Figura 5.1 Interacción FIR y servidor centralizador

La interacción del servidor correlacionador con el servidor web, se hace directamente sin pasar por el firewall, debido a que están en la misma red, caso similar es la interacción del servidor web con el servidor de base de datos.

El servidor web de aplicaciones tiene instalado el sistema operativo Centos 6.5, con 8 GB RAM y 120 GB de disco duro, en el cual se encuentra instalado Apache/2.2.15 (Unix), Python y todas librerías necesarias.

La base de datos se aloja en un servidor con sistema operativo Centos 6.5, con 8 GB RAM y 250 GB de disco duro. En este servidor se encuentra instalado el motor de base de datos PostgreSQL versión 9.6.

Para que los usuarios del centro de operaciones puedan acceder al portal web FIR se ha propuesto la siguiente topología, la misma que está protegida por un firewall perimetral para poder acceder a los servidores de la DMZ.

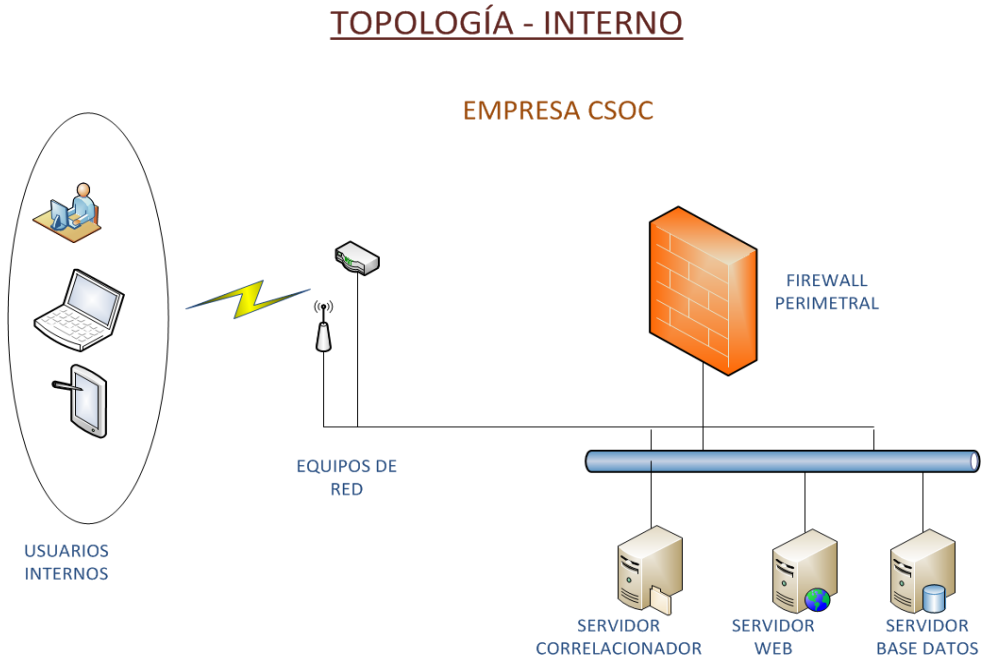


Figura 5.2 Topología para usuarios internos

Para que los clientes puedan acceder al portal web FIR, se propone la siguiente topología en la cual se debe configurar un túnel vpn para cada cliente. Este túnel será configurado entre el firewall o router del cliente y el firewall perimetral del centro de operaciones. Este túnel será de tipo ipsec

utilizando el modo side-to-side el cual nos permitirá configurar un enrutamiento seguro.

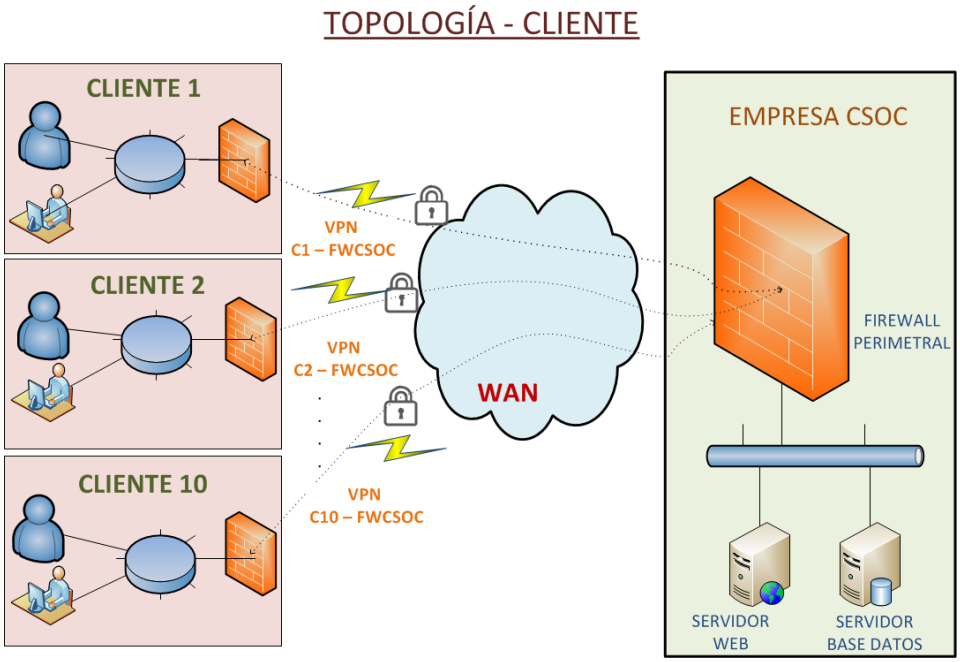


Figura 5.3 Topología para clientes

5.2 Implementación del software FIR

El software FIR es un proyecto open source realizado por la empresa CERT Société Générale. Este fue desarrollado en el lenguaje de programación Python y utilizaron el framework Django versión 1.9, ademas utiliza Bootstrap 3 y librerías Ajax. Este proyecto puede ser utilizado con cualquier motor de base de datos, porque tiene un adaptador a cualquier base.

Este proyecto será instalado en el servidor de aplicaciones en el que se tiene alojado un sistema interno.

Para la implementación es necesario instalar Python y las librerías que se van a utilizar para el uso del aplicativo, descargar el proyecto del repositorio github donde se encuentra alojado y crear una ambiente virtual de python y activarlo para comenzar a instalar las librerías necesarias.

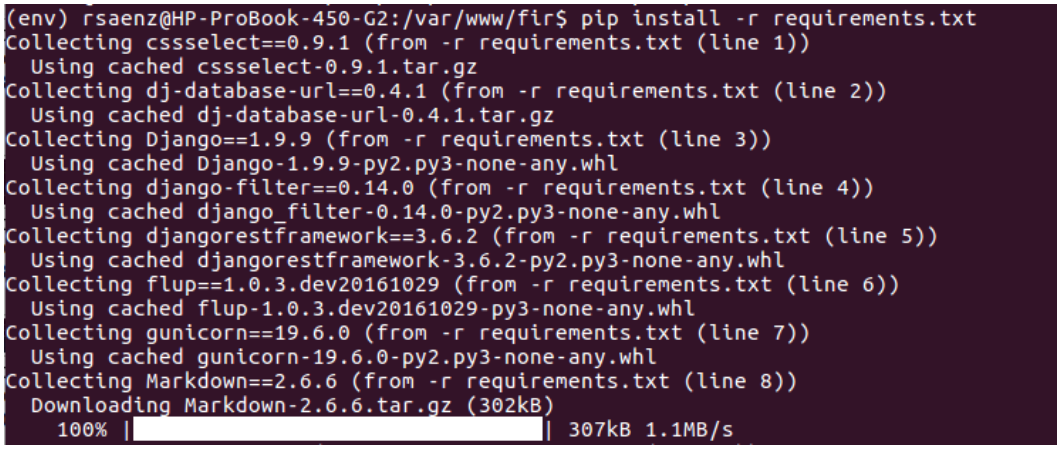


Figura 5.4 Proceso de implementación del software FIR

Es necesario, además modificar los archivos de configuración para setear las conexiones a la base de datos, y habilitar el uso de librerías y de plugins para el uso del aplicativo. Luego hay que proceder con la modificación de los módulos y la creación de las tablas en la base de datos, el framework Django nos facilita ese trabajo utilizando los comandos makemigrations y migrate.

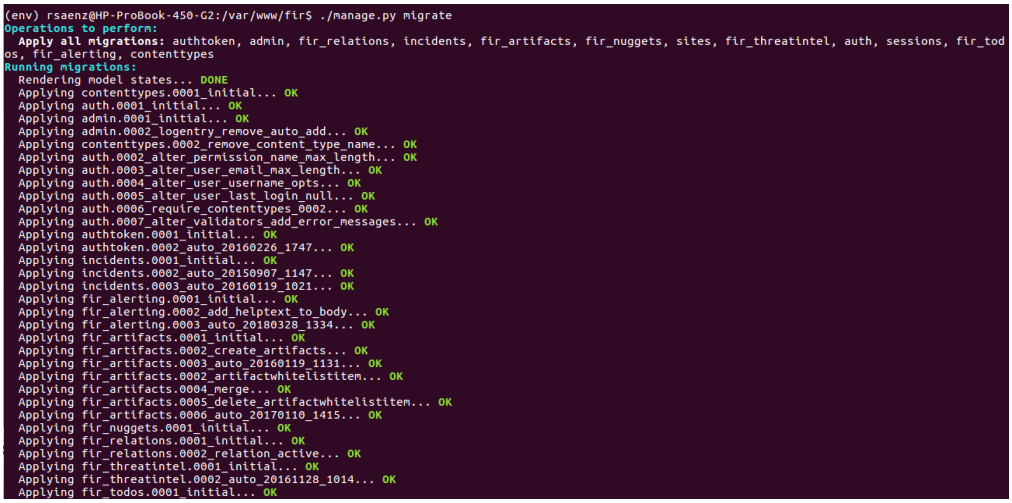


Figura 5.5 Proceso de implementación del software FIR

Luego hay que ejecutar los siguientes comandos para levantar el servidor:

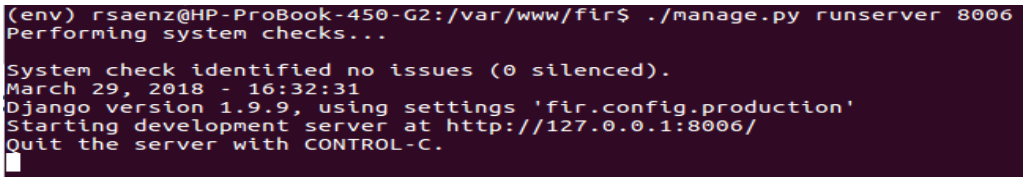


Figura 5.6 Pasos para levantar el servidor

Luego de seguir todos los pasos, el sistema estará habilitado para poder utilizarlo.

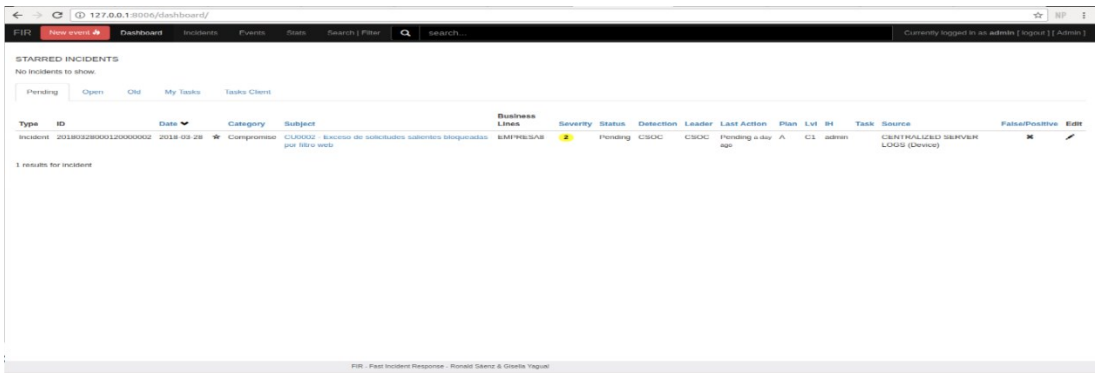


Figura 5.7 Software instalado

En esta fase de implementación se procederá a la insertar los valores iniciales de los parámetros del sistema para poder utilizarlo.

Roles de Usuarios:

En esta sección se registrarán los roles que serán utilizados para la asignación de permisos para los usuarios.

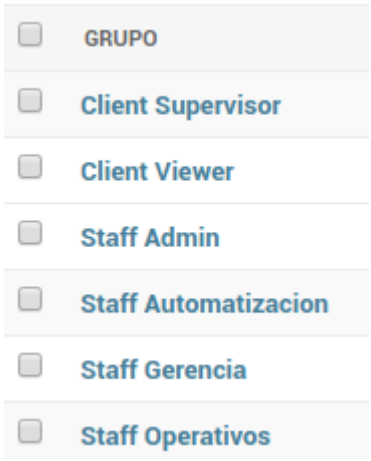


Figura 5.8 Roles configurados en el software

Se crearon roles a partir de los clientes y de la empresa. Entre los roles que se crean para los clientes están los siguientes:

Client Supervisor – Cliente Supervisor

Este rol tiene privilegio de gestionar los incidentes (crear, editar, borrar), y podrá interactuar con él incidentes como por ejemplo añadir comentarios, añadir archivos, crear tareas, interactuar con los artefactos. Aparte tendrá acceso a las estadísticas y los reportes.

Client Viewer – Cliente Lectura

Este rol tiene privilegio de lectura de incidentes, en el cual podrá sólo ver los incidentes y ver las estadísticas y reportes.

Entre los roles que se crean para los clientes están los siguientes:

Staff Admin, Staff Automatization, Staff Gerencia - Administradores

Estos roles tienen habilitado todos los privilegios, para que pueda administrar el aplicativo, y aparte gestionar completamente los incidentes.

Staff Operation - Operativo

Este rol tiene privilegio de gestionar los incidentes (crear, editar, borrar), y podrá interactuar con él incidentes como por ejemplo añadir comentarios, añadir archivos, crear tareas, interactuar con los artefactos. Aparte tendrá acceso a las estadísticas y los reportes.

Líneas de negocio:

En esta sección se registrarán las líneas de negocio, las cuales serán para referenciar los clientes afectados por los incidentes creados, en este caso hemos creado las diez empresas que actualmente tenemos como clientes de monitoreo y además hemos agregado a nuestro departamento de CSOC.

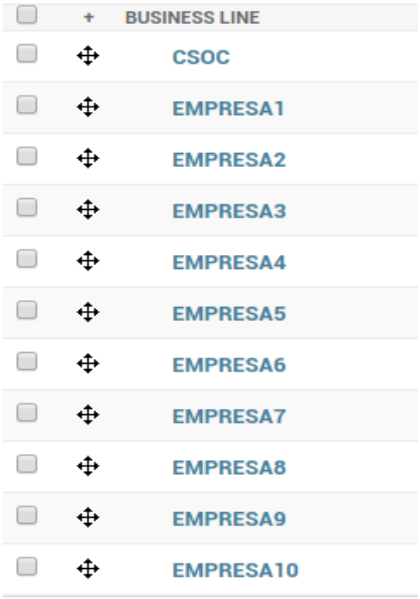


Figura 5.9 Clientes registrados

Categorías de Incidentes:

Esta categoría será para distinguir el tipo del incidente, en él se han ingresado los incidentes más relevantes.

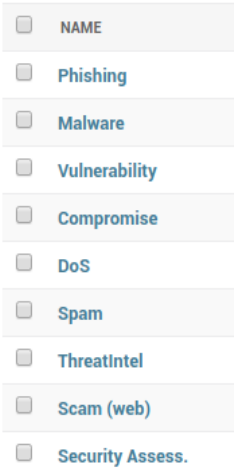


Figura 5.10 Categorías registradas

Etiquetas de Detección:

Servirá para describir quien fue que detectó el incidente para que sea registrado, en este caso hemos creado los departamentos de las empresas que interactúan con el centro de operaciones.

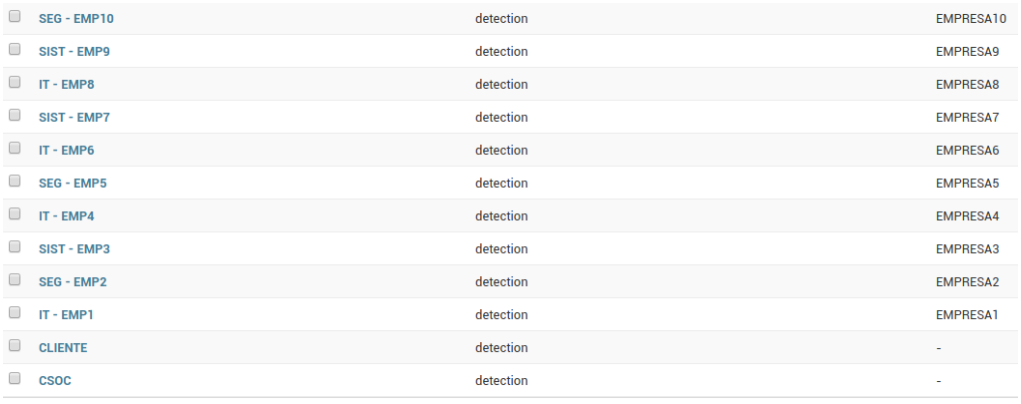


Figura 5.11 Áreas registradas

Acciones:

Servirá para identificar los registros que se guardarán en la sección de comentarios.

Figura 5.12 Posibles acciones de los incidentes

Plan:

Servirá para registrar el tipo de plan que será utilizado para realizar la investigación y la mitigación del incidente. Estos planes aún no son definidos, por tal motivo sólo será creado uno por defecto llamado **"A"**

Actor:

Servirá para registrar los actores que intervendrán en la resolución del incidente. En este caso hemos creado por defecto el valor de "**CSOC**"

Fuentes de información:

En esta sección se registrarán las fuentes de información del origen donde el incidente ocurrió o desde donde se presentó.

En este caso hemos ingresado la información que viene del servidor centralizador de logs (Centralized Server Logs) y de fuentes ingresadas por personas (External) y otras fuentes que son equipos de seguridad, que pudieron verse afectados, y que estuvieron fuera del alcance del servidor centralizador de logs.

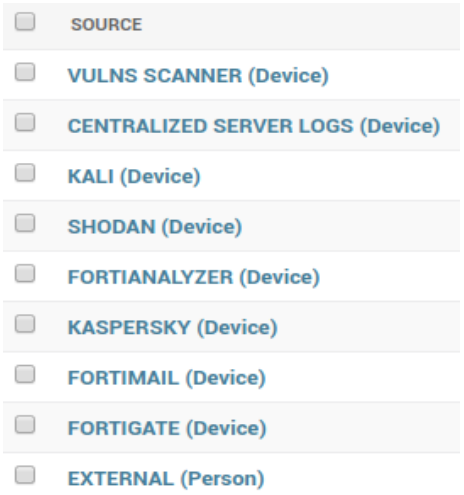


Figura 5.13 Fuentes de origen de incidentes

5.3 Desarrollo de las pruebas del software FIR

Para estas pruebas nos basaremos en el diseño de pruebas que se mencionan en el capítulo 4.4.

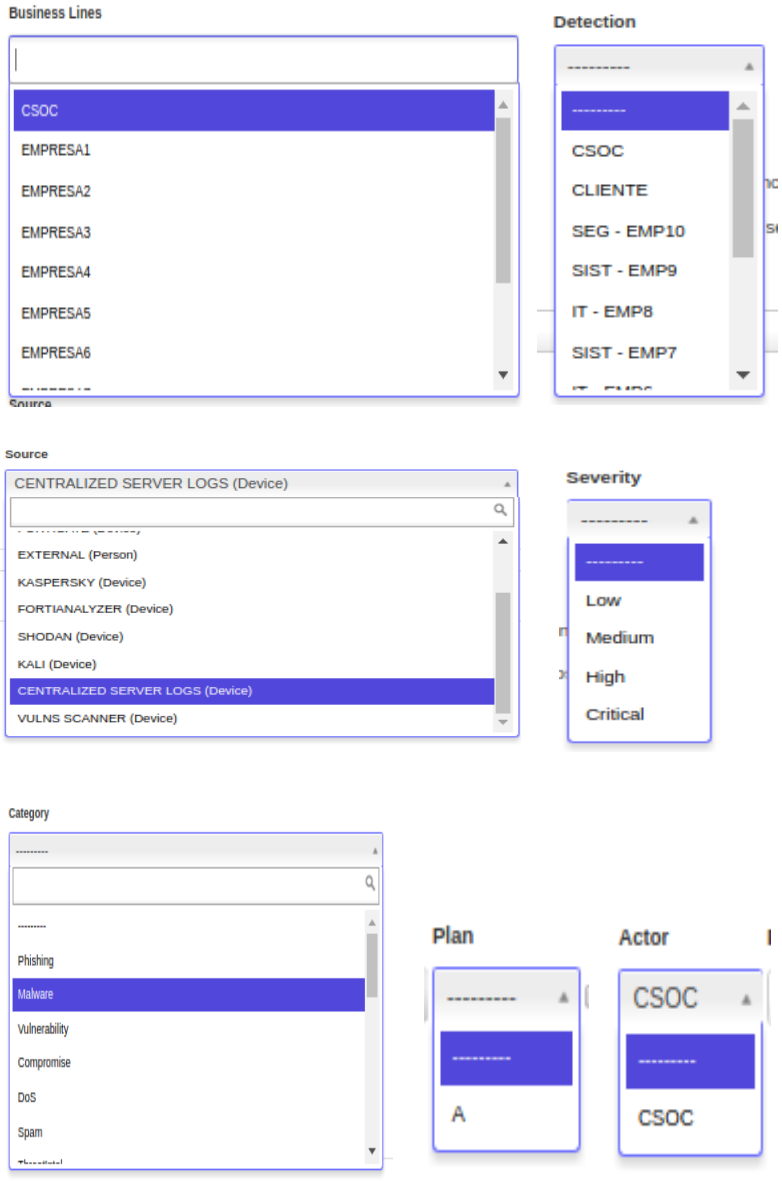
5.3.1 Pruebas del Proceso de Administración e Ingreso al Sistema

Las primeras pruebas corresponden a la Administración e Ingreso al Sistema que se mencionan en el subcapítulo 4.4.1.1, estas pruebas se las realizó en la etapa de Implementación por parte de los Ingenieros Automatización de CSOC, en el cual tuvieron que ingresar todos los parámetros iniciales para que el sistema pueda ser utilizado por los usuarios. Además tuvieron que crear los perfiles de usuarios y asignarle a los usuarios respectivamente, y realizaron las pruebas de ingreso al sistema.

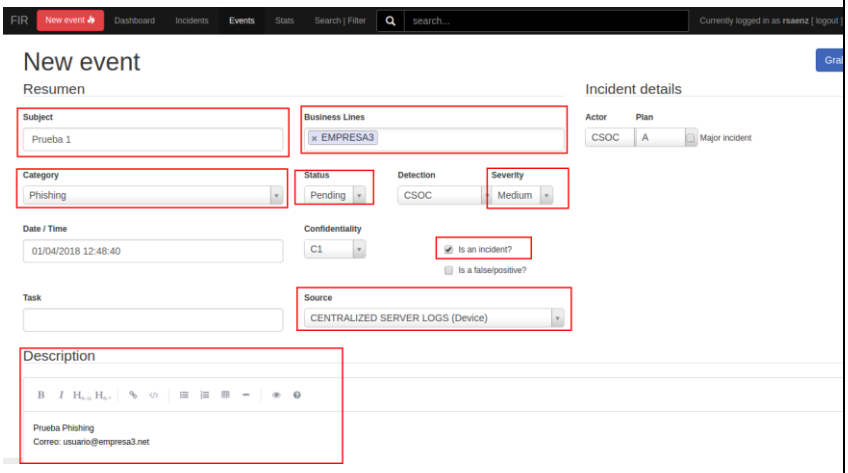
5.3.2 Pruebas del Proceso de Registro y Clasificación de Incidente

Estas pruebas se mencionan en el subcapítulo 4.4.1.2.

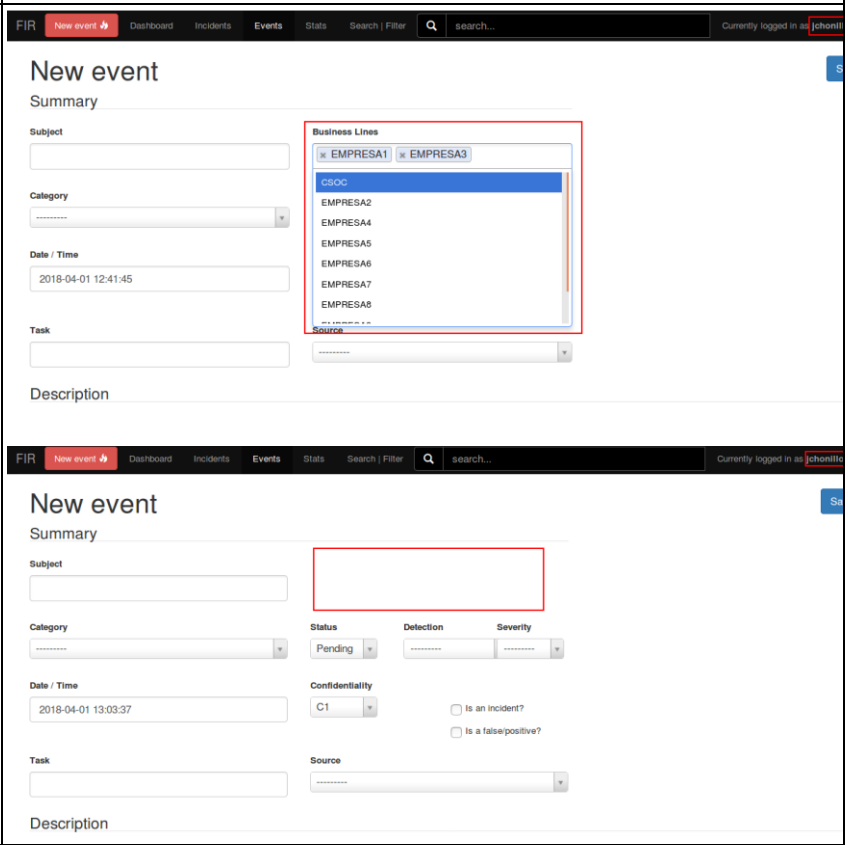
Id Prueba	TEST-REG-001
Descripción Prueba	Validar que en la pantalla de registro de incidentes se cargue correctamente toda la información básica del sistema.
Técnicas	Al dar click en “New event” nos cargará un formulario para ingresar un nuevo incidente. Comprobar que cada caja de selección cargue correctamente sus opciones.

Interfaz Gráfica	
Resultados	Esperado
Comentarios	

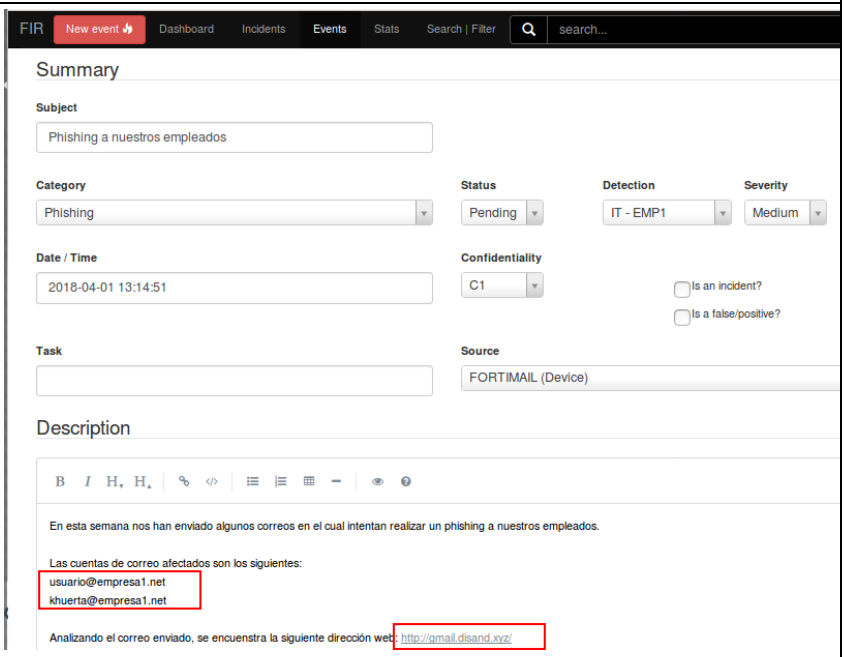
Id Prueba	TEST-REG-002

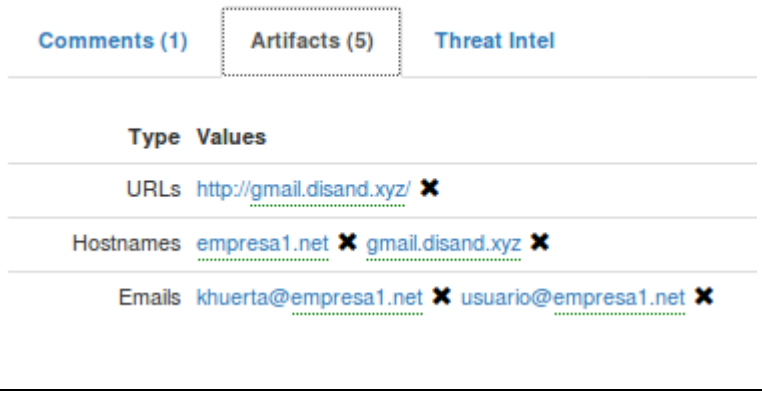
Descripción Prueba	Registro de un nuevo incidente validando que en la información ingresada se solicite: • Título • Categoría • Estado • Usuario • Criticidad • Fuente de información • Descripción El estado inicial de un incidente debe ser “Pending”.
Técnicas	Al dar click en “New event” nos cargará un formulario para ingresar un nuevo incidente. Ingresar cada uno de los parámetros solicitados para crear el incidente.
Interfaz Gráfica	
Resultados	Esperado
Comentarios	

Id Prueba	TEST-REG-003
Descripción Prueba	Validar que un usuario pueda crear únicamente incidentes de la empresa a la que está asociado.
Técnicas	Al dar click en “New event” nos cargará un formulario para ingresar un nuevo incidente.

	Para los usuarios del CSOC debe cargar un campo llamado “Business Line”, el cual mostrará todos los clientes. Para los usuarios de los clientes no debería cargar. Probar con el usuario “jchonillo” del cliente “Empresa1”.
Interfaz Gráfica	
Resultados	No Esperado
Comentarios	Al intentar crear un incidente con el usuario “jchonillo” del cliente “Empresa1” se le mostró el campo “Business Line” con la información de todos los clientes, dándole la opción de asignar otra empresa a la que no pertenece. Luego de estas pruebas se verificó el inconveniente y se desarrolló la solución, y luego de otra prueba ya no mostraba el campo “BusinessLine”

Id Prueba	TEST-REG-004

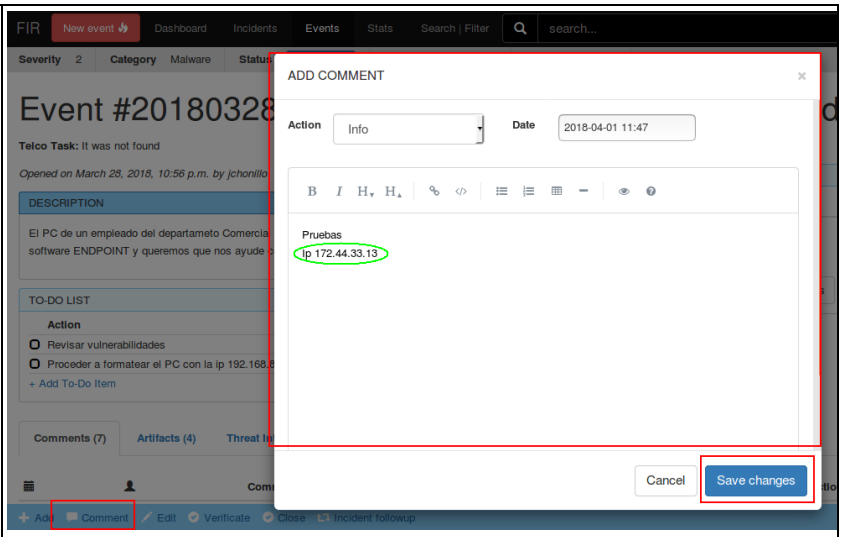
Descripción Prueba	Verificar que el campo descripción, identifique correctamente los artefactos. Los campos que deben considerarse artefactos son: • Direcciones ips • Nombres de dominio • Correos electrónicos
Técnicas	Al dar click en “New event” nos cargará un formulario para ingresar un nuevo incidente, en el cual existe un campo llamado “Description” en el que se podrá ingresar cualquier texto relevante que puede ser utilizado para la extracción de artefactos. Probar el ingreso de nombres de dominios, correos electrónicos, en este campo.
Interfaz Gráfica	

	
Resultados	Esperado
Comentarios	

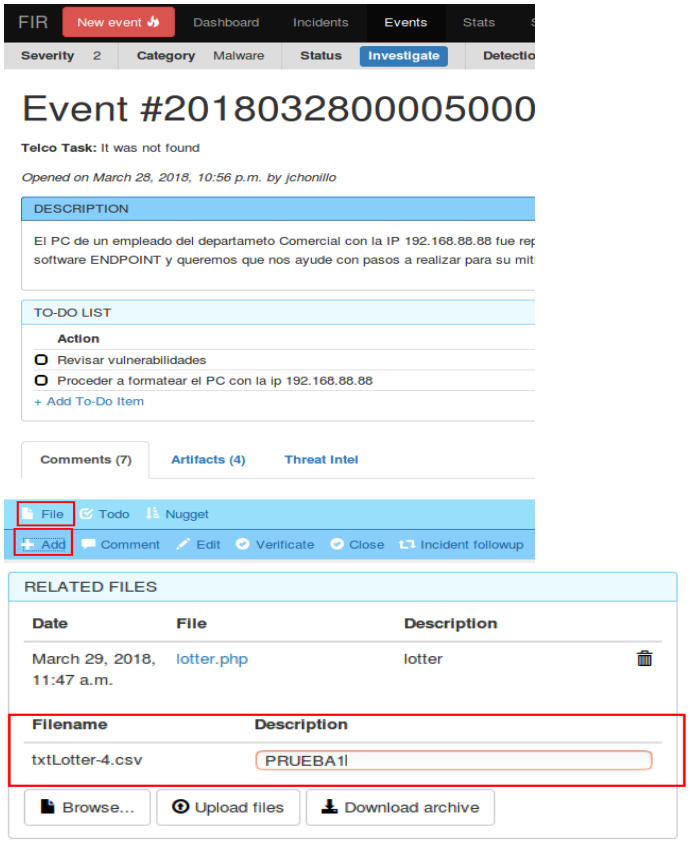
5.3.3 Pruebas del Proceso de Investigación y resolución de incidente

Estas pruebas se mencionan en el subcapítulo 4.4.1.3.

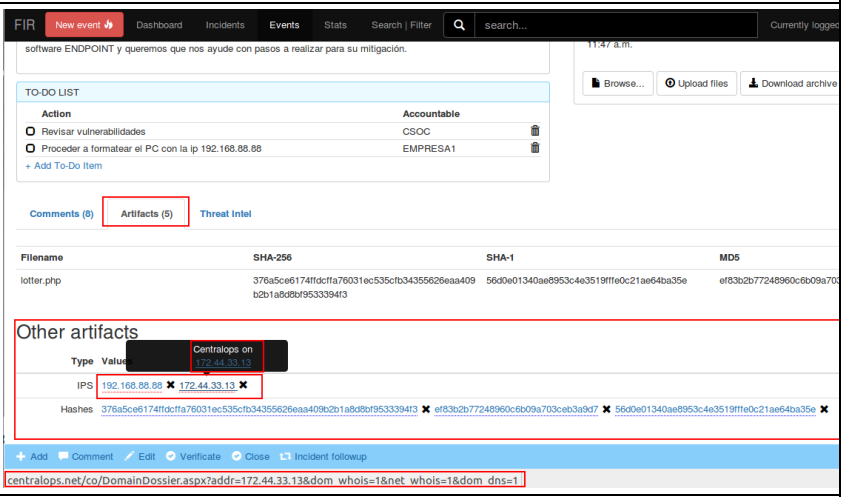
Id Prueba	TEST-SOL-001
Descripción Prueba	Verificar que el sistema permita agregar comentarios a un incidente previamente ingresado. Este campo debe identificar automáticamente los artefactos: • Direcciones ips • Nombres de dominio • Correos electrónicos
Técnicas	En la vista del incidente dar click en el botón “Comment”, el cual abrirá una ventana para registrar el comentario. Luego hay que ingresar los datos del formulario y dar click en “Save Changes”

Interfaz Gráfica	
Resultados	Esperado
Comentarios	

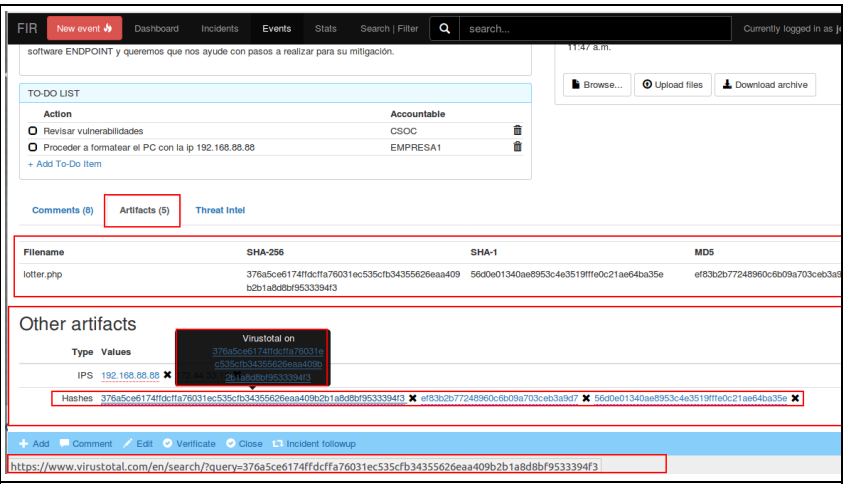
Id Prueba	TEST-SOL-002
Descripción Prueba	Verificar que el sistema permita agregar archivos a un incidente previamente ingresado. Este campo debe identificar automáticamente los hashes de los archivos y reconocerlos como artefactos.
Técnicas	En la vista del incidente dar click en el botón “Add - File”, el cual permitirá subir un archivo. Luego se cargará en la sección “Related Files” con el nombre del archivo que se subió, y en el cual debe llenar un campo de texto con la descripción del archivo que se subió.

Interfaz Gráfica	
Resultados	Esperado
Comentarios	

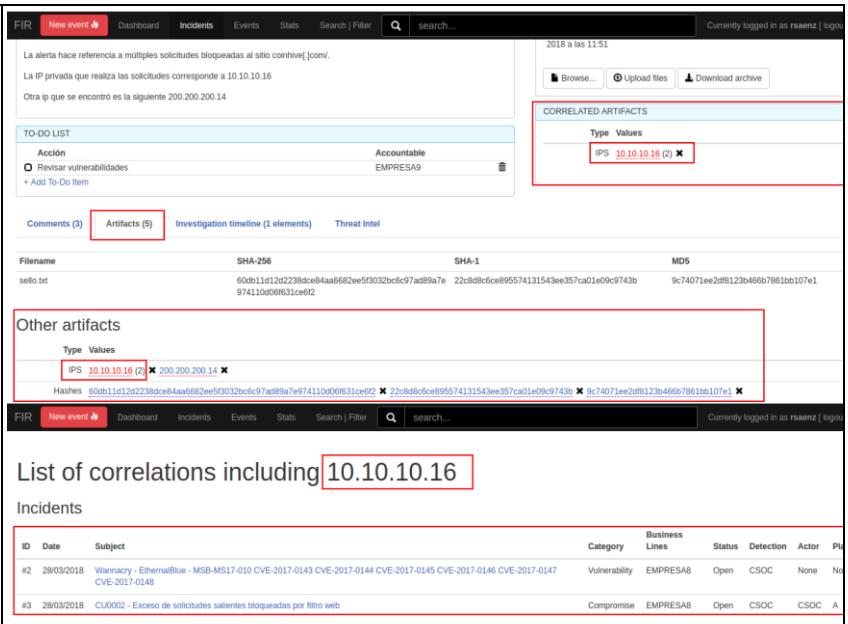
Id Prueba	TEST-SOL-003
Descripción Prueba	Verificar que las direcciones de dominio y las direcciones ip se identifiquen como artefactos, además que en el reporte se muestren el tooltip que permite redirigir a centralops.net para que se muestre la información referente a este artefacto.
Técnicas	En la vista del incidente dar click en la pestaña “Artifacts”, el cual nos mostrará todos los artefactos que el sistema ha podido extraer de la información registrada. Debajo del título Other Artifacts muestra una tabla con los artefactos, en el cual podemos ver las direcciones ips, direcciones

	dominio, cuentas de correo. Al pasar el mouse se puede observar el tooltip con un url de la página centralops.net.
Interfaz Gráfica	
Resultados	Esperado
Comentarios	

Id Prueba	TEST-SOL-004
Descripción Prueba	Verificar que todos los archivos que se carguen al sistema, generen el hash del archivo cargado, y sea identificado como artefacto y que además se muestre el tooltip que permite redirigir a virustotal.com, en el cual se mostrará si el hash coincide con alguna firma de un virus reconocido por esta página.
Técnicas	En la vista del incidente dar click en la pestaña “Artifacts”, el cual nos mostrará todos los artefactos que el sistema ha podido extraer de la información registrada. Arriba del título Other Artifacts se muestra una tabla con los archivos cargados al sistema con sus respectivos hashes. Debajo del título Other Artifacts se muestra una tabla con los artefactos, en el cual podemos ver los hashes de los archivos cargados. Al pasar el mouse se puede observar el tooltip con un url de la página virustotal.com.

Interfaz Gráfica	
Resultados	Esperado
Comentarios	

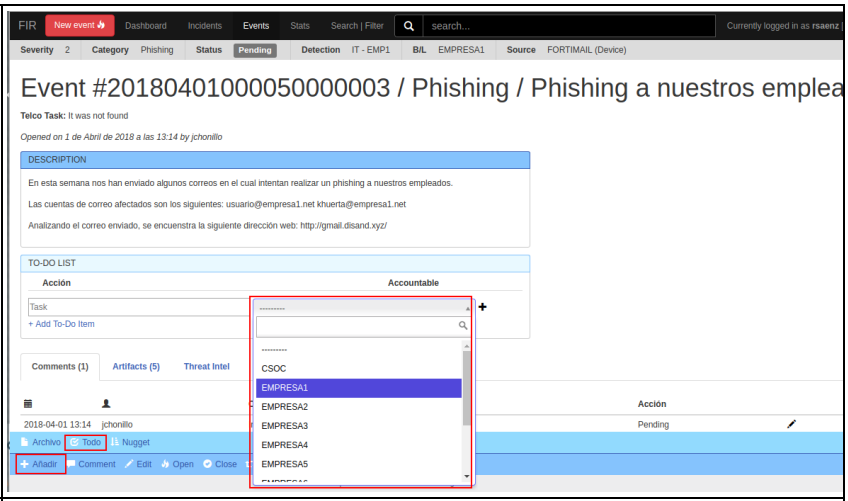
Id Prueba	TEST-SOL-005
Descripción Prueba	Verificar que el sistema haga correctamente la correlación de artefactos entre incidentes anteriores.
Técnicas	En la vista del incidente dar click en la pestaña “Artifacts”, el cual nos mostrará todos los artefactos que el sistema ha podido extraer de la información registrada. Se mostrará de color rojo si es un incidente correlacionado. En la sección “Correlated Artifacts” se mostrarán todos los artefactos que se han ingresado en más de un incidente. Al dar click en el registro, nos redirigirá a otra página en el cual se mostrarán todos los incidentes relacionados con este artefacto.

Interfaz Gráfica	
Resultados	Esperado
Comentarios	

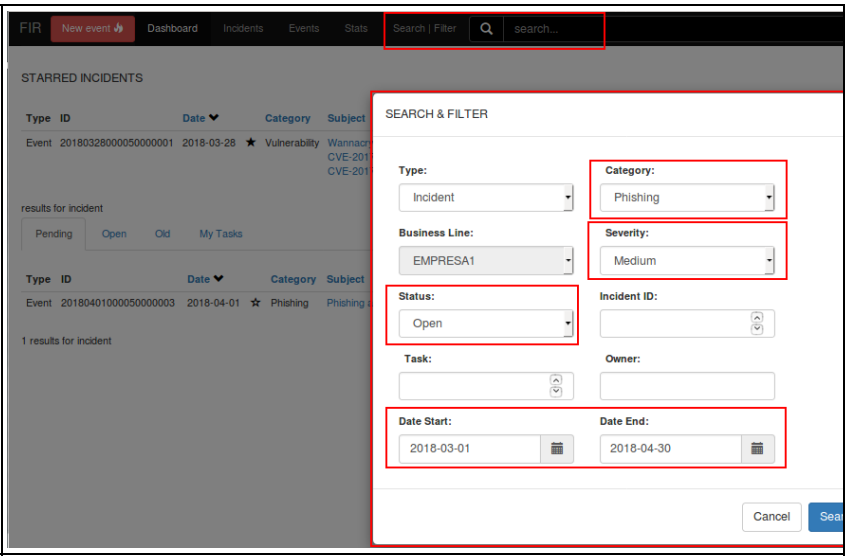
5.3.4 Pruebas del Proceso de envío de solución e informes al cliente

Estas pruebas se mencionan en el subcapítulo 4.4.1.4.

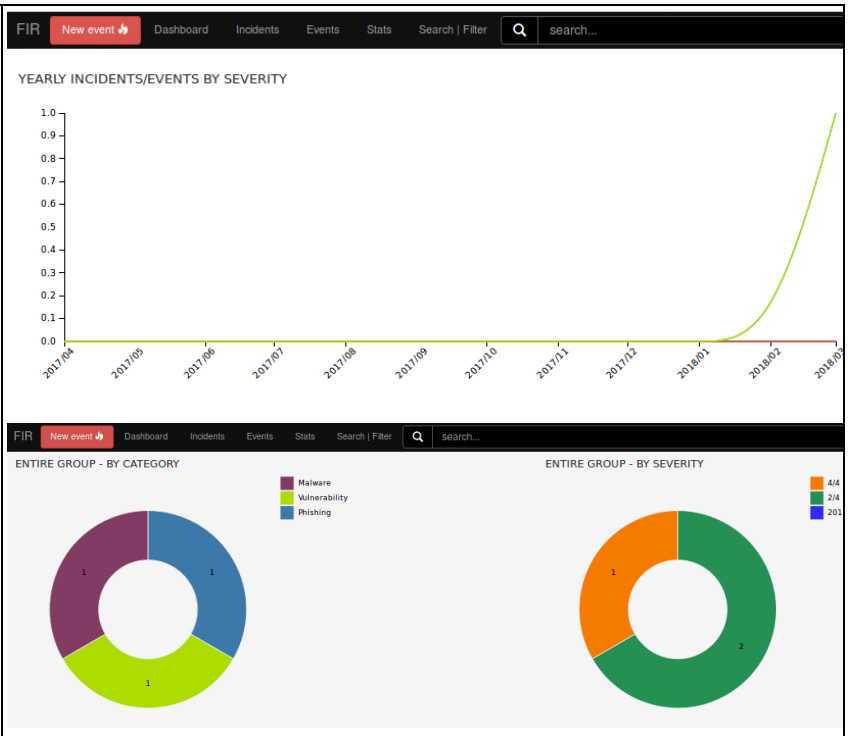
Id Prueba	TEST-REP-001
Descripción Prueba	Verificar que en el sistema se puedan crear tareas para los incidentes y que estas permitan asignarle al cliente como al departamento CSOC.
Técnicas	En la vista del incidente dar click en la pestaña “Add - Todo”, el cual abrirá la sección TO-DO LIST que permitirá ingresar una tarea, y asignarla al CSOC o a los clientes.

Interfaz Gráfica	
Resultados	Esperado
Comentarios	

Id Prueba	TEST-REP-002
Descripción Prueba	Verificar que el sistema permita consultar los incidentes creados: • por estado • por nivel de criticidad • por categoría • por fechas
Técnicas	En la barra superior existe una opción llamada “Search|Filter”, el cual abrirá una ventana en el cual podemos filtrar los incidentes. Probar que se pueda filtrar por estado, nivel de criticidad, categoría y por fechas.

Interfaz Gráfica	
Resultados	Esperado
Comentarios	

Id Prueba	TEST-REP-003
Descripción Prueba	Verificar el correcto funcionamiento de los reportes estadísticos que deben permitir analizar la información por trimestre o por año de los incidentes según su criticidad, o categoría.
Técnicas	En la barra superior existe una opción llamada “Stats”, el cual abrirá un submenú que muestra lo siguiente: • Yearly • Quarterly • Compare with previous year • Major Incidents • Sandbox • Attributes Seleccionar la opción “Yearly” y “Quarterly” y luego verificar las estadísticas.

Interfaz Gráfica	

	
Resultados	Esperado
Comentarios	

5.4 Plan de implementación y capacitación

Luego de haber realizado la instalación y haber confirmado la correcta ejecución de los guiones de pruebas definidos, se pone en marcha el plan para la implementación de la plataforma FIR en el ambiente de producción, para esto se han establecido las siguientes tres etapas:

5.4.1 Aceptación del software

Como parte del aseguramiento de la calidad del software, se valida que las pruebas del software FIR, cumplan con el diseño especificado en la propuesta, además se prueba que cada módulo funciona bien por separado, que todos los módulos se integran correctamente y que el software ofrece las funciones esperadas.

El gerente técnico se reúne con los ingenieros de automatización para revisar los resultados de las pruebas realizadas y se da por aceptado el funcionamiento del software FIR en el entorno operativo.

5.4.2 Estrategia de implementación

Se plantea la realización de un piloto con la participación de todos los ingenieros de monitoreo y dos de los clientes, los que se consideren más accesibles, y colaboradores, de modo que se den el tiempo de navegar por la plataforma y validar las características del software.

Los perfiles habilitados durante el piloto serán:

- Perfil Operativo
- Perfil Cliente Lectura

Los ingenieros de monitoreo ingresarán al software con las opciones que corresponden al Perfil Operativo.

Los clientes que participaran del piloto ingresaran al software únicamente en modo consulta, con el Perfil Cliente Lectura, de modo que puedan interactuar con la plataforma, revisar y validar los reportes y estadísticas que ofrece el sistema y transmitir sus observaciones acerca del mismo.

5.4.3 Plan de Riesgos

Si bien es cierto, para esta implementación, se ha trabajado bajo las necesidades del departamento, y en vista de que el proceso de gestión de incidentes se hacía manualmente, la inclusión de una herramienta de automatización como lo es el software FIR, supone una mejora considerable para los ingenieros de monitoreo y en el peor escenario los incidentes pueden continuar tratándose como hasta el momento, sin embargo se ha previsto realizar un piloto para reducir el impacto de los riesgos suscitados.

Durante la etapa de implementación pueden existir situaciones o condiciones inesperadas que afecten directamente a la puesta en

producción del software, es por esto que se han previsto algunos posibles riesgos y se los ha clasificado para su tratamiento.

Tabla 20 Tratamiento de riesgos de implementación

Riesgo	Impacto	Probabilidad	Tratamiento
Problemas de integración del software FIR con el servidor centralizador.	Medio	Medio	El servidor centralizador continuará enviando las alertas por correo electrónico para evitar pérdidas de información.
Indisponibilidad de la plataforma, independientemente de la causa.	Alto	Bajo	Registro manual de incidentes, mientras se recupere el acceso al sistema.
Daños en base de datos.	Bajo	Bajo	Backups automáticos con periodicidad diaria. La notificación de incidentes vía correo se mantiene para evitar perdida de información.
Los reportes y estadísticas del software no satisfacen al cliente.	Medio	Bajo	No se presentarán las opciones para todos los clientes, sino únicamente a dos de ellos, los más accesibles, de modo que se reciba retroalimentación por parte de ellos y se realicen pequeños ajustes en caso de que sea requerido.
Cambios en requerimientos en etapa Piloto	Medio	Bajo	Se analiza tiempos y magnitud de los cambios y se pueden ir aplicando gradualmente en función de la prioridad y según la autorización del gerente técnico.

5.4.4 Capacitación de usuarios

Se prepara un plan de capacitación del uso del software FIR para los clientes y el personal técnico, que incluye un detallado manual de usuario.

Además, se brinda capacitación a los clientes que participarán en el piloto de las opciones habilitadas para su perfil, y se organiza la capacitación al personal técnico para que tengan total conocimiento del proyecto.

5.4.5 Operación

Luego de realizar la capacitación a los usuarios finales, se inician las operaciones en el ambiente de producción, brindando el respectivo acompañamiento y soporte a los usuarios que participan del piloto, para asegurar el correcto funcionamiento de la plataforma.

En esta etapa pueden surgir oportunidades de mejoras, producto de la utilización del software, las mismas que el gerente técnico ha definido que serán consideradas en una siguiente fase.

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1 Análisis de los resultados

Luego de la implementación del software FIR y luego de las respectivas pruebas realizadas por los miembros del departamento, con el fin de validar que se estén cumpliendo las necesidades del departamento, se puedo evidenciar que la implementación de software ayuda notablemente a la labor diaria del departamento.

Se cumplieron satisfactoriamente las pruebas realizadas, además se conversa con los ingenieros y gerentes del centro de operaciones para recibir sugerencias o posibilidades de mejoras, se monitorea el funcionamiento y los logs de la aplicación.

Los ingenieros de automatización serán los encargados de realizar revisiones periódicas a la aplicación. Además, serán los responsables de dar el

mantenimiento respectivo al software, para incluir características y funcionalidades nuevas que sean requeridas por el departamento, con la finalidad de incluir o automatizar procesos.

6.2 Comparativa del tiempo de respuesta de incidentes de manera manual vs software FIR

Luego del periodo de pruebas y capacitación, la interacción de los usuarios con el software mejoró. Las ventajas de la plataforma ayudaron a que los ingenieros de monitoreo, atiendan más casos por día, ya que los incidentes llegan y se registran automáticamente en la plataforma.

Como producto de este piloto se pudo realizar las comparativas con el proceso tradicional, en donde de 35 incidentes reportados, solo se lograban registrar 15, y en vista del tiempo que esto llevaba los ingenieros resolvían aproximadamente 12 casos por día.

Con la ayuda del software, se evaluó la información de un mes y de 35 incidentes promedio reportados, quedaron registrados automáticamente los 35, y se lograron atender 18 casos por día.

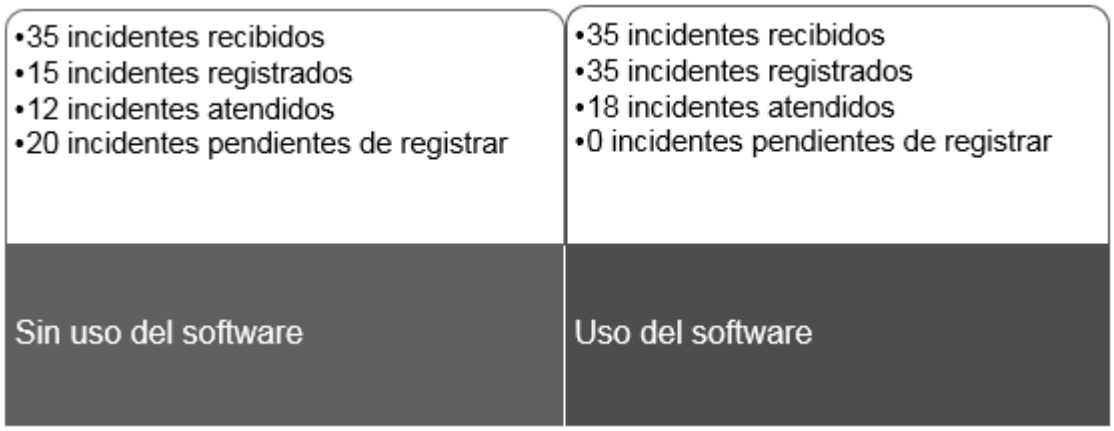


Figura 6.1 Comparativa uso del software vs. Proceso manual

Se validó, también que, el tiempo que les tomaba a los ingenieros en ingresar los incidentes manualmente a la hoja de Excel que manejaban normalmente, era considerable, pues les quitaba tiempo para resolver y atender incidentes.

Se le facilitó un manual de usuario sencillo a un cliente, con las opciones específicas asociadas a los reportes y las estadísticas y se le dio acceso a la plataforma para que revise los incidentes creados y navegue en el sistema. De esta forma se comprobó la facilidad para interactuar con la plataforma y se recibieron buenos comentarios por parte del cliente sobre la utilidad de los reportes y gráficos que provee el software.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Luego de haber evidenciado los problemas del centro de operaciones de ciberseguridad, se confirma la necesidad de un software de gestión que permita atender de manera eficiente los incidentes que se presentan a los clientes.

2. Se analizan los requerimientos y se busca una plataforma de software libre que solvente en gran medida las necesidades del centro, para esto se entrevista a los involucrados, incluso se plantea una encuesta que evidencia el malestar de los clientes, por problemas de gestión.

3. Con la implementación del software FIR para la gestión de incidentes, se logra automatizar el registro de incidentes, el proceso investigativo y la presentación de resultados a los clientes, de este modo mejoran los tiempos de respuesta y se ofrece mayor interacción al cliente.
4. Como parte de las mejoras, se identifican puntos de acción para crear nuevas funcionalidades que permitan automatizar aún más la resolución de los casos, y también que disminuyan el tiempo de la gestión del incidente.

RECOMENDACIONES

1. Se recomienda armar un plan de capacitación y acompañamiento para los clientes que no participaron del piloto, y habilitar los accesos a la plataforma, de modo que todos los clientes puedan ingresar al sistema y se familiaricen con él.

2. Es primordial dar el seguimiento respectivo a la plataforma y que se escuche las nuevas necesidades de los ingenieros, de modo que el

software mejore continuamente. Para esto se sugiere que se trabaje en un plan que permita atender estos requerimientos en una segunda fase.

3. En vista de que los incidentes son registrados automáticamente en el software FIR, se debe realizar un análisis de todas las fuentes de información que actualmente no están soportadas por el servidor centralizador, para disminuir el ingreso manual de incidentes.

BIBILIOGRAFÍA

[1] Hernández Sampieri Roberto, Definición del alcance la investigación, https://idolotec.files.wordpress.com/2012/04/sampieri-cap-4.pdf, 2012

[2] Agencia de Regulación y Control de las Telecomunicaciones, Boletín #6 Estadístico del sector de las Telecomunicaciones, http://www.arcotel.gob.ec/wp-content/uploads/2015/11/Boletin6.pdf, 2015

[3] Diario El Telégrafo, El Internet en el mundo está conectado a través de 365 cables submarinos, https://www.eltelegrafo.com.ec/noticias/94/30/el-internet-en-el-mundo-esta-conectado-a-traves-de-365-cables-submarinos, 2017

[4] URVIO Revista Latinoamericana de Estudios de Seguridad, Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa, http://revistas.flacsoandes.edu.ec/urvio/article/view/2571/1605, 2017

[5] ECUCERT, Sección Acerca de Nosotros, https://www.ecucert.gob.ec/nosotros.html, 2017

[6] Diario el Comercio, ¿Cómo está Ecuador en materia de Ciberseguridad?, http://www.elcomercio.com/guaifai/ecuador-seguridad-internet-hackeo-ciberataque.html, 2017

[7] Congreso Nacional del Ecuador, Ley de comercio electrónico, firmas electrónicas y mensajes de datos, Quito: Editorial Jurídica del Ecuador, 2002.

[8] Revista Líderes, Definición del alcance la investigación, https://idolotec.files.wordpress.com/2012/04/sampieri-cap-4.pdf, 2012

[9] Ministerio de Justicia, Derechos Humanos y Cultos, Subsecretaría de Desarrollo Normativo, Código Orgánico Integral Penal, Quito: Gráficas Ayerve C. A., 2014.

[10] International Telecommunication Union, Global Cybersecurity Index 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf, 2017

[11] ESET, ¿Cómo determinar el nivel de ciberseguridad de un país?, https://www.welivesecurity.com/la-es/2016/09/02/determinar-nivel-de-ciberseguridad-pais/, 2016

[12] CISCO, Security Operations Center, CISCO Press, 2016

[13] Carson Zimmerman, Ten Strategies of a World-Class Cybersecurity Operations, MITRE Corporate Communication and Public Affairs, 2016

[14] CSIRT, Implementing an incident response team, http://www.csirt.org/incident_response/csirt.pdf, 2016

[15] Secur-IT CRS, CERT/CSIRT, https://securitcrs.wordpress.com/knowledge-base/certcsirt/, 2017

ANEXOS

Anexo “A”. Formulario de entrevistas para clientes

Formulario de Entrevista		
Entrevista No.	**Lugar de la entrevista**	**Fecha de la entrevista**
Datos de la persona entrevistada		
Nombres:		
Cargo:		
1) ¿Qué piensa Ud sobre la actual realidad sobre los incidentes de ciberseguridad de sus clientes?		
2) ¿Cuál considera Ud. es una de las debilidades que su departamento tiene en el proceso de gestión de respuesta ante incidentes de ciberseguridad?		
3) ¿Qué proceso considera Ud. que es el más afectados ante la falta de un sistema de gestión de respuesta ante incidentes de ciberseguridad?		
4) ¿Cómo es el proceso de registro de incidentes y de la categorización de los mismos?		
5) ¿Actualmente cómo se realiza la correlación con incidentes previamente atendidos?		

6) ¿Cómo se procesa actualmente las evidencias encontradas en la fase de investigación?
7) ¿Actualmente cuál es el tiempo estimado promedio para preparar y presentar un reporte al cliente o a los directivos de la empresa? Y con qué frecuencia se lo hace?
8) ¿Cuál cree que es el tiempo estimado promedio de resolución de un incidente?
9) ¿Cree usted que la implementación de un sistema de gestión mejoraría el tiempo de respuesta ante los incidentes?
10) ¿De qué forma cree Ud. que la implementación de un sistema de gestión ayudaría a los ingenieros y especialistas de seguridad?
Observaciones

Anexo “B”. Formulario de encuestas

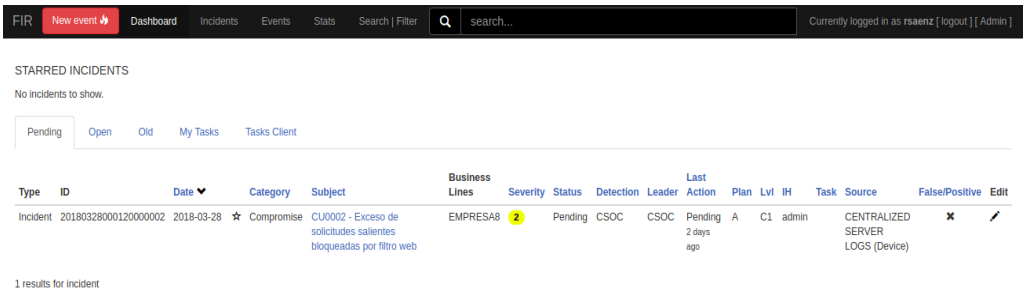
Formulario de Encuesta					
Encuesta No.	**Lugar de la encuesta**		**Fecha de la encuesta**		
Datos de la persona encuestada					
Nombres:					
Institución / Empresa					
Cargo:					
1) ¿Cuál es su nivel de conocimiento sobre la actualidad de los incidentes informáticos que afectan a su empresa?					
Nada	**Poco**	**Suficiente**	**Mucho**	**Muchisímo**	
2) ¿Cuál de los siguientes incidentes de seguridad son los que comúnmente afectan a su empresa?					
Infección de Malware	**SPAM**	**Phishing**	**Ataques de denegación de servicio (DoS)**	**Vulnerabilidades**	**Equipos comprometidos**	**Otros**
3) ¿Cuál es su nivel de satisfacción en cuanto al servicio de monitoreo 24/7 de CSOC que ustedes han contratado?					
Nada	**Poco**	**Suficiente**	**Mucho**	**Muchisímo**	
4) ¿Cuál es su nivel de satisfacción en cuanto a la interacción actual con el CSOC?					
Nada	**Poco**	**Suficiente**	**Mucho**	**Muchisímo**	
5) ¿Cuál es su nivel de satisfacción en cuanto a la frecuencia y el contenido de los reportes recibidos por el CSOC?					
Nada	**Poco**	**Suficiente**	**Mucho**	**Muchisímo**	
6) ¿Cree usted que el CSOC atiende los incidentes de ciberseguridad más críticos con prioridad?					
SI	**NO**				

7) ¿Cree usted que el tiempo de respuesta ante los incidentes por parte del CSOC es el adecuado?				
SI	**NO**			
8) ¿Cuánto le gustaría a Ud. que el CSOC implementase un software que le permita a Ud. revisar el avance de los incidentes reportados?				
Nada	**Poco**	**Suficiente**	**Mucho**	**Muchisímo**
Observaciones				

Anexo “C”. Manual de usuario del software FIR

Antes de entrar al sistema, es requerido un inicio de sesión, para lo cual deberán digitar el usuario y la clave para autenticación:

Luego de eso, cargará la página con los permisos habilitados para el usuario logueado.



Menú

El menú nos muestra las siguientes opciones:

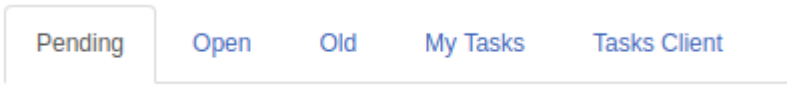
Crear Incidentes: Esta opción puede efectuarse al dar click en el botón New Event.

Ver Incidentes: Esta opción puede realizarse a través de los botones Dashboard, Incidents, Events, Search|Filter y Search.

Ver Estadísticas: Esta opción se puede acceder desde Stats.

Dashboard

Al iniciar el sitio web, nos carga por defecto la opción Dashboard, el cual nos muestra los incidentes, seccionados por pestañas.



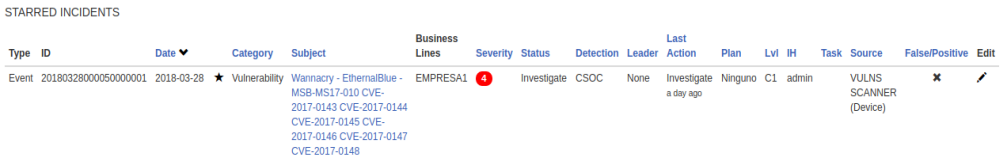
Estas pestañas son las siguientes:

- En la pestaña “Pending” se mostrarán los eventos e incidentes que tienen estado Pendiente.
- En la pestaña “Open” se mostrarán los eventos e incidentes que tienen estado Abierto, Investigación y Verificación.
- En la pestaña “Old” se muestran los incidentes antiguos.
- En la pestaña “My Task” se mostrarán sólo las tareas que fueron asignadas a CSOC.
- En la pestaña “Task Client” se mostrarán sólo las tareas que fueron asignadas a los clientes, esta opción no será visible para los clientes.

En el Dashboard existe una sección que se llama “Starred Incidents”, en el cual se mostrarán los incidentes con mayor relevancia, o que necesitan su pronta resolución, y para que el incidente aparezca en esta sección hay que darle click en la estrella.

Incidente marcado como favorito: ★

Incidente normal: ☆


STARRED INCIDENTS

Type	ID	Date		Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Task	Source	False/Positive	Edit
Event	20180328000050000001	2018-03-28	★	Vulnerability	Wannacry - EthernalBlue - MSB-MS17-010 CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	EMPRESA1	4	Investigate	CSOC	None	Investigate a day ago	Ninguno	C1	admin		VULNS SCANNER (Device)	✖	

Los incidentes y eventos que son creados pueden verse en esta tabla y se pueden ordenar a gusto del usuario a través del título de cada columna.

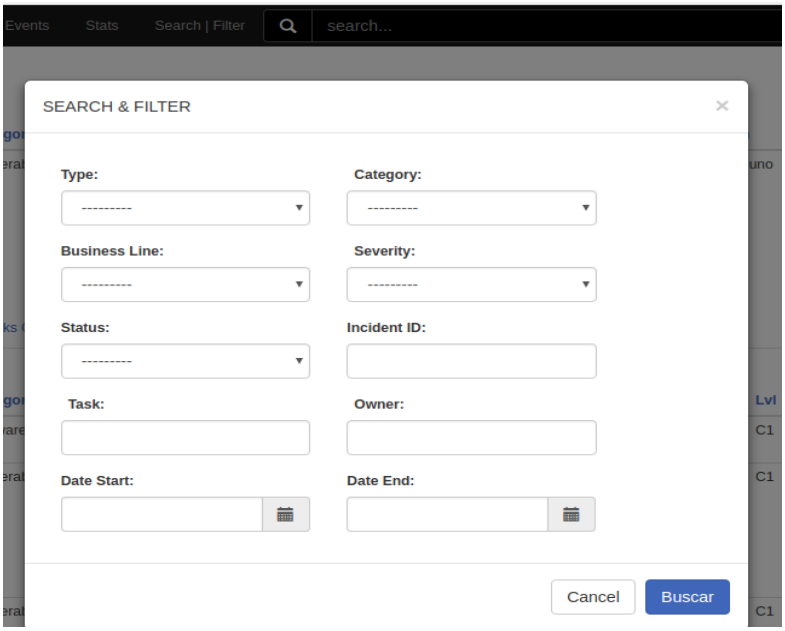
Algo que se destaca de este reporte es el color que se le da a la severidad del incidente, para lo cual utilizan el color rojo para la severidad crítica (4), color naranja para la severidad alta (3), color amarillo para la severidad media (2) y verde para la severidad baja (1).

Type	ID	Date		Category	Subject	Business Lines	Severity	Status	Detection	Leader	Last Action	Plan	Lvl	IH	Task	Source	False/Positive	Edit
Event	20180328000050000002	2018-03-28	☆	Malware	Ip reportada con Malware	EMPRESA1	2	Investigate	IT - EMP1	None	Investigate a day ago	Ninguno	C1	jchonillo		KASPERSKY (Device)	✖	
Event	20180328000120000001	2018-03-28	☆	Vulnerability	Wannacry - EthernalBlue - MSB-MS17-010 CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	EMPRESA8	4	Open	CSOC	None	Opened 2 days ago	Ninguno	C1	admin		VULNS SCANNER (Device)	✖	
Event	20180328000050000001	2018-03-28	★	Vulnerability	Wannacry - EthernalBlue - MSB-MS17-010 CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	EMPRESA1	4	Investigate	CSOC	None	Investigate a day ago	Ninguno	C1	admin		VULNS SCANNER (Device)	✖	

Para ingresar al incidente se puede dar click en el valor de color azul de la columna Subject, o se puede editar el incidente en el botón de editar .

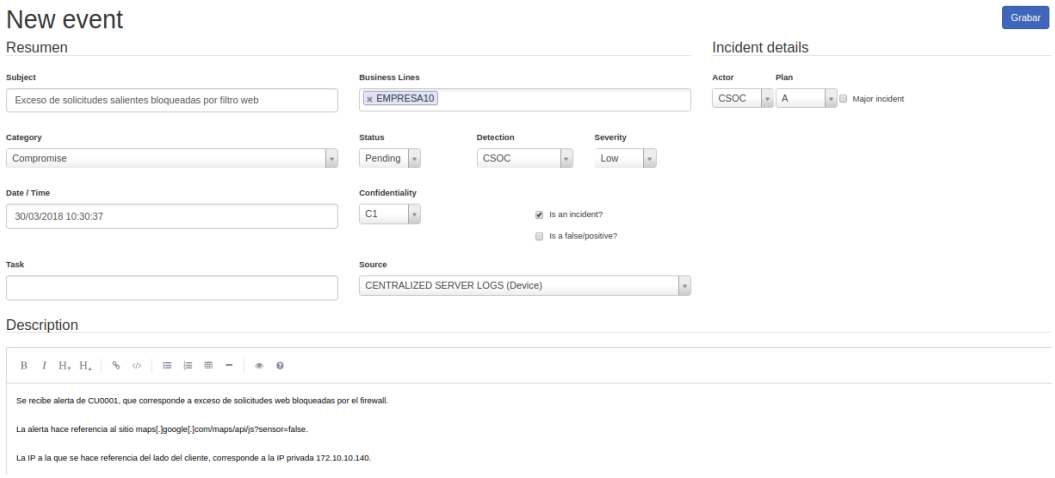
Búsqueda y Filtros de Incidente

Esta opción de filtros se añadió para que la búsqueda sea más específica, en la cual podemos escoger el tipo del registro (Evento o incidente), o por la categoría del incidente, o podemos filtrar por el cliente específico en (Business Line), también por la severidad del incidente(bajo, medio, alto, crítico), por el estado del incidente (pendiente, abierto, investigación, verificación, cerrado), además se permite ingresar el id del incidente, número de tarea, y por un rango determinado de fechas.



Creación de Incidente

Para la creación de un incidente o para editarlo, nos aparecerá el siguiente formulario:



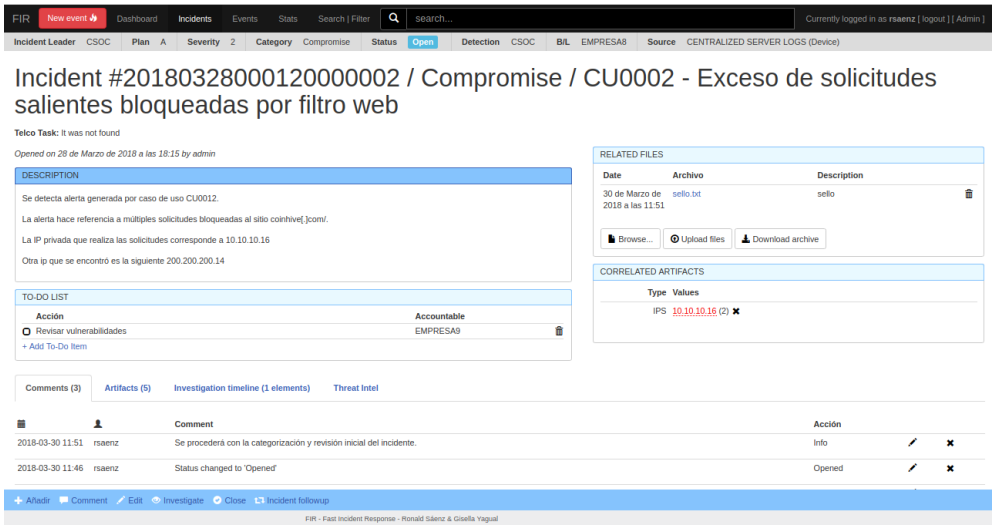
En este formulario nos muestra los siguientes campos que deben ser ingresados:

- **Subject:** Representa al título del incidente o evento que estamos registrando.
- **Category:** Se debe escoger un tipo para identificar el incidente.
- **Date /Time:** Por defecto se carga la hora actual, pero puede ser modificado por el usuario.
- **Task:** Se añadió esta opción para que exista trazabilidad con el sistema de gestión de tareas de la empresa.
- **Business Line:** Aquí se pueden escoger los clientes que fueron afectados en el incidente.
- **Status:** Por defecto se carga el estado Pending.
- **Detection:** Se debe escoger quien fue la entidad que detectó el incidente, por lo general se escoge CSOC.
- **Severity:** Inicialmente se debe escoger un nivel de severidad de acuerdo a la criticidad del incidente.
- **Confidentiality:** Se debe escoger el nivel de confidencialidad que afecta el incidente.
- **Source:** En este campo se debe escoger la fuente de información donde fue detectado el incidente, como por ejemplo el servidor centralizado de

logs, puede ser externo, osea que fue ingresado a mano, o se puede escoger alguna herramienta de seguridad que se haya afectado.

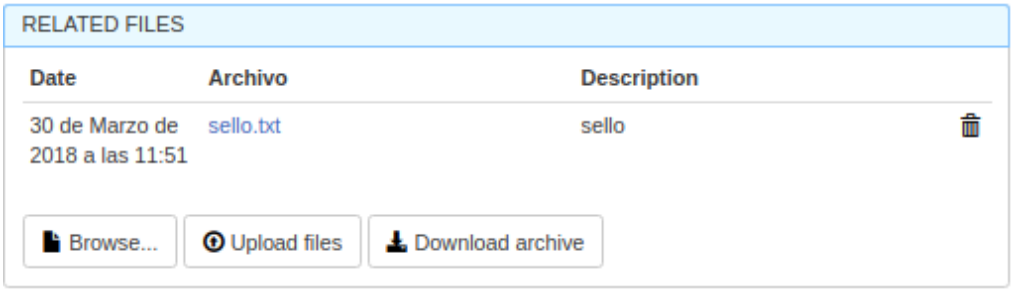
- **Is an incident?:** Este campo debe ser marcado si es que el registro quiere ser identificado como incidente, caso contrario será identificado como evento. Al marcar como incidente se habilitará varios campos adicionales:
  - **Actor:** Este campo permitirá escoger los actores que resolverán el incidente, en este caso, sólo está registrado CSOC.
  - **Plan:** Este campo permitirá escoger los distintos planes que serán una guía para la resolución del incidente. En este caso no hemos definido los planes, por tal motivo sólo existe un registro con valor A.
  - **Major Incident:** Es un campo para identificar si fue un incidente de suma relevancia.
- **Is a False/Positive?:** Este campo servirá para distinguir si uno de los eventos o incidentes creados no representan ningún patrón anómalo, por lo cual es considerado como falso positivo.
- **Description:** En este campo se puede ingresar el contenido del incidente, en el cual se debe ingresar información relevante que pueden ser tomados como artefactos (evidencias), como por ejemplo: ip afectada, ip del atacante, host de un sitio web, cuenta de correo, subred.

Interacción del Incidente

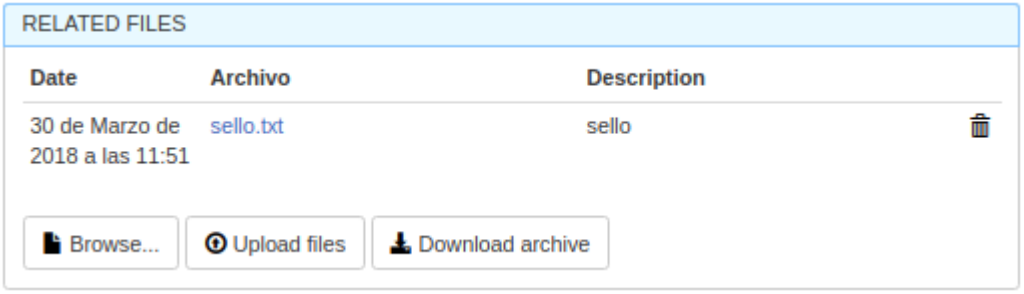


Para interactuar con el incidente se debe abrir esta pantalla, en la cual nos muestra la información del incidente en secciones:

- **Barra superior:** Nos muestra información del incidente que fue ingresada en la creación.
- **Título:** Mostrará el código generado para el incidente, el tipo del incidente, y el título del incidente.
- **Description**: En esta sección se mostrará la descripción ingresada al crear el incidente.
- **Related Files:** A la derecha se encuentra una sección que nos mostrará los archivos que se han ingresado por el sistema. Aquí se puede interactuar, abriendo el archivo, o se puede eliminar el registro.



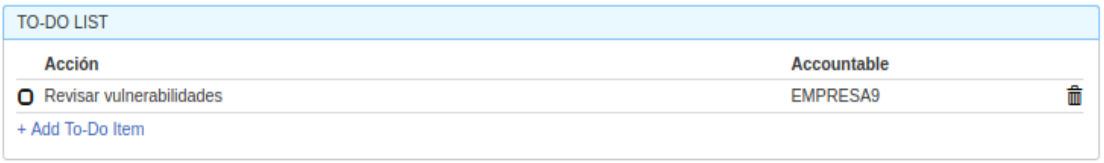
- **Correlated Artifacts:** En esta sección nos mostrará los artefactos (evidencias) que se han registrado en diferentes incidentes, gracias a esta correlación se puede acceder a incidentes que ya han sido solucionados.



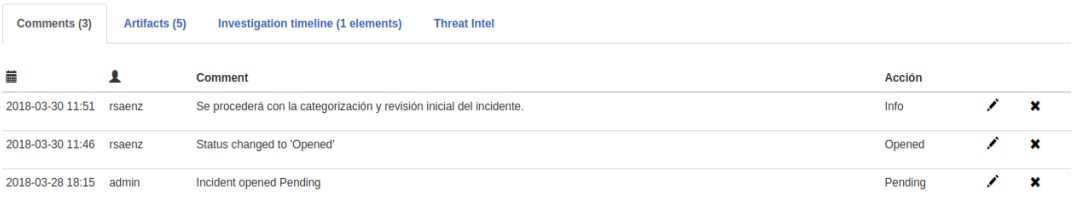
Al dar click en el registro correlacionado, nos mostrará otra pantalla en la cual aparecen todos los incidentes que tienen relacionado el mismo artefacto.

- **TO-DO List:** En esta sección nos mostrará la opción de crear tareas, en la cual se puede escoger qué entidad los debe realizar, en esta caso se muestra

CSOC, y todos clientes. Además en esta opción podemos darle check en el botón ○ y se pueden eliminar las tareas con el botón 🗑



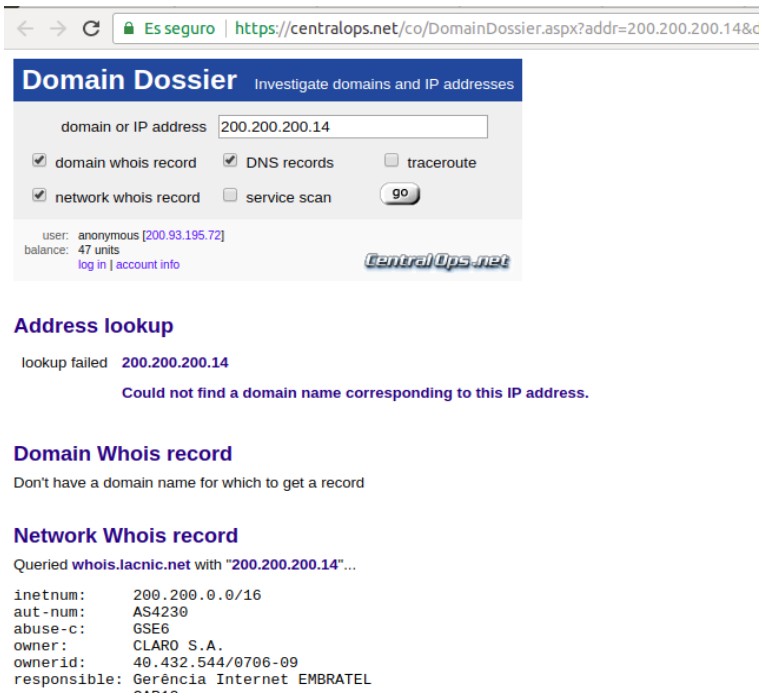
- **Comments:** En la parte inferior existe una sección en el cual muestra algunas pestañas, y una de ellas hace referencia a los comentarios, que son registrados automáticamente al cambiar el estado del incidente, y además pueden ser ingresado por el usuario. Los comentarios pueden ser editados o eliminados.



- **Artifacts:** En esta pestaña nos mostrará los artefactos (evidencias), los cuales son extraídos automáticamente por el aplicativo. Estos elementos pueden ser ip address, hostnames, urls, email address, hashes de archivos. Los artefactos que fueron correlacionados con otros incidentes se mostrará de color rojo.

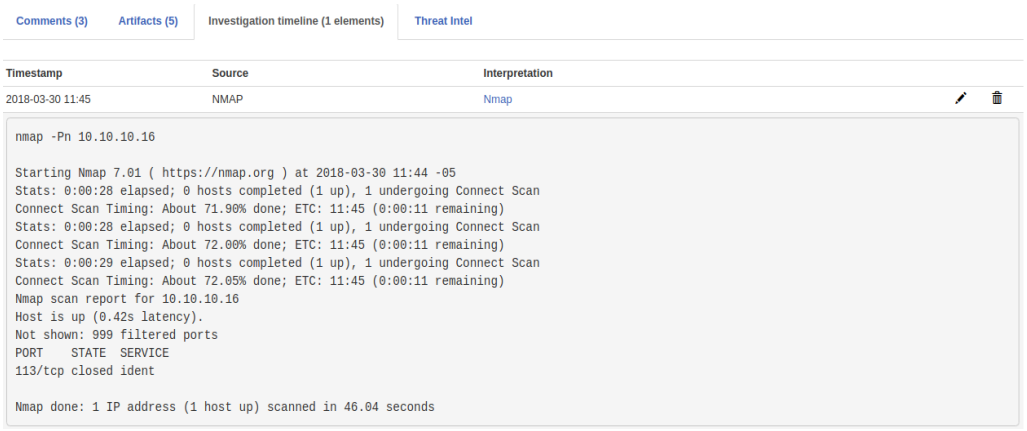
Para los registros de ips de hostnames podemos pasar el mouse por encima del valor, y nos mostrará un tooltip con una url que nos redireccionará a la página https://centralops.net la cual nos muestra información de donde proviene esa ip.

Al dar click, nos redirecciona a la página https://centralops.net

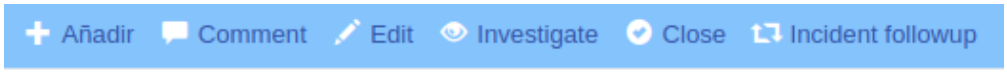


Para los registros de hashes de archivos podemos pasar el mouse por encima del valor, y nos mostrará un tooltip con una url que nos redireccionará a la página https://www.virustotal.com y nos mostrará si el hash de ese archivo es conocido por virustotal y nos podrá indicar qué herramientas de antivirus podemos utilizar para mitigar el incidente.

- **Investigation Timeline:** En esta pestaña nos mostrará los registros ingresados por la opción Nugget, el cual nos permite ingresar líneas de logs.



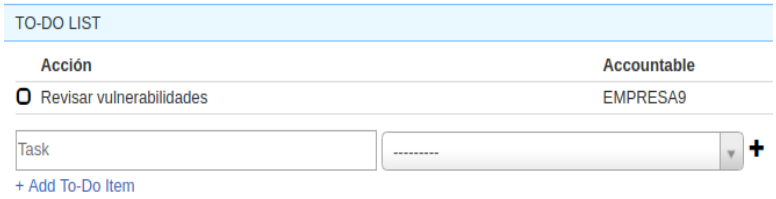
- **Barra Inferior:** En la barra inferior aparece un menú en el cual podemos interactuar con el incidente.



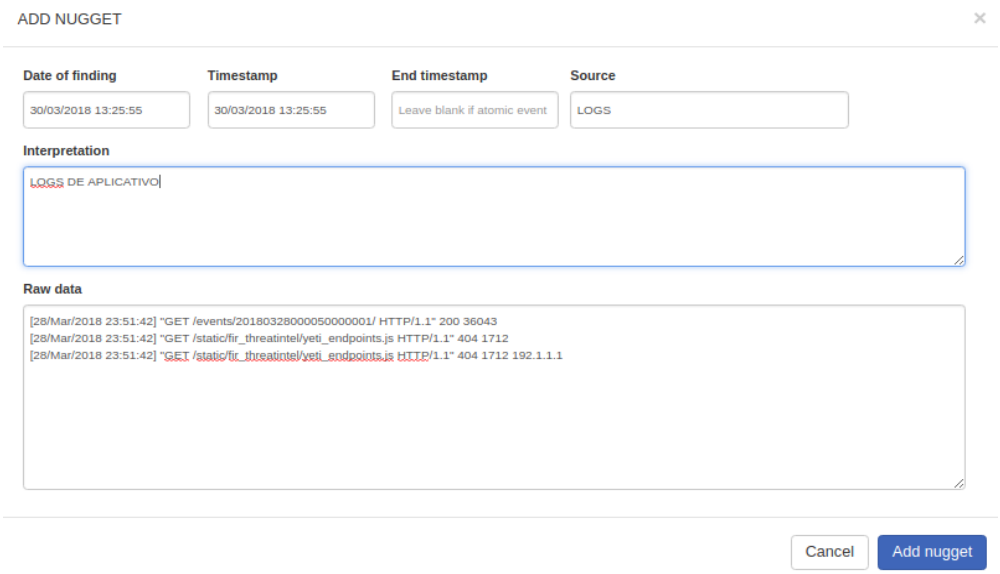
- **Añadir:** Al presionar este botón nos mostrará otro menú:

- **Archivo:** En esta opción se pueden agregar archivos, que después será extraído el hash para ser registrado como artefactos.

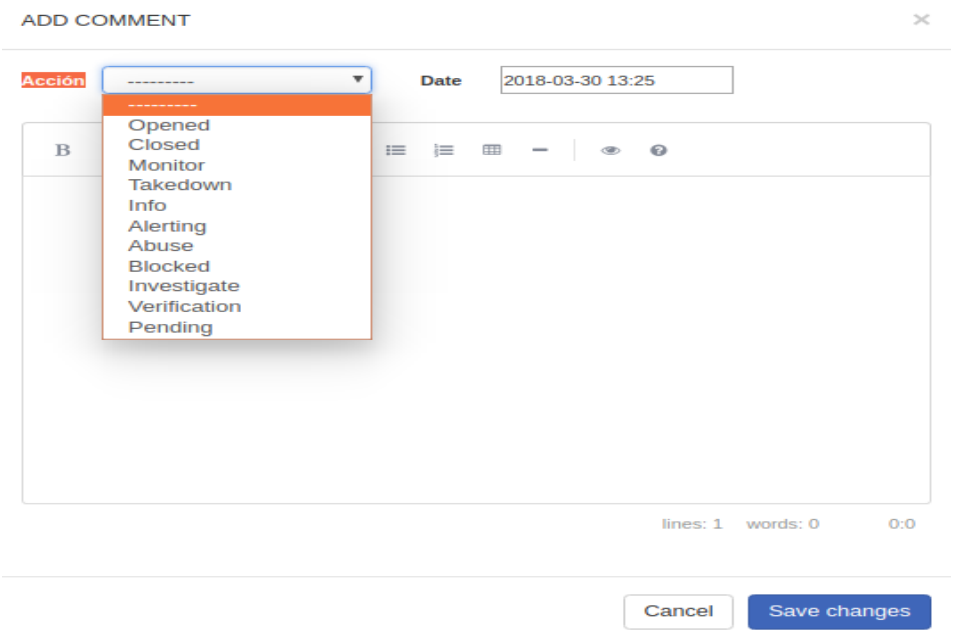
- **Todo:** En esta opción se habilitará la sección TO-DO LIST y se permitirá ingresar una nueva tarea.



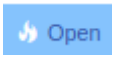
- **Nugget:** Esta opción abrirá un formulario para registrar las evidencias que pueden ser relacionadas a logs, configuraciones, etc.



- **Comment:** Esta opción abrirá una ventana en el cual podemos registrar los comentarios que serán de importancia en la investigación del incidente.

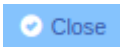


- **Edit:** En esta opción nos redirigirá para poder editar la información inicial que se registró al crear el incidente.
- **Open:** Esta opción servirá para cambiar el estado del incidente con el valor “Open” (Abierto).



- **Investigate:** Esta opción servirá para cambiar el estado del incidente con el valor “Investigate” (Investigación).

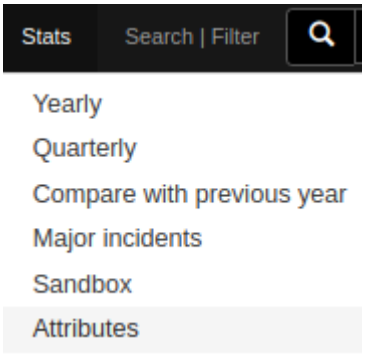
- **Verification:** Esta opción servirá para cambiar el estado del incidente con el valor “Verification” (Verificación). 

- **Close:** Esta opción servirá para cambiar el estado del incidente con el valor “Close” (Cerrado). 

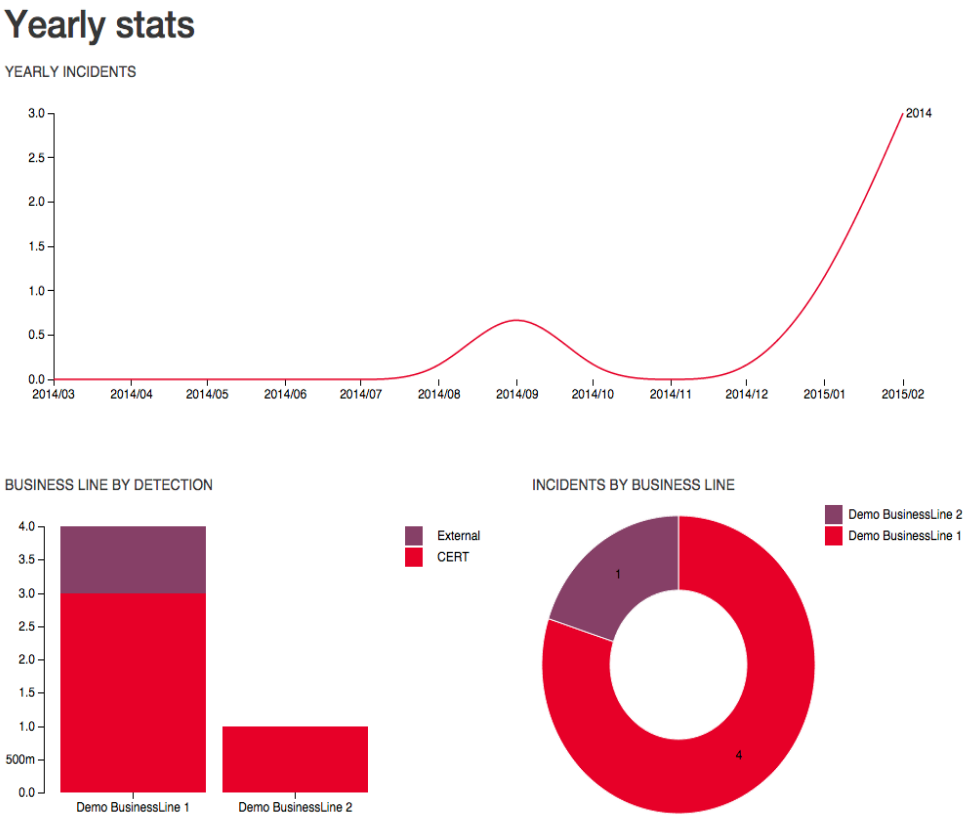
- **Incident Followup:** Esta opción nos mostrará un resumen del incidente con toda la información de la investigación realizada.

Estadísticas del Incidente

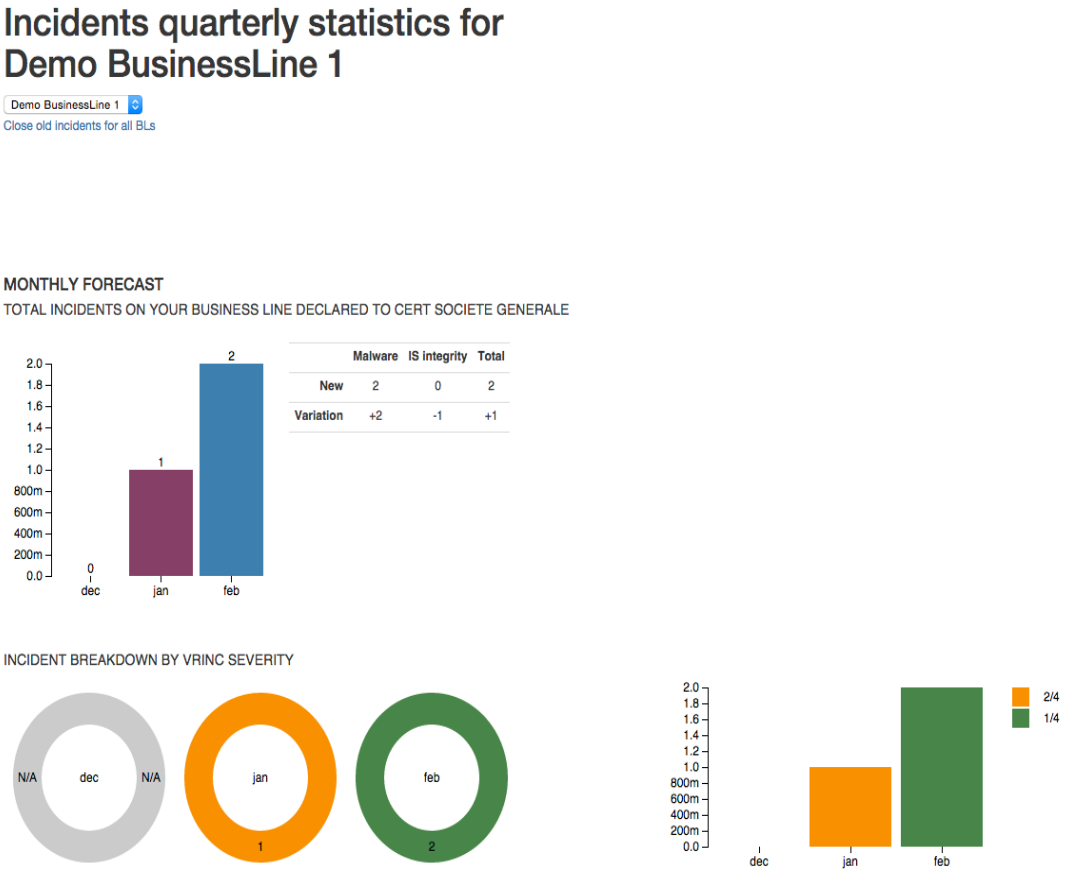
Dentro del módulo de estadísticas existen varios ítems, en las cuales se pueden observar en el siguiente gráfico:



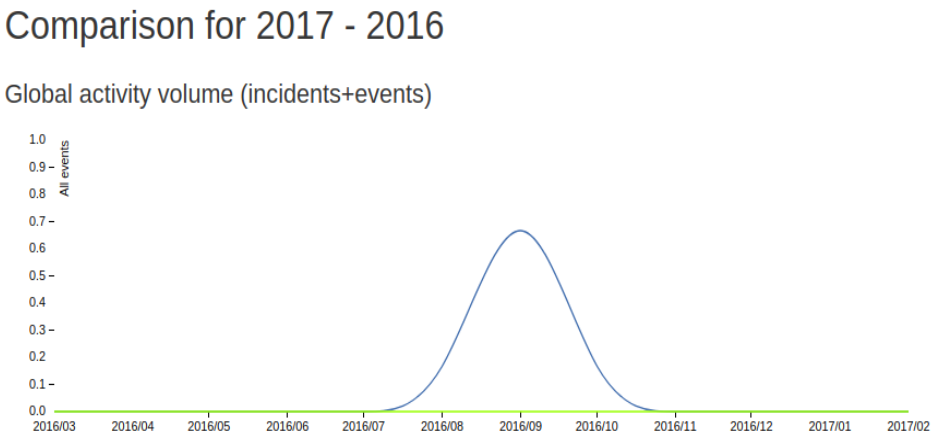
- **Yearly:** Este módulo nos muestra una estadística basado en los incidentes registrados en el último año. Los gráficos que se muestran son agrupados por clientes (Business Line), por detección, por nivel de severidad, y por categoría del incidente.



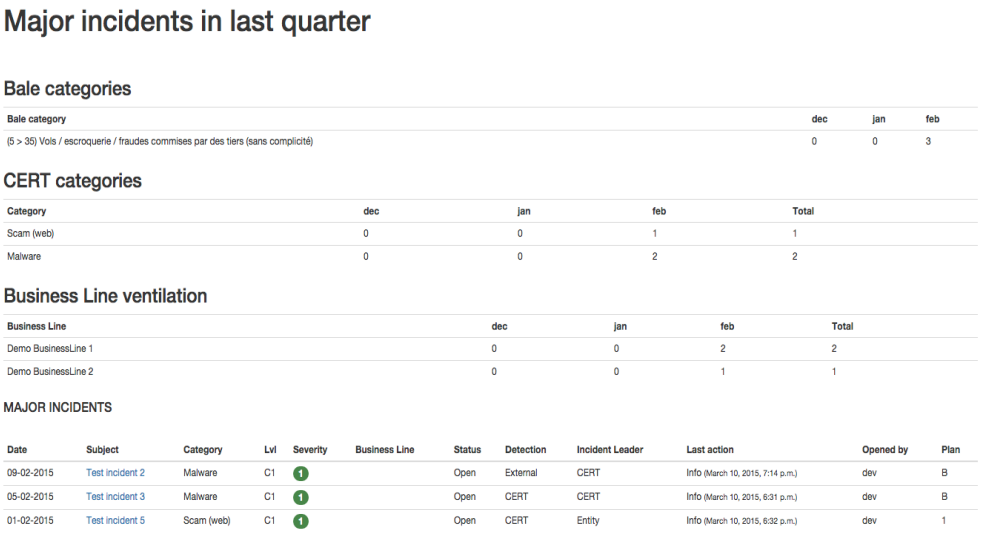
- **Quarterly:** Este módulo nos muestra una estadística basado en los incidentes registrados en el último trimestre. Los gráficos que se muestran son agrupados por clientes (Business Line), por detección, por nivel de severidad, y por categoría del incidente.



- **Compare with previous year:** Este módulo nos muestra una estadística que servirá para comparar los datos actuales con los datos de un año anterior. Se podrá observar la evolución y el crecimiento desde hace un año atrás.



- **Major Incidents:** Este módulo nos muestra los incidentes que fueron registrados con el campo “major incident” cuando se crea o edita un incidente. La información que se muestra en este reporte está basada en el último trimestre.



Major incidents in last quarter

Bale categories

Bale category	dec	jan	feb
(5 > 35) Vols / escroquerie / fraudes commises par des tiers (sans complicité)	0	0	3

CERT categories

Category	dec	jan	feb	Total
Scam (web)	0	0	1	1
Malware	0	0	2	2

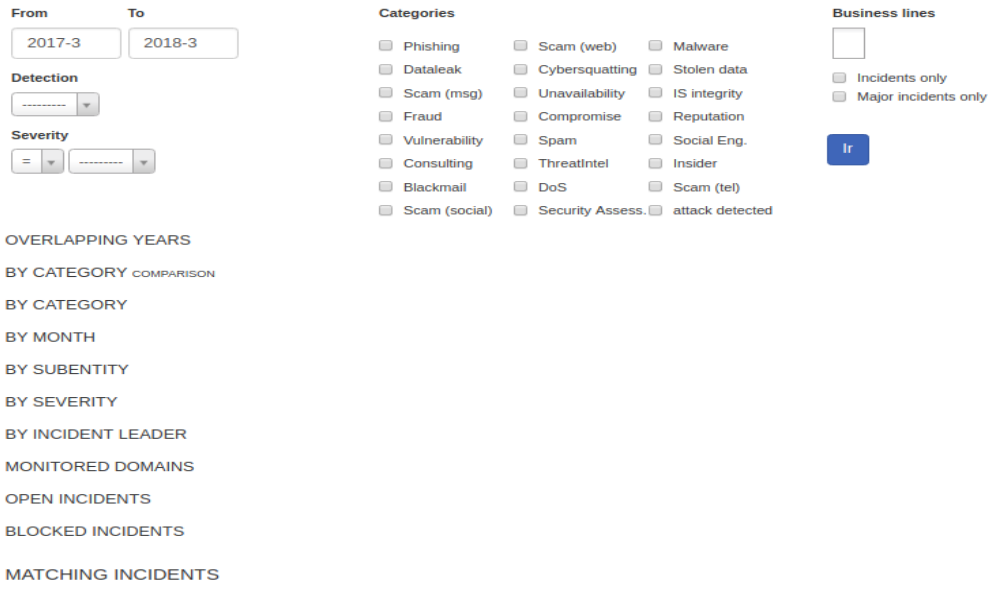
Business Line ventilation

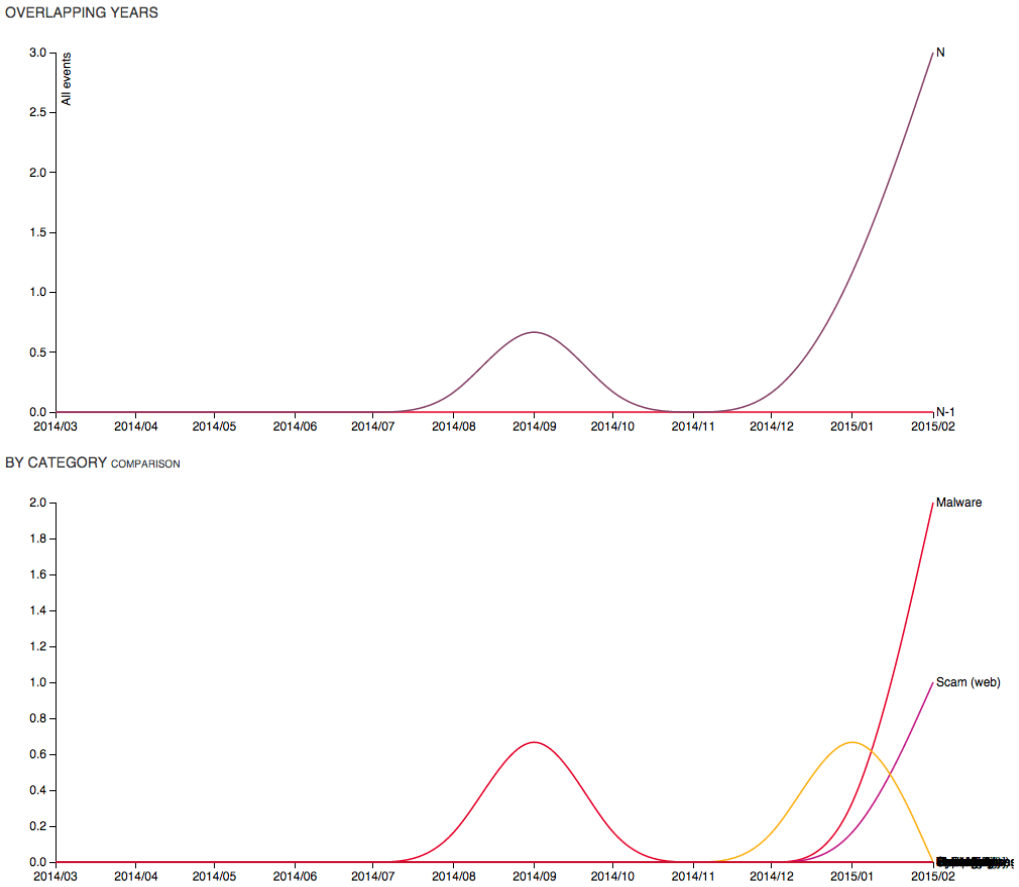
Business Line	dec	jan	feb	Total
Demo BusinessLine 1	0	0	2	2
Demo BusinessLine 2	0	0	1	1

MAJOR INCIDENTS

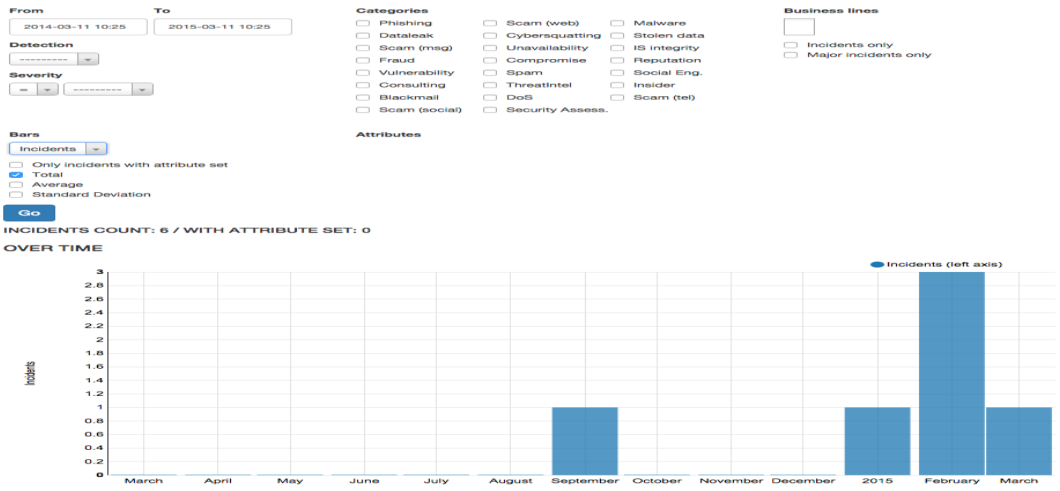
Date	Subject	Category	Lvl	Severity	Business Line	Status	Detection	Incident Leader	Last action	Opened by	Plan
09-02-2015	Test incident 2	Malware	C1	1		Open	External	CERT	Info (March 10, 2015, 7:14 p.m.)	dev	B
05-02-2015	Test incident 3	Malware	C1	1		Open	CERT	CERT	Info (March 10, 2015, 6:31 p.m.)	dev	B
01-02-2015	Test incident 5	Scam (web)	C1	1		Open	CERT	Entity	Info (March 10, 2015, 6:32 p.m.)	dev	1

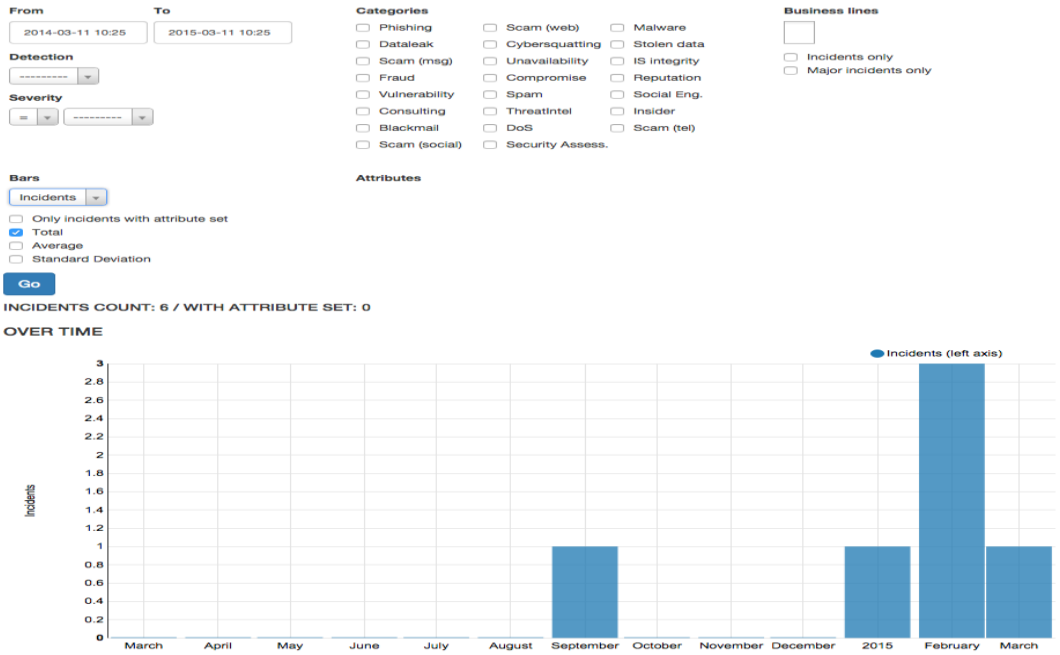
- **Sandbox:** Esta es una vista especial en el cual podemos generar estadísticas y podemos filtrar la información de acuerdo a lo que necesitamos. Los gráficos son agrupados por categoría, por mes, por severidad, incidentes abiertos.





- **Attributes:** Esta es una vista especial en el cual podemos generar estadísticas y comparar con un eventual atributo, podemos filtrar la información para tener un gráfico específico. Como por ejemplo podemos filtrar por un tipo de categoría y en el gráfico nos mostrará cuantos incidentes fueron ingresado por ese tipo agrupados por mes.


From
2014-03-11 10:25
To
2015-03-11 10:25
Detection
Severity
Categories
Phishing
Dataleak
Scam (msg)
Fraud
Vulnerability
Consulting
Blackmail
Scam (social)
Scam (web)
Cybersquatting
Unavailability
Compromise
Spam
ThreatIntel
DoS
Security Assess.
Malware
Stolen data
IS integrity
Reputation
Social Eng.
Insider
Scam (tel)
Business lines
Incidents only
Major incidents only
Bars
Incidents
Attributes
Only incidents with attribute set
Total
Average
Standard Deviation
Go
INCIDENTS COUNT: 6 / WITH ATTRIBUTE SET: 0
OVER TIME
Incidents (left axis)
Incidents
March
April
May
June
July
August
September
October
November
December
2015
February
March


From
2014-03-11 10:25
To
2015-03-11 10:25
Detection
Severity
Categories
Phishing
Dataleak
Scam (msg)
Fraud
Vulnerability
Consulting
Blackmail
Scam (social)
Scam (web)
Cybersquatting
Unavailability
Compromise
Spam
ThreatIntel
DoS
Security Assess.
Malware
Stolen data
IS integrity
Reputation
Social Eng.
Insider
Scam (tel)
Business lines
Incidents only
Major incidents only
Bars
Incidents
Attributes
Only incidents with attribute set
Total
Average
Standard Deviation
Go
INCIDENTS COUNT: 6 / WITH ATTRIBUTE SET: 0
OVER TIME
Incidents (left axis)
Incidents
March
April
May
June
July
August
September
October
November
December
2015
February
March

Anexo “C”. Manual de usuario del software FIR

Para la implementación es necesario instalar Python y las librerías que se van a utilizar para el uso del aplicativo, por tal motivo se procederá con la ejecución de los siguientes comandos:

```
$ sudo apt-get update
$ sudo apt-get install python-dev python-pip python-lxml git libxml2-dev libxslt1-dev libz-dev
$ sudo pip install virtualenv
```

Proceder a descargar el proyecto del repositorio github donde está alojado el proyecto:

```
$ git clone https://github.com/certsocietegenerale/FIR.git
```

Crear una ambiente virtual de python y activarlo para comenzar a instalar las librerías necesarias:

```
$ python3 pyvenv -v env
$ source env/bin/activate
```

$ pip install -r requirements.txt

Es necesario, además modificar los archivos de configuración para setear las conexiones a la base de datos, y habilitar el uso de librerías y de plugins para el uso del aplicativo.

fir/config/installed_apps.txt

fir/config/production.py

Luego hay que proceder con la modificación de los módulos y de la creación de las tablas en la base de datos, el framework Django nos facilita ese trabajo utilizando estos comandos:

./manage.py makemigrations

./manage.py migrate