UNIVERSIDAD NACIONAL DE INGENIERIA

Facultad de Ingeniería Industrial y de Sistemas

IMPLEMENTACIÓN DE UNA HERRAMIENTA SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT) EN UNA EMPRESA DE SEGUROS

INFORME DE SUFICIENCIA

PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS

PRESENTADO POR

JESÚS ARTURO CRUZ ORTIZ

LIMA – PERU

2014

Dedicatoria

Este trabajo va dedicado a mi madre Lida Ortiz Ramírez y a mi padre Marino Cruz Martínez, personas a quienes más admiro, por su constante apoyo en todo este proceso y su insistencia sincera y necesaria en terminar esta fase de mi vida: el de convertirme en Ingeniero de Sistemas.

Agradecimientos

Agradezco a todas las personas que hicieron posible llegar a esta meta de mi formación profesional. Desde mis padres, colegio, academia y a mi Alma Máter, la Universidad Nacional de Ingeniería.

Agradezco a todos los profesores que a lo largo de estos años me inculcaron los conocimientos que ahora me son útiles para mi base y crecimiento profesional y también personal.

Agradezco a los buenos amigos que conseguí en esta gran Universidad, gracias a ellos, todo este tiempo fue muy ameno.

A todos ellos, muchas gracias.

ÍNDICE

RESUMEN

El presente trabajo propone un marco de referencia para la implementación de una herramienta SIEM (o correlacionador de eventos como se suele llamar en el mercado peruano) en una empresa de seguros, basado en buenas prácticas y experiencias anteriores. Esta elaboración se sustenta en tres necesidades principales: identificar la causa de los incidentes de seguridad, absolver las observaciones de entes regulatorios y reducir la carga operativa en las actividades de análisis del incidente y monitoreo de eventos.

El trabajo se encuentra dividido en cuatro capítulos, en el primero se aborda la semblanza de la empresa de estudio, se describen sus procesos, misión, visión y una matriz FODA que derivará en la estrategia elegida.

El capítulo dos contiene toda la literatura utilizada para el desarrollo del proyecto, se explican temas de seguridad de la información, protocolos de redes, entre otros.

El capítulo tres detalla todo el proceso de la solución, empezando por la problemática, evaluación de alternativas y el desarrollo en sí de la solución. En el mismo se describe el marco de referencia propuesto, el cual plantea cuatro grandes fases para abordar este trabajo: el inventario y clasificación de activos, para conocer cuál será el foco de atención del SIEM; la definición de políticas de correlación, para determinar los eventos a monitorear; la implementación y pruebas, que viene a ser la configuración de la herramienta; el afinamiento de políticas, para eliminar o reducir los falsos positivos; y la declaración de eventos de seguridad, donde se valida y evidencia del evento o incidente.

En el capítulo cuatro se plasman los resultados logrados, tanto a nivel técnico como económico con un cuadro de flujo de caja.

La implementación de la herramienta permitió identificar las causas raíces de los incidentes de seguridad de la información y reducir la carga operativa

incurrida en la búsqueda de evidencias. Por tales motivos resulta beneficioso contar con una herramienta de este tipo, por ello se muestra un análisis económico de forma que sirva como base ante alguna propuesta futura que se haga en cualquier organización del sector seguros, financiero o servicios en general, puesto que todos comparten un entorno tecnológico bastante similar.

DESCRIPTORES TEMÁTICOS

- SIEM (Security Informatión and Event Management)
- Seguridad perimetral
- Gestión de incidentes de seguridad de la información
- Activos de información de tecnología
- Controles de seguridad de la información
- Monitoreo de eventos de seguridad

INTRODUCCIÓN

Desde inicios del nuevo siglo, las amenazas de seguridad de la información se han ido incrementando y cada vez con mayor celeridad, esto se debe a que existe una gran cantidad ataques que se pueden realizar sin necesidad de tener un conocimiento altamente especializado, y por otro lado, existen amenazas que se pueden materializar con mayor complejidad y resultan más difíciles de detectar y contener.

En ese sentido, mientras las amenazas de seguridad de la información de hoy en día aumentan en cantidad y gravedad, la diversidad de los entornos de red se incrementa de forma mucho más rápida. Considerando que en la actualidad, las organizaciones ya no manejan entornos netamente homogéneos, la diversidad de las herramientas tecnológicas hacen que la administración de los mismos sea más tediosa y a su vez tengan mayor complejidad, no solo por la administración en sí, sino también por las consideraciones de seguridad que se deben tener en todo el ciclo de vida de la tecnología, es decir, en el diseño, la implementación y el monitoreo cuando dicha tecnología ya está en funcionamiento. Del mismo modo, existe una relación directa entre el número de tecnologías implementadas en una organización y las amenazas de seguridad de la información que estas conllevan si es que no se tiene los estándares adecuados.

Las empresas de seguros no están ajenas a esta realidad. El riesgo latente y manifiesto que existe ha dado pie a que las regulaciones sean cada vez más exigentes, pues se trata de proteger los intereses de los clientes ante amenazas de cualquier tipo, es decir, ya no solamente se centra en el riesgo financiero, operativo, ahora también se habla de riesgos de seguridad de la información.

En el caso particular de la empresa de seguros estudiada en este trabajo, se han presentado diversos eventos e incidentes que han comprometido la disponibilidad y confidencialidad de la información, la capacidad de reacción ha sido baja pues no se tiene el personal suficiente para dar seguimiento a

todos estos casos, sobre todo por la gran cantidad de herramientas tecnológicas existentes, donde el descubrimiento de incidentes resulta verdaderamente tedioso. Es necesario, entonces, contar con un mecanismo que brinde eficiencia en el monitoreo de la seguridad de la información del entorno tecnológico de la empresa, de tal forma que permita prevenir, controlar, identificar y documentar los incidentes. Asimismo, debe facilitar el cumplimiento regulatorio relacionado a la gestión de incidentes, con la finalidad de no tener observaciones que puedan acarrear a multas por incumplimiento de las normas.

El objetivo del presente trabajo es la implementación de una tecnología SIEM (o correlacionador de eventos como también se suele conocer), en el mismo se considerará la descripción de la organización, una base teórica que permita estar familiarizado con el tema tratado, la problemática de la empresa y la implementación de la solución, tanto en el diseño de la arquitectura, el despliegue, la configuración y parametrización a modo de buenas prácticas que puedan ser usados en entornos similares.

CAPÍTULO I

PENSAMIENTO ESTRATÉGICO

1.1 DIAGNÓSTICO FUNCIONAL

En esta sección se describirán los procesos principales de las unidades de negocio de la empresa con la finalidad de determinar el alcance de mercado que tiene y obtener una idea del tipo de tecnología sobre la cual necesita soportarse.

La empresa pertenece al rubro de seguros, es de capital peruano con más de 70 años de experiencia en el mercado nacional. Es una sociedad anónima y cuenta con una serie de accionistas corporativos, asimismo cotiza en la bolsa de valores. Tiene una gama de productos orientados a todo el umbral de seguros que son los de Vida y Seguros Generales.

Asimismo, cuenta con agencias distribuidas en Lima y provincias donde los clientes pueden comprar productos, consultar sobre su seguro, realizar reclamos, entre otros servicios.

1.1.1 SERVICIOS

Principalmente se cuenta con los siguientes servicios:

- ***Rentas vitalicias:*** es una de las modalidades por las que un afiliado al Sistema Privado de Pensiones (SPP) puede optar para jubilarse, y tiene como característica principal la de ofrecer una pensión garantizada de por vida
- ***Seguros de protección familiar:*** son indemnizaciones económicas por fallecimiento y un servicio de sepelio ante la eventualidad de la pérdida de un integrante de la póliza contratada.

- ***Seguros de vida obligatorios:*** son los seguros de:
  - *Vida Ley:* Es de carácter obligatorio para los empleados y obreros que prestan servicios a un mismo empleador por un período mayor a 4 años y opcionalmente, para aquellos trabajadores que prestan servicios a un empleador a partir de los tres meses. El pago del aporte está a cargo de la entidad empleadora.
  - *Seguro Complementario de Trabajo de Riesgo (SCTR):* Otorga cobertura adicional en los casos de accidentes de trabajo y enfermedades profesionales a los afiliados regulares de EsSalud que desempeñan actividades de riesgo indicadas en D.L. 26790.
- ***Seguros de salud:*** Para cobertura de salud en clínicas.
- ***Seguros vehiculares:*** Para siniestros de daños vehiculares e incluso responsabilidades civiles.
- ***Seguros de accidentes:*** Es un seguro que protege económicamente a la familia del asegurado, cuando a raíz de un accidente, este fallece o queda en estado de invalidez permanente.
- ***Seguro domiciliario:*** Cubre los daños o robos de vivienda.
- ***SOAT:*** cubre las lesiones corporales y muerte, que tú y tus acompañantes y peatones pueden sufrir por causa de un accidente de tránsito.
- ***Seguro de viajes:*** Cubre cualquier imprevisto o emergencia durante tu viaje de placer y/o trabajo, brindándote protección durante tu viaje, las 24 horas del día y los 365 días del año.
- ***Seguros de propiedad:*** Enfocado a empresas, cubre los siniestros de los activos de las empresas.
- ***Seguros para PYMES:*** Cubre siniestros de responsabilidad civil, accidentes personales y transportes de mercadería.
- ***Seguro agropecuario:*** Brinda protección a las actividades agropecuarias, ante la ocurrencia de riesgos climáticos y otros riesgos como incendio y terremoto.
- ***Microseguros:*** Son seguros de fácil acceso con primas bajas y coberturas limitadas.
- ***Seguros de Affinity:*** Es la distribución masiva de seguros a una base de clientes de un Socio (empresa con acceso a un alto volumen de clientes o prospectos), que tengan de preferencia un control sobre el cobro, con la posibilidad de desarrollar estrategias de comercialización de productos, tales como tiendas por departamento, bancos, cajas rurales, etc.

1.1.2 CLIENTES

Se pueden dividir en clientes corporativos y clientes finales, estos últimos son las personas naturales que compran directamente los productos a la empresa. Entre los clientes corporativos tenemos:

- Iberia Líneas Aéreas de España
- Arcor de Perú S.A.
- Universidad de Piura
- Banco de Comercio
- Ferreyros S.A.A.
- Banco de la Nación
- ONP
- Sedapal
- Banco Interamericano de Finanzas (BIF)
- Mi Banco
- Banco Financiero
- Scotiabank
- Caja de Luren
- Corporación Cervesur
- Profuturo
- Graña y Montero
- Creditex
- ESSALUD
- Universidad Garcilaso de la Vega
- Maestro
- Banco de Materiales
- Banco Fallabella
- COSAPI
- Claro
- Cia Minera Castrovirreyna
- Cía de Minas Buenaventura
- Repsol
- PROFINANZAS
- Edpyme Confianza HUANCAYO
  Caja Rural de Ahorro y Crédito Señor de Luren ICA

1.1.3 PROVEEDORES

Entre los principales proveedores tenemos:

- **Brokers:** Son los intermediarios entre la empresa de seguros y los clientes finales, entre los principales tenemos Corredores de Seguro Falabella, Grupo Prado, La Protectora, entre otros.
- **Proveedores de inversiones:** Proveen servicios al área de inversiones, tenemos a Bloomberg, Datatec, Reuters, PMS, Sociedad de Agente de Bolsa, BanBif, Banco Continental, entre otros.
- **Socios de servicio:** Proveedores que apoyan en los servicios de la empresa, tales como talleres mecánicos, funeraria Jardines de la Paz, funeraria San Martin, estudio de abogados Rosello, SMP Courier, Reniec.
- **Proveedores de tecnología:** Tanto como proveedores de personal y soporte de herramientas, tenemos a los siguientes: Torioux (provee personal de soporte de infraestructura), Qnet (provee analistas helpdesk), MDP (provee analistas programadores), Claro (para los enlaces de comunicaciones), Iqsoft (soporte del software financiero), Digiware (soporte de herramientas de seguridad informática), HP (soporte de servidores), Cosapi (soporte de switches y routers Cisco), IBM (venta de equipos storage), Arquinfo (soporte de base de datos Informix, Oracle y SQL server).

1.1.4 PROCESOS

En esta sección se detallarán los procesos generales dividiéndolos en procesos core, operativos y de soporte, como se muestra en la figura 1.

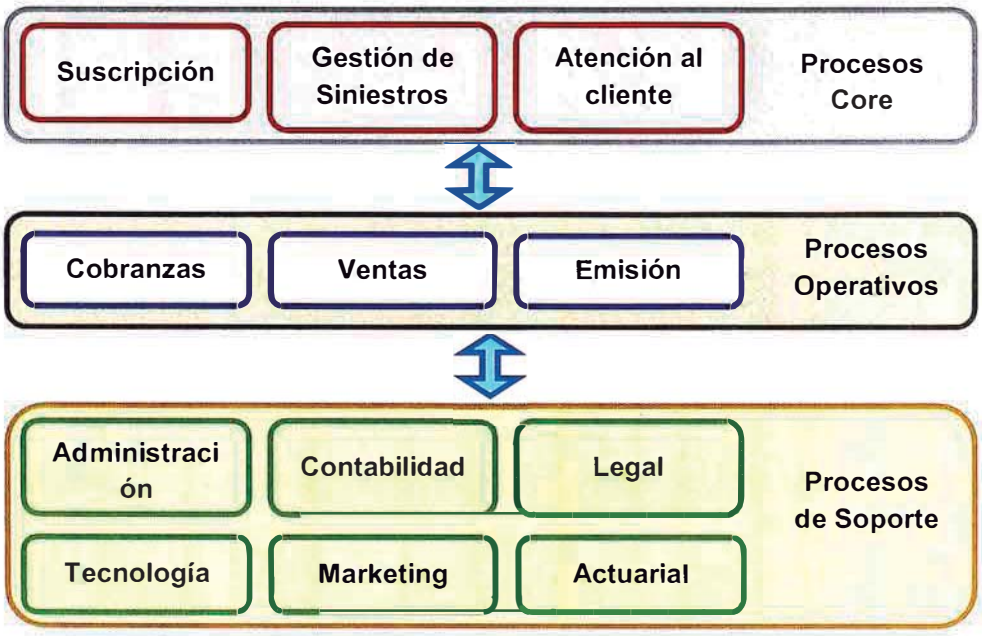

Figura 1 – Procesos de negocio
Fuente: Elaboración propia

1.1.4.1 PROCESOS CORE

Suscripción de riesgos

Inicia con la venta y suscripción de una póliza nueva. En ese caso, se recibe la cotización del cliente o del corredor, y se define el nivel de riesgo. Una vez que se realiza la evaluación, se puede confirmar la cuenta ganada o bien se rechaza la propuesta de cotización y solicita una emisión al respecto. El proceso también puede empezar por medio de un concurso público o adjudicación directa de entidades del Estado. Para esto, se compran las bases por el OSCE y se presenta la propuesta en la convocatoria.

Respecto a la distribución de sus productos, la estructura de primas se compone tal como se muestra en la figura 2:

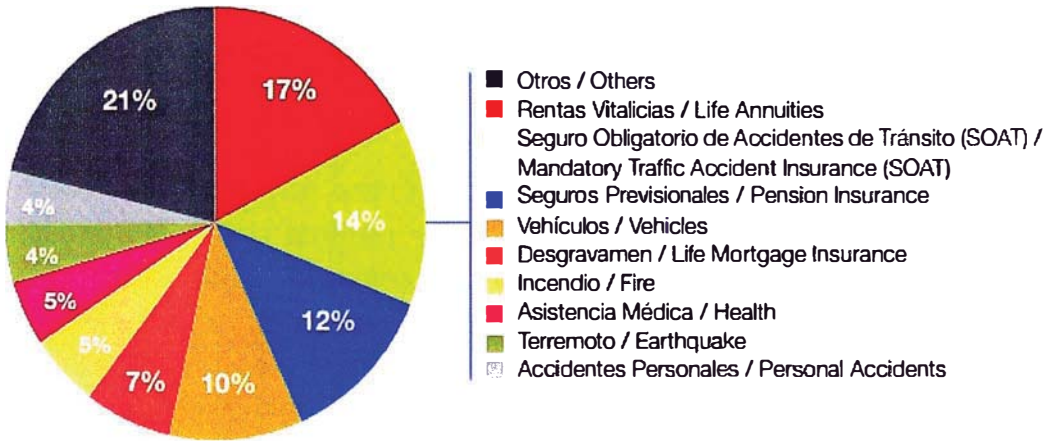

Figura 2 – Distribución de productos vendidos
Fuente: Memorias 2013 de la compañía de estudio

Gestión de siniestros

Inicia cuando el asegurado comunica la materialización del siniestro. Se asigna el caso a atender y se envía a un representante al lugar del siniestro, mientras que se procede a registrar los datos del siniestro.

Luego se procede a evaluar el caso, y se gestionan los pasos necesarios a seguir para llegar a la solución (dependerá del tipo de ramo del seguro). Los resultados de la evaluación se envían y, en caso sea válido, se procede a la aprobación del presupuesto. En caso no sea válido, se le comunica al cliente las razones del rechazo mediante una carta formal. En este caso, el cliente puede realizar un reclamo por parte por diferentes medios, el cual se registra y se procede a elaborar una carta de respuesta al cliente para informarle los motivos que justifican la resolución dada.

Atención al cliente

La atención se puede iniciar, ya sea por teléfono, página web o en agencia. En todos los casos se genera un ticket de y se procede a dar atención según el caso consultado que puede ser información sobre productos, información sobre deudas, reclamos, entre otros.

1.1.4.2 PROCESOS OPERATIVOS

Emisión

Tiene como input la suscripción de la póliza del asegurado, donde se recibe la solicitud con datos del cliente y datos del riesgo a emitir y se emite la póliza, se imprime y se envía a un compaginador. Cuando el proceso de emisión de la póliza se termina, se da el proceso de compaginación y despacho. Para esto, las pólizas debidamente autorizadas son enviadas a un despacho, y al cliente vía courier que en este caso es la empresa SMP.

Cobranzas

El proceso inicia con una solicitud de financiación. Después de un proceso de emisión, las pólizas pueden haber sido gestionadas con financiamiento a un determinado plazo, o quizás a una sola cuota. Luego el cliente solicita una financiación o reprogramar las cuotas pendientes, para lo cual el personal de Cobranzas valida si la financiación se encuentra dentro de las políticas para proceder con la misma, o solicitar las autorizaciones respectivas.

1.1.4.3 PROCESOS DE SOPORTE

Se expone el proceso de Tecnología, debido a su importancia en este informe.

Tecnología

Existen varios subprocesos en tecnología, para el caso de desarrollo existe una Subgerencia de Proyectos que se encarga de “traducir” las necesidades de negocio en proyectos de tecnología, sobre la cual se destinará un presupuesto y tiempo para la ejecución. Asimismo existe una Subgerencia de Desarrollo que se encarga de gestionar los requerimientos del área. Todo desarrollo implica el diseño y construcción del código, luego vía un formato pasa al área de calidad quien se encarga de evaluar la funcionalidad de la aplicación según los requerimientos relevados por el analista funcional.

También existe el proceso de soporte de infraestructura tecnológica donde se lleva a cabo la administración de las bases de datos, principalmente Informix (base de datos del sistema core de Vida) y SQL server (base de datos del sistema core de Seguros Generales). También se da soporte a los equipos de comunicaciones (router y switches Cisco, firewall Juniper), en el caso del enlace a internet se trabaja con Claro como principal y Telefónica como contingencia. Se cuenta con un data center in house y uno alterno en la empresa GMD que soporta los procesos críticos definidos según Continuidad de Negocio. Respecto a los servidores en su mayoría son blades y cuchillas HP. Respecto a los aplicativos administrados se cuenta con alrededor de 70 aplicativos entre Vida y Seguros Generales, los principales son Insunix (core de Vida), Visual Time (core de Seguros Generales), Jubilare (para rentas vitalicias), Iqsoft (sistema financiero), PMS (sistema de inversiones), Oficina Virtual (para los brokers), Spring (sistema de recursos humanos), entre otros.

Dentro del área de tecnología se encuentra el departamento de Seguridad de la Información, cuyo objetivo es resguardar la confidencialidad, integridad y disponibilidad de la información sensible de la compañía. Para ellos cubre los frentes descritos en la figura 3:

Figura 3 – Marco de referencia de Seguridad de la Información
Fuente: Elaboración propia

1.1.5 ORGANIZACIÓN

La empresa se estructura bajo el siguiente organigrama (orden: parte central, parte izquierda y parte derecha).

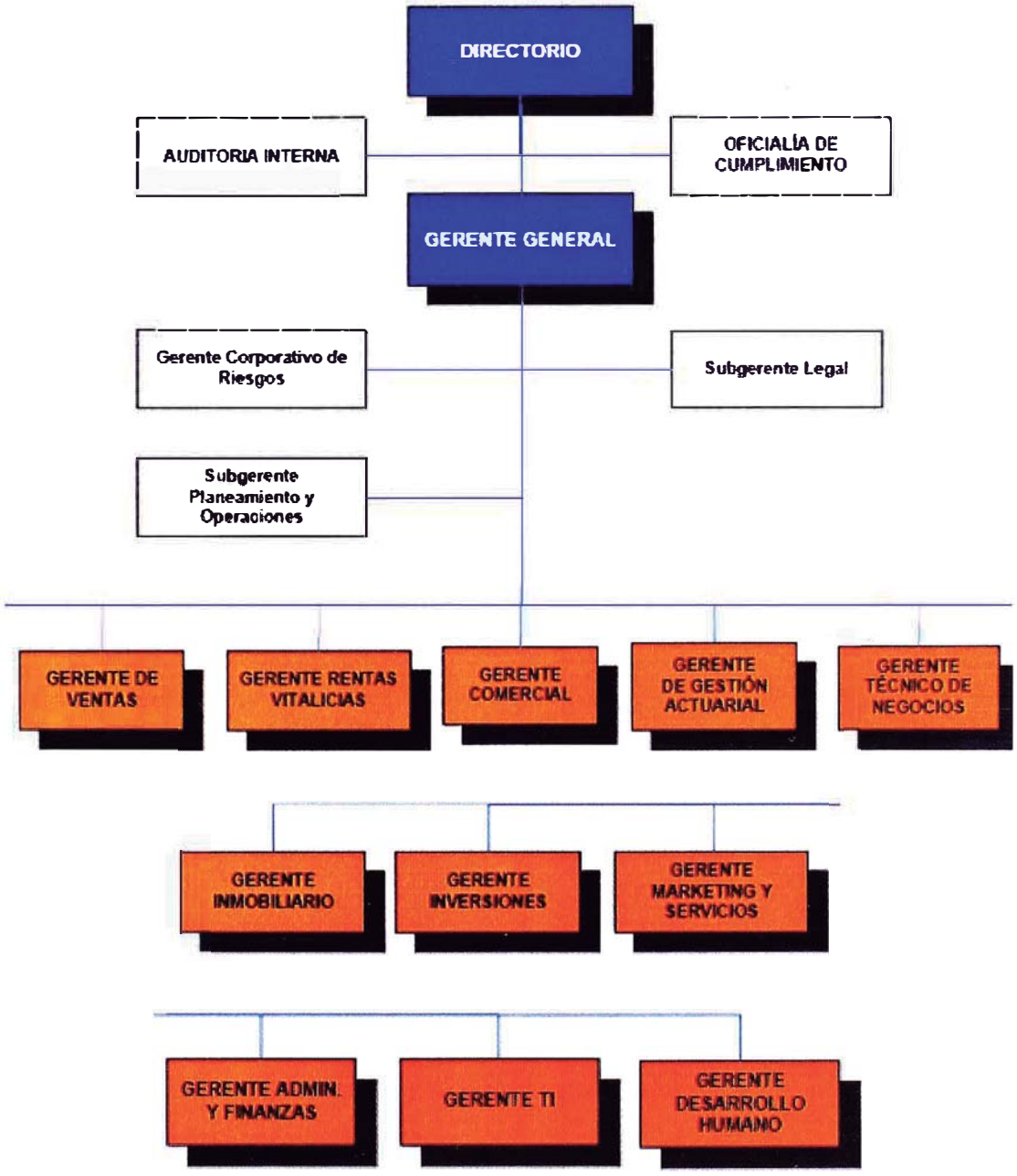

Figura 4 – Organigrama de la Empresa
Fuente: Compañía de seguros de estudio

1.2 DIAGNÓSTICO ESTRATÉGICO

1.2.1 VISIÓN Y MISIÓN

Visión

Ser la mejor opción del mercado asegurador.

Misión

Somos una empresa experta en gestión de riesgos enfocada en lograr una alta penetración de mercado a través de nuestros productos innovadores, utilizando múltiples canales de acceso, con excelencia y rapidez de respuesta en nuestro servicio.

1.2.2 OBJETIVOS ESTRATÉGICOS

- Especialización en los seguros SOAT y vehiculares.
- Fortalecer la negociación en reaseguros para que las pérdidas de seguros netas no afecten la liquidez y patrimonio.
- Aportar en el desarrollo del país promoviendo obras sociales y difusión de la cultura.
- Promover los microseguros para los mercados masivos.
- Consolidar alianzas con el Estado, Cajas Municipales, Cooperativas, entre otros, para llegar a zonas alejadas del país.

1.2.3 FORTALEZAS Y DEBILIDADES

Fortalezas

- Corporativamente se tiene un incremento anual de los activos de la compañía, actualmente asciende a 3,000,000 miles de nuevos soles.
- Similar es el caso del patrimonio que asciende a 455,000 miles de nuevos soles.
- Es una empresa con más de 70 años de experiencia en el mercado asegurador peruano.
- Cuenta con una participación de mercado del 50% en el ramo de SOAT, siendo el primero respecto a las demás aseguradoras. El segundo lugar es Rímac con 20%, lo cual representa una diferencia importante del 30%.
- Cuenta con accionistas importantes como Suramericana, Coporación Cervesur, Corporación Ferreyros, Corporación Financiera Internacional.

- Cuenta con inversiones en empresas top del mercado como Mibanco, Creditex, Banco Continental, Refinería La Pampilla, Graña y Montero, Alicorp, Minera Volcán, Minera Atacocha.
- Se encuentra en el puesto 13 de los mejores lugares para trabajar según Great Place to Work.
- Cuenta con una compañía EPS propia.
- Cuenta con certificación de calidad ISO 9001:2008.

Debilidades

En el último año ha sido desplazado del tercer a cuarto lugar en participación de mercado, superado por Mapfre, Pacifico y Rimac respectivamente.

En relación a su infraestructura tecnológica, la base de datos y el sistema core de Vida se basan en tecnología obsoletas y por ende difíciles de mantener, estos son Informix e Insunix respectivamente, este último funciona sobre línea de comandos sin interfaz gráfica, pero sin la robustez de un AS400.

- El sistema de administración financiera Iqsoft no tiene interfaces correctamente desarrolladas y ha crecido de forma desordenada, constantemente se tienen que hacer cuadres manuales y el cierre de mes contable de mes toma varios días, más de una semana.
- Se tienen problemas por indisponibilidad de servicios, algunas veces ocasionados por inconvenientes en la red interna de la compañía, originado por mala configuración de equipos, tecnologías obsoletas, entre otros.
- Debido al poco orden en la administración de la infraestructura tecnológica, existen retrasos en el soporte a usuarios y en la respuesta a incidentes.

1.2.4 OPORTUNIDADES Y AMENAZAS

Oportunidades

- Incremento de compra de viviendas, se puede explotar el ramo de seguros de vivienda, por ejemplo para siniestros de terremotos, robos, incendios, entre otros.
- Mayor poder adquisitivo de las personas y poca conciencia de compra de seguros. Dentro de Latinoamérica, Perú es uno de los países cuyos habitantes adquieren menos servicios de seguros.
- Incremento de la compra de vehículos nuevos por parte de las personas naturales. Genera un mercado para los seguros vehiculares.

Incremento de las exportaciones, en donde existe un riesgo de siniestralidad por pérdida de los productos, así como cascos, aviones y responsabilidad civil frente a terceros.
- Incremento de jubilados afiliados a alguna AFP, cuya elección de pago de la jubilación puede ser directa o por rentas vitalicias.
- Población peruana con mayor preparación, se ha incrementado los estudios de maestrías y diplomados.
- Incremento en el uso de medios tecnológicos para la compra de productos.
- Tecnologías emergentes que dan flexibilidad a la gestión de TI, como el cloud computing, software como servicio, entre otros.

Amenazas

- Incremento de inversiones en publicidad de las empresas competidoras.
- Nuevas leyes que implican gastos para la adecuación de los procesos de la empresa (Ley de Protección de Datos Personales).
- Nuevas leyes para controlar las inversiones y comisiones.
- Sofisticación de los ataques cibernéticos debido al incremento en el uso de canales electrónicos para cotizaciones, ventas, entre otros.
- Incremento del robo de vehículos y viviendas lo cual incremente el desembolso por siniestralidad.

1.2.5 MATRIZ FODA

Tabla 1 – Matriz de Fortalezas, Debilidades, Oportunidades y Amenazas
Fuente: Compañía de seguros de estudio

	Fortalezas (F)	**Debilidades (D)**
	1. Incremento de los activos de la compañía. 2. Patrimonio de aproximadamente medio millón de soles. 3. Más de 70 años de experiencia. 4. Primer lugar en el ramo de seguros de SOAT (50% de cuota de mercado). 5. Accionistas importantes 6. Inversiones en empresas rentables (mineras, financieras, etc.) 7. Buena posición en la encuesta de Great Place To Work. 8. Cuenta con EPS propia. 9. Certificación ISO 9001:2008.	1. El 2013 bajó a cuarto lugar en participación de mercado de seguros. 2. Infraestructura tecnológica obsoleta del core de Vida. 3. Sistema de gestión financiera no óptima (requiere realizar reprocesos manuales) 4. Continuos problemas de indisponibilidad de servicios por problemas en la red. 5. Retrasos en la atención de soporte a usuarios y respuesta a incidentes.
Oportunidades (O) 1. Mayor demanda en la compra de viviendas. 2. Mayor poder adquisitivo de las personas. 3. Incremento de la compra de vehículos nuevos. 4. Incremento de las exportaciones.	- Invertir en otros productos de seguros vehiculares, ya que se tiene participación en este sector (F1, F4, O3). - Obtener personal altamente calificado (F7, O6). - Invertir en tecnología para dar mayor soporte a los procesos de	- Diseñar nuevos tipos de seguros con características de rapidez y facilidad (D1, O2). - Investigar sobre nuevas tecnologías que permitan rapidez en el soporte a usuarios y respuesta a incidentes (D2, D3, D4, D5, O8).

5. Incremento de jubilados afiliados a alguna AFP. 6. Personas más preparadas académicamente. 7. Mayor uso de medios tecnológicos para la compra de productos. 8. Tecnologías emergentes.	negocio (F1, F2, O8). - Diseñar nuevos productos que combinen seguros con EPS (F8, O2). - Promover la compra se seguros de vivienda (F1, O1).	- Desarrollar el las herramientas electrónicas como canal para la venta de productos (D1, O7).
Amenazas (A) 1. Mayor publicidad de la competencia. 2. Publicación de nuevas leyes que implican rediseño de procesos. 3. Nuevas leyes para controlar las inversiones y comisiones. 4. Incremento y mayor sofisticación en ataques cibernéticos. 5. Incremento del robo de vehículos y viviendas.	- Realizar una publicidad agresiva en televisión y radio (F1, A1). - Utilizar el conocimiento en ISO 9001 para acoplar nuevos procesos según las leyes (F9, A2). - **Invertir en herramientas de seguridad informática para prevenir, detectar, contener y mitigar los ataques cibernéticos (F1, F2, A4).**	- No promover los seguros de vida hasta optimizar el sistema core (D2, A1). - No invertir de forma inmediata en el uso de canales electrónicas para la venta de productos hasta que se tenga la seguridad adecuada (D4, D5, A4).

Nota: Esta tabla es la continuación de la página anterior (tabla 1)

Estrategia elegida:

En base a la matriz FODA (tercer cuadrante de la tabla 1) se elige la estrategia detallada en el tercer cuadrante:

Invertir en herramientas de seguridad informática para prevenir, detectar, contener y mitigar los ataques cibernéticos.

CAPÍTULO II

MARCO TEÓRICO

2.1 SEGURIDAD DE LA INFORMACIÓN

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente interconectado de negocios. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades.[1]

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización.

Dentro de un marco de referencia, los controles están orientados hacia tres frentes: confidencialidad, integridad y disponibilidad.

---

[1] NTP-ISO/IEC 17799 – 2007: Norma Técnica Peruana, Código de Buenas Prácticas para la Gestión de la Seguridad de la Información

Figura 5 – Pilares de la seguridad de la información
Fuente: Wikipedia

Confidencialidad

La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

2.2 SEGURIDAD INFORMÁTICA

La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura

computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

El concepto de seguridad de la información no debe ser confundido con el de "seguridad informática", ya que este último solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Puesto simple, la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores. Nadie a cargo de seguridad debe determinar quién y cuándo se puede tomar acciones apropiadas sobre un ítem en específico. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización a organización. Independientemente, cualquier compañía con una red debe de tener una política de seguridad que se dirija a conveniencia y coordinación.

2.3 MODELO OSI

El modelo de referencia OSI describe cómo la información de un usuario o aplicación cliente en un computador se mueve, a través de una interconexión de redes, a una aplicación u otro host. El modelo OSI es un modelo conceptual compuesto por siete capas (ver figura 6), cada una funciones de red particulares.[2]

[2] ISO/IEC 7498-1. Estándar Internacional del Modelo de Referencia de Interconexión de Sistemas Abiertos (Modelo OSI por sus siglas en inglés).

Figura 6 – Modelo OSI
Fuente: Wikipedia

El modelo OSI fue desarrollado por la Organización Internacional de Normalización (ISO) en 1984, y ahora es considerado el modelo arquitectónico primario para las comunicaciones entre redes. Cada capa del modelo es razonablemente independiente, de forma que las tareas asignadas a cada capa se pueden implementar de forma autónoma.

Capa1: Capa Física

Se ocupan de las características físicas del medio físico. Conectores, pins, corrientes eléctricas, codificación y modulación de luz, son parte de diferentes especificaciones de la capa física. Por ejemplo, RJ-45 define la forma del conector y el número de cables / los pernos en el cable. Ethernet y 802.3 definen el uso de cables / pines 1, 2, 3 y 6. Para utilizar un cable de categoría 5 con un conector RJ-45 para una conexión Ethernet, Ethernet y se utilizan conectores RJ-45 especificaciones de la capa física.

Capa 2: Capa de enlace de datos

Esta capa se ocupa del direccionamiento físico, del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo. Es uno de los aspectos más importantes que revisar en el momento de conectar dos ordenadores, ya que está entre la capa 1 y 3 como parte esencial para la creación de sus protocolos básicos (MAC, IP), para regular

la forma de la conexión entre computadoras así determinando el paso de tramas, verificando su integridad, y corrigiendo errores. Dadas estas situaciones cabe recalcar que el dispositivo que usa la capa de enlace es el switch que se encarga de recibir los datos del router y enviar cada uno de estos a sus respectivos destinatarios.

Capa 3: Capa de red

Se encarga de identificar el enrutamiento existente entre una o más redes. Los paquetes se pueden clasificar en protocolos enrutables y protocolos de enrutamiento.

- Enrutables: viajan con los paquetes (IP, IPX, APPLETALK)
- Enrutamiento: permiten seleccionar las rutas (RIP, IGRP, EIGRP, OSPF, BGP)

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan routers. Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas.

En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

Capa 4: Capa de transporte

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que esté utilizando. La PDU de la capa 4 se llama Segmento o Datagrama, dependiendo de si corresponde a TCP o UDP. Sus protocolos son TCP y UDP; el primero orientado a conexión y el otro sin conexión.

Capa 5: Capa de sesión

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de

principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

Capa 6: Capa de presentación

El objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas..

Capa 7: Capa de aplicación

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (Post Office Protocol y SMTP), gestores de bases de datos y servidor de ficheros (FTP), por UDP pueden viajar (DNS y Routing Information Protocol).

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

2.4 PROTOCOLOS DE COMUNICACIÓN

2.4.1 SNMP

El Protocolo Simple de Administración de Red o SNMP (del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.[3]

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

[3] RFC 1157 - Request for Comments de la Internet Engineering Task Force (IETF) para establecer el protocolo de red SNMP v2

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad; sin embargo no ha sido mayoritariamente aceptado en la industria.

Una red administrada a través de SNMP consiste de tres componentes claves:

- Dispositivos administrados: contiene un agente SNMP y reside en una red administrada. Pueden ser los switches, hubs, routers, impresoras, etc.
- Agentes: módulo de software de red que reside en un dispositivo administrado, posee conocimiento local del dispositivo y traduce la comunicación a formato SNMP.
- Sistemas administradores de red (Network Management Systems, NMS's): ejecuta aplicaciones que supervisan y controlan a los dispositivos administrados. Los NMS's proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red. Uno o más NMS's deben existir en cualquier red administrada.

Para realizar las operaciones básicas de administración anteriormente nombradas, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar un pequeño grupo de mensajes (PDUs) entre los administradores y agentes.

Los puertos comúnmente utilizados para SNMP son el 161 y 162.

La arquitectura SNMP se muestra en la figura 7.

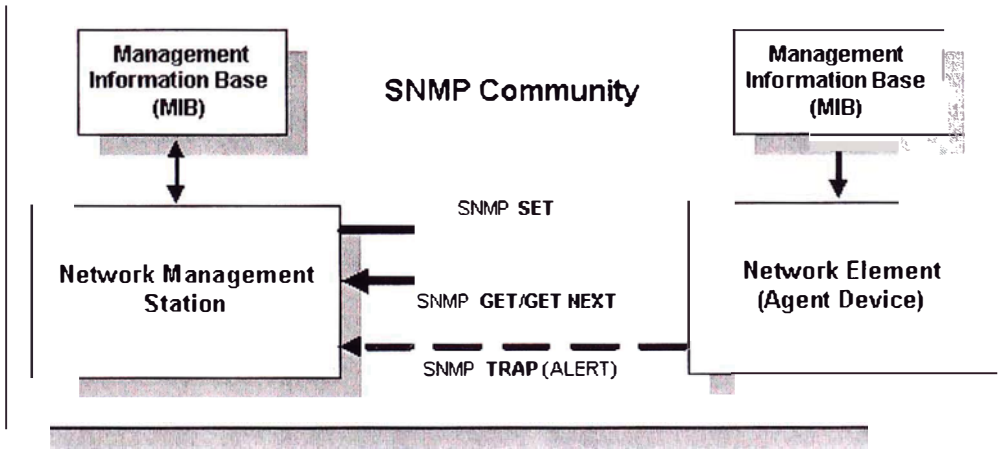

Figura 7 – Arquitectura SNMP
Fuente: Wikipedia

Los paquetes utilizados para enviar consultas y respuestas SNMP poseen el siguiente formato:

Versión	*Comunidad*	*SNMP PDU*

- Versión: Número de versión de protocolo que se está utilizando (por ejemplo 1 para SNMPv1);
- Comunidad: Nombre o palabra clave que se usa para la autenticación. Generalmente existe una comunidad de lectura llamada "public" y una comunidad de escritura llamada "private";
- SNMP PDU: Contenido de la unidad de datos del protocolo, el que depende de la operación que se ejecute.

Trap

Una trap es generada por el agente para reportar ciertas condiciones y cambios de estado a un proceso de administración. El formato de la PDU es diferente:

Tipo	*Enterprise*	*Dirección del agente*	*Tipo genérico de trap*	*Tipo específico de trap*	*Timestamp*	*Enlazado de variables*

- Enterprise: Identificación del subsistema de gestión que ha emitido el trap;
- Dirección del agente: Dirección IP del agente que ha emitido el trap;
- Tipo genérico de trap:
  - Cold start (0): agente ha sido inicializado o reinicializado;
  - Warm start (1): configuración del agente ha cambiado;
  - Link down (2): interfaz de comunicación se encuentra fuera de servicio;
  - Link up (3): interfaz de comunicación se encuentra en servicio;
  - Authentication failure (4): agente ha recibido un requerimiento de un NMS no autorizado (normalmente controlado por una comunidad);
  - EGP neighbor loss (5): sistemas en que los routers están utilizando el protocolo EGP, un equipo colindante se encuentra fuera de servicio;
  - Enterprise (6): en esta categoría se encuentran todos los nuevos traps incluidos por los vendedores.

2.4.2 SYSLOG

Syslog es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro.

El registro incluye, por ejemplo:

Un intento de acceso con contraseña equivocada
Un acceso correcto al sistema
- Anomalías: variaciones en el funcionamiento normal del sistema
- Alertas cuando ocurre alguna condición especial
- Información sobre las actividades del sistema operativo
- Errores del hardware o el software

También es posible registrar el funcionamiento normal de los programas; por ejemplo, guardar cada acceso que se hace a un servidor web, aunque esto suele estar separado del resto de alertas. Los componentes que envían logs se muestran en la figura 8.

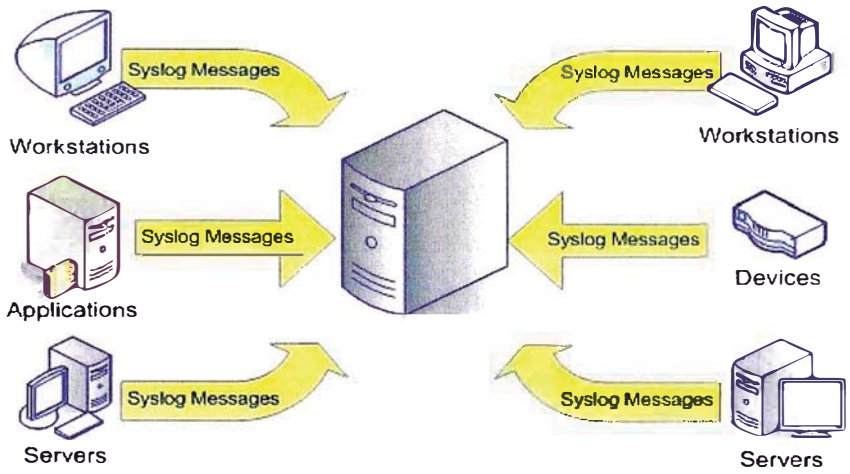

Figura 8 – Comunicación Syslog
Fuente: Wikipedia

El protocolo syslog es muy sencillo: existe un ordenador servidor ejecutando el servidor de syslog, conocido como syslogd (demonio de syslog). El cliente envía un pequeño mensaje de texto (de menos de 1024 bytes).

Los mensajes de syslog se suelen enviar vía UDP, por el puerto 514, en formato de texto plano. Algunas implementaciones del servidor, como syslog-ng, permiten usar TCP en vez de UDP, y también ofrecen Stunnel para que los datos viajen cifrados mediante SSL/TLS.

2.5 HERRAMIENTAS DE SEGURIDAD PERIMETRAL

A continuación se describen algunas herramientas de seguridad perimetral y de infraestructura en general. Se incluye en el marco teórico pues son herramientas con las que el SIEM interactúa.

2.5.1 FIREWALL

Es una herramienta de seguridad de red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los firewall se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del firewall, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Un firewall correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

Zona Desmilitarizada

En seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa; los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS.

Una DMZ se crea a menudo a través de las opciones de configuración del firewall, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama firewall en trípode (three-legged firewall). A modo de ejemplo se muestra la figura 9.

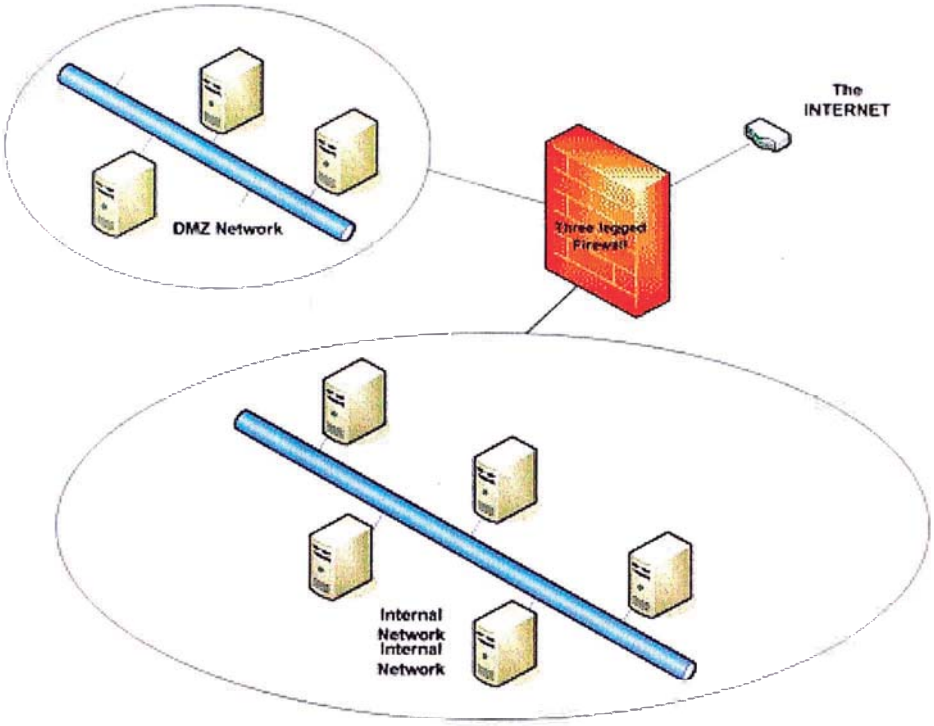

Figura 9 – Ejemplo de topología de red con firewall
Fuente: Cisco Network Consultants Handbook

2.5.2 SISTEMA DE PREVENCIÓN DE INTRUSOS

Un sistema de prevención de intrusos (o por sus siglas en inglés IPS) es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.

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

Un sistema de prevención de intrusos funciona por medio de módulos, estableciendo políticas de seguridad para proteger el equipo o la red de un ataque; se podría decir que un IPS protege al equipo proactivamente.

Los IPS se categorizan en la forma que detectan el tráfico malicioso:

Detección basada en firmas

Una firma tiene la capacidad de reconocer una determinada cadena de bytes en cierto contexto, y entonces lanza una alerta. Por ejemplo, los ataques

contra los servidores Web generalmente toman la forma de URLs. Por lo tanto se puede buscar utilizando un cierto patrón de cadenas que pueda identificar ataques al servidor web. Sin embargo, como este tipo de detección funciona parecido a un antivirus, el administrador debe verificar que las firmas estén constantemente actualizadas.

Detección basada en políticas

En este tipo de detección, el IPS requiere que se declaren muy específicamente las políticas de seguridad. Por ejemplo, determinar que hosts pueden tener comunicación con determinadas redes. El IPS reconoce el tráfico fuera del perfil permitido y lo descarta.

Detección basada en anomalías

Este tipo de detección tiende a generar muchos falsos positivos, ya que es sumamente difícil determinar y medir una condición 'normal'. El IPS analiza el tráfico de red por un determinado periodo de tiempo y crea una línea base de comparación. Cuando el tráfico varía demasiado con respecto a la línea base de comportamiento, se genera una alarma.

2.5.3 ROUTER

Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante bridges), y que por tanto tienen prefijos de red distintos.

Por ser los elementos que forman la capa de red, tienen que encargarse de cumplir las dos tareas principales asignadas a la misma:

- Reenvío de paquetes (forwarding): cuando un paquete llega al enlace de entrada de un encaminador, éste tiene que pasar el paquete al enlace de salida apropiado. Una característica importante de los encaminadores es que no difunden tráfico difusivo.
  Encaminamiento de paquetes (routing): mediante el uso de algoritmos de encaminamiento tiene que ser capaz de determinar la ruta que deben seguir los paquetes a medida que fluyen de un emisor a un receptor.

La figura 10 muestra una arquitectura estándar con firewall, IPs y router.

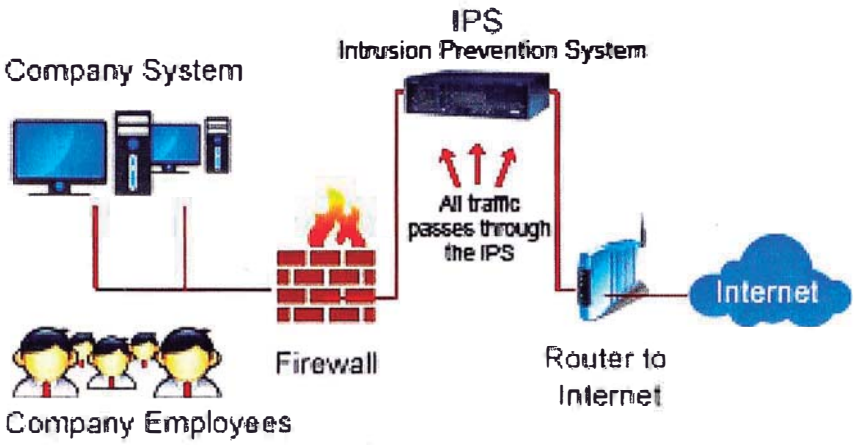

Figura 10 – Topología con router de borde e IPS
Fuente: Cisco Network Consultants Handbook

2.5.4 SWITCH

Un conmutador o switch es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

2.5.5 RED PRIVADA VIRTUAL (VPN)

Una sesión de VPN es un canal o túnel autenticado y encriptado de comunicaciones, a través de algún tipo de red pública, tal como internet. Debido a que la red se considera insegura, el cifrado y la autenticación se utilizan para proteger los datos mientras está en tránsito. Por lo general, un servicio de VPN es independiente, lo que significa que casi todas las operaciones del cliente son transparentes para el usuario y que toda la información intercambiada entre los dos anfitriones (WWW, FTP, etc.) se transmite a través del canal cifrado. Se tienen dos tipos de VPN:

- **VPN IPSec de sitio a sitio:** Esta alternativa a Frame Relay o a las redes WAN de línea alquilada permite a las empresas llevar los recursos de la red a las sucursales, las oficinas instaladas en casa y los sitios de partners comerciales.

- **VPN de acceso remoto:** Esta modalidad lleva prácticamente cualquier aplicación de datos, voz y vídeo emulando el escritorio de la oficina principal. Una VPN de acceso remoto puede instalarse utilizando VPN SSL, IPsec o ambas, dependiendo de los requisitos de implementación. Una arquitectura estándar se muestra en la figura 11.

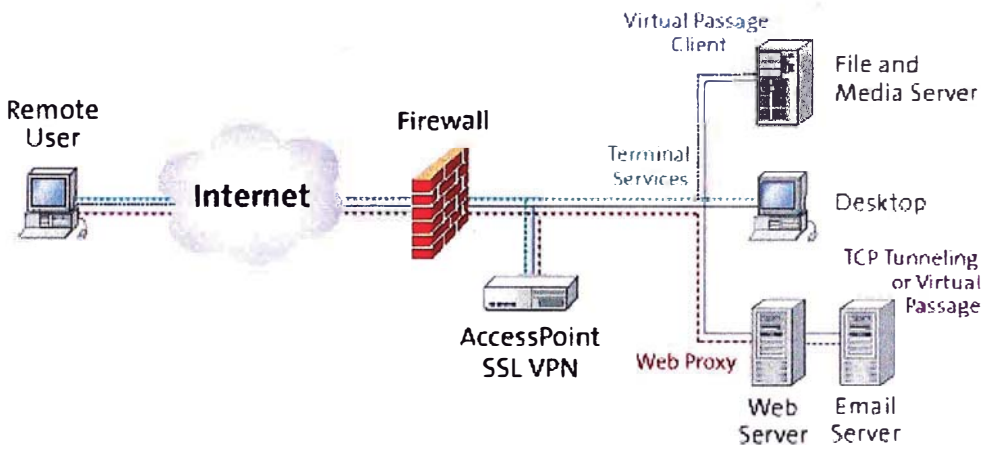

Figura 11 – Arquitectura VPN
Fuente: Cisco Network Consultants Handbook

2.5.6 PROXY

Un proxy, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro, esto es, si una hipotética máquina A solicita un recurso a una C, lo hará mediante una petición a B; C entonces no sabrá que la petición procedió originalmente de A. Esta situación estratégica de punto intermedio suele ser aprovechada para soportar una serie de funcionalidades: proporcionar caché, control de acceso, registro del tráfico, prohibir cierto tipo de tráfico, etc.

Su finalidad más habitual es la de servidor proxy, que consiste en interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc. Esta función de servidor proxy puede ser realizada por un programa o dispositivo.

2.6 INFRAESTRCUTURA TECNOLÓGICA

2.6.1 ACTIVE DIRECTORY

Active Directory (AD) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (principalmente LDAP, DNS, DHCP, Kerberos).

De forma sencilla se puede decir que es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.

Active Directory permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera. Un Active Directory almacena información de una organización en una base de datos central, organizada y accesible. Pueden encontrarse desde directorios con cientos de objetos para una red pequeña hasta directorios con millones de objetos.

Su funcionamiento es similar a otras estructuras de LDAP (Lightweight Directory Access Protocol), ya que este protocolo viene implementado de forma similar a una base de datos, la cual almacena en forma centralizada toda la información relativa a un dominio de autenticación.

A su vez, cada uno de estos objetos tendrá atributos que permiten identificarlos en modo unívoco (por ejemplo, los usuarios tendrán campo *nombre*, campo *email*, etc., las impresoras de red tendrán campo *nombre*, campo *fabricante*, campo *modelo*, campo *usuarios que pueden acceder*, etc.). Toda esta información queda almacenada en Active Directory replicándose de forma automática entre todos los servidores que controlan el acceso al dominio.

2.6.2 SERVIDORES BLADE

Los servidores blade están diseñados para su montaje en bastidores al igual que otros servidores. La novedad estriba en que los primeros pueden compactarse en un espacio más pequeño gracias a sus principios de diseño.

Cada servidor blade es una delgada "tarjeta" que contiene únicamente microprocesador, memoria y buses. Es decir, no son directamente utilizables ya que no disponen de fuente de alimentación ni tarjetas de comunicaciones.

Estos elementos más voluminosos se desplazan a un chasis que se monta en el bastidor ocupando únicamente de cuatro (4U) a seis alturas (6U). Cada chasis puede albergar del orden de dieciséis "tarjetas" o servidores blade (según fabricante). El chasis lleva integrados los siguientes elementos, que son compartidos por todos los servidores:

- Fuente de alimentación: redundante y hot-plug.
- Ventiladores o elementos de refrigeración.

- Conmutador de red redundante con el cableado ya hecho, lo que simplifica su instalación.
- Interfaces de almacenamiento. En particular, es habitual el uso de redes SAN (Storage Area Network) de almacenamiento.

Además, estos servidores suelen incluir utilidades software para su despliegue automático. Por ejemplo, son capaces de arrancar desde una imagen del sistema operativo almacenada en disco. Es posible arrancar una u otra imagen según la hora del día o la carga de trabajo, etc.

2.6.3 BASES DE DATOS

Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido; una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.

Existen programas denominados sistemas gestores de bases de datos, abreviado DBMS, que permiten almacenar y posteriormente acceder a los datos de forma rápida y estructurada. Las propiedades de estos DBMS, así como su utilización y administración, se estudian dentro del ámbito de la informática.

2.7 SECURITY INFORMATION AND EVENT MANAGEMENT

2.7.1 SECURITY INFORMATION MANAGEMENT (SIM)

Este término se refiere a la recolección de datos (logs, SNMP trap, etc.) en un repositorio central para el análisis de tendencias. Los productos SIM comprenden en general de los agentes de software que se ejecutan en los sistemas informáticos, los cuales se pueden monitorear, luego envía la información de registro a un servidor central que actúa como una "consola de seguridad". La consola muestra típicamente los informes, tablas y gráficos de esa información, a menudo en tiempo real. Algunos agentes de software pueden incorporar filtros locales, para reducir y manipular los datos que se envían al servidor, aunque por regla general desde el punto de vista forense le recopilar todos los registros de auditoría y contabilidad para asegurarse de que puede recrear un incidente de seguridad.

Los datos que se envían al servidor, se normalizan por los agentes de software en una forma común, por lo general XML. Esos datos se agregan, con el fin de reducir su tamaño total.

2.7.2 SECURITY EVENT MANAGER (SEM)

Es el cerebro de una solución SIEM. Se encarga del análisis automatizado o los miles de millones de registros en busca de comportamientos inusuales, similar a una herramienta de inteligencia de negocios.

Para ser considerado un verdadero SEM, la solución debe ser capaz de controlar los comportamientos, en lugar de eventos individuales. Un número de soluciones será capaz de correlacionar eventos, pero no todos de correlación es igual en la capacidad.

2.7.3 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Es un término para software y productos que combinan los servicios del SIM del SEM. Las tecnologías SIEM ofrecen un análisis en tiempo real de las alertas de seguridad generadas por el hardware y las aplicaciones de red. El SIEM se vende como software, appliance[4] o servicios gestionados. Se utilizan también para registrar los datos de seguridad y generar informes para fines de cumplimiento.

El principio fundamental de un sistema SIEM es que correlacionar los logs seguridad de una empresa, los cuales se producen en múltiples ubicaciones. La herramienta debe ser capaz de mirar a todos los datos desde un solo punto de vista, haciendo que sea más fácil de detectar tendencias y ver los patrones que son fuera de lo común.

Los sistemas SIEM realizan registros y otra documentación relacionada con la seguridad para su análisis. La mayoría de los sistemas SIEM trabajan mediante la implementación de varios agentes de la colección de una manera jerárquica para recopilar eventos relacionados con la seguridad de los dispositivos de los usuarios finales, servidores, equipos de red - e incluso el equipo de seguridad especializado como firewalls, antivirus o sistemas de prevención de intrusos. Los colectores reenvian eventos a una consola de gestión centralizada, que realiza inspecciones y estudio de anomalías. Para permitir que el sistema identifique eventos anómalos, es importante que el administrador del SIEM cree primero un perfil del sistema en condiciones normales de eventos.

---

[4] Dispositivo de hardware con un software dedicado, diseñado específicamente para proporcionar un recurso informático especifico. Se hicieron conocidos como "appliance" debido a su similitud con los aparatos electrodomésticos, que generalmente son "cerrados y sellados".

La figura 12 muestra los niveles sobre los cuales trabaja el SIEM, desde los dispositivos a monitorear, la categorización y análisis de eventos.

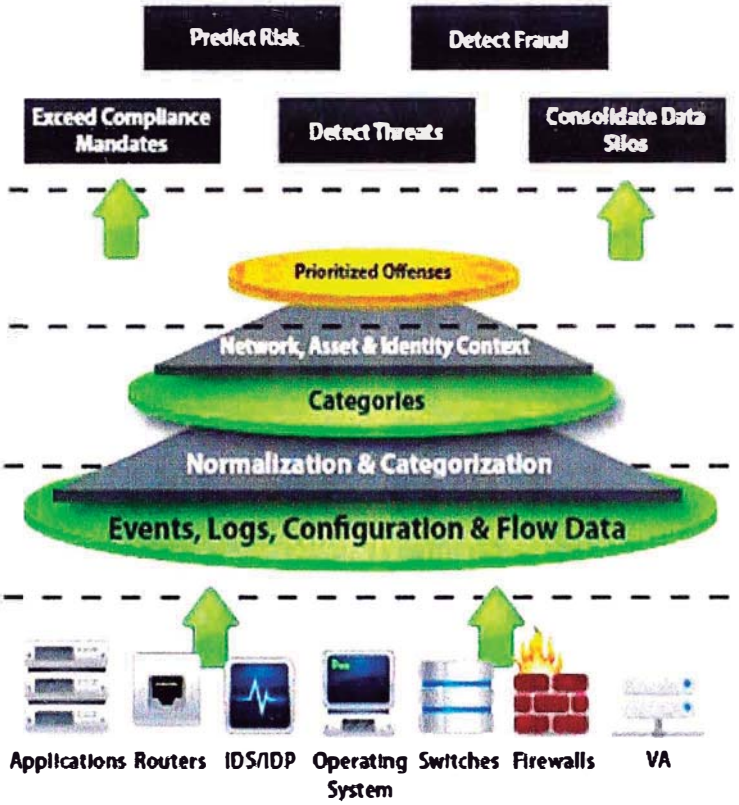

Figura 12 – Arquitectura de una solución SIEM
Fuente: Libro Security Information and Event Management (SIEM) Implementation

En el nivel más básico, en un sistema SIEM puede haber reglas basadas en emplear un motor de correlación estadística para establecer relaciones entre las entradas del registro de eventos. En algunos sistemas, el pre-procesamiento puede ocurrir en los colectores de borde, con sólo ciertos eventos que se pasaron a través de un nodo de gestión centralizada. De esta manera, el volumen de información que se comunica y almacenado se puede reducir. El peligro de este enfoque, sin embargo, es que los eventos pertinentes pueden ser filtrados a cabo demasiado pronto.

Los sistemas SIEM son típicamente costosos de implementar y complejos para operar y administrar. Mientras que el estándar de cumplimiento PCI DSS (Payment Card Industry) ha impulsado tradicionalmente adopción SIEM en las grandes empresas, la preocupación por las amenazas persistentes avanzadas (APT) han llevado a las organizaciones más pequeñas a ver los beneficios de un SIEM con un proveedor de servicios gestionados de seguridad.

2.7.4 SIEM ARCSIGHT[5]

ArcSight es un sistema de software diseñado para permitir a las organizaciones recopilar, vigilar, analizar y actuar sobre la información logs de seguridad informática de una manera eficiente y eficaz. Está diseñado para ingerir grandes volúmenes de información de archivo de registro heterogéneo, correlacionar de forma inteligente y presentar esa información a una variedad usuarios de diversos perfiles de una manera que permite la toma adecuada de decisiones.

ArcSight se entrega con una configuración de seguridad predeterminada, tanto en procesamiento y configuración del informe, sin embargo se puede configurar a casos específicos y prioridades de seguridad.

Asimismo está diseñado para permitir el acceso autorizado, para permitir la gestión y tratamiento de datos, el almacenamiento seguro y la recuperación de varias categorías de datos, el transporte seguro de datos, y la retención de la información con fines legales y de auditoría.

Los módulos principales de Arcsight son:

Arcsight ESM

El appliance ESM (Enterprise Security Management), es aquel que brinda todo el procesamiento inteligente, sus funcionalidades permiten:

- Detectar y detener las amenazas que no pueda predecir
- Automatizar los análisis de patrones y la detección de anomalías
- Proteger las transacciones críticas de las aplicaciones
- Almacenar de forma segura los datos confidenciales

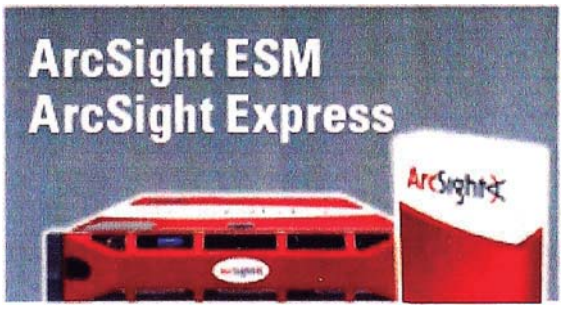

Figura 13 – Arsight ESM
Fuente: Web HP Arcsight

[5] Arcsight es una familia de productos de seguridad pertenecientes a la empresa HP

Arcsight Logger

Es un appliance colector cuyas funcionalidades permiten

- Almacenar todos los datos de registros de la empresa
- Gestionar años de datos en una única instancia
- Buscar terabytes de registros en segundos
- Automatizar los informes de cumplimiento
- Obtener inteligencia empresarial para los registros

Figura 14 – Arcsight Logger
Fuente: Web HP Arcsight

CAPÍTULO III

PROCESO DE TOMA DE DECISIONES

3.1 PLANTEAMIENTO DEL PROBLEMA

3.1.1 SITUACIÓN ACTUAL

Para entender la situación actual, es importante considerar la estructura del área de Tecnología, a nivel macro y de forma resumida tenemos la estructura mostrada en la figura 15 de la página siguiente.

El departamento de Proyectos es responsable del desarrollo de nuevas implementaciones o funcionalidades en los sistemas de información. Se encarga de la evaluación de las unidades de negocio en relación al uso de las tecnologías con la finalidad de proponer nuevas soluciones, así como alinear el uso de las tecnologías con el Plan Estratégico de la empresa. Asimismo, se encarga de monitorear todo el ciclo de vida de proyectos y el desempeño del mismo lo cual se traduce en el balance score card del área de TI.

El departamento de Aplicaciones se encarga del mantenimiento de los sistemas informáticos, tales como incidentes reportados por service desk, atención de requerimientos y el desarrollo de sistemas propuestos por el departamento de Soluciones. Para ello cuenta con analistas funcionales y programadores. Los primeros se encargan del relevamiento de información del negocio y traducción a un estándar “técnico” para que los programadores puedan desarrollar la aplicación.

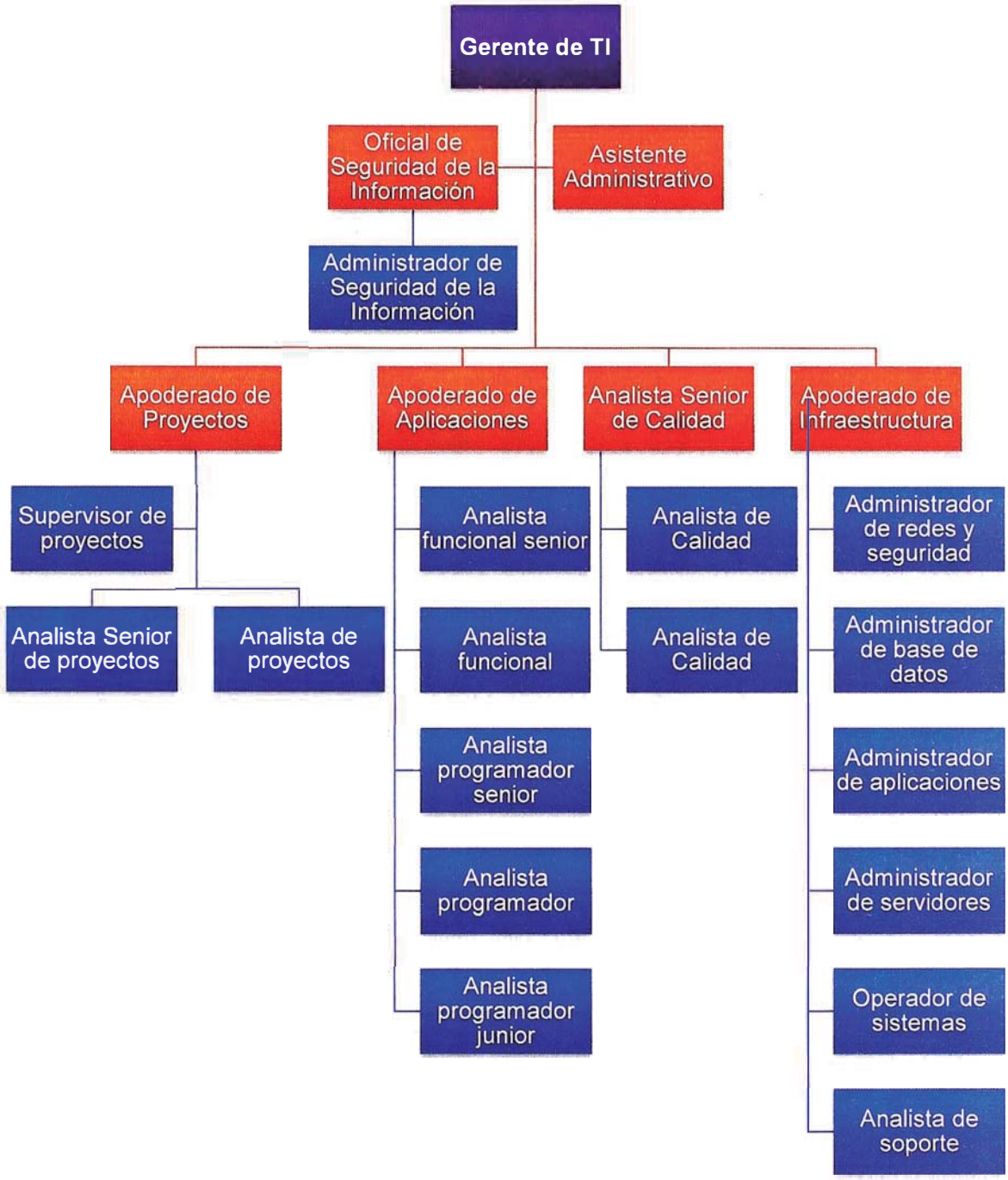

Figura 15 – Organigrama del área de Tecnología
Fuente: Compañía de seguros de estudio

El departamento de Calidad de Software no cuenta con un apoderado, el Analista Senior es responsable de asegurar que los pases a producción cumplan con los estándares con la finalidad de que se reduzcan los incidentes de las aplicaciones por errores no identificados previamente. Para ello se realizan una serie de pruebas a nivel funcional y técnico.

Respecto al departamento de Infraestructura tiene como objetivo velar por la disponibilidad de los servicios a cargo de la Gerencia de TI. Así como asesorar en el uso de nuevas tecnologías que faciliten la administración de los sistemas.

El administrador de redes y seguridad es responsable de diseñar, configurar, implementar y mantener todas las redes de la empresa, es decir la LAN, WAN, WLAN, entre otros. Asimismo, garantiza que la seguridad tenga los niveles adecuados en base a las políticas de la compañía.

La administración de la base de datos y servidores es realizada tanto por personal interno como outsource quienes brindan servicios a la compañía. Por el lado del soporte técnico, hay un analista de soporte y un departamento de helpdesk de nivel 1 y nivel 2, quienes dan asistencia a usuarios vía telefónica y/o por escritorio remoto y de forma presencial respectivamente. En relación a la administración de accesos existen dos responsables quienes se encargan de la administración de usuarios (creación, desactivación, eliminación, modificación de perfil) en los 70 diferentes sistemas con los que cuenta la compañía.

Entre las tareas más importantes realizadas por el área de infraestructura tenemos:

- Pases a producción: pasar a ambientes de producción los desarrollos o cambios realizados por Aplicaciones y validados por Calidad. Para ello se lleva un registro en excel de cada pase realizado con su código de identificación. Asimismo, por cada pase existe otro formato excel donde se coloca el detalle del pase, criticidad, actividades puntuales, posibles impactos y plan de rollback. Se debe considerar que todo pase a producción debe ser previamente aprobado por el Apoderado de Aplicaciones, el Analista Senior de Calidad, el Apoderado de Infraestructura y el Líder usuario. Asimismo, los pases tienen un horario definido según la aplicación que corresponda, para sistemas críticos, el pase se realiza fuera del horario de oficina.
- Monitorear el estado de los servidores y equipos de comunicaciones: Se cuenta con un Natgios para verificar la disponibilidad de los servidores, este realiza peticiones echo reply para ver si el servidor responde o no, similar es el caso para los equipos de comunicaciones.
- Dimensionar, monitorear, controlar y dar seguimiento a acciones correctivas de los servidores de aplicaciones, bases de datos, entre otros.
- Controlar y realizar los procesos de backups y restore.

- Resolución de incidentes de caída de servicio, sobrecarga en la red wireless, infección de equipos con virus, cambios en bases de datos de calidad sin autorización correspondiente
- Realizar las pruebas de Disaster Recovery Planning (DRP) simulando caída del data center principal y levantando el data center de contingencia el cual se encuentra terciarizado por la empresa GMD.

Análisis de riesgos

La seguridad de información como disciplina existe para gestionar los riesgos relacionados con la confidencialidad, la integridad y la disponibilidad. La gestión de riesgos es también un factor clave para gestionar los requerimientos regulatorios y encaminar a la Organización a alcanzar un equilibrio eficaz entre concretar oportunidades para obtener ganancias y minimizar las vulnerabilidades y las pérdidas. Esto suele alcanzarse garantizando que el impacto de las amenazas que explotan las vulnerabilidades esté dentro de los límites y costos aceptables para la Organización.

En términos generales, la gestión de riesgos significa que los riesgos se gestionan de tal manera que no tengan un impacto significativo para el negocio, y que los niveles aceptables de aseguramiento y previsibilidad sobre los resultados deseados de cualquier actividad importante para la compañía.

Asimismo, la estrategia de seguridad de la información de la compañía se define como:

"Determinar el enfoque óptimo para alinear los procesos, tecnología y comportamiento de la compañía, con el fin de aceptar, mitigar o rechazar riesgos de seguridad de información que sean identificados como parte del proceso, mediante el Análisis y Clasificación de los activos de información y cálculo del riesgo asociado. Así se podrá efectuar el plan de tratamiento de los riesgos en base al nivel de tolerancia acordado por parte del Comité de Seguridad de Información y de la Alta Dirección."

El análisis de riesgos está compuesto por la identificación de los riesgos, el análisis y la evaluación de riesgos sobre los activos de información de los procesos de negocio y operacionales de la compañía.

La fase de la evaluación de riesgos incluye:

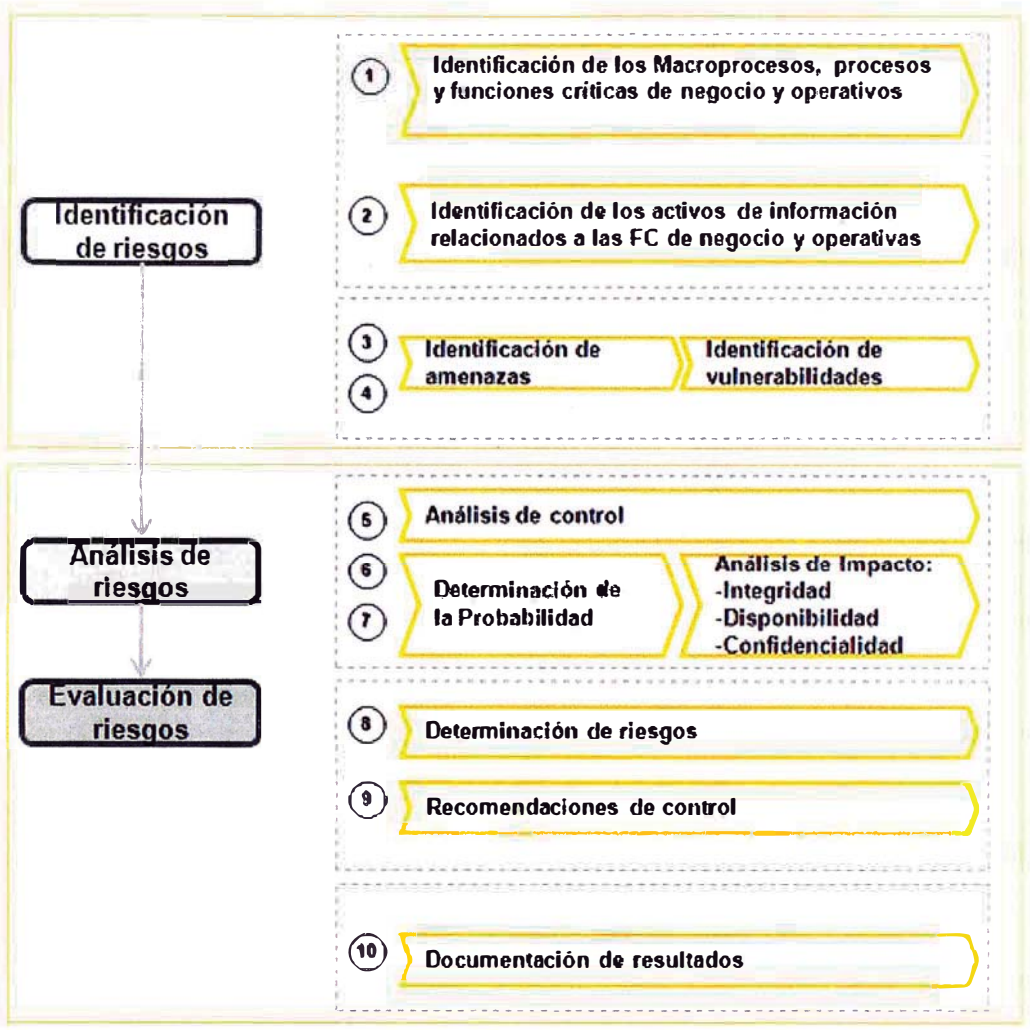

Figura 16 – Esquema de análisis de riesgos
Fuente: Compañía de seguros de estudio

El análisis de riesgos se documenta en matrices en Excel, el modelo de los mismos se detalla en el Anexo 2.

3.1.2 PROBLEMÁTICA

La problemática se encuentra en el contexto de la administración de la infraestructura tecnológica y la gestión de incidentes de seguridad de la información, si bien tiene impacto en la operatividad del negocio, no es transversal a los procesos del mismo; por lo cual el enfoque será directo a la administración de tecnologías de la información.

La empresa ha tenido múltiples incidentes de caída de servicios tales como el Insunix que es el sistema core de Vida, esto ha provocado inconvenientes en las tareas operativas de las Gerencias Comercial, Administración,

Marketing, Ventas y Técnica, sobre todo en esta última pues usan el Insunix para registrar las pólizas de productos de Vida. Como medida reactiva se reiniciaron los servicios, sin embargo no se han revisado a detalle los logs arrojados tanto por la aplicación como por el servidor sobre el cual se aloja (es un cluster de 5 nodos).

Otra problemática que afecta a todos los usuarios, sobre todo los usuarios remotos, es decir de agencias o destacados en clínicas, es la lentitud en la transferencia de datos a nivel de la red. A pesar de tener un ancho de banda aceptable, existen horas picos donde la red se carga de forma intempestiva.

En relación a las aplicaciones web, se han dado casos de indisponibilidad de servicios en el sistema Oficina Virtual, el cual está publicado en internet y es usado por corredores y analistas de la Gerencia Comercial, este sistema tiene un workflow para la autorización de una póliza.

Por otro lado, también se ha dado un caso de acceso no autorizado a la base de datos del sistema Jubilare (sistema de gestión de rentas vitalicias), la investigación dio a conocer que se trataba de un problema de difusión masiva del broadcast[6] y de tráfico SNMP sin cifrar.

Relacionado a la seguridad perimetral, existen múltiples intentos de conexión desde diferentes IP públicas que se encuentran escaneando la red de la Empresa, no existe la capacidad suficiente a nivel de falta de personal para realizar un monitoreo integrado del IPS, firewall, VPN, servidor de correos y otras aplicaciones que tienen conectividad con internet.

En general los incidentes acontecidos tienen como común denominador la poca eficiencia en el monitoreo de los sistemas, no solamente porque no se cuentan con las herramientas, sino que el personal del área de Tecnología no es suficiente para dedicarse netamente a realizar el monitoreo de todos los sistemas. Asimismo, estos eventos no son casos aislados que se cierran sólo una vez, sino son casos que se han venido repitiendo de forma sistemática, sobre todo los relacionados a las vulnerabilidades de red. Las herramientas de monitoreo detectan cuando el servicio ya cayó, cuando la web esta indisponible, u otros eventos *post ocurridos*, pero para algunos casos no existe un sistema de alertas que notifique vía correo u otro tipo de señal cuando está ocurriendo un evento o incidente de seguridad de la información.

[6] Es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Dentro del marco de la gestión de incidentes se cuenta con una política que da los lineamientos ante este tipo de casos, básicamente son los lineamientos para identificar, detectar, contener, reaccionar y abordar los incidentes de seguridad de la información. De más está decir que está política no se cumple en su totalidad puesto que no se tiene la capacidad suficiente para la identificación del incidente debido a los problemas mencionados en párrafos anteriores.

A modo de evidencia se presenta la el siguiente cuadro extraído de la Bitácora de Incidentes, en el mismo se muestran los casos más representativos documentados por el área de Seguridad de la Información (Obs: el cuadro se muestra en dos partes, la segunda parte es la continuación horizontal de la primera):

Tabla 2 – Bitácora de incidentes de seguridad de la información (parte 1)
Fuente: Compañía de seguros de estudio

Registro			Reporte	Descripción			Tipificación	
ID	Día del incidente	Hora del incidente	Área reportante	Evento/ Incidente	Tema	Descripción	Categoría	Sub-Categoría
COD2012-14	22/05/2012	16:00:00	Infraestructura Tecnológica	Evento	Monitoreo de Trafico SQL	Se evidenció que la prueba de concepto (POC) con la solución IMPERVA no capturaba el tráfico de sentencias SQL a través de la red.	Denegación del servicio	Servicio(s) interno(s) inaccesibles sin razones aparentes
COD2012-42	16/06/2012		Infraestructura Tecnológica	Incidente	Ataque Denial of Service desde red interna	Fernando Palomares, remitió una incidencia de ataques de UDP flood e IP Spoofing desde las PCs de usuarios a la red.	Acceso no autorizado	Intentos recurrentes y no recurrentes de acceso no autorizado
COD2012-47	25/06/2012	08:45:00	Tecnología de Información	Incidente	Indisponibilidad de Servicio Web Oficina Virtual	El día 25 de octubre de 2012, diversos usuarios, presentaron problemas para poder ingresar al aplicativo de Oficina Virtual, debido a que este último no autentificaba el usuario y contraseña de los diversos usuarios.	Denegación del servicio	Servicio(s) interno(s) inaccesibles sin razones aparentes
COD2012-51	12/07/2012	15:00:00	Infraestructura Tecnológica	Incidente	Bloqueo continuo de cuenta de red	Bloque recurrente de la cuenta de red "iovasq0"	Denegación del servicio	Servicio(s) interno(s) inaccesibles sin razones aparentes
COD2012-57	06/08/2012	13:00:00	Seguridad de Información	Evento	Monitoreo de Trafico a DNS malicioso	Actividades de monitoreo referentes al malware DNSChanger	Escaneos, pruebas o intentos de obtención de información	Detección de Vulnerabilidades

COD2012-59	13/08/2012	16:00:00	Seguridad de Información	Incidente	Intermitencia en conexión de in/out de red	Problemas de acceso a sistemas de información internos y problemas de acceso a internet	Denegación del servicio	Servicio(s) interno(s) inaccesibles sin razones aparentes
COD2012-66	23/10/2012	17:00:00	Seguridad de información	Incidente	Borrado de tablas de base de datos en ambiente de producción	Usuario del Ambiente de desarrollo a borrado tablas importantes del ambiente de Producción.	Denegación del servicio	Servicio(s) interno(s) inaccesibles sin razones aparentes
COD2012-68	29/10/2012	09:45:00	Infraestructura Tecnológica	Incidente	Corte de la red de datos	Hoy a las 9:45 am aprox. se perdió la comunicación del piso 9a con los servidores.	Denegación del servicio	Servicio(s) interno(s) inaccesibles sin razones aparentes
COD2012-69	12/11/2012	11:00:00	Tecnología de Información	Incidente	Lentitud de las comunicaciones debido al corte de fibra óptica en la Zona Sur	Inconvenientes con las comunicaciones en las Agencias de la Región Sur debido a una avería masiva de telefónica (corte de fibra óptica en el sur chico).	Denegación del servicio	Servicio(s) Externo(s) inaccesibles sin razones aparentes
COD2012-70	10/12/2012	13:54:00	Tecnología de Información	Incidente	Incidentes con las aplicaciones de google (Gmail, Drive, Google Chat, entre otras...)	Entre las 13:45 y 14:13 hrs GMT-5, una actualización de rutina al software balanceador de google fue puesta en producción. Un bug en la actualización del software causó que se interpretara de forma incorrecta los Data Centers como no disponibles.	Denegación del servicio	Tiempos de respuesta muy bajos sin razones aparentes.
COD2012-71	27/12/2012	21:20:00	Tecnología de Información	Incidente	Intento fallido de conexiones a la red de datos de la Empresa	Se ha identificado un Evento de Seguridad IFC - Intento fallido de conexiones, la evaluación preliminar realizada por nuestro grupo (Proveedor Digiware) de analistas requiere de su participación activa en la valoración del evento	Acceso no autorizado	Intentos recurrentes y no recurrentes de acceso no autorizado

Tabla 3 – Bitácora de incidentes de seguridad de la información (parte 2)
Fuente: Compañía de seguros de estudio

Tipificación		Impacto			Causa Raíz	Solución
Naturaleza	**Origen**	**Nivel de Impacto: 1 (inferior) --> 5 (catastrófico)**	**Gerencias afectadas**	**Proceso afectado**	**Causa Raíz**	**Solución**
Comunicaciones	Red de datos	2	Tecnologías de la Información	Seguridad de Información / Infraestructura tecnológica	Dos conexiones ethernet no se les realizó la configuración de port mirroring	Se solicitó la configuración al administrador de red quien realizó la configuración y el appliance Imperva empezó a recibir el tráfico hacia las bases de datos.
Comunicaciones	Red de Datos	2	Todas	Infraestructura tecnológica	No identificada	No se tomó acción
Sistemas de Información	Segurinet	4	Todas	Seguridad de Información	El gestflujo causo problemas al IIS del servidor srvappprod al consumir muchos recursos.	Depuración de la base de datos
Comunicaciones	Red de Datos	2	Tecnologías de la Información	Infraestructura tecnológica	Al parecer se trataba de un software (malicioso o no) que autenticaba automáticamente al usuario. No se determinó la causa raiz definitiva	Se procedió a crear nuevamente el perfil en el computador afectado.
Comunicaciones	DNS's	2	Todas	Seguridad de Información	Malware identificado que dejaría sin conexión a Internet a las computadoras infectadas por el mismo.	Se solicitó al proveedor de correlación de logs de seguridad perimetral que monitoree las conexiones de red maliciosas durante el periodo 06/ 07-09/ 07y que emita un informe después del mismo. El informe no arrojó conexiones maliciosas a los DNS que afectarían el servicio.

Comunicaciones	Red de datos	3	Todas	Infraestructura tecnológica	No identificada	No se tomó acción
Software	BD-INFORMIX	4	Tecnologías de la Información	Seguridad de Información	El borrado de las tablas de la base de datos por parte del usuario de soporte de tercer nivel.	Restore de la base de datos
Comunicaciones	Red de datos	3	Tecnologías de la Información	Seguridad de Información	No se identificó el motivo principal, pero se pudo haber ocasionado debido a problemas en el switch principal o el de distribución o algún intento de ataque man-in-the-middle	Reinicio del switch
Servicios terceros	Internet-Telefónica	2	Todas	Infraestructura tecnológica	No se identificó la causa raíz.	Solución dada por Telefónica
Servicios terceros	Google Apps (Correo-Docs-Sites-Calendar)	4	Todas	Infraestructura tecnológica	La causa raíz de la disrupción del servicio fue un issue con la carga del software balanceador.	Reinicio del servicio
Comunicaciones	Red de Datos	2	Tecnologías de la Información	Infraestructura tecnológica	No se identificó la causa raíz.	No se tomó acción
Sistemas de Información	Red de datos	4	Todas	Infraestructura tecnológica	Vulnerabilidad 0 day en la versión 7 update 41 del java	Desinstalar el java en las máquinas que no lo necesiten

Gestión de Incidentes[7]

La compañía cuenta con una política de gestión de incidentes, el cual señala:

Todo incidente de Seguridad de la Información, deberá ser reportado de manera detallada y oportuna, por medio del procedimiento correspondiente, tanto al Propietario de la Información, como al Oficial de Seguridad de la Información.

Todos los incidentes de Seguridad de la Información, deberán ser reportados como parte de la Gestión de Riesgos. Estos deberán ser priorizados para su solución oportuna, acorde al impacto que tienen sobre las operaciones de la empresa. Con este fin, se deberá tener en consideración la clasificación de la Información involucrada en el incidente, y realizar la Evaluación de Riesgo pertinente.

Asimismo, se definen las siguientes pautas:

- Medidas preventivas: todos los controles de seguridad de la información con los que cuenta la compañía.
- Plan de respuesta a incidentes: se definen responsabilidades, niveles de escalamiento y lineamientos en las acciones inmediatas a tomar en caso de algún incidente, para la contención y mitigación.
- Referencias normativas: la gestión de incidentes está acorde a la política de seguridad de la información de la compañía, tanto en el tratamiento así como el equipo de respuesta a incidentes.
- Medidas preventivas: lecciones aprendidas que permitirán la materialización de incidentes futuros.

Cabe señalar que los incidentes son comunicados a las áreas interesadas de la empresa, con la finalidad de evaluar si ha comprometido los aspectos legales, de riesgo operativo, entre otros.

En el Anexo 3 se presentan dos flujogramas de la gestión de incidentes, el cual incluye el plan de respuesta y la comunicación de resultados.

Estadísticas de incidentes

A modo de resumen tenemos algunos cuadros estadísticos de incidentes reportados del periodo enero a diciembre del 2012:

[7] ISO/IEC 27035:2011 – Técnicas para la administración de incidentes de seguridad de la información.

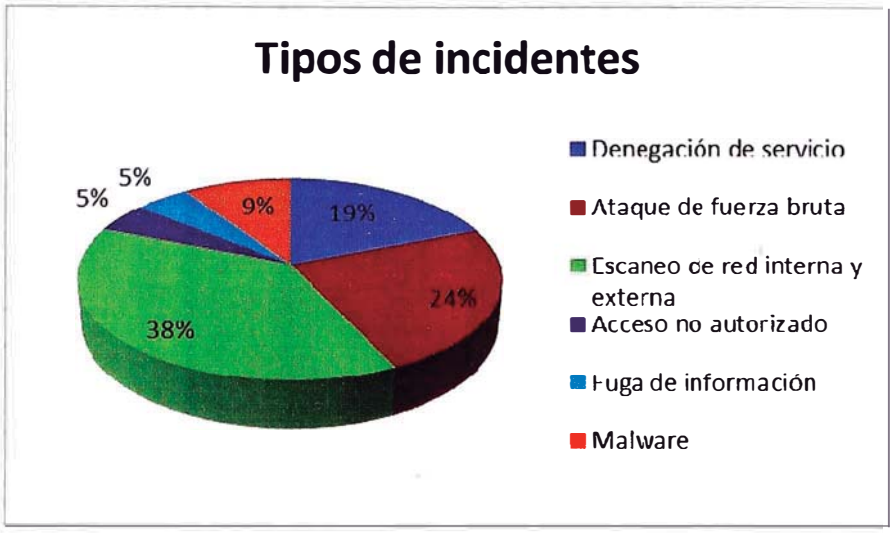

Figura 17 – Estadísticas de incidentes ocurridos
Fuente: Compañía de seguros de estudio

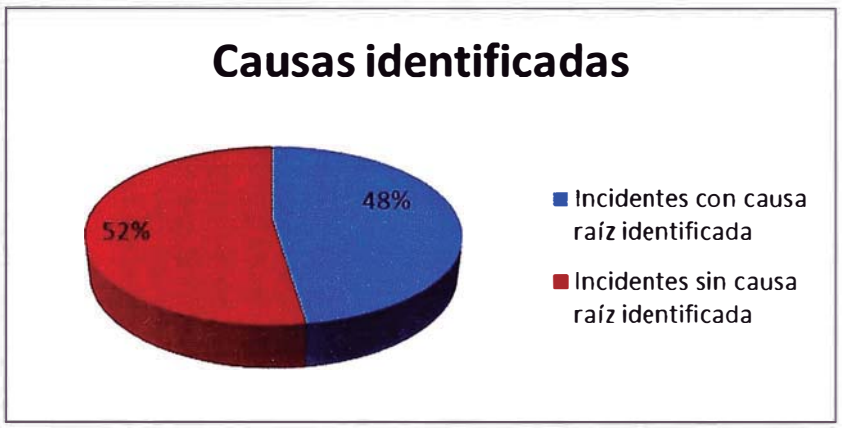

Figura 18 – Estadísticas de causas identificadas de incidentes
Fuente: Compañía de seguros de estudio

Asimismo, para calcular las pérdidas monetarias se hace uso del cálculo monetario del riesgo según Global Crossing[8] (mayor información del cálculo realizado en el anexo 1).

En resumen, el costo anual de pérdida por incidentes de seguridad de la información asciende a US$ 44,344.00. Incluso, por no tener una adecuada gestión de incidentes, en el peor de los casos la multa de la SBS asciende a aproximadamente US$ 40,000.00[9]

[8] Compañía de telecomunicaciones perteneciente desde el 2011 a la empresa de telecomunicaciones y proveedor de servicios de internet (ISO por sus siglas en inglés) Level 3 Communications.
[9] Teniendo como referencia 29 UIT. Información obtenida de la web de la SBS, artículo de faltas graves de los lineamientos dados por dicha institución.

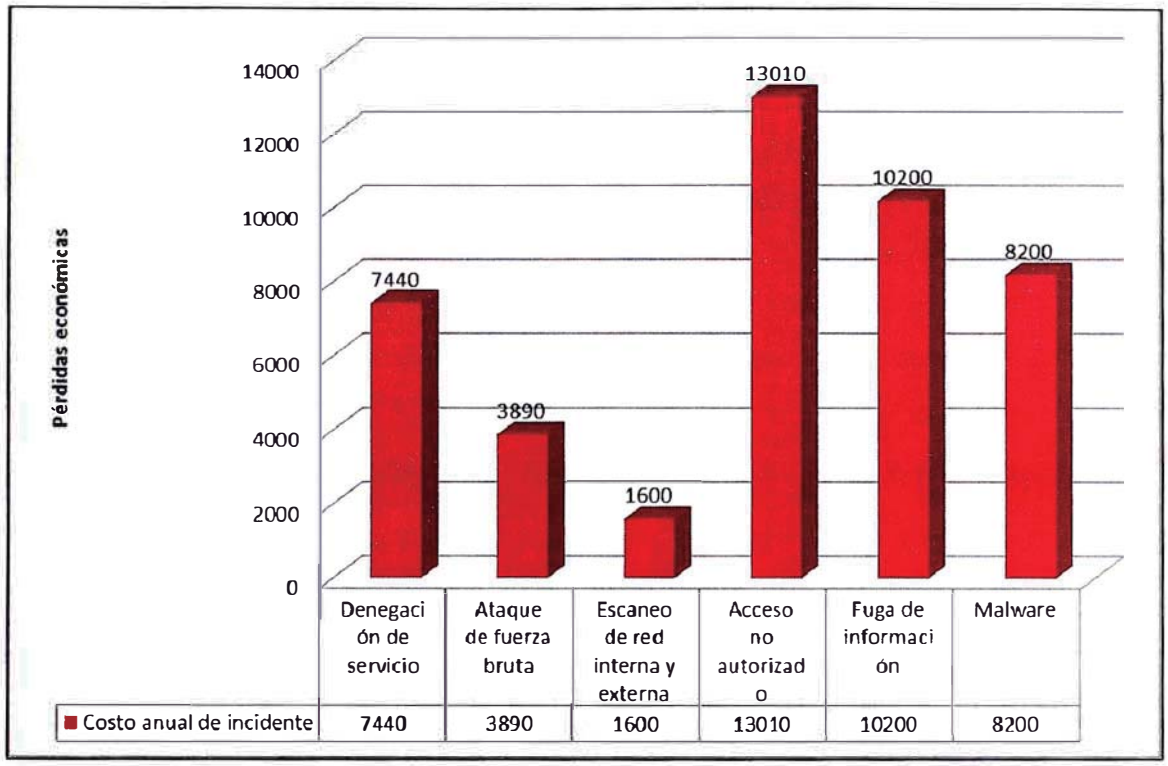

Figura 19 – Datos de costos incurridos por incidente
Fuente: Compañía de seguros de estudio

Como se puede observar los incidentes de acceso no autorizado, fuga de información y malware son los de mayor riesgo, ya que representan mayores pérdidas.

3.1.3 FORMULACIÓN DEL PROBLEMA

En base a la problemática expuesta, el problema se puede formular de la siguiente manera:

¿De qué manera se puede tener una visibilidad completa del ciclo de la gestión de incidentes, que aborde el monitoreo, detección, contención, documentación y prevención de forma eficiente?

3.2 ALTERNATIVAS DE SOLUCIÓN

Alternativa 1: Adquirir una herramienta SIEM de un fabricante tercero.

Comprar, implementar y parametrizar una herramienta SIEM elaborada por un tercero. Para este caso se propone una herramienta de la empresa HP llamada Arcsight.

Ventajas:

- Rapidez en la implementación y no requiere un esfuerzo en el desarrollo.
- Empresa especializada en el desarrollo de esta herramienta.
- Conocimiento para asesorar el afinamiento de políticas de monitoreo.

Desventajas:

- Costo elevado de la herramienta.
- Personalización limitada ya que es un appliance que no permite interfaces, con otros sistemas.

Alternativa 2: Desarrollar de forma in-house una herramienta de correlación de logs.

A modo de proyecto desarrollar una herramienta con la capacidad de leer diferentes tipos de logs, tales como un syslog, snmp-trap, entre otros. De tal forma que estos se copien en un servidor que tenga una aplicación que relacione diferentes logs por índices como dirección IP, dirección MAC, usuario de red, entre otros que permitan el rastreo de eventos.

Ventajas:

- Alto nivel de personalización, el desarrollo de la herramienta se hace a medida.
- Conocimiento detallado sobre los incidentes de la empresa.

Desventajas:

- Demanda un gran tiempo el desarrollo de esta herramienta.
- Conocimiento técnico limitada sobre protocolos de red y de logs.

3.3 METODOLOGÍA DE EVALUACIÓN DE SOLUCIONES

La alternativa a elegir se tomará en base a los siguientes criterios:

- **Manejo de precios sobre cada alternativa:** Costos del desarrollo, compra, personal, licenciamientos, entre otros.
- **Rapidez del tiempo de desarrollo y/o implementación:** Tiempo del desarrollo y/o implementación y afinamiento de políticas de monitoreo.
- **Disponibilidad de soporte:** Disponibilidad para solucionar incidentes propios de la herramienta.
- **Estabilidad de la herramienta:** Funcionamiento correcto sin caídas y rollback de los pases a producción.

- **Visibilidad de eventos e incidentes:** Capacidad para leer diferentes tipos de logs.
- **Personalización de la herramienta:** Capacidad para elaborar diferentes políticas de monitoreo y alertas
- **Experiencia en el desarrollo e implementación:** Conocimientos técnicos sobre el tema.

Asimismo, se aplicará la siguiente escala de valoración, cabe indicar que tanto los criterios así como la escala de valoración fueron elegidos por juicio de expertos en el Comité de la Gerencia de Tecnología donde se hacía seguimiento al proyecto:

Tabla 4 – Escala de valoración de alternativas de solución
Fuente: Compañía de seguros de estudio

Nivel de cumplimiento	Calificación
Muy alto	5
Alto	4
Medio	3
Bajo	2
Muy bajo	1

3.4 TOMA DE DECISIÓN

En base a los criterios y calificación se elabora el siguiente cuadro donde la alternativa elegida es la Alternativa 1.

Tabla 5 – Tabla de evaluación de alternativas
Fuente: Compañía de seguros de estudio

Criterio	Peso	Calificación		Valor	
		Alternativa 1	Alternativa 2	Alternativa 1	Alternativa 2
Manejo de precios	0.15	2	4	0.3	0.6
Rapidez del tiempo de desarrollo/implementación	0.12	5	2	0.6	0.24
Disponibilidad de soporte	0.08	3	3	0.24	0.24
Estabilidad de la herramienta	0.10	4	3	0.4	0.3
Visibilidad de eventos	0.20	5	4	1	0.8
Personalización	0.15	4	5	0.6	0.75
Experiencia	0.13	5	3	0.65	0.39
			Valoración total	**3.79**	**3.32**

3.5 DESARROLLO DE LA SOLUCIÓN

Objetivo

La solución propuesta tiene como objetivo contar con una mejor gestión de incidentes al contar con un mecanismo que permite tener mayor visibilidad y trazabilidad de los eventos e incidentes de seguridad de la información

Propósito

Para alcanzar el objetivo se implementará una herramienta SIEM, y se configurará en los componentes tecnológicos que tienen mayor interacción con incidentes potenciales.

Finalidad

La finalidad de esta implementación es reducir los incidentes o eventos sin causas identificadas y prevenir otros futuros incidentes para que la compañía pueda desempeñar sus funciones sin mayores problemas de seguridad de la información.

Para el desarrollo de la solución se seguirá el siguiente flujo de trabajo:

Figura 20 – Marco metodológico del proyecto
Fuente: Elaboración propia

3.5.1 INVENTARIO DE ACTIVOS CRÍTICOS DE TI

Esta primera parte del trabajo consistirá en determinar que activos son los que formarán parte del monitoreo de la herramienta SIEM. Para ello nos basaremos en tres factores:

- Criticidad de los activos tecnológicos.

- Activos que fueron afectados o participaron directamente en algún incidente de seguridad de la información.
  Equipos críticos en base a la topología de red.

3.5.1.1 Criticidad de los activos tecnológicos

Respecto a este punto, la organización realizó una evaluación de riesgos integral de seguridad de la información, en el mismo se inventariaron y clasificaron todos los activos en todos los niveles. Para el caso de los sistemas de información, la siguiente matriz se utilizó como base para determinar la criticidad de los activos tecnológicos:

Tabla 6 – Matriz de clasificación de riesgos de información de sistemas tecnológicos
Fuente: Compañía de seguros de estudio

ID	Activo	Gerencias usuarias	CRITERIOS			VALOR
			Confidencialidad	Integridad	Disponibilidad	
1	Insunix	Gerencia Comercial	Catastrófico	Catastrófico	Mayor	**Catastrófico**
		Gerencia de Administración y Finanzas	Catastrófico	Catastrófico	Catastrófico	**Catastrófico**
		Gerencia Técnica de Negocios	Moderado	Mayor	Catastrófico	**Catastrófico**
2	Visual Time	Gerencia Comercial	Moderado	Mayor	Mayor	**Mayor**
3	Oficina Virtual	Gerencia Comercial	Moderado	Mayor	Catastrófico	**Catastrófico**
		Gerencia de Gestión de Desarrollo Humano	Menor	Moderado	Moderado	**Moderado**
		Gerencia Técnica de Negocios	Moderado	Catastrófico	Mayor	**Catastrófico**
4	Query	Gerencia Comercial	Moderado	Mayor	Mayor	**Mayor**
		Gerencia Técnica de Negocios	Mayor	Menor	Menor	**Mayor**
5	SIG	Gerencia de Gestión Actuarial	Moderado	Moderado	Menor	**Moderado**
		Gerencia Técnica de Negocios	Mayor	Mayor	Moderado	**Mayor**
6	OnDemand	Gerencia de Administración y Finanzas	Catastrófico	Catastrófico	Catastrófico	**Catastrófico**
		Gerencia Técnica de Negocios	Mayor	Mayor	Mayor	**Mayor**
7	IQSoft	Gerencia de Administración y Finanzas	Catastrófico	Catastrófico	Mayor	**Catastrófico**
		Gerencia Inmobiliaria	Moderado	Moderado	Moderado	**Moderado**
		Gerencia Comercial	Moderado	Moderado	Moderado	**Moderado**
8	PMS	Gerencia de Administración y Finanzas	Mayor	Catastrófico	Mayor	**Catastrófico**
		Gerencia de Inversiones	Mayor	Catastrófico	Mayor	**Catastrófico**
9	AD Audit	Gerencia de Tecnología	Mayor	Mayor	Mayor	**Mayor**

10	Antivirus	Gerencia de Tecnología	Menor	Moderado	Moderado	**Moderado**
11	Bugzilla	Gerencia de Tecnología	Menor	Moderado	Menor	**Moderado**
12	Cálculo de Reservas (IBNR)	Gerencia de Gestión Actuarial	Moderado	Moderado	Menor	**Moderado**
13	Canal de Atención de Comunicación Interna	Gerencia de Marketing	Inferior	Mayor	Menor	**Mayor**
14	Corel Draw	Gerencia de Gestión Humana	Inferior	Menor	Menor	**Menor**
15	Discoverer	Gerencia de Administración y Finanzas	Mayor	Catastrófico	Mayor	**Catastrófico**
16	Herramientas de Desarrollo	Gerencia de Tecnología	Menor	Menor	Moderado	**Moderado**
17	Ilustrator	Gerencia de Gestión Humana	Inferior	Menor	Menor	**Menor**
18	Imperva	Gerencia de Tecnología	Mayor	Mayor	Moderado	**Mayor**
19	Internet	Gerencia de Administración y Finanzas	Moderado	Moderado	Mayor	**Mayor**
20	Jubilare	Gerencia de Gestión Actuarial	Mayor	Catastrófico	Mayor	**Catastrófico**
		Gerencia de Rentas Vitalicias	Moderado	Moderado	Moderado	**Moderado**
21	Mantis	Gerencia de Tecnología	Moderado	Mayor	Moderado	**Mayor**
22	Meller	Gerencia Técnica de Negocios	Mayor	Mayor	Mayor	**Mayor**
23	OCSInventory	Gerencia de Tecnología	Moderado	Moderado	Moderado	**Moderado**
24	Página Web	Gerencia de Marketing	Menor	Mayor	Mayor	**Mayor**
25	Photoshop	Gerencia de Gestión Humana	Inferior	Menor	Menor	**Menor**
26	Qlikview	Gerencia Comercial	Moderado	Mayor	Mayor	**Mayor**
		Gerencia de Marketing	Catastrófico	Mayor	Mayor	**Catastrófico**
27	SCAP	Gerencia Técnica de Negocios	Moderado	Mayor	Mayor	**Mayor**
		Gerencia de Gestión Actuarial	Mayor	Catastrófico	Mayor	**Catastrófico**
28	Spring	Gerencia de Gestión de Desarrollo Humano	Mayor	Mayor	Mayor	**Mayor**
29	SED	Gerencia Comercial	Mayor	Moderado	Mayor	**Mayor**
30	Segurinet	Gerencia de Tecnología	Moderado	Mayor	Mayor	**Mayor**
31	Sistema de Cuenta Corriente	Gerencia Técnica de Negocios	Mayor	Mayor	Mayor	**Mayor**
32	Intranet	Gerencia de Marketing	Moderado	Moderado	Menor	**Moderado**
33	Site de Seguridad de Información	Gerencia de Tecnología	Menor	Moderado	Menor	**Moderado**
34	Sucave	Gerencia Técnica de Negocios	Menor	Mayor	Moderado	**Mayor**
35	Websphere	Gerencia Legal	Moderado	Menor	Mayor	**Mayor**
36	WorkFlow SPF	Gerencia Técnica de Negocios	Moderado	Catastrófico	Mayor	**Catastrófico**

Como salida de esta actividad se definen los activos con nivel de riesgo catastrófico:

Insunix
Visual Time
Oficina Virtual
Ondemand
IQsoft
PMS
Discoverer
Jubilare
Qlikview
SCAP (Sistema de Calce de Activos y Pasivos)
WorkFlow SPF

Los servidores de aplicaciones y bases de datos que soportan estos activos son los que pasarán al segundo análisis para determinar su participación en la herramienta SIEM.

3.5.1.2 Activos afectados por incidentes

En base a las tablas 2 y 3 (Bitácora de incidentes de seguridad de la información), seleccionamos los incidentes que han afectado directamente a la organización. Estos se presentan a continuación a modo de resumen:

Tabla 7 – Incidentes representativos
Fuente: Compañía de seguros de estudio

Registro	Descripción		Tipificación			Impacto
Día del incidente	**Evento/ Incidente**	**Tema**	**Categoría**	**Sub-Categoría**	**Origen**	**Nivel de Impacto**
16/06/2012	Incidente	Ataque Denial of Service desde red interna	Acceso no autorizado	Intentos recurrentes y no recurrentes de acceso no autorizado	Red de Datos	2
25/06/2012	Incidente	Indisponibilidad de Servicio Web Oficina Virtual	Denegación del servicio	Servicio(s) interno(s) inaccesibles sin razones aparentes	Segurinet	4
12/07/2012	Incidente	Bloqueo continuo de cuenta de red	Denegación del servicio	Servicio(s) interno(s) inaccesibles sin razones aparentes	Red de Datos	2
06/08/2012	Evento	Monitoreo de Trafico a DNS malicioso	Escaneos, pruebas o intentos de obtención de información	Detección de Vulnerabilidades	DNS's	2
13/08/2012	Incidente	Intermitencia en conexión de in/out de red	Denegación del servicio	Servicio(s) interno(s) inaccesibles sin razones aparentes	Red de datos	3

23/10/2012	Incidente	Borrado de tablas de base de datos en ambiente de producción	Denegación del servicio	Servicio(s) interno(s) inaccesibles sin razones aparentes	BD-INFORMIX	4
12/11/2012	Incidente	Lentitud de las comunicaciones debido al corte de fibra óptica en la Zona Sur	Denegación del servicio	Servicio(s) Externo(s) inaccesibles sin razones aparentes	Internet-Telefónica	2
20/02/2013	Evento	Cambios no autorizados a equipos de la compañía con el Java instalado	Acceso no autorizado	Intentos recurrentes y no recurrentes de acceso no autorizado	Red de datos	4

En base a esta evidencia se seleccionan los siguientes dispositivos:

Controladores de dominio
Base de datos Informix
Firewall perimetral
Servidor del sistema Oficina Virtual

3.5.1.3 Topología de red

Basado en el análisis del administrador de seguridad de la información en coordinación con el personal del área de tecnología se determinarán los otros dispositivos según la topología de red mostrada en la figura 21 de la página siguiente.

El diagrama está dividido en dos partes, la parte superior muestra los equipos que componen la seguridad perimetral, tales como el firewall, el IPS, un balanceador de carga y los routers; se consideran estos dispositivos ya que tienen una gran interacción con tráfico de una red no segura que es internet, sobre esta red la compañía no tiene control, salvo la protección del tráfico entrante. La parte inferior muestra la topología de la red interna, es importante también tener visibilidad de eventos, tráfico y logs sobre la red interna puesto que los empleados de la compañía también pueden violar las políticas de seguridad de la información, sobre todo en temas de fuga de información. Asimismo, en la red interna se puede identificar malware propagado en otros segmentos de red, caídas de servicios, entre otros.

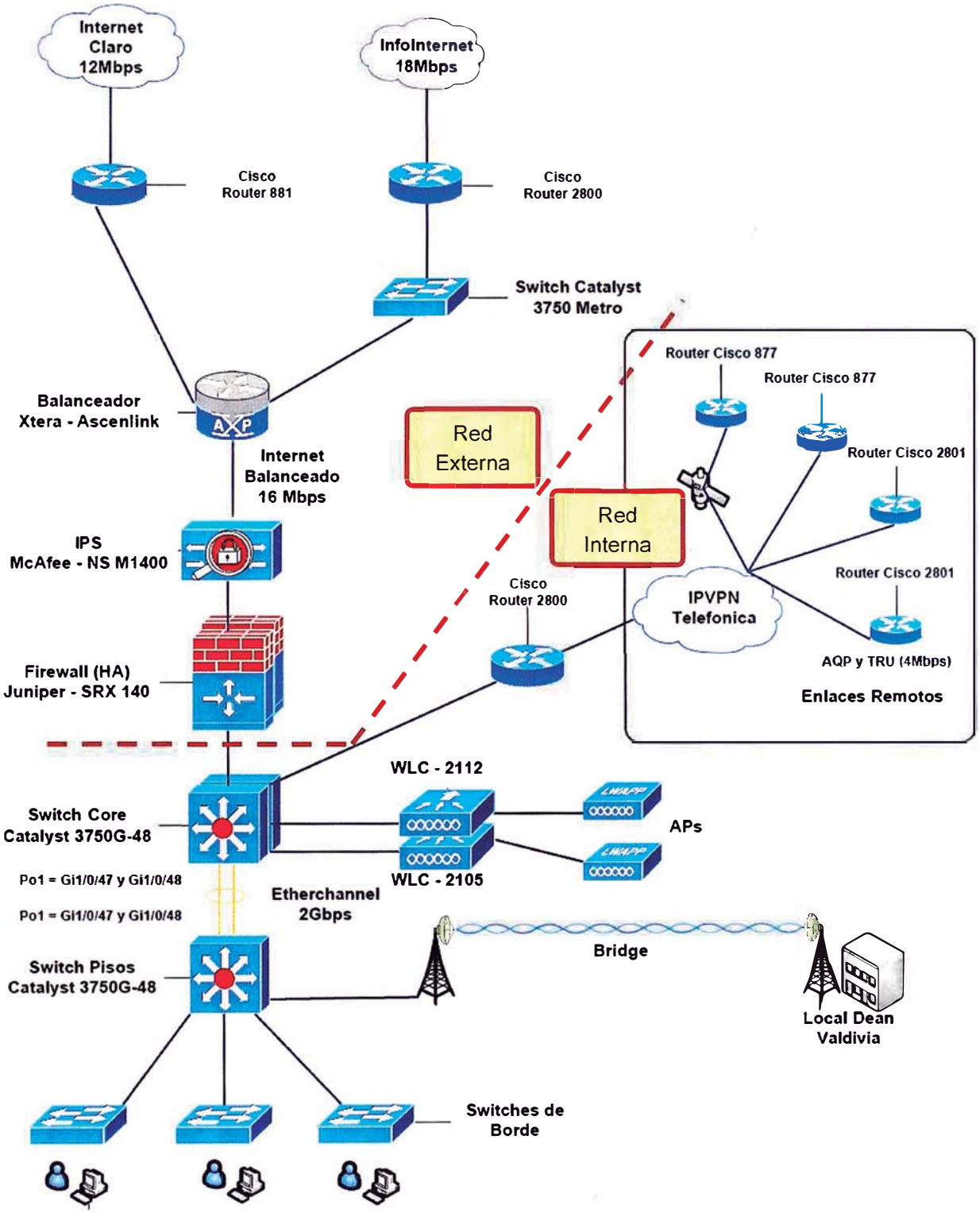

Figura 21 – Topología de red de la Empresa
Fuente: Compañía de seguros de estudio

Para la selección se toma el criterio de cuáles son los dispositivos con mayor probabilidad de interactuar con un ataque, evidentemente son aquellos que operan con transacciones de internet:

Firewall Juniper
IPS McAfee
Router de cabecera
Servidor Proxy Websense
VPN Juniper

3.5.1.4 Activos seleccionados

Como conjugación de las tres alternativas seleccionamos los siguientes activos tecnológicos, a su vez definimos la criticidad de las mismas en base al conocimiento propio del personal de tecnología, el cual se puede enmarcar en el concepto de juicio de expertos (el cuadro está dividido en dos partes, la segunda parte es la continuación en sentido horizontal de la primera):

Tabla 8 – Activos tecnológicos seleccionados (parte 1 del cuadro)
Fuente: Compañía de seguros de estudio

IDENTIFICACIÓN DE ACTIVOS						
No.	IP	ZONA	DESCRIPCIÓN	CRITICIDAD	CRITERIO	APLICATIVO DE NEGOCIO
1	192.168.105.1	LAN	Router Cisco Arequipa	Alto	I, D	-
2	192.168.120.1	LAN	Router Cisco Trujillo	Alto	I, D	-
3	192.168.121.1	LAN	Router Cisco Cusco	Alto	I, D	-
4	192.168.122.1	LAN	Router Cisco Piura	Alto	I, D	-
5	192.168.110.1	Wirless	Wireless LAN	Alto	I, D	-
6	192.168.115.1	Wirless	Wireless guest	Alto	I, D	-
7	172.17.10.1	LAN	SW core gateway sede 1	Alto	I, D	-
8	172.17.18.1	LAN	SW core gateway sede 2	Alto	I, D	-
9	172.17.150.1	LAN	SW core gateway sede 3	Alto	I, D	-
10	50.0.0.28	DMZ	Juniper Netscreen VPN	Crítico	I, D	-
11	10.100.60.15	Internet	NSM McAfe (IPS)	Crítico	I, D	-
12	10.0.5.1	Internet	Firewall Juniper	Crítico	I, D	-
13	10.10.30.53	LAN	EPO McAfee	Alto	I, D	-
14	50.0.0.18	LAN	Proxy Websense	Alto	I, D	-
15	10.10.35.83	LAN	Servidor Windows	Alto	I, D	PMS
16	10.10.35.103	LAN	Servidor Windows	Alto	I	Qlikview
17	50.0.0.130	LAN	Servidor Windows	Medio	C, D	Iqsoft, VTime (Calidad)
18	50.0.0.83	LAN	Servidor Windows	Crítico	C, D, I	Visual Time
19	50.0.0.31	LAN	Servidor Windows	Alto	I, D	Domain controller, DNS
20	50.0.0.63	LAN	Servidor Windows	Alto	I, D	Domain controller, DNS
21	50.0.0.101	LAN	Servidor Windows	Crítico	C, D, I	SQL Server 2005

22	50.0.0.110	LAN	Servidor Windows	Crítico	C, D, I	Informix
23	50.0.0.74	LAN	Servidor Windows	Crítico	C, D, I	Oracle 10g
24	10.10.35.24	LAN	Servidor Windows	Crítico	I, D	Jubilare
25	50.0.0.58	LAN	Servidor Windows	Alto	I, D	SED, SPF
26	50.0.0.249	LAN	Servidor Windows	Alto	I, D	Oficina Virtual
27	50.0.0.45	LAN	Servidor Windows	Alto	C	Cotizador web

Tabla 9 - Activos tecnológicos seleccionados (parte 2del cuadro)
Fuente: Compañía de seguros de estudio

IDENTIFICACIÓN DE ACTIVOS				
No.	**PROCESO DEL NEGOCIO**	**FUNCION**	**SISTEMA OPERATIVO**	**PUBLICADO EN INTERNET**
1	Infraestructura	Infraestructura de red	Cisco IOS	No
2	Infraestructura	Infraestructura de red	Cisco IOS	No
3	Infraestructura	Infraestructura de red	Cisco IOS	No
4	Infraestructura	Infraestructura de red	Cisco IOS	No
5	Infraestructura	Infraestructura de red	Cisco IOS	No
6	Infraestructura	Infraestructura de red	Cisco IOS	No
7	Infraestructura	Infraestructura de red	Cisco IOS	No
8	Infraestructura	Infraestructura de red	Cisco IOS	No
9	Infraestructura	Infraestructura de red	Cisco IOS	No
10	Infraestructura	Seguridad perimetral	ScreenOS	Sí
11	Infraestructura	Seguridad perimetral	Windows Server 2003	No
12	Infraestructura	Seguridad perimetral	ScreenOS	Sí
13	Infraestructura	Seguridad perimetral	Windows Server 2008	No
14	Infraestructura	Seguridad perimetral	ISA Server 2006	No
15	Inversiones	Servidor de aplicación	Windows Server 2008	No
16	Comercial	Servidor de aplicación	Windows Server 2008	No
17	SQA	Servidor de aplicación	Red Hat 4	No
18	Comercial y Técnica	Servidor de aplicación	Windows Server 2003	No
19	Todos	Servidor de aplicación	Windows Server 2008	No
20	Todos	Servidor de aplicación	Windows Server 2008	No
21	Todos	Servidor de base de datos	Windows Server 2003	No
22	Todos	Servidor de base de datos	HV-UX V11	No
23	Todos	Servidor de base de datos	HV-UX V11	No
24	Rentas Vitalicias	Servidor web	Windows Server 2003	No
25	Comercial y Técnica	Servidor web	Windows Server 2003	No
26	Comercial	Servidor web	Windows Server 2008	Sí
27	Clientes	Servidor web	Windows Server 2003	Sí

3.5.2 DEFINICIÓN DE POLÍTICAS DE CORRELACIÓN

A modo de marco de referencia las políticas de correlación de la Empresa están orientadas a los "Veinte Controles Críticos para SIEM" elaborado por

el SANS Institute[10]. De estos 20 controles se han seleccionado 10, que son los que se considerarán dentro del alcance del proyecto:

Tabla 10 – Diez controles críticos según la SANS
Fuente: SANS Institute

Control Crítico	Módulo SIEM relacionado
1) Inventario de dispositivos autorizados y no autorizados	La herramienta SIEM debe utilizarse como la base de datos de inventario de la información de activos autorizados. Para cada uno de ellos referenciar su criticidad, clasificación, entre otros atributos.
2) Configuraciones seguras para los dispositivos de red	Alguna configuración incorrecta en los dispositivos de red también debe ser informada al SIEM para el análisis consolidado.
3) Mantenimiento, monitoreo y análisis de registros de auditoría	Recoger y centralizar los datos de auditoría de todas las aplicaciones inscritas en el SIEM.
4) Seguridad en las aplicaciones de software	Las vulnerabilidades que se descubran en las aplicaciones de software también deben ser reportadas al SIEM, el mismo sirve para almacenar los resultados de exploración y correlacionar la información con los datos con la red y determinar si las vulnerabilidades se explotan en tiempo real.
5) Control de usuarios con permisos de administrador	Cuando los principios de buen uso de una cuenta administradora no se cumpla (o las credenciales de acceso sean conocidas por otro usuario no autorizado) SIEM puede correlacionar los registros de acceso para detectar un evento o incidente y generar una alerta.
6) Evaluación de la vulnerabilidad continua	SIEM puede correlacionar la vulnerabilidad con la actividad real del sistema para determinar si dichas vulnerabilidades están siendo explotadas.
7) Defensas contra malware	El malware descubierto se registrará de acuerdo con este control. Las herramientas anti-malware deben reportar sus hallazgos al SIEM, ya que al estar correlacionado con otros sistemas puede determinar que activos son los de mayor exposición al riesgo.
8) Control de los puertos de red, protocolos y servicios	Si un sistema tiene un puerto, protocolo o servicio en ejecución que no haya sido autorizado, también debe ser reportado al SIEM para realizar la correlación con otros sistemas en búsqueda de posibles vulnerabilidades. La organización puede utilizar este control para determinar los puertos y servicios que son útiles para el negocio, los que no lo son se pueden restringir.
9) Control de dispositivos inalámbricos	Errores de configuración de dispositivos y las intrusiones inalámbricas deben ser reportados al SIEM, para consolidar la información y utilizarla para la correlación con la red o la detección de amenazas

[10] SysAdmin Audit, Networking and Security Institute, institución internacional que agrupa alrededor de 165 mil profesionales de seguridad con la finalidad de elaborar estándares y buenas prácticas.

	a la infraestructura inalámbrica.
10) Prevención de Pérdida de Datos	El SIEM debe poder correlacionar los eventos de pérdida de datos con el inventario o la información de activos, así como otro sistema y actividad de los usuarios para detectar las infracciones sobre los datos sensibles.

En ese sentido, y teniendo como referencia las buenas prácticas dadas por SANS, definimos las siguientes políticas de correlación:

- Tráfico entrante de internet bloqueado
  Detección de ataques zero-day
- Detección de ataques SQL injection
- Detección de ataques XSS
- Escaneo de la red interna
- Escaneo de los servicios publicados
- Ataques de fuerza bruta
- Malware detectado
- Fuga de información
- Denegación de servicio sobre aplicaciones publicadas en internet
- Accesos no autorizados a las aplicaciones
- Escalamiento de privilegios
- Spoofing de IP
- Captura de todo tipo de logs para evitar la pérdida de otros eventos

3.5.3 IMPLEMENTACIÓN CONFIGURACIÓN Y PRUEBAS

En esta fase se explicará la arquitectura de los appliance Arcsight y la configuración de los mismos para la captura de datos de forma efectiva.

Los componentes de Arcsight a implementar serán:

- ArcSight ESM v4.5: El componente será un appliance, el cual es relativamente fácil de poner en marcha en un corto período de tiempo El appliance está diseñado para ser una solución llave en mano y estar en marcha y funcionando en un corto tiempo. Uno de los beneficios a largo plazo del funcionamiento ArcSight ESM v4.5 como appliance es que no se tendrá que asignar personal para administrar los parches para el sistema operativo o realizar otras tareas de mantenimiento. El modelo y características del appliance a instalar será:

Model	E7200
Maximum EPS	5000 EPS
Sustainable EPS	3000 EPS
CPU	2 * Intel Xeon E5504 Quad Core
RAM	24GB
Storage	6 * 600GB SAS drives (RAID 10)
Network interfaces	4 * gigabit Ethernet
Power supply	Redundant

- ArcSight SmartConnectors: es la aplicación que recolecta los logs desde los mismos dispositivos. Están preconfigurados para que puedan traer y analizar adecuadamente los registros de más de 250 dispositivos. Una vez que los logs se recolectan de sus dispositivos, estos se normalizan al formato de evento común ArcSight (CEF). Esto permite que el ArcSight ESM procese los registros más rápidamente, ya que la normalización se realiza en el conector. El modelo de SmarConnector a implementar es:

Model	Maximum EPS	Cache Size
C1000	400	120GB

- ArcSight Logger: permite combinar la gestión de los logs de administración, logs de dispositivos de infraestuctura de TI y logs de eventos de seguridad. El ArcSight Logger permite la búsqueda de todos estos logs a través de consultas de querys estructurados o no estructurados. Una vez que estos registros se encuentran en el aparato Logger, puede enviar los logs necesarios para el ArcSight ESM y realizar el análisis inteligente. Este producto no es necesariamente un componente deln ArcSight ESM, pero añade una capa de gestión de registro que representa una mejora.

La arquitectura usual se puede ver en la siguiente figura:

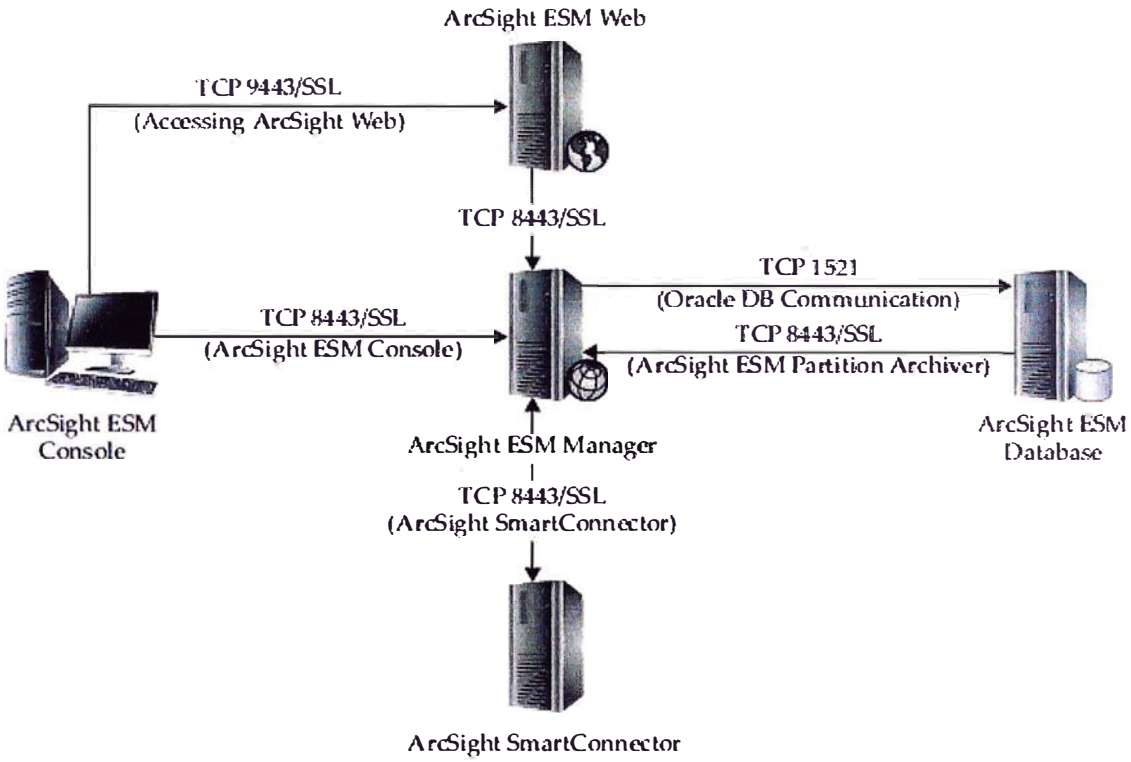

Figura 22 – Arquitectura del Arcsight ESM
Fuente: Libro Security Information and Event Management (SIEM) Implementation

3.5.3.1 CONFIGURACIÓN

En el caso del Arcsight a modo appliance consiste en definir la arquitectura dedicada a la captura de eventos de los activos seleccionados. No es una instalación propiamente dicha ya que el appliance viene listo para configurar. A continuación se muestra figura 23 que detalla la arquitectura y dispositivos sobre los cuales el Arcsight se encargará de la captura de eventos:

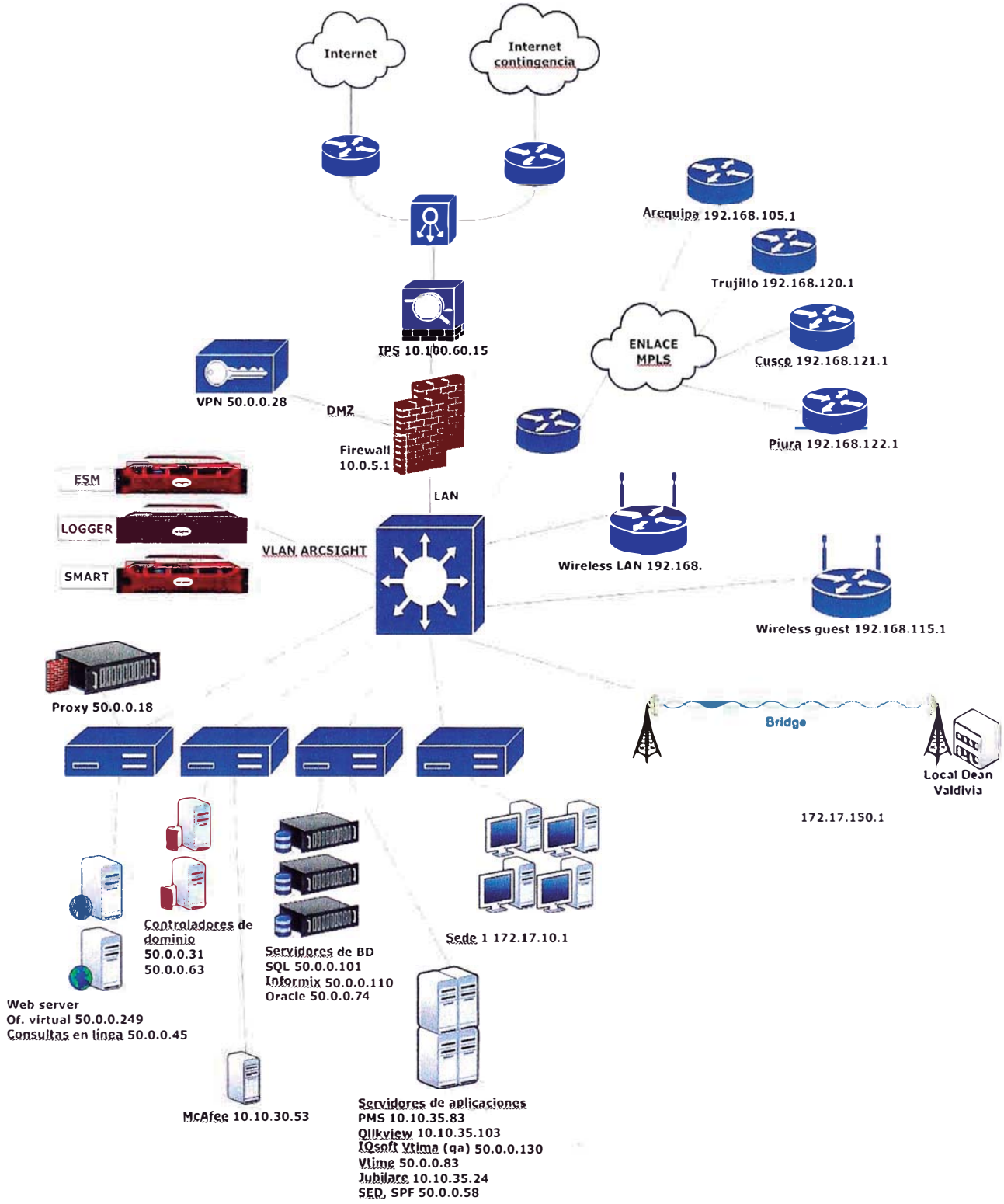

Figura 23 – Topología de red con SIEM implementado
Fuente: Compañía de seguros de estudio

En el mismo se enumeran los dispositivos con sus direcciones IP. En ese sentido, el proceso de configuración tendrá los siguientes pasos:

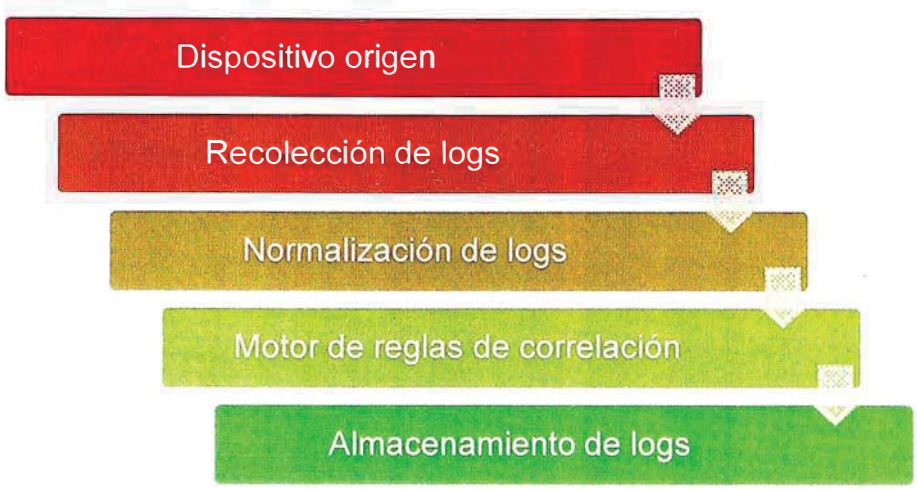

Figura 24 – Esquema de configuración del SIEM
Fuente: Elaboración propia

Recolección de logs

En el caso del Arcsight, este cuenta con agentes que se instalan en cada dipositivo quienes se encargarán de la captura y envió de logs al Logger Appliance. El método de captura de logs será *Push Log Collection,* el cual tiene la ventaja de la facilidad de instalación y configuración. Una vez instalado el agente en el dispositivo, éste se encargará de capturar el syslog y traps SNMP. Al configurar el dispositivo fuente utilizando syslog, configurar la dirección IP o el nombre DNS de un servidor syslog en su red, y el dispositivo se iniciará automáticamente el envío de sus registros a través de agente al receptor Arcsight Logger.

Hay que tener cuidado para los eventos UDP syslog en su entorno introduce algunas vulnerabilidades de seguridad que tendrá que se deben tener en cuenta al implementar el SIEM. La naturaleza inherente de utilizar syslog estándar a través de UDP significa que nunca se puede asegurar que los paquetes lleguen a su destino, ya que UDP es un protocolo sin conexión. Si se produce una situación en la red en la que la utilización es extremadamente alta, por ejemplo, cuando un virus se propaga agresivamente en toda la red, es posible que no reciba los paquetes de registro del sistema para el SIEM. Para ello el agente instalado incluye una funcionalidad que no solo reenvía los logs sino que también empaqueta las tramas UDP syslog de tal forma que al ser recibido por el Arcsight se asegure que efectivamente incluye todos los datos completos.

Otro control es que en la compañía se debe configurar y usar una comunidad SNMP propia y personalizada de versión 3, de tal forma que no

se pueda leer las tramas de forma anónima, lo cual podría incurrir en violaciones a la integridad de la data.

Normalización de logs

Los logs capturados por el agente no pueden ser enviados tal como se capturan del dispositivo, previamente se tiene que formatear en un único estándar que pueda ser utilizado por el SIEM. El hecho de cambiar todos estos diferentes tipos de registros en un solo formato se llama normalización.

Es por ello que los agentes no son iguales para cualquier dispositivo. Existe un agente diferente para cada tipo de sistema operativo, versión, base de datos, servidores web, router, firewall, etc. El agente se encarga de normalizar los logs de cada dispositivo de tal forma que el Logger lo reciba en un formato estándar.

Por ejemplo, en el firewall tenemos este tipo de log:

Priority	Hostname	Message
Local4.Info	192.168.1.1	%ASA-sys-6-605005: Login permitted from 192.168.1.18/42925 to INSIDE:192.168.1.1/ssh for user "aiel"

Figura 25 – Ejemplo de log de firewall
Fuente: Libro Security Information and Event Management (SIEM) Implementation

En un sistema operativo Windows tenemos lo siguiente:

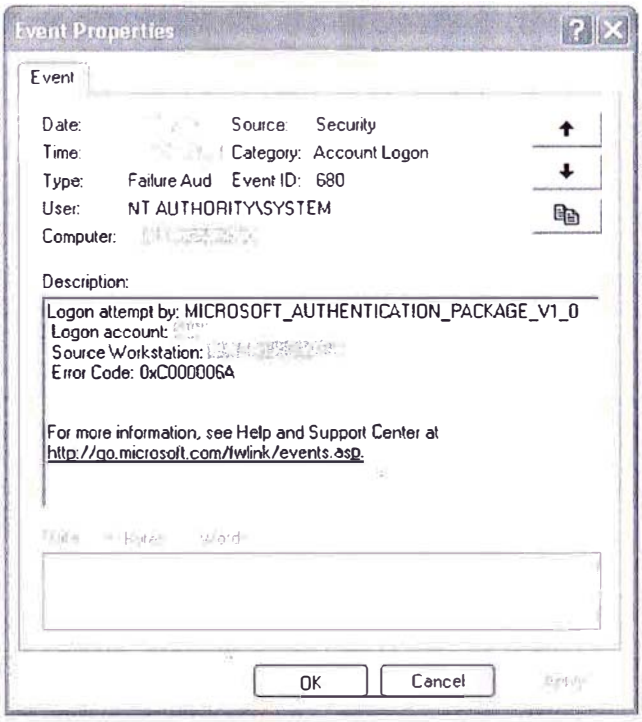

Figura 26 – Ejemplo de log de Windows
Fuente: Libro Security Information and Event Management (SIEM) Implementation

El agente se encargará de normalizar las diferentes lecturas de log a algo similar a la siguiente figura (obviamente con más datos):

Time	Date	Source Device IP Address	Event Message	Event ID
22:54:53 CST	17-Jan-10	192.168.1.1	User login	ASA-sys-6-605005
22:54:53 CST	17-Jan-10	192.168.1.18	User login	Security: 680

Figura 27 – Log normalizado
Fuente: Libro Security Information and Event Management (SIEM) Implementation

Como puede ver, los logs de diferentes dispositivos ahora se pueden leer en el mismo formato. Este es el resultado final para todos los diferentes tipos de registros que llegan al Logger, todos ellos deben ser legibles en el mismo formato. La normalización de los acontecimientos, no sólo hace que sea más fácil de leer estos registros, pero también hace que sea más fácil y permite un formato estándar de la generación de reglas.

Motor de reglas de correlación

El motor de reglas se expande sobre la normalización de eventos de diferentes dispositivos con el fin de activar las alertas en el SIEM debido a determinadas condiciones específicas en estos registros. El método de plasmar las normas SIEM generalmente comienza de manera bastante simple, pero puede llegar a ser muy compleja. Para este caso se especifican las reglas usando una lógica booleana para determinar si se cumplen las condiciones específicas y examinar de coincidencia de patrones dentro de los campos de datos.

En la figura 28 se muestra un ejemplo de regla de correlación, que también se aplicó a la presente implementación. Independientemente del sistema operativo que sea se declara una variable de "Super administrador" el cual puede tomar el valor de *administrador* para el caso de Windows Server o *root* para el caso de un servidor Linux. Esta es una única regla que identifica si un usuario que esos niveles de permisos se está logueando de forma remota, lo cual puede implicar un escalamiento de privilegios.

Figura 28 – Regla de correlación: logueo remoto de root
Fuente: Elaboración propia

Lo que el motor de correlación hace es capturar varios eventos estándar de diferentes fuentes en un solo evento correlacionado. Esto se hace con el fin de simplificar los procedimientos de respuesta a incidentes en la empresa, mostrando un solo evento que se desencadenó en múltiples eventos de diversos dispositivos.

En la figura 29 se muestra múltiples eventos de inicio de sesión que llegan al SIEM durante un período de 10 segundos. Al observar esto, se puede ver las fallas de inicio de sesión y logueos exitosos de varias fuentes a varios destinos. Se puede observar que los logueos fallidos se originan desde una IP determinada, la 192.168.1.200. Esto podría ser un intento de fuerza bruta contra ese servidor de destino.

Time	Event Number	Source	Destination	Event
10:10:01 CST	1035	192.168.1.200	10.10.10.25	Failed login to server
10:10:02 CST	1036	192.168.1.90	10.10.10.21	Successful login to server
10:10:03 CST	1037	192.168.1.200	10.10.10.25	Failed login to server
10:10:04 CST	1038	192.168.1.91	10.10.10.35	Failed login to server
10:10:05 CST	1039	192.168.1.10	10.10.10.2	Successful login to server
10:10:06 CST	1040	192.168.1.10	10.10.10.3	Successful login to server
10:10:07 CST	1041	192.168.1.200	10.10.10.25	Failed login to server
10:10:08 CST	1042	10.10.10.54	192.168.1.201	Failed login to server
10:10:09 CST	1043	10.10.10.34	192.168.1.10	Failed login to server
10:10:10 CST	1045	192.168.1.200	10.10.10.25	Successful login to server

Figura 29 – Captura de evento en el SIEM
Fuente: Libro Security Information and Event Management (SIEM) Implementation

Para casos reales, con herramientas de hacking no se tienen 10 intentos cada segundo, sino que pueden llegar a 100 intentos de login por segundo. Recolectar manualmente esta información es prácticamente imposible. El SIEM implementado se encarga de eliminar toda la información relacionada en los logs y sólo se da un seguimiento de los eventos específicos que podrían indicar que un evento malicioso propagado a través de múltiples intentos fallidos de login.

En la figura 30 se muestra la lógica de funcionamiento del SIEM: Agrupa los eventos individuales, que pueden formar parte de un incidente malicioso, en un solo evento mostrado en la consola del Arcsight. Así, en lugar de tener que buscar a través de diversos logs la relación entre los eventos, se utiliza la lógica del SIEM para identificar la acción correlacionada.

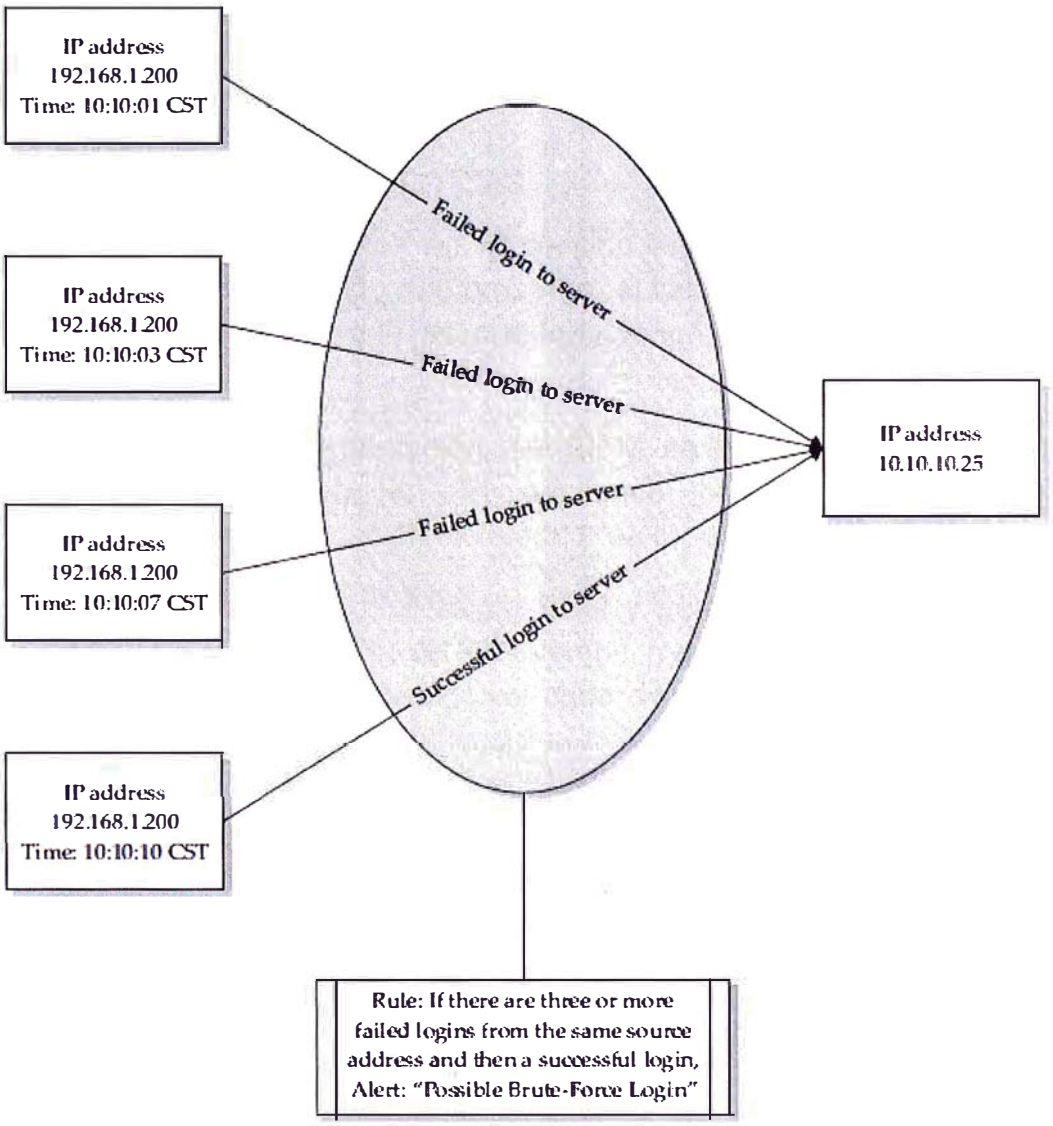

Figura 30 – Evento de correlación
Fuente: Libro Security Information and Event Management (SIEM) Implementation

Tomando como referencia la figura 28, a nivel de pseudocódigo la lógica es la siguiente:

If [(Login fallidos >= 3) and then (Login exitoso)] from Mismo origen en 20 seconds = Posible ataque de fuerza bruta.

Almacenamiento de logs

En Arcsight existen tres maneras en que el SIEM puede almacenar sus registros: en una base de datos, un archivo de texto plano, o un archivo binario. Para el caso de esta empresa se eligió el almacenamiento en archivos binarios. La ventaja es que el espacio consumido en disco es mucho menor que el método de almacenamiento de base de datos y archivos de texto, sin embargo, este tipo de logs solo puede ser leído desde la misma consola del Arcsight ya que es un formato propietario y potenciado para su arquitectura.

3.5.4 AFINAMIENTO DE POLÍTICAS

Con las actividades descritas en la sección anterior ya se tiene el SIEM correctamente implementado. Sin embargo, el valor real de esta herramienta consiste en el provecho que se puede obtener al afinar las políticas de correlación.

En esta etapa de implementación del SIEM se trabaja con los registros almacenados en el Logger. El appliance brinda una consola de administración, como aplicación instalada o de modo web.

Esta interfaz corresponde al Arcsight ESM y permitirá al administrador de seguridad una vista completa de los eventos. Ya no se tendrá la necesidad de consultar directamente los logs de cada dispositivo. El SIEM permite la visualización y el análisis de todos estos diferentes registros de forma más fácil debido a que el SIEM normaliza los datos. En la consola también será posible modificar las reglas de correlación. Para este caso, el Arcisght cuenta con una serie de políticas optimizadas para su captura y análisis, esta facilidad se debe a que el agente normaliza los datos y es posible realizar la correlación de manera más sencilla.

Dentro de la librería de políticas del Arcsight tenemos las siguientes políticas optimizadas (figura 31):

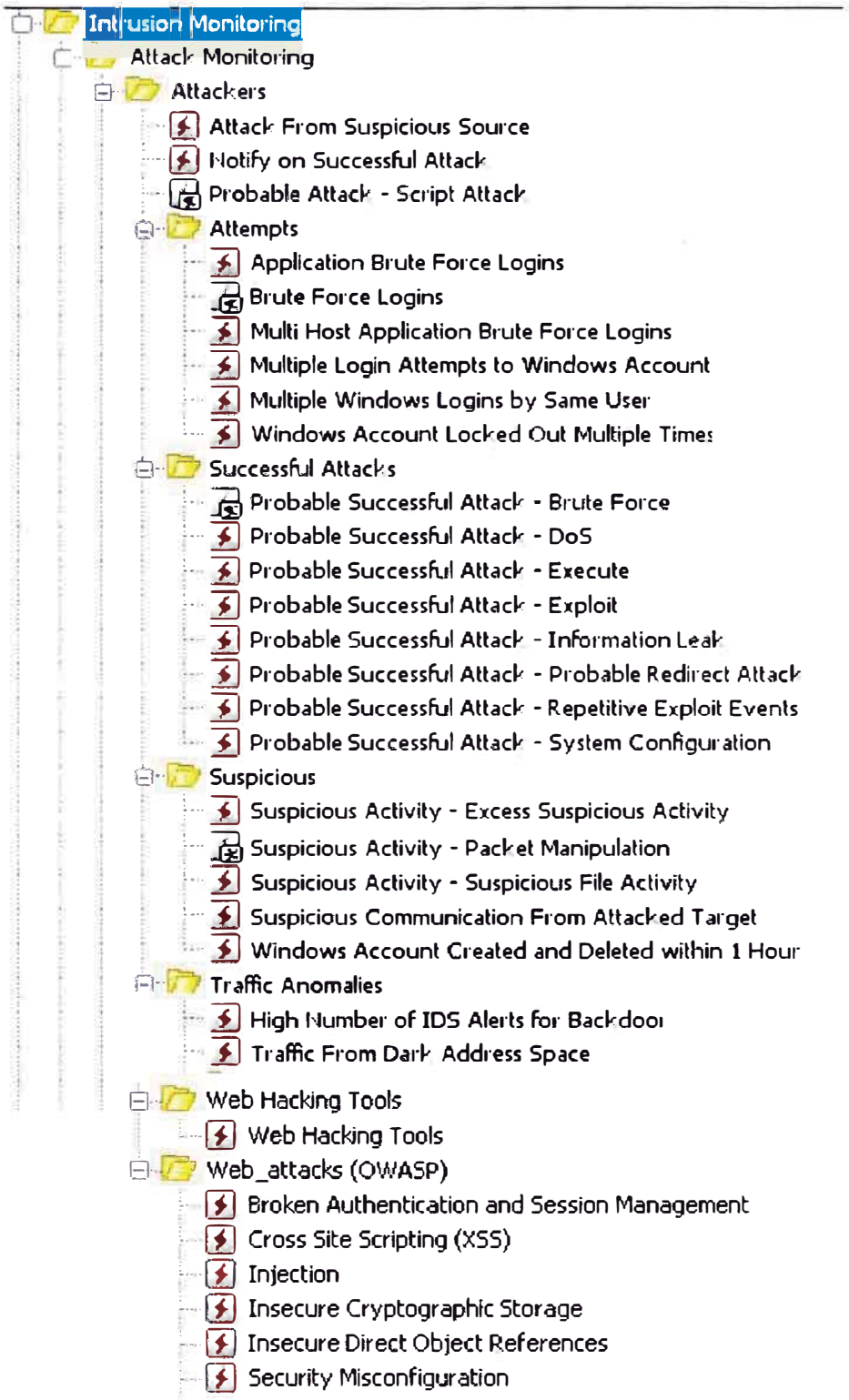

Figura 31 – Políticas de correlación predefinidas en Arcsight
Fuente: Consola de administración del Arcsight

3.5.5 DECLARACIÓN DE EVENTO DE SEGURIDAD

Los eventos de seguridad están dados por los eventos capturados, sobre los cuales se realizará el análisis.

En la figura 32 se muestra diversos eventos de cambios a nivel de sistema del servidor 192.191.254.201. Esta es la IP pública de uno de los servidores publicados en internet.

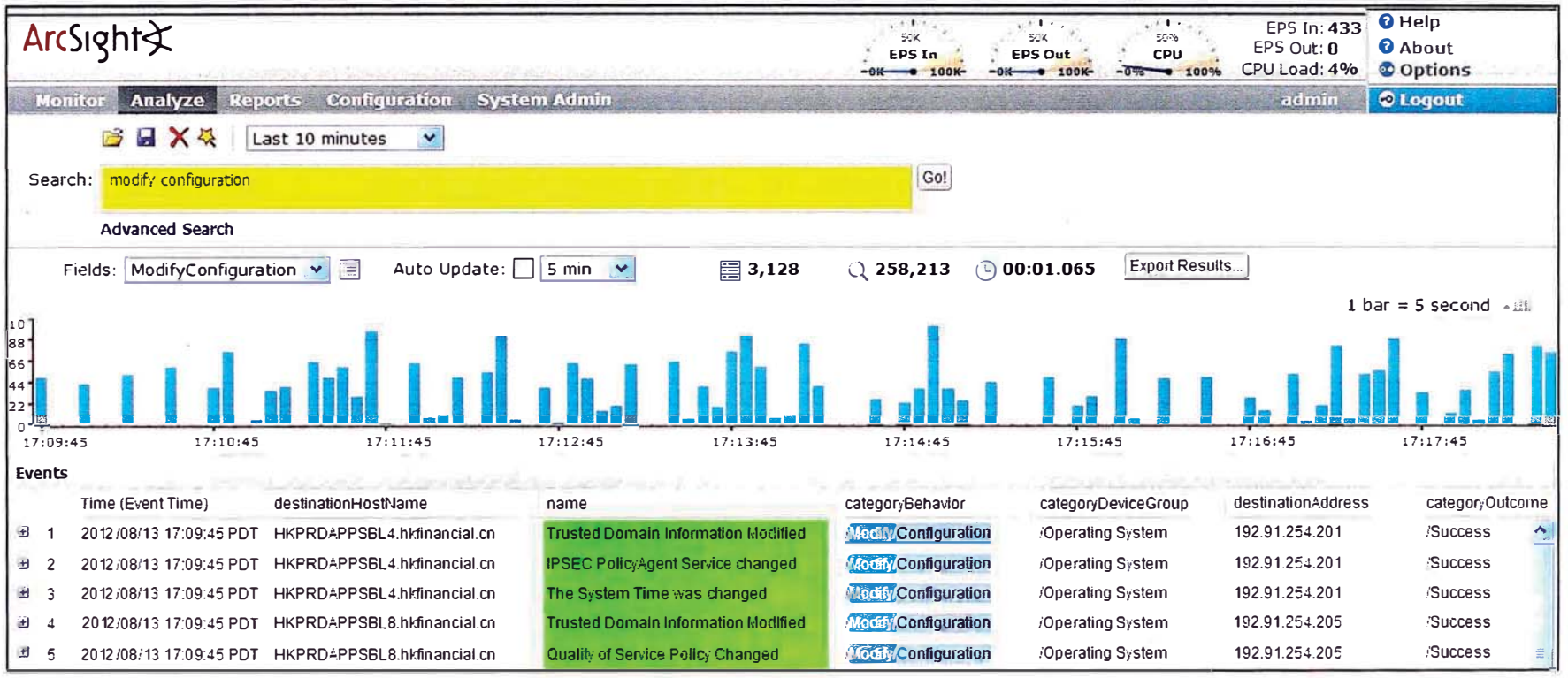

Figura 32 – Eventos de sistema leídos por el ESM
Fuente: Consola de administración del Arcsight

El siguiente cuadro muestra los eventos que el agente instalado en el firewall y servidor web envió al Logger, en el mismo se puede ver intentos de conexión, consultas con cadenas HTTP extensas, entre otros.

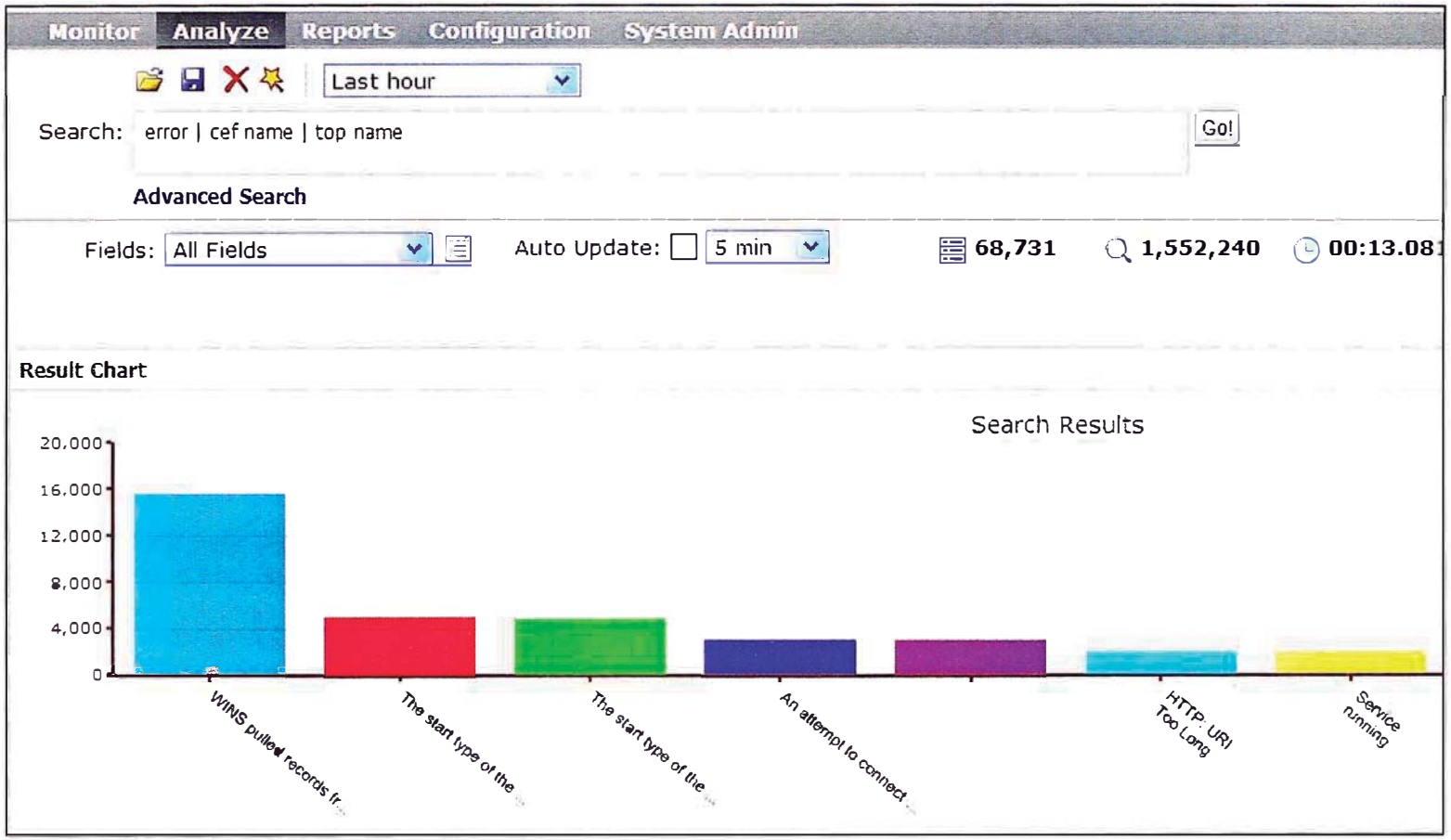

Figura 33 - Eventos en firewall y servidor web
Fuente: Consola de administración del Arcsight

En la siguiente figura muestra la captura de eventos en la base de datos.

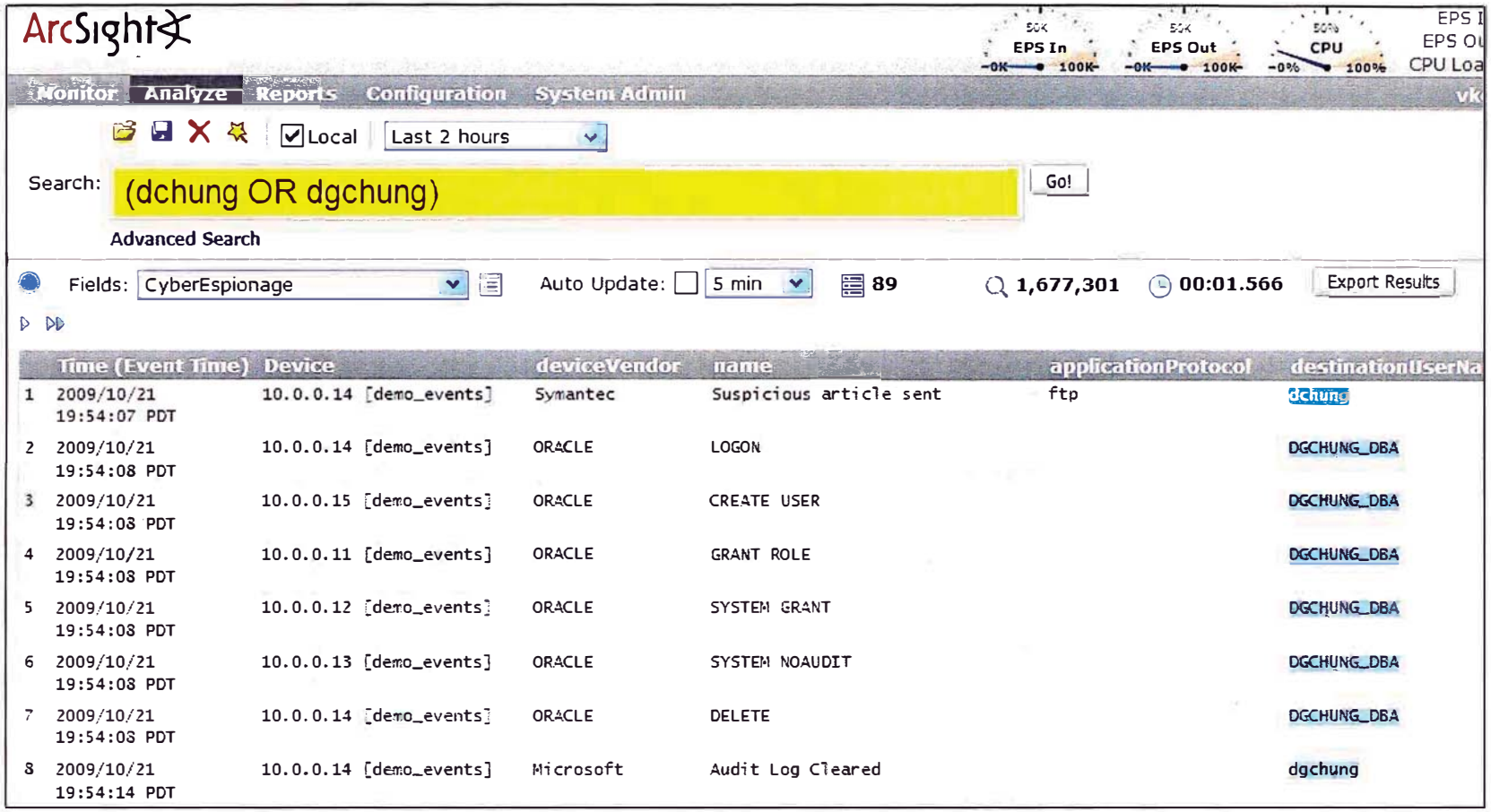

Figura 34 – Eventos en la base de datos
Fuente: Consola de administración del Arcsight

3.5.6 CRONOGRAMA DE ACTIVIDADES DE IMPLEMENTACIÓN

A continuación se presenta el cronograma de actividades que siguió la compañía, cabe resaltar que para fines de otros entornos los tiempos dependerán de la cantidad de recursos a utilizar y el nivel de detalle de afinamiento que se requiera dar a la herramienta SIEM. Para este caso, el nivel de detalle de afinamiento es medio (de una escala, bajo, medio, alto) y se utilizaron 5 recursos, uno dedicado al 100% y los otros cuatro dedicados a un 50%. Asimismo, los días están especificados en días laborales.

Tabla 11 – Cronograma de actividades
Fuente: Compañía de seguros de estudio

CRONOGRAMA DE ACTIVIDADES		
ID	**ACTIVIDAD**	**DURACIÓN**
1	**Desarrollo del proyecto**	**91 días**
2	**Inventariar los activos críticos de TI**	**20 días**
2.1	Identificar criticidad de activos tecnológicos	5 días
2.2	Identificar activos afectados por incidentes	5 días
2.3	Elaborar y analizar la topología de red	8 días
2.4	Definir activos seleccionados para la correlación	2 días
3	**Definir políticas de correlación**	**5 días**
4	**Implementar la herramienta SIEM**	**46 días**
4.1	Elaborar topología de red con todos los equipos implementados	3 días
4.2	Rackear los appliance	5 días
4.3	Instalar los agentes en los equipos elegidos	20 días
4.4	*Configurar la herramienta*	*18 días*
4.4.1	Definir método de recolección de logs	2 días
4.4.2	Normalizar los logs	3 días
4.4.3	Definir reglas de correlación	10 días
4.4.4	Configurar método de almacenamiento de logs	3 días
5	**Afinar políticas de correlación**	**10 días**
6	**Mostrar resultados de las políticas**	**5 días**
7	**Feedback del proyecto**	**10 días**

CAPÍTULO IV

RESULTADOS

4.1 BENEFICIOS CUALITATIVOS

4.1.1 RESULTADO LOGRADO

La implementación de la herramienta SIEM permitió tener una visibilidad completa de los eventos y potenciales incidentes de seguridad de la información. El detalle de los resultados fue parte de los indicadores del área. Algunos de ellos se muestran a continuación:

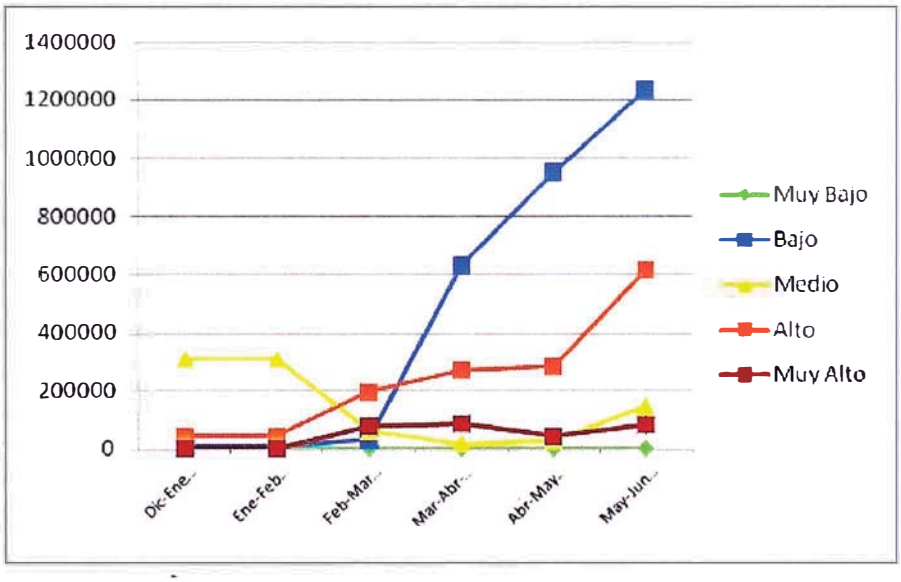

Figura 35 – Evolución de eventos detectados
Fuente: Compañía de seguros de estudio

Tabla 12 – Tipos de eventos detectados
Fuente: Compañía de seguros de estudio

ID	Name	Category/Technique	Sum	%
1	High Number of Denied Connections for A Source Host		204857	64%
2	Possible Outbound Network Sweep		46439	15%
3	Multiple Login Attempts to Windows Account		12388	4%
4	Probable Successful Attack - Execute	/Brute Force	9430	3%
5	Suspicious Communication From Attacked Target		8749	3%
6	Firewall - Network Port Scan	/Scan/Port	8583	3%
7	A privileged service was called.	/Brute Force	8430	3%
8	Compromise - Attempt		5147	2%
9	Firewall - Application Protocol Scan	/Scan/Service	3995	1%
10	Firewall - Pass After Repetitive Blocks		3120	1%
11	Firewall - Host Port Scan	/Scan/Port	2644	1%
12	Brute Force Logins	/Brute Force/Login	2382	1%
13	The Password Policy Checking API was called.	/Brute Force	1193	0%
14	Insecure Direct Object References	/Insecure Direct Object References	999	0%
15	Firewall - Repetitive Block - In Progress	/Brute Force	833	0%

En líneas generales se logró lo siguiente:

- Identificación de causas raíces de los incidentes que afectaron la empresa.
- Identificación de una mayor cantidad de eventos debido a que la herramienta tiene una gran cantidad de políticas predefinidas. Algunas de ellas pueden corresponder a eventos que no afectaron o afectaron de manera silenciosa.
- Detección en línea de eventos de fuga de información.
- Detección de ataques SQL Injection, ya que el servidor web y la base de datos se encuentran correlacionadas es posible saber desde que IP se

realizó el ataque y bajo que patrones (por ejemplo 30 consultas por minuto con el SQL map[11]).

- Contar con evidencias para las auditorías. Permitió dar respuestas a la sección de gestión de incidentes lo cual representó un ahorro ante una posible multa de la SBS. A nivel de Auditoría Interna también se pudo dar una respuesta de manera rápida y precisa.

4.2 BENEFICIOS CUANTITATIVOS

4.2.1 EVALUACIÓN COSTO BENEFICIO

Para determinar el beneficio económico se elaboró un flujo de caja. El detalle se muestra a continuación:

Tomando en cuenta los datos de la figura 18, un gasto anual de US$ 44,344.00 y una posible multa de la SBS de US$ 40,000.00. Llevando a un valor mensual, tenemos un resultado de US$ 7,028.67, esto lo representamos en el flujo de caja como un ahorro ya que representa dinero que no se desembolsará.

El resultado se muestra en la Tabla 12 de la siguiente página. El valor actual neto es de US$ 6,781.31. Cabe mencionar que como todo proyecto de seguridad, este no tiene implicancias directas con los resultados financieros, su equivalente se debe traducir a nivel de riesgo, por lo cual no se puede tener el mismo análisis que otro tipo de proyectos orientados netamente a la reducción de costos o incremento de ingresos. En estos se evalúa riesgos, y regulaciones normativas.

[11] Herramienta open source de penetration testing, que automatiza el proceso de detectar y explotar los errores de inyección SQL y vulnerar los servidores de bases de datos.

Tabla 13 – Flujo de caja del proyecto
Fuente: Compañía de seguros de estudio

	Horizonte del Proyecto												
	Mes 0	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
Ahorro	$ -	$7,028.67	$7,028.67	$7,028.67	$7,028.67	$7,028.67	$7,028.67	$7,028.67	$7,028.67	$7,028.67	$7,028.67	$7,028.67	$7,028.67
Egresos	$ 50,000.00	$2,000.00	$2,000.00	$2,000.00	$2,000.00	$2,000.00	$2,000.00	$2,000.00	$2,000.00	$2,000.00	$2,000.00	$2,000.00	$2,000.00
Pago mensual de la herramienta		2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000	2,000
Flujo Periodo	**$ -50,000.00**	**$5,028.67**	**$5,028.67**	**$5,028.67**	**$5,028.67**	**$5,028.67**	**$5,028.67**	**$5,028.67**	**$5,028.67**	**$5,028.67**	**$5,028.67**	**$5,028.67**	**$5,028.67**

		Descuento mensual:	**0.95%**
VAN DEL PROYECTO	$ 6,781.31	**TIR DEL PROYECTO**	**3.02%**

4.2.2 COMPARATIVO ANTES Y DESPUÉS

Es necesario resaltar en esta parte que una herramienta SIEM permite dar una mayor visibilidad a los eventos ocurridos, por lo tanto, si anteriormente se tenía un control reactivo (pues se reaccionaba luego de ocurrido el incidente), ahora se tiene un control detectivo, es decir, el incidente no se lleva a cabo sin embargo se detecta en su estado de evento, es decir, cuando aún no hace daño a la compañía. Bajo esta observación, se presentan los siguientes cuadros:

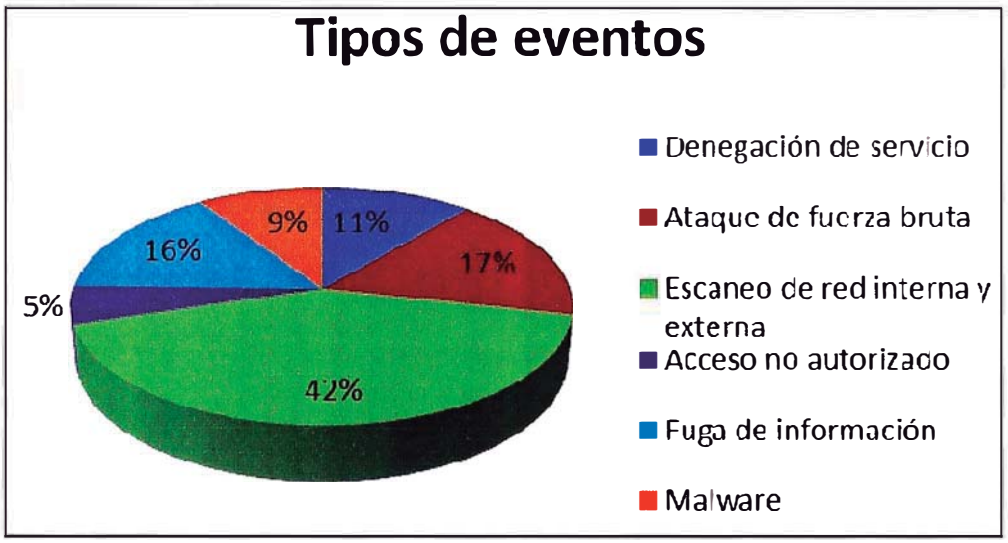

Figura 36 – Eventos de seguridad post implementación SIEM
Fuente: Compañia de seguros de estudio

Respecto a la cantidad de eventos mostrados en la figura 36, esta cifra no corresponde a la cantidad de eventos detectados por la herramienta, sino aquellos que ocasionaron una alerta. La cantidad de eventos detectados sobrepasa los cientos o miles de eventos, la cifra mostrada son sobre los cuales se debe actuar para mitigar y controlar los incidentes.

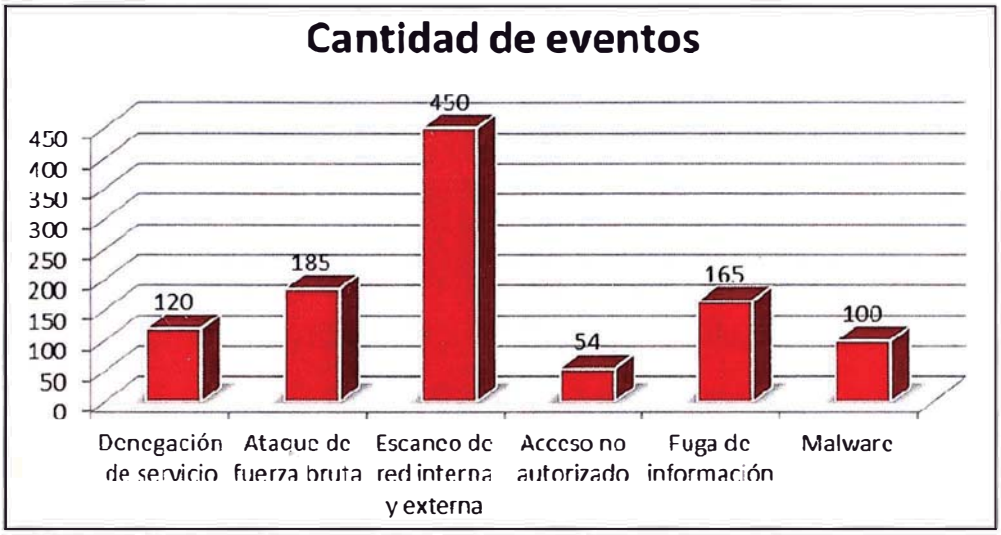

Figura 37 – Cantidad de eventos post implementación SIEM
Fuente: Compañía de seguros de estudio

El descubrimiento de los eventos permitió identificar las causas que ocasionaban los mismos, cabe resaltar que en algunos casos, una serie de eventos es ocasionada por una determinada causa. Para el caso del presente informe, los eventos de fuga de información eran ocasionados por configuración incorrecta de la autenticación en la red inalámbrica. Igualmente un filtrado débil en el firewall incrementaba el escaneo de la red.

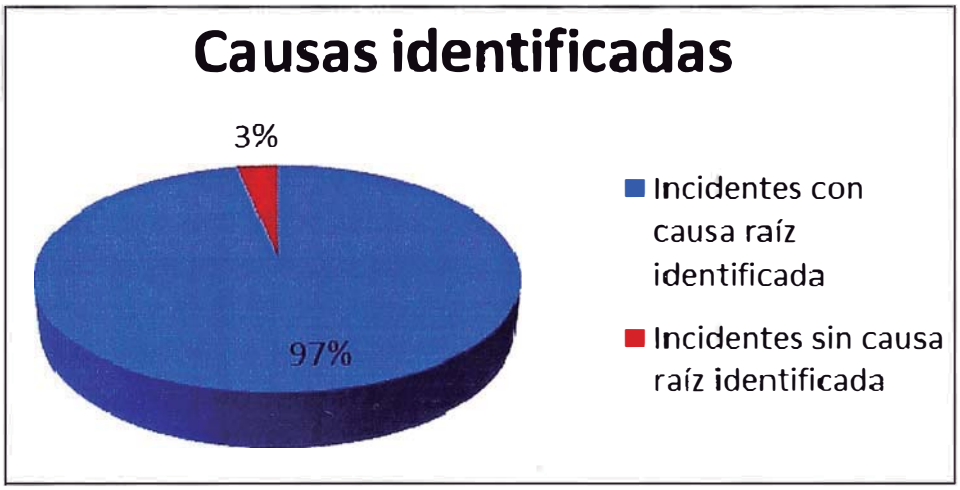

Figura 38 – Eventos con causas identificadas
Fuente: Elaboración propia

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. El contar con una metodología permitió cumplir con los tiempos asignados al proyecto de implementación.
2. La metodología utilizada permitió la implementación ordenada y mejoró la gestión de incidentes.
3. Realizar la documentación y clasificación de activos es sumamente necesario antes de implementar la herramienta. Ello facilita la configuración del inicial de las reglas de correlación.
4. Las referencias de instituciones prestigiosas como la SANS Institute son necesarias para este tipo de implementaciones. No solo se debe enfocar al alcance de los incidentes que afectaron a la Empresa, sino otros que aún no han sido realizados o que si se realizaron pero no se identifican.
5. Para la sustentar la inversión es importante contar con estadísticas de incidentes del entorno. Tanto para la cuantificación de los mismos así como la información en pérdidas económicas incurridas.
6. Es importante tener estadísticas semanales o mensuales de los eventos detectados y el nivel de criticidad de los mismos, esto con la finalidad de ver la evolución de los mismos y evaluar la eficacia de la capacidad de respuesta del personal de tecnología para la solución de incidentes.
7. Los eventos considerados críticos y altamente críticos deben ser configurados a modo de alerta para que envíe un correo al administrador de seguridad de la información, al personal responsable de la administración de los equipos y dueños del activos

RECOMENDACIONES

1. La implementación es un proceso que demora aproximadamente un par de meses. Con la finalidad de sustentar la inversión a la Gerencia se recomienda configurar determinadas reglas de correlación que ataques los incidentes actuales. Esto permitirá demostrar la efectividad de la herramienta.
2. Se recomienda tener un analista dedicado en monitorear la herramienta a tiempo parcial. No se recomienda a tiempo completo debido a la amplitud de la Empresa (entre 1000 y 2000 personas) y porque los eventos e incidentes críticos son alertados vía correo.
3. En esta implementación no se usaron todos los módulos del SIEM, en este punto se pueden recomendar dos alternativas: identificar en que proceso de Tecnología puede ayudar los módulos que no son usados o buscar una herramienta con el alcance específico de la necesidad.
4. Se puede hacer uso del ciclo de mejora continua (planear, hacer, verificar actuar) para el afinamiento de las políticas de correlación.
5. Se debe hacer partícipe a toda el área de Tecnología tanto durante todo el proceso del proyecto así como los nuevos procesos luego de la implementación. Estos nuevos procesos es el escalamiento de la notificación de incidentes para la resolución del mismo.
6. Dentro del proceso de inventario de activos se recomienda realizarlo dentro de la herramienta SIEM cuando se trate de servicios que soporte procesos de impacto moderado a alto. Esto ayudará a contar con mayor información para la detección de eventos.

BIBLIOGRAFÍA

1. El Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos – EDI (2007). Documento de Tecnología de la Información. Código de buenas prácticas de seguridad de la información NORMA TÉCNICA PERUANA NTP-ISO/IEC 17799:2007. INDECOPI. 1 – 173. Recuperado de: www.bvindecopi.gob.pe/normas/isoiec17799.pdf [Consultado el 03 de febrero del 2014]

2. TAM FOX, F. (2009). Circular SBS G-140. Superintendencia de Banca y Seguros. 1 9. Recuperado de: http://intranet1.sbs.gob.pe/IDXALL/FINANCIERO/DOC/CIRCULAR/PDF/G-140-2009.C.PDF [Consultado el 02 de febrero del 2014]

3. Marcos G. (2011), Return On Security Investments. Global Crossing. Recuperado de: http://www.slideshare.net/jarvel/rosi-return-on-security-investments-2008 [Consultado el 08 de marzo del 2014]

4. Gómez Vieites. A (2007) Seguridad de la Información. Wikipedia. Recuperado de http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n [Consultado el 05 de febrero del 2014]

5. 2014 - Seguridad informática. Wikipedia. Recuperado de http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica [Consultado el 05 de febrero del 2014]

6. 2014 - Firewall. Wikipedia. Recuperado de http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica) [Consultado el 05 de febrero del 2014]

7. 2014 - IPS. Wikipedia. Recuperado de http://es.wikipedia.org/wiki/Sistema_de_prevenci%C3%B3n_de_intrusos [Consultado el 05 de febrero del 2014]

8. 2013 - Microsoft Technet. Active Directory. Recuperado de http://support.microsoft.com/kb/196464/es [Consultado el 10 de febrero del 2014]

9. Castelli M. (2001) *Cisco Network Consultants Handbook*. Estados Unidos. Indiana: Editorial Cisco Press.

10. Tarala J. (2011). Implementing the 20 Critical Controls with Security Information and Event Management (SIEM) Systems. Sans Institute Whitepaper. Recuperado de https://www.sans.org/reading-room/analysts-program/siem-systems-arcsight
[Consultado el 08 de marzo del 2014]

11. Miller D., Harris S., Harper A., VanDyke S., Blask C. (2011). *Security Information and Event Management (SIEM) Implementation*. Chicago. Editorial Mc Graw Hill.

12. Chaitanya Thota K. (2003). *Hackers' Network Security Handbook*. California: Editorial Netsec.

13. Chuvakin A. (2009). Implementing and Running SIEM. Security Warrior Consulting. Recuperado de http://www.slideshare.net/anton_chuvakin/siem-st-andrews-2009-rel
[Consultado el 05 de marzo del 2014]

14. Voorhes J. (2007). *Distilling Data in a SIM: A Strategy for the Analysis of Events in the ArcSight ESM*. SANS Institute. Recuperado de http://www.sans.org/reading-room/whitepapers/detection/distilling-data-sim-strategy-analysis-events-arcsight-esm-1916
[Consultado el 05 de marzo del 2014]

15. Science Applications International Corporation Common Criteria Testing Laboratory (2012). ArcSight ESM Version 4.5 SP3 Patch 2 Security Target ArcSight, an HP Company. Recuperado de https://www.commoncriteriaportal.org/files/epfiles/st_vid10423-st.pdf
[Consultado el 06 de marzo del 2014]

16. Sadowsky G. Dempsey J., Greenberg A., Mack B., Schwartz A. (2003). Information Technology Security Handbook. Washington: Editorial Infodev

17. Verry J. (2009). SIEM: 5 Best Practices for Implementation Success. Pivot Point Security. Recuperado de http://www.pivotpointsecurity.com/siem-5-best-practices-for-implementation-success

[Consultado el 18 de febrero del 2014]

18. Rothke B. (2011). Security Information and Event Management (SIEM) Implementation. InfoSec island. Recuperado de http://www.infosecisland.com/blogview/12105-Security-Information-and-Event-Management-SIEM-Implementation.html
[Consultado el 18 de febrero del 2014]

GLOSARIO

- *SQL Injection:* es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación (por lo general aplicación web) en el nivel de validación de las entradas para realizar consultas a una base de datos.
- *XSS (Cross site scripting):* es un tipo de inseguridad informática típico de las aplicaciones Web, que permite a una tercera parte inyectar en páginas web vistas por el usuario código JavaScript o en otro lenguaje script similar (ej: VBScript), evitando medidas de control como la Política del mismo origen.
- *DDoS (Denegación de servicio distribuido):* es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.
- *Man-in-the-middle:* es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.
- *Malware:* es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.
- *Ataques zero-day:* es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que, por lo general, son desconocidas para la gente y el fabricante del producto. Esto supone que aún no hayan sido arregladas. Este tipo de exploit circula generalmente entre las filas de los potenciales atacantes hasta que finalmente es publicado en foros públicos.
- *Ataques de fuerza bruta:* se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.
- *Spoofing:* hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

- *Escalamiento de privilegios:* consiste en conseguir permisos de administrador en un equipo tecnológico, ya sea por una vulnerabilidad o consiguiendo la clave del administrador.
- *Store procedure:* es un programa (o procedimiento) el cual es almacenado físicamente en una base de datos. La ventaja de un procedimiento almacenado es que al ser ejecutado, en respuesta a una petición de usuario, es ejecutado directamente en el motor de bases de datos, el cual usualmente corre en un servidor separado.
- *Escaneo de puertos:* acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por un firewall.
- *Referencia directa a objetos insegura:* ocurre cuando un programador expone una referencia hacia un objeto interno de la aplicación, tales como un fichero, directorio, registro de base de datos, o una clave tal como una URL o un parámetro de formulario Web. Un atacante podría manipular este tipo de referencias en la aplicación para acceder a otros objetos sin autorización, a menos que se aplique un control de accesos como medida de prevención.

ANEXOS

ANEXO 1

Según el cálculo de la empresa Global Crossing.

- Rehacer: reponer el servidor, recuperar la data perdida, realizar el análisis forense.
- Mitigar: contener el incidente de forma reactiva en el momento que se está ejecutando.
- Implementar: dar una solución posterior luego de mitigado el incidente.
- Indisponibilidad: pérdida de disponibilidad del servicio.
- Las horas son el tiempo de los analistas en realizar los trabajos, en el caso de indisponibilidad es el tiempo que el servicio no está disponible.
- El costo promedio del analista es de US$ 8 la hora, en algunos casos se necesitan dos analistas. En el caso de algún especialista el costo es de US$ 10 la hora. Para los casos de indisponibilidad se interpreta el dinero perdido durante las horas que no está disponible el sistema o las horas muertas del personal que no pueden usar el servicio.

Denegación de servicio	Horas	Costo	Total
Rehacer	10	16	160
Mitigar	2	8	16
Implementar	10	16	160
Indisponibilidad	15	100	1500
Costo total por incidente			1836
Incidentes promedio en un año			4
Costo total anual por incidente			**7344**

Ataque de fuerza bruta	Horas	Costo	Total
Rehacer	40	10	400
Mitigar	1	8	8
Implementar	10	8	80
Indisponibilidad	5	50	250
Costo total por incidente			738
Incidentes promedio en un año			5
Costo total anual por incidente			**3690**

Escaneo de red interna y externa	Horas	Costo	Total
Rehacer			0
Mitigar	5	10	50
Implementar	5	10	50
Indisponibilidad			0
Costo total por incidente			100
Incidentes promedio en un año			8
Costo total anual por incidente			**800**

Acceso no autorizado	Horas	Costo	Total
Rehacer	20	20	400
Mitigar	1	10	10
Implementar	10	10	100
Indisponibilidad	5	3000	15000
Costo total por incidente			15510
Incidentes promedio en un año			1
Costo total anual por incidente			**15510**

Fuga de información	Horas	Costo	Total
Rehacer			0
Mitigar	10	10	100
Implementar	4	2500	10000
Indisponibilidad			0
Costo total por incidente			10100
Incidentes promedio en un año			1
Costo total anual por incidente			**10100**

Malware	Horas	Costo	Total
Rehacer	50	8	400
Mitigar	10	10	100
Implementar	50	8	400
Indisponibilidad	4	1500	6000
Costo total por incidente			6900
Incidentes promedio en un año			1
Costo total anual por incidente			**6900**

ANEXO 2:

El siguiente cuadro es una muestra de la matriz de inventario de activos de información, es el primer paso para realizar el análisis de riesgos, para este ejemplo se detalla algunos activos identificados en la Gerencia Técnica:

Tabla 14 – Inventario de Activos
Fuente: Compañía de seguros de estudio

Gerencia	Proceso	Activo	Tipo	Descripción	Clasificación	Impacto				Propietario		Custodio		Frecuencia de Uso
						Confidencialidad	Integridad	Disponibilidad	VALOR	Nombre	Cargo	Nombre	Cargo	
Gerencia Técnica de Negocios	Gestión de Prevención	Asistentes de Emision de ONP	Recurso Humano	Colaboradores del área que reciben la información del cliente. Son el punto de atención del cliente.	**USO INTERNO**	Menor	Mayor	Mayor	**Mayor**	Alfonso Lizarraburu	Gerente Técnico de negocios	Maria Pia Cabrejos	Gerente Gestión Humana	Alta
Gerencia Técnica de Negocios	Gestión de Prevención	Base de datos Registro de ventas	Información electrónica	Excel con la información de todos los clientes de ONP y reasaeguros. Es importante la integridad de esta información, la ONP podría sancionarlos.	**PÚBLICA**	Menor	Mayor	Mayor	**Mayor**	Alfonso Lizarraburu	Gerente Técnico de negocios	Sergio Angulo	Apoderado de Prevención de Riesgos	Alta
Gerencia Técnica de Negocios	Gestión de Prevención	Matriz de información por trabajador	Información electrónica	Para la parte minera se realizan verificaciones del empleado con esta información. Indica que grado de menoscabo tienen los trabajadores.	**CONFIDENCIAL**	Mayor	Mayor	Mayor	**Mayor**	Alfonso Lizarraburu	Gerente Técnico de negocios	Sergio Angulo	Apoderado de Prevención de Riesgos	Alta
Gerencia Técnica de Negocios	Gestión de Prevención	Entregables a la ONP	Información electrónica	Archivos electrónicos que se envían a la ONP para que generen el pago.	**USO INTERNO**	Moderado	Moderado	Mayor	**Mayor**	Alfonso Lizarraburu	Gerente Técnico de negocios	Sergio Angulo	Apoderado de Prevención de Riesgos	Media

Como segunda parte se tiene la matriz de riesgos, en donde por cada activo de información identificado se evalúan distintos escenarios de riesgos, por cada uno de ellos se determina el nivel de riesgo neto para luego especificar los controles y determinar el valor del riesgo residual.

Tabla 15 – Matriz de riesgos
Fuente: Compañía de seguros de estudio

Proceso	Activo	Tipo	Escenario de Riesgo	Propiedad	Impacto Neto	Riesgo Neto	Riesgo neto por activo	Control	Eficacia del Control	Control Clave	Impacto Residual	Riesgo Residual	Riesgo residual por activo
Gestión de Prevención	Base de datos Registro de ventas	Información electrónica	La información del archivo o base de datos se dañe o pierda debido a que personas que no requieren permisos de modificación, podrían alterarlo accidentalmente.	I, D	Mayor	A	A	Procedimiento de gestión de usuarios: - Creación / autorización	A		Mayor	A	A
								Procedimiento de gestión de usuarios: - Definición de roles y perfiles	A	X			
								Procedimiento de gestión de usuarios: - Gestión de contraseñas	M				
								Procedimiento de gestión de usuarios: - Concientización en manejo de contraseñas	A				
								Procedimiento de gestión de usuarios: - Rotación / terminación de usuarios	M				
			La información del archivo o base de datos se dañe o pierda debido a un virus informático	I, D	Mayor	A		Política de Gestión de Medios Removibles	A		Mayor	A	
								Sistemas de Antivirus	A	X			
								Copias de respaldo	M	X			
								Concientización específica para código malicioso	B				
			La información del archivo o base de datos se divulgue, se pierda o sea robada, debido a que los controles para su almacenamiento son inadecuados, con	C, D	Mayor	A		Establecimiento de una política de clasificación de información	B		Menor	B	
								Definición de procedimientos para el manejo de la información en base a su clasificación	B	X			

			respecto a su nivel de sensibilidad (p.e. el archivo es altamente confidencial y el control de acceso no es estricto, o el archivo no está cifrado, o el archivo se almacena en memorias USB, iPods, etc.)											

ANEXO 3:

Flujograma del plan de respuesta de un incidente, desde el reporte hasta su mitigación:

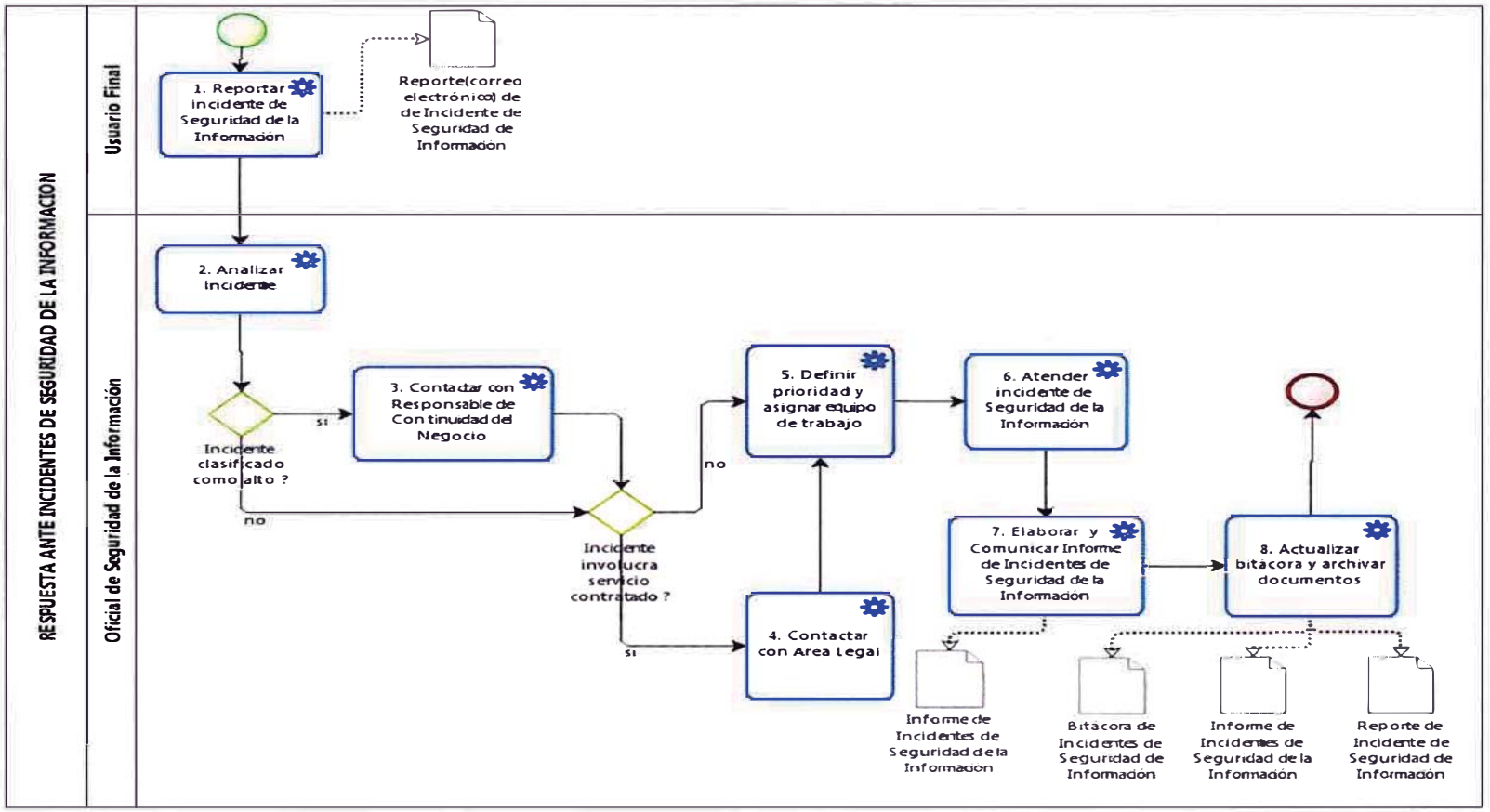

Figura 39 – Flujograma de respuesta ante incidentes
Fuente: Compañía de seguros de estudio

Flujograma de la comunicación de los resultados de los incidentes luego de la contención y mitigación realizada.

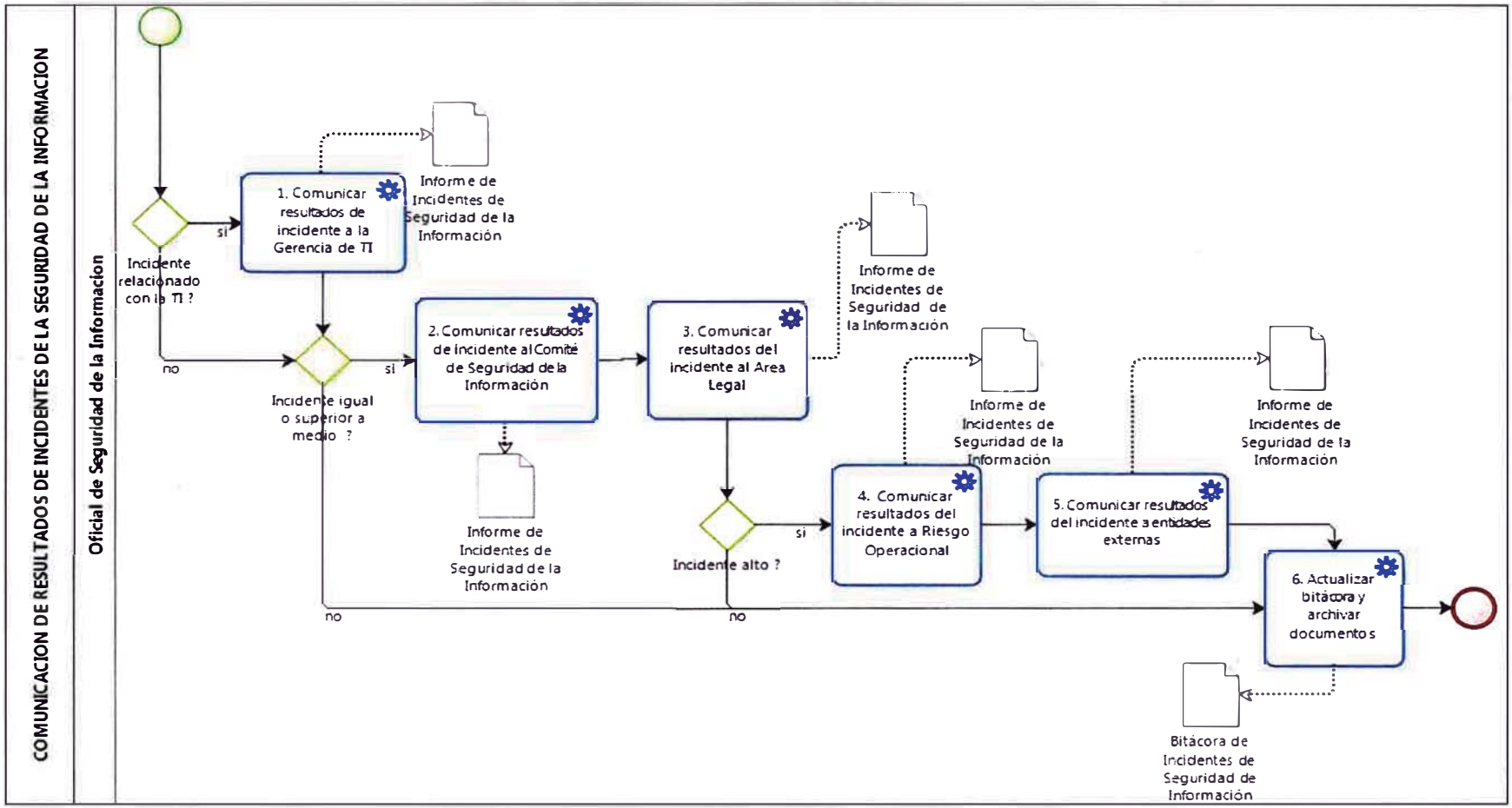

Figura 40 – Flujograma de comunicado de resultados de incidente
Fuente: Compañía de seguros de estudio

ÍNDICE DE TABLAS

INDICE DE FIGURAS