DISEÑO DE LA METODOLOGÍA PARA EL MANEJO DE INCIDENTES TI MEDIANTE FORÉNSICA DIGITAL

PROYECTO DE GRADO

MARGARITA MARIA CORRALES ARRUBLA

MARIA DEL PILAR OSORIO ALVAREZ

CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS
POSTGRADO DISTANCIA
ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS
COLOMBIA
2015

DISEÑO DE LA METODOLOGÍA PARA EL MANEJO DE INCIDENTES TI MEDIANTE FORÉNSICA DIGITAL

Presentado por:

MARGARITA MARIA CORRALES ARRUBLA

MARIA DEL PILAR OSORIO ALVAREZ

PROPUESTA DE PROYECTO DE GRADO

PROYECTO DE GRADO

CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS
POSTGRADO DISTANCIA
ESPECIALIZACIÓN EN GERENCIA DE PROYECTOS
COLOMBIA
2015

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

Introducción

El Hospital General de Medellín lleva más de 73 años dedicada a la prestación de servicios de salud de alta calidad y seguridad. Con el presente trabajo se pretende, diseñar una metodología para el manejo de incidentes en tecnologías de información mediante procesos de forénsica digital.

Dicha metodología, apoyará al Hospital General de Medellín en la examinación minuciosa de los diferentes incidentes que se presentan y afectan la seguridad de la información y por consiguiente; no permitir a personas o empresas inescrupulosas aprovecharse de ello, teniendo en cuenta que el valor más significativo para el hospital es su información.

La metodología para el manejo de incidentes en el Hospital General de Medellín permitirá coordinar y apoyar la respuesta rápida a los incidentes informáticos a través de, diversas alternativas que plantearan soluciones y propuestas de mejoramiento que se describirán a lo largo del desarrollo del trabajo, además, amplía la visión del equipo de analistas sobre las políticas y procedimientos establecidos para preservar las evidencias necesarias y así inspeccionar que la información del hospital sea confiable, integra y autentica.

Aplicar la forénsica digital en el Hospital General de Medellín es fundamental e importante en los procesos de respuesta a incidentes cuando de seguridad se trata, ya que aplicando la metodología permitirá establecer datos como el qué, quién, cuándo, cómo, y en algunos casos, el por qué de un incidente.

1. Presentación de la empresa

1.1 Breve historia del Hospital General de Medellín

El Hospital General de Medellín es una entidad de tercer nivel de atención con una categoría especial de entidad pública descentralizada de propiedad del Municipio de Medellín, con Personería Jurídica, patrimonio propio y autonomía administrativa.

Su fundación se remonta al año 1942, prestando servicios como un Centro de Atención Obstétrica. La Sociedad de Mejoras Públicas y un grupo de personas del que hacía parte la señora Luz Castro de Gutiérrez, impulsaron la idea de rendir un homenaje a las madres, como respuesta a una necesidad sentida de la comunidad, que carecía de un sitio adecuado para la atención de las mujeres a la hora de sus partos. Más tarde el Concejo Municipal de Medellín le dio vida jurídica mediante el Acuerdo 18 del 1 de agosto de 1949, con el nombre de Clínica de Maternidad del Municipio de Medellín, y posteriormente la Junta Directiva, en reconocimiento al gran esfuerzo y la labor desarrollada por doña Luz Castro de Gutiérrez, agregó el nombre de ella al que tenía la Institución.

Tras muchas décadas de lucha, el Hospital General de Medellín desarrolló una férrea voluntad de servicio, consolidándose como una institución unida al alma de la región, avanzando al paso del cambio de los tiempos y a las escalonadas demandas de la comunidad. El crecimiento, la diversificación, la investigación y una loable vocación, imprimieron el sello a los años que transcurrieron desde su fundación y enmarcaron el esfuerzo en esas épocas de transición que transcurrieron entre los años 1950 y 1990.

Después de la promulgación de la ley 100 de 1993, el Hospital General de Medellín, Luz Castro de Gutiérrez, ha venido consolidando su proceso de transformación empresarial, convirtiéndose en Empresa Social del Estado.

En desarrollo del Sistema Obligatorio de Garantía de la Calidad, en el componente del Sistema Único de Acreditación, el Hospital fue postulado entre otras instituciones, por el Ministerio de la Protección Social para el acompañamiento en el proceso de Acreditación en Salud para las IPS Públicas, convirtiéndose en el primer Hospital público del país en ser evaluado y Certificado en ACREDITACIÓN EN SALUD por el Ministerio de la Protección Social y el Icontec.

1.2 Misión

El Hospital General de Medellín es una Empresa Social del Estado que presta servicios de salud hasta la alta complejidad, centrados en la seguridad del paciente, brindando afecto, confianza, satisfacción y promoviendo el desarrollo científico, docente e investigativo así como las buenas prácticas de gestión.

1.3 Visión

El Hospital General de Medellín será para el año 2015 una institución hospitalaria que ofrecerá servicios de salud de alta calidad, innovadora, competitiva, hasta la máxima complejidad, brindando una atención excelente, oportuna, cálida y segura, con solidez científica, docente e investigativa y con rentabilidad económica y social.

1.4 Valores corporativos

- Compromiso
- Justicia
- Honestidad
- Respeto
- Responsabilidad
- Rectitud
- Seguridad
- Transparencia

1.5 Portafolio de servicios

- Cirugía
- Consulta externa
- Cuidados críticos
- Hospitalización
- Urgencias
- Obstetricia
- Laboratorio clínico y de patología
- Ayudas diagnósticas – Imagenología
- Otros servicios: central de esterilización, laboratorio de metrología
- Otros servicios de apoyo a la atención de la salud: banco de sangre y medicina transfusional, central de mezclas de nutrición parental y enteral, programa de clínica de heridas.

1.6 Área problemática

En el Hospital General del Medellín, el área de sistemas es la encargada de centralizar la información proveniente de las diferentes áreas externas a Tecnologías de la Información (TI), puesto que es ésta la fuente única de los datos y acorde a la estructura de gobierno de datos y de TI estructurado son los encargados de agrupar, auditar y verificar la fuente primaria de los datos.

La centralización de esta información se realiza por medio de la plataforma SAP (Sistemas, Aplicaciones y Productos para el procesamiento de datos) y no se pueden presentar recuperaciones parciales de información, sino que debe recuperarse la totalidad de esta, para no afectar la integridad de la información y la generación de los reportes a los entes de control gubernamentales.

2. Planteamiento del problema

El planteamiento del problema de investigación se describirá, de forma clara, precisa y completa, igualmente, se formulará la pregunta de investigación como se describe a continuación.

2.1 Descripción del problema

Los avances en el campo de la tecnología de la información son cada día más sofisticados y complejos, algo que indudablemente hace que sea más útil para las diferentes empresas, pero también la hace más vulnerable. Es esta debilidad la que permite el aprovechamiento de fallas, sea humana, procedimental o tecnológica sobre infraestructuras de procesamiento de datos, lo que ofrece un escenario perfecto para que se cultiven tendencias relacionadas con intrusos informáticos.

El campo de la forénsica digital es relativamente joven. Hace muchos años, las cortes judiciales internacionales consideraban las evidencias encontradas en los ordenadores, no muy diferentes a las evidencias convencionales. A medida que la tecnología en los ordenadores fue avanzando y mejorando se dieron cuenta que estas evidencias podían ser fáciles de corromper, destruir o cambiar.

El análisis forense involucra aspectos como la preservación, descubrimiento, identificación, extracción, documentación y la interpretación de datos informáticos, analizando, a partir de esto, los elementos que sean evidencia digital. Este tipo de evidencia es primordial para el equipo de analistas del Hospital General de Medellín, sin embargo, cuenta con algunas desventajas ya que ésta es volátil, anónima, duplicable, alterable, modificable y eliminable. Por tal motivo, dicho equipo de analistas debe tener conocimiento pleno de los procedimientos, técnicas y herramientas tecnológicas para obtener, custodiar, analizar, revisar y presentar esta evidencia. Así mismo, deben tener conocimiento de las normas legales para que las pruebas encontradas sean confiables y ofrezcan los elementos necesarios para poder inculpar a alguien.

Los ataques virtuales, delitos informáticos al igual que los delitos comunes, son analizados por grupos de analistas en forénsica digital, los cuales buscan encontrar a él o los culpables y es precisamente esto, lo que se pretende implantar en el Hospital.

En países de América Latina como México, Colombia, Chile, Argentina, Cuba, Venezuela, Brasil, Ecuador, El Salvador, Perú, Guatemala, Panamá, Paraguay, Perú, República Dominicana y Uruguay, cuentan con equipos y analistas en forénsica digital, los cuales se encargan de investigar los posibles incidentes que sean reportados. Sin embargo, en la aplicación de la forénsica digital se

presentan deficiencias en su uso, ya que existen demasiados elementos que permiten un control más avanzado y no se están adecuando a la tecnología, sólo se están limitando a instalaciones con funcionamiento básico, tales como, configuraciones estándar, verificaciones y controles periódicos, entre otras; desperdiciando así, otros beneficios que se podrían obtener a través de estas prácticas tecnológicas tan desarrolladas, como lo es la seguridad en la información y lograr un funcionamiento confiable, íntegro y autentico; es esta la necesidad que se debe cubrir en el hospital.

También se identifica, que una causa para que el manejo de la forénsica digital no se aplique en los diferentes sistemas de información, es la falta de conocimiento en los posibles beneficios que se podrían obtener para que la comunicación de los diferentes dispositivos informáticos sea segura, intacta, legitima y que esté disponible en el momento que sea necesario.

Uno de los mayores problemas del HGM es la falta de metodologías y procedimientos claros al momento de recolectar la información del incidente, como también, la carencia de estrategias que permitan identificar y sabor como gestionar los inconvenientes de este tipo que se presenten. El mayor reto que enfrentan los analistas en el HGM es encontrar y proteger cualquier evidencia, para que de esta manera, la confirmación de la misma pueda estar a salvo y se logre presentar a las autoridades competentes y sea válida, ya que si la evidencia no es manipulada con los procedimientos que exige la parte legal, es posible que no sea tomada como evidencia válida.

Una diferencia clave entre los forenses tradicionales y los digitales, es que los primeros se basan en huellas digitales, estudios de la dentadura y lo más reciente el ADN. En cambio, la evidencia digital requiere más cuidado a la hora de estar recolectando todos los datos, una documentación,

un acceso restringido a la información, y estar muy atento a la que la manipulación de las evidencias sea la correcta con el fin de preservarla. En el Hospital General de Medellín, se requiere fortalecer el manejo de la evidencia digital ya que se necesita un equipo de analistas con conocimiento especializado en el uso de la tecnología tanto en hardware como software, incluyendo varios sistemas operativos, técnicas de almacenaje de archivos, y técnicas para recuperar archivos utilizando los lineamientos establecidos.

2.2 Formulación del problema

¿Cómo diseñar una metodología, que utilice los principios de la forensita digital, para el manejo de incidentes tecnológicos de la base de información del Hospital General de Medellín?

3. Delimitación de la investigación

En este aparte, se precisará la cobertura que tiene la investigación en lo relativo a: Espacio geográfico, es decir, el lugar donde se realiza la investigación y el tiempo, especificando el periodo de tiempo en el que se realizará.

3.1 Espacial

La ubicación donde se va a realizar la investigación será para el Hospital General de Medellín.

El espacio geográfico está constituido por los sitios en los cuales se encuentra el material bibliográfico, documentos, escenarios virtuales y físicos donde se llevarán a cabo las asesorías técnicas y metodológicas, e igualmente, el espacio en donde se realizarán las entrevistas y la recopilación de casuísticas con el personal que hará uso del procedimiento para el manejo de incidentes.

3.2 Temporal

El estudio se llevará a cabo durante 7 meses iniciando en el mes de octubre de 2014 hasta mayo de 2015.

4. Justificación

Uno de los aspectos que más impacto ha generado en las sociedades es el acelerado desarrollo de la tecnología y, particularmente, de la informática. Dado tal desarrollo, la seguridad de la información se ha vuelto un asunto de vital importancia, es por esto, que surge la necesidad de resguardar la confidencialidad, la integridad y la disponibilidad de la información y además, garantizar la autenticidad de los datos, que además viene en todo tipo de formas: bases de datos, correo electrónico, archivos almacenados, entre otros.

En las empresas de hoy y particularmente en el Hospital General de Medellín, no existe un conocimiento explícito sobre la forénsica digital que permita al equipo de analistas del Hospital solucionar de manera oportuna y adecuada cualquier tipo de incidentes que se presenten. La forénsica digital entonces, es la que permitirá a los analistas encontrar evidencias digitales después de que un incidente ha ocurrido.

Las prácticas en forénsica digital han venido avanzando y armonizándose de tal forma que los profesionales de esta disciplina, consiguen cada vez resultados más confiables y tecnologías más efectivas; sin embargo, la misma dinámica de las vulnerabilidades tecnológicas y la inseguridad informática propia de los sistemas computacionales hace que día a día los esfuerzos de

homogenización de dichas prácticas reciban mensajes nuevos, que exijan repensar nuevamente la manera de cómo se adelantan las investigaciones y los análisis.

Cuando se materializó el primer gusano en Internet, diseñado por Robert Morris, en el año 1988, que aprovechándose de una falla en los sistemas de correo electrónico logró poner fuera de servicio más de 60.000 sistemas de correo electrónico en los Estados Unidos, podemos observar que la investigación subsiguiente del hecho, debió demandar un análisis detallado del protocolo de correo SMTP, largas horas de seguimiento de los mensajes entre los diferentes destinos y, sobre manera, el conocimiento de la funcionalidad del gusano creado. Para esa época probablemente las herramientas forenses disponibles no eran tan abundantes, lo que exigió de los investigadores participantes mucho ingenio, conocimiento técnico y habilidad para encontrar respuesta a los interrogantes planteados.

Con el paso del tiempo, durante los años noventa, las fallas de seguridad o vulnerabilidades se fueron especializando. El buffer overflow, los programas denominados shellcodes, el IP Spoofing, la manipulación de la pila de protocolos, particularmente de TCP/IP y la inundación de redes o sistemas de comunicaciones con altas cantidades de paquetes válidos e inválidos, fueron la constante que pusieron en alerta a todas las empresas y sus mecanismos de seguridad para identificar y contrarrestar dichas manifestaciones y tratar de mantener el “control” aparente del funcionamiento de sus infraestructura de computación y comunicaciones.

Este panorama de los años noventa fue un gran reto para los investigadores forenses; ajustar sus prácticas y procedimientos, generalmente orientados a máquinas o dispositivos específicos, y

adaptarlos a escenarios en redes donde la diversidad de sistemas operacionales, operaciones y comportamientos eran parte inherente del escenario de análisis.

Finalizando los años noventa e iniciando el nuevo milenio, nuevas formas de ataques siguieron apareciendo. Los temas orientados a la WEB, la inyección de código SQL, la suplantación de sitios web, el phishing, las fallas en las bases de datos, la manipulación de paquetes de comunicación, la ingeniería inversa como estrategia para superar medidas de seguridad y control y nuevos gusanos, ahora más elaborados y con capacidad de contagio y expansión más evidente, gracias a las conexiones vía web y los códigos ejecutables embebidos en sus páginas, muestran un panorama más exigente y más elaborado para adelantar investigaciones forenses en informática.

Los anteriores ataques descritos, son los que se han presentado desde el 2013 hasta la actualidad en el Hospital General y lo que ha llevado al personal del área de sistemas a repensar la forma en la que realizan sus actividades diarias y a adoptar las buenas prácticas que sugiere el medio para minimizar los riesgos derivados de estos ataques que afectan directamente el activo más valioso de la organización que es la información.

El Hospital consciente de la falencia de conocimiento técnico en este campo, solicitó a su aliado tecnológico UNE el apoyo para determinar una metodología apropiada para el manejo de dichos incidentes, y el adiestramiento a su personal de sistemas del conocimiento técnico de los ataques y sus implicaciones; así como simulaciones en laboratorios y ejercicios prácticos controlados, para poder detallar los hallazgos y elaborar las conclusiones necesarias que más tarde podrán servir en la aplicabilidad de los incidentes reales detectados en el seguimiento y gestión de su plataforma tecnológica.

5. Objetivos

5.1 Objetivo general

Diseñar la metodología apropiada para el manejo de incidentes en tecnologías de información mediante procesos de forénsica digital para el Hospital General de Medellín.

5.2 Objetivos específicos

- Identificar metodologías existentes en la comunidad tecnológica y científica para el manejo de los incidentes que afecten la vulnerabilidad de las tecnologías de la información a través del entendimiento y práctica de la forénsica digital.
- Analizar el estado actual de los incidentes tecnológicos presentados en el Hospital General de Medellín.
- Diseñar una metodología que permita la identificación, preservación y análisis de la información del Hospital General de Medellín.

6. Alcance

Se realizará un diseño de una metodología que permita conocer claramente las etapas o fases a llevar a cabo en el momento que ocurra un incidente en la seguridad informática a través de la forénsica digital. Igualmente, se establecerán los procedimientos a seguir después de reportado el incidente para ayudar a las áreas de negocios a continuar con sus actividades normales.

La expectativa con este documento es que se convierta en una fuente de información integral acerca de la metodología y fases necesarias para tratar incidentes de seguridad en la información a través de la forénsica digital, que describa de forma completa, detallada y clara los pasos generales para enfrentar cualquier incidente dentro de una organización. Con este material recopilado se beneficiarán empresas, investigadores y todas aquellas personas interesadas en el tema de la forénsica digital y el manejo de incidentes al tener documentación de investigación sobre esta área.

7. Referentes teóricos

A continuación se realizará una descripción detallada de cada uno de los elementos esenciales en la investigación en los que intervienen la parte histórica, teórica y legal.

7.1 Marco histórico

Un jueves por la tarde comienza a circular por Internet un nuevo ‘gusano’. Éste aprovecha una vulnerabilidad de Microsoft Windows que había sido publicada oficialmente un par de semanas atrás y que se acompañó del correspondiente ‘parche’. Se conoce que el ‘gusano’ se extiende auto-enviándose por e-mail usando todas las direcciones que encuentra en el sistema infectado. Además, está programado para generar diferentes nombres de archivos adjuntos y sus extensiones pueden variar, al tiempo que elige entre un centenar de asuntos y cuerpos de mensaje diferentes. Cuando el ‘gusano’ infecta un sistema realiza una escalada de privilegios hasta obtener derechos de administrador, realizando entonces la descarga, desde diferentes direcciones IP y vía FTP.

Su organización ya ha sufrido una infección importante por la ejecución del ‘gusano’ unas tres horas antes de que se instale la actualización del antivirus y este se encuentra activo en algunos sistemas de su red.

Ante un escenario de este tipo, se podrá realizar las siguientes preguntas:

- ¿Tiene en su organización un equipo de respuesta a incidentes como parte de su política de seguridad?
- ¿Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación?

- ¿Podría informar y justificar a sus empleados una anulación temporal de sus cuentas de correo electrónico para su investigación?
- Si el ataque de denegación de servicio distribuido está programado para atacar al servidor Web de otra organización, por ejemplo a la mañana siguiente, ¿Sería capaz de manejar una situación en la que dicha organización le pidiese responsabilidades tras detectar que el ataque se ha producido desde direcciones IP suyas?

Este tipo de situaciones no son casos aislados o anecdóticos, según un estudio realizado por la compañía centrada en soluciones de prevención de intrusiones y gestión de riesgos McAfee, revela el grado de desprotección de las organizaciones a la hora de gestionar su seguridad.

Casi la mitad de 600 ejecutivos europeos de tecnologías de la información pertenecientes a diferentes compañías, afirmaron que su infraestructura informática nunca está protegida al 100 por ciento frente a las vulnerabilidades.

La inclusión en la política de seguridad de procedimientos capaces de recibir, analizar y posteriormente responder a este tipo de incidentes, ya sean inminentes o en curso, se convierte en un componente indispensable de la infraestructura de los sistemas informáticos de la organización, puesto que los ataques a dichos sistemas no sólo han aumentado en número sino que también lo han hecho en variedad y capacidad destructiva.

7.2 Marco teórico

Organizar un equipo de respuesta a incidentes requiere establecer procedimientos y métodos de análisis que permita identificar, recuperar, reconstruir y analizar evidencias de lo ocurrido; es por

esto, que la ciencia que cubre estas necesidades es la ciencia forense. Esta ciencia aporta técnicas y principios necesarios para realizar la investigación, ya sea de tipo criminal o no.

Si esta ciencia se lleva al plano de los sistemas informáticos, hablamos entonces de "Análisis Forense Digital". Esta disciplina es relativamente nueva y se aplica tanto para la investigación de delitos "tradicionales" (homicidios, fraude financiero, narcotráfico, terrorismo), como para los propiamente relacionados con las tecnologías de la información y las comunicaciones, entre los que destacan piratería de software y comunicaciones, distribución de pornografía infantil, intrusiones y "hacking" en las organizaciones, spam, phishing, entre otros.

Se puede definir el análisis forense digital como un conjunto de principios y técnicas que comprenden los procesos de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial. Por evidencia digital se entiende el conjunto de datos en formato binario, esto es, comprender los ficheros, su contenido o referencias a éstos que se encuentren en los soportes físicos o lógicos del sistema atacado.

La mayoría de estas investigaciones se hacen por el abuso de Internet de los empleados, espionaje industrial, evaluación de daños (cuando se habla sobre un accidente), el uso no autorizado de información y datos de una empresa, ya sea accidental o intencional, fraudes criminales, casos de decepción, en general casos criminales, ya que muchos criminales guardan información importante en su computadora.

Cualquier persona que use una computadora deja a su vez un rastro. Este rastro puede revelar muchas cosas, por ejemplo qué archivos fueron accesados, cuándo y por quién; qué archivos fueron

modificados, cuándo y por quién; qué páginas de internet visitó y cuáles de ellas están capturadas en la memoria cache. El sistema operativo crea este rastro para hacer más rápido el acceso cuando se quiera volver a acceder a él. Cuando una persona utiliza el computador para cometer un crimen, todo este rastro que deja es muy importante para los investigadores ya que ésta información es muy útil. Cuando una persona cree que porque borró un archivo, se perdió todo registro y todo rastro, está muy equivocado porque la evidencia sigue ahí nada más que guardada de otra manera.

Por lo anterior, y ya que los criminales de la tecnología informática siempre dejan un rastro, la informática forense es solamente el hecho de encontrar la evidencia del incidente causado, pero encontrar la evidencia no siempre es fácil. La evolución en las tecnologías crece día con día, es por eso que los sistemas se vuelven cada vez más complicados y a veces es muy difícil encontrar a los criminales. Otro dato importante es que como las tecnologías crecen día a día, las técnicas criminales se vuelven cada vez más sofisticadas y mejor coordinadas, es por eso que a veces las investigaciones requieren mucho tiempo, una labor muy detallada y mucha dedicación y paciencia en el caso.

La informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y la protección de los datos, de una manera que se apegue a los estándares de evidencia para que puedan ser aceptadas en un proceso judicial. Es importante que estas investigaciones sean tecnológicas-legales en vez de que sean solamente tecnológicas o solamente legales ya que de esta manera se hace más eficiente la investigación.

La Informática forense sirve para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información. Consiste en la investigación de los sistemas de información con el fin de detectar

evidencias de la vulneración de los sistemas y la finalidad de la informática forense es perseguir objetivos preventivos, anticipándose al posible problema u objetivos correctivos, para una solución favorable a las que la vulneración y las infracciones ya se han producido.

Las metodologías que utiliza la informática forense incluyen la recogida segura de datos de diferentes medios digitales y evidencias digitales, sin alterar los datos de origen. Cada fuente de información se cataloga preparándola para su posterior análisis y se documenta cada prueba aportada. Las evidencias digitales recabadas permiten elaborar un dictamen claro, conciso, fundamentado y con justificación de las hipótesis que en él se barajan a partir de las pruebas recogidas.

Los objetivos de la informática forense son, la utilización de la informática forense con una finalidad preventiva, en primer término. Como medida preventiva sirve a las empresas para auditar, mediante la práctica de diversas pruebas técnicas, que los mecanismos de protección instalados y las condiciones de seguridad aplicadas a los sistemas de información son suficientes. Asimismo, permite detectar las vulnerabilidades de seguridad con el fin de corregirlas. Cuestión que pasa por redactar y elaborar las oportunas políticas sobre uso de los sistemas de información facilitados a los empleados para no atentar contra el derecho a la intimidad de esas personas.

Por otro lado, cuando la seguridad de la empresa ya ha sido vulnerada, la informática forense permite recoger rastros probatorios para averiguar, siguiendo las evidencias electrónicas, el origen del ataque (si es una vulneración externa de la seguridad) o las posibles alteraciones, manipulaciones, fugas o destrucciones de datos a nivel interno de la empresa para determinar las actividades realizadas desde uno o varios equipos concretos.

En el análisis de las cuestiones técnicas y legales de la informática forense se requiere un equipo multidisciplinar que incluya profesionales expertos en derecho de las tecnologías de la información y expertos técnicos en metodología forense. Es así porque se trata de garantizar el cumplimiento tanto de los requerimientos jurídicos como los requerimientos técnicos derivados de la metodología forense.

Las ventajas de la informática forense son evidentes: mayor facilidad en el manejo de la información, rapidez en la recolección y análisis de la misma, alta disponibilidad tanto en tiempo como en localidad. Sin embargo, las desventajas y riesgos en los que se incurre no son tan obvios: vulnerabilidad de la información a ser borrada, la fácil replicación de la información, la explotación de la información por vulnerabilidades en el sistema.

Existen varios usos de la informática forense, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática forense:

A. **Prosecución criminal:** Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
B. **Litigación civil**: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.
C. **Investigación de seguros:** La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

D. **Temas corporativos:** Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.
E. **Mantenimiento de la ley:** La informática forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

7.2.1 Fases del análisis forense digital

Dentro del análisis forense digital existen las siguientes fases, que serán desarrolladas a lo largo de esta investigación:

1. **Identificación del incidente:** esta fase comprende el proceso de identificación del incidente, que lleva aparejado la búsqueda y recopilación de evidencias.

2. **Análisis de la evidencia**: en esta fase el principal objetivo es reconstruir todos los datos disponibles la línea temporal del ataque o timeline, determinando la cadena de acontecimientos que tuvieron lugar desde el instante inmediatamente anterior al inicio del ataque, hasta el momento de su descubrimiento.

3. **Preservación de la evidencia:** en esta fase es imprescindible definir métodos adecuados para el almacenamiento y etiquetado de las evidencias.

4. **Documentación y presentación de los resultados:** tan pronto como el incidente se haya detectado, es muy importante comenzar a tomar notas sobre todas las actividades que se lleven a cabo. Cada paso dado debe ser documentado y fechado desde que se descubre el incidente hasta que finalice el proceso de análisis forense, esto le hará ser más eficiente y efectivo al tiempo que reducirá las posibilidades de error a la hora de gestionar el incidente.

Para desarrollar las fases es necesario definir otro concepto importante: INCIDENTE DE SEGURIDAD INFORMÁTICA. En principio, un incidente de este tipo se entendía como cualquier evento anómalo que pudiese afectar a la seguridad de la información, como podría ser una pérdida de disponibilidad, su integridad o confidencialidad, entre otros.

Pero la aparición de nuevos tipos de incidentes ha hecho que este concepto amplíe su definición. Actualmente, un incidente de seguridad informática puede considerarse como una violación o intento de violación de la política de seguridad, de la política de uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos.

7.2.2 Introducción a los ataques informáticos

Cualquier equipo conectado a una red informática puede ser vulnerable a un ataque.

Un ataque, es el término para describir el aprovechamiento de la vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.

Los ataques casi siempre se producen en internet o a través de una red corporativa, a razón de varios ataques por minuto en cada equipo conectado. En su mayoría, se lanzan automáticamente desde equipos infectados (a través de virus, troyanos, gusanos, entre otros.) sin que el propietario sepa lo que está ocurriendo. En casos atípicos, son ejecutados por piratas informáticos.

Para bloquear estos ataques, es importante estar familiarizado con los principales tipos y tomar medidas preventivas frente a estos. Los ataques pueden ejecutarse por diversos motivos:

- Para obtener acceso al sistema.
- Para robar información, como secretos industriales o propiedad intelectual.
- Para recopilar información personal acerca de un usuario.
- Para obtener información de cuentas bancarias.
- Para obtener información acerca de una organización.
- Para afectar el funcionamiento normal de un servicio.
- Para utilizar el sistema de un usuario como un “rebote” para un ataque.
- Para usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable.

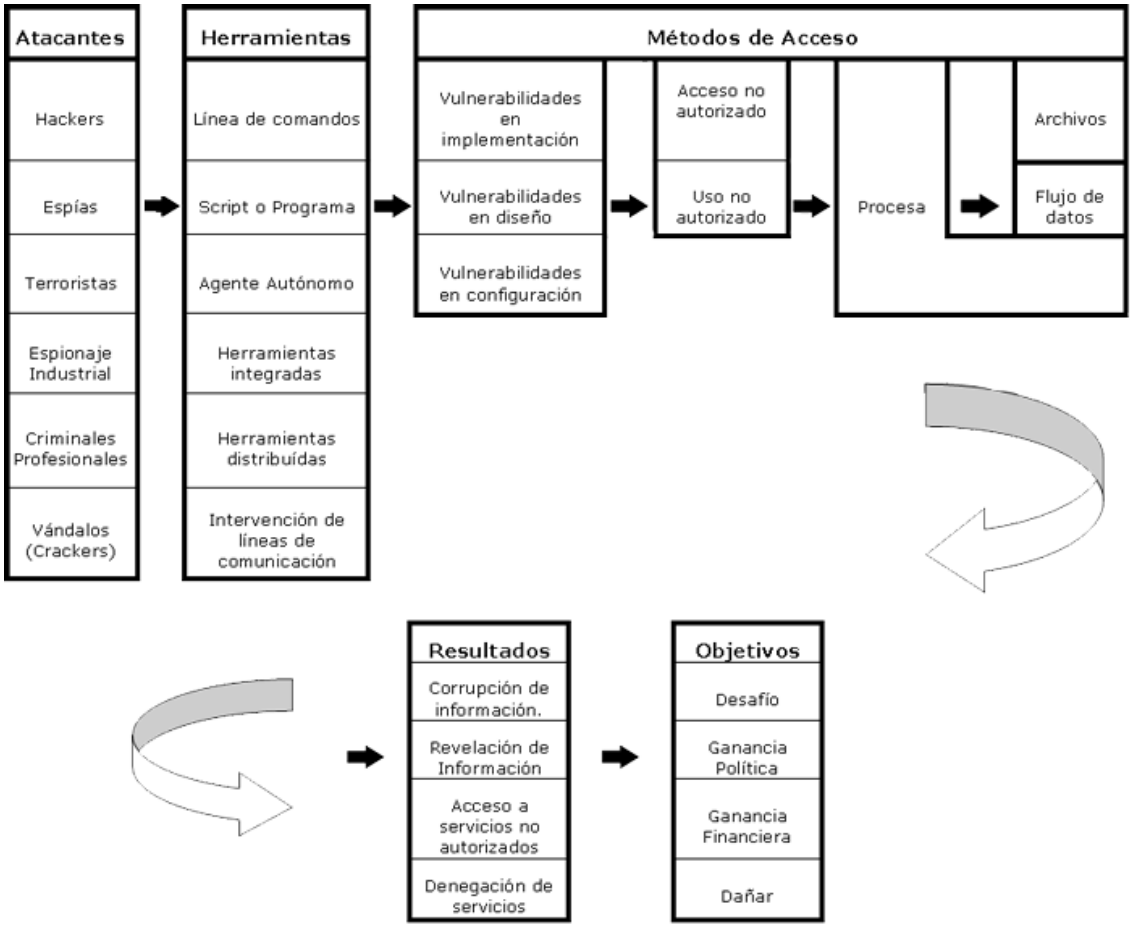


Figura 1. Tipos de ataques, resultados y objetivos.

7.2.3 Tipos de ataques informáticos

Los sistemas informáticos usan una diversidad de componentes, desde electricidad para suministrar alimentación a los equipos hasta el programa de software ejecutado mediante el sistema operativo que usa la red.

Los ataques se pueden producir en cada eslabón de esta cadena, siempre y cuando exista una vulnerabilidad que pueda aprovecharse. El esquema que figura a continuación repasa brevemente los distintos niveles que revisten un riesgo para la seguridad.

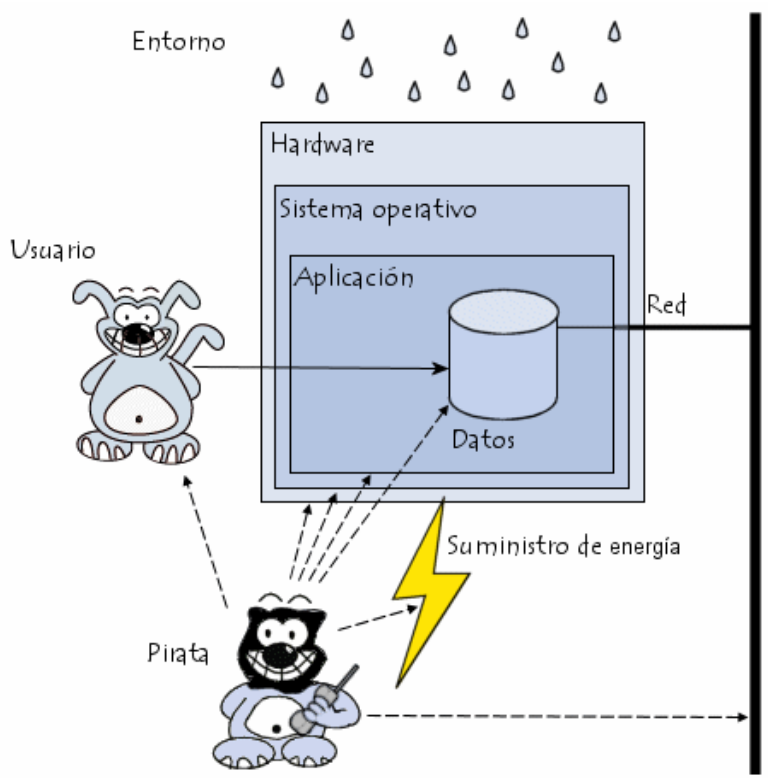


Figura 2. Niveles de riesgo.

Los ataques informáticos se pueden clasificar de la siguiente manera:

1. **Acceso físico:** En este caso, el atacante tiene acceso a las instalaciones e incluso a los equipos:
   - Interrupción del suministro eléctrico.
   - Apagado manual del equipo.
   - Vandalismo.
   - Apertura de la carcasa del equipo y robo del disco duro.
   - Monitoreo del tráfico de red.

2. **Intercepción de comunicaciones:** este tipo de ataque se da mediante la instalación de una serie de programas malintencionados, los cuales son instalados en el equipo de la víctima

y estos tienen a su vez como funcionalidad, el guardar o grabar todos y cada uno de los movimientos con el mouse o teclado de la víctima:

- Secuestro de sesión.
- Falsificación de identidad.
- Redireccionamiento o alteración de mensajes.

3. **<u>Denegaciones de servicio (Dos):</u>** el objetivo de estos ataques reside en interrumpir el funcionamiento normal de un servicio. Por lo general, las denegaciones de servicio se dividen de la siguiente manera:

- Explotación de las debilidades del protocolo TCP/IP.
- Explotación de las vulnerabilidades del software del servidor.

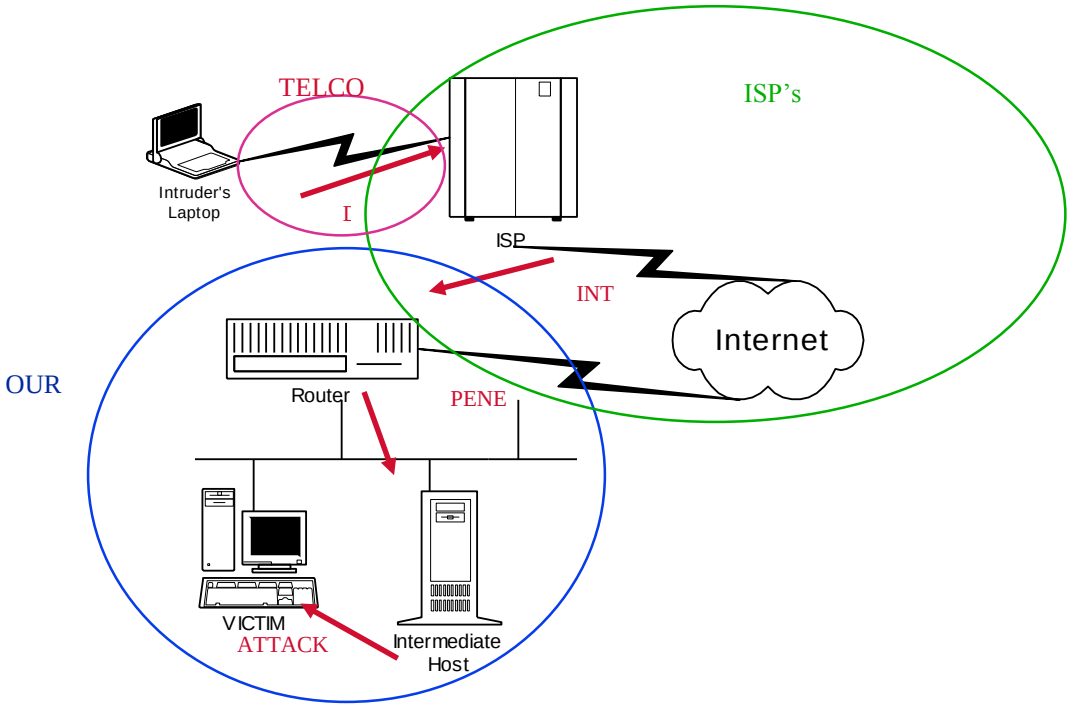


Figura 3. Denegación de servicio.

Un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), 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.

Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no dé abasto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo.

4. **Denegación de servicios distribuida (Ddos):** El llamado DDoS (siglas en inglés de Distributed Denial of Service, denegación de servicio distribuida) es una ampliación del ataque DoS, se efectúa con la instalación de varios agentes remotos en muchas computadoras que pueden estar localizadas en diferentes puntos. El invasor consigue coordinar esos agentes para así, de forma masiva, amplificar el volumen del flood o saturación de información, pudiendo darse casos de un ataque de cientos o millares de computadoras dirigidas a una máquina o red objetivo. Esta técnica se ha revelado como una de las más eficaces y sencillas a la hora de colapsar servidores, la tecnología distribuida ha ido sofisticándose hasta el punto de otorgar poder de causar daños serios a personas con escaso conocimiento técnico.

   En ocasiones, esta herramienta ha sido utilizada como un notable método para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y perjudicar los servicios que desempeña. Un administrador de redes puede así conocer la capacidad real de cada máquina.

Un ataque por denegación de servicios (DoS), puede ser perpetrado en un sin número de formas. Aunque básicamente este consisten en: consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.

- Alteración de información de configuración, tales como información de rutas de encaminamiento.
- Alteración de información de estado, tales como interrupción de sesiones TCP (TCP reset).
- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que ya no puedan comunicarse adecuadamente.

En la actualidad existen una serie de ataques DoS, los cuales se mencionaran a continuación, con el fin de poder tener una claridad frente a la forma de operar de cada uno de estos.

5. **Elevación de privilegios:** este tipo de ataque consiste en aprovechar una vulnerabilidad en una aplicación al enviar una solicitud específica (no planeada por su diseñador). En ciertos casos, esto genera comportamientos atípicos que permiten acceder al sistema con derechos de aplicación. Los ataques de desbordamiento de la memoria intermedia (búfer) usan este principio.

6. **Ingeniería social:** en la mayoría de los casos, el eslabón más débil es el mismo usuario. Muchas veces es él quien, por ignorancia o a causa de un engaño, genera una vulnerabilidad

en el sistema al brindar información (la contraseña, por ejemplo) al pirata informático o al abrir un archivo adjunto. Cuando ello sucede, ningún dispositivo puede proteger al usuario contra la falsificación: sólo el sentido común, la razón y el conocimiento básico acerca de las prácticas utilizadas pueden ayudar a evitar este tipo de errores.

7. **Puertas trampa:** son puertas traseras ocultas en un programa de software que brindan acceso a su diseñador en todo momento. Es por ello que los errores de programación de los programas son corregidos con bastante rapidez por su diseñador apenas se publica la vulnerabilidad. En consecuencia, queda en manos de los administradores (o usuarios privados con un buen conocimiento) mantenerse informados acerca de las actualizaciones de los programas que usan a fin de limitar los riesgos de ataques.

8. **Esfuerzo de protección:** La seguridad del sistema de un equipo generalmente se denomina "asimétrica" porque el pirata informático debe encontrar sólo una vulnerabilidad para poner en peligro el sistema, mientras que el administrador debe, por su propio bien, corregir todas sus fallas.

9. **Ataque por rebote:** Cuando se ejecuta un ataque, el pirata informático siempre sabe que puede ser descubierto, por lo que generalmente privilegia los ataques por rebote (en oposición a los ataques directos). Los primeros consisten en atacar un equipo a través de otro para ocultar los rastros que podrían revelar la identidad del pirata (como su dirección IP) con el objetivo de utilizar los recursos del equipo atacado.

Esto comprueba la importancia de proteger su red o PC, ya que podría terminar siendo cómplice de un ataque y, si las víctimas realizan una denuncia, la primera persona cuestionada será el propietario del equipo que se utilizó como rebote.

Con el desarrollo de las redes inalámbricas, este tipo de situación podría ser cada vez más común ya que estas redes no son demasiado seguras y los piratas ubicados en sus inmediaciones podrían usarlas para ejecutar un ataque.

10. **Ataque por inundación Syn (SYN FLOODS):** La inundación SYN envía un flujo de paquetes TCP/SYN (varias peticiones con el FLAG SYN en la cabecera), muchas veces con la dirección de origen falsificada. Cada uno de los paquetes recibidos es tratado por el destino como una petición de conexión, causando que el servidor intente establecer una conexión al responder con un paquete TCP/SYN-ACK y esperando el paquete de respuesta TCP/ACK (Parte del proceso de establecimiento de conexión TCP de 3 vías). Sin embargo, debido a que la dirección de origen es falsa o la dirección IP real no ha solicitado la conexión, nunca llega la respuesta.

    Estos intentos de conexión consumen recursos en el servidor y limitan el número de conexiones que se pueden hacer, reduciendo la disponibilidad del servidor para responder peticiones legítimas de conexión.

11. **Ataque Land:** Un incidente o ataque LAND se realiza al enviar un paquete TCP/SYN falsificado con la dirección IP del servidor objetivo como si fuera la dirección origen y la dirección destino a la vez, además de usar un puerto abierto TCP, tanto de destino como de

origen. Esto causa que el servidor se responda a sí mismo continuamente hasta colapsar sus recursos.

Para evitar el ataque LAND, la mayoría de los firewalls deberían interceptar el paquete malicioso. Adicionalmente, routers deberían ser configurados con filtros tanto de entrada como de salida, para bloquear tráfico donde la dirección IP origen se encuentra en el mismo espacio de direcciones que la dirección destino. Algunos sistemas operativos han generado actualizaciones para específicamente cubrir este problema de seguridad.

12. **Ataque por inundación ICMP (ICMP FLOODS):** Es una técnica DoS que pretende agotar el ancho de banda de la víctima. Consiste en enviar de forma continuada un número elevado de paquetes ICMP echo request (ping) de tamaño considerable a la víctima, de forma que esta ha de responder con paquetes ICMP echo reply (pong) lo que supone una sobrecarga tanto en la red como en el sistema de la víctima.

    Dependiendo de la relación entre capacidad de procesamiento de la víctima y atacante, el grado de sobrecarga varía, es decir, si un atacante tiene una capacidad mucho mayor, la víctima no puede manejar el tráfico generado.

13. **Ataque Smurf:** Existe una variante a ICMP floods denominado Smurf que amplifica considerablemente los efectos de un ataque ICMP.

    Existen tres partes en un ataque smurf: El atacante, el intermediario y la víctima (comprobaremos que el intermediario también puede ser víctima).

En smurf el atacante dirige paquetes ICMP tipo “echo request” (ping) a una dirección IP de broadcast, usando como dirección IP origen, la dirección de la víctima (Spoofing). Se espera que los equipos conectados respondan a la petición, usando echo reply, a la maquina origen (víctima).

Se dice que el afecto es amplificado, debido a que la cantidad de respuestas obtenidas, corresponde a la cantidad de equipos en la red que puedan responder. Todas estas respuestas son dirigidas a la víctima intentando colapsar sus recursos de red.

Como se mencionó anteriormente, los intermediarios también sufren los mismos problemas que las propias víctimas.

14. **Ataque por inundación UDP (UDP FLOODS):** Básicamente este ataque consiste en generar grandes cantidades de paquetes UDP contra la víctima elegida. Debido a la naturaleza sin conexión del protocolo UDP, este tipo de ataques suele venir acompañado de IP spoofing.

    Es usual dirigir este ataque contra máquinas que ejecutan el servicio hecho de forma que se generan mensajes “echo” de un elevado tamaño.

15. **Ataque por incidente Ping de la muerte:** El Ping de la muerte, es un tipo de ataque enviado a una computadora que consiste en mandar numerosos paquetes ICMP muy pesados (mayores a 65.535 bytes) con el fin de colapsar el sistema. Los atacantes

comenzaron a aprovecharse de esta vulnerabilidad en los sistemas operativos en 1996, vulnerabilidad que en 1997 sería corregida.

Este tipo de ataque no tiene efecto sobre los sistemas operativos actuales, sino que implica enviar un ping deformado a una computadora. Un ping normalmente tiene un tamaño de 64 bytes; algunas computadoras no pueden manejar pings mayores al máximo de un paquete IP común, que es de 65.535 bytes. Enviando pings de este tamaño puede hacer que los servidores se caigan. Este fallo fue fácil de usar, generalmente, enviar un paquete de 'Ping de la Muerte' de un tamaño de 65.536 bytes es ilegal según los protocolos de establecimiento de una red, pero se puede enviar un paquete de tal tamaño si se hacen fragmentos del mismo; cuando la computadora que es el blanco de ataque vuelve a montar el paquete, puede ocurrir una saturación del buffer, que causa a menudo un fallo del sistema. Este exploit ha afectado a la mayoría de Sistemas Operativos, como Unix, Linux, Mac, Windows, impresoras, y los routers. No obstante la mayoría de los sistemas operativos desde 1997-1998 han arreglado este problema, por lo que el fallo está solucionado.

16. **Ataque Malware Ó Código Malicioso:** malicious software, también llamado badware, software malicioso o software malintencionado, el Malware o código malicioso, es un software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas, ya que en esta categoría encontramos desde un troyano a un spyware.

Esta expresión es un término general muy utilizado por profesionales de la computación para definir una variedad de software o programas de códigos hostiles e intrusivos. Muchos

usuarios de computadores no están aún familiarizados con este término y otros incluso nunca lo han utilizado. Sin embargo la expresión ‘virus informático’ es más utilizada en el lenguaje cotidiano y a menudo en los medios de comunicación para describir todos los tipos de malware. Se debe considerar que el ataque a la vulnerabilidad por malware, puede ser a una aplicación, una computadora, un sistema operativo o una red.

Dos tipos comunes de malware son los virus y los gusanos informáticos, este tipo de programas tienen en común la capacidad para auto replicarse es decir, pueden contaminar con copias de sí mismos y en algunas ocasiones mutando, la diferencia entre un gusano y un virus informático radica en la forma de propagación, un gusano opera a través de una red, mientras que un virus lo hace a través de ficheros a los que se añade.

Los virus informáticos utilizan una variedad de portadores. Los blancos comunes son los archivos ejecutables que son parte de las aplicaciones, los documentos que contienen macros (Virus de macro), y los sectores de arranque de las USB y discos duros (Virus de boot, o de arranque). En el caso de los archivos ejecutables, la rutina de infección se produce cuando el código infectado es ejecutado, ejecutando al primero el código del virus. Normalmente la aplicación infectada funciona correctamente. Algunos virus sobrescriben otros programas con copias de ellos mismos, el contagio entre computadoras se efectúa cuando el software o el documento infectado van de una computadora a otra y es ejecutado.

17. **Ataque Crimeware Ó Software Criminal:** El Crimeware o software criminal, se encuentra encaminado al aspecto financiero, la suplantación de personalidad y el espionaje, al identificar las pulsaciones en el teclado o los movimientos del ratón o creando falsas páginas de bancos o empresas de contratación y empleo para con ello conseguir el número

de cuenta e identificaciones, registros oficiales y datos personales con el objetivo de hacer fraudes o mal uso de la información. También es utilizando la llamada ingeniería social, que consiste en conseguir la información confidencial del propio usuario mediante engaños, como por ejemplo, mediante un correo en donde mediante engaños se solicita al usuario enviar información privada o entrar a una página falsificada de Internet para hacerlo.

18. **Ataque por acceso no autorizado:** Es un incidente que abarca desde el ingreso hasta la operación no autorizado a los sistemas. Estos pueden ser exitosos o no. En esta categoría se incluyen:
    - Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos.
    - Robo de información.
    - Borrado de información.
    - Alteración de la información.
    - Intentos recurrentes (o no) de acceso no autorizado.
    - Abuso y/o mal uso de los servicios informáticos internos o externos que requieren autenticación.

19. **Ataque por uso inapropiado:** Se dan cuando los usuarios se ‘saltan’ la política de uso apropiado de los sistemas (por ejemplo ejecutando aplicaciones P2P en la red interna de la organización para la descarga de música).

20. **Ataque Múltiple:** Se produce cuando el incidente implica varios de los tipos anteriores. La mayoría de los incidentes que se dan en la realidad, pueden enmarcarse en varias de las categorías, por lo que una buena forma de identificarlos es por el mecanismo de transmisión

empleado. Por ejemplo un virus que crea en el sistema atacado una puerta trasera debe ser manejado como un incidente de código malicioso y no como un acceso no autorizado, ya que el virus es el mecanismo de transmisión.

Para la prevención de ataques a sistemas es necesario, detectar un ataque a los sistemas informáticos antes de que se produzca, o en el peor de los casos en el instante en el que comienza, siempre será mejor tener que recuperar el sistema recurriendo a las copias de seguridad.

Es muy importante para proteger su actividad productiva, mantener el número de incidentes razonablemente bajo. Si los controles de seguridad son insuficientes y sufre continuos ataques a los sistemas, éstos pueden repercutir negativamente en las actividades del negocio, tanto desde el punto de vista económico como el de imagen de la organización.

7.2.4 Recomendaciones para asegurar los sistemas de información

La mayoría de los ataques se basan en fallos de diseño inherentes a internet (y sus protocolos), cualquier conexión de red y a los sistemas operativos utilizados, por lo que no son “solucionables” en un plazo breve de tiempo.

La solución inmediata en cada caso es mantenerse informado sobre todos los tipos de ataques existentes y las actualizaciones que permanentemente lanzan las empresas desarrolladoras de software, principalmente de sistemas operativos.

Las siguientes son medidas preventivas. Medidas que toda red y administrador deben conocer y desplegar cuanto antes. A continuación, algunas recomendaciones con las cuales se podrá asegurar toda la plataforma tecnológica de una organización, en cuanto lo que se refiere a sistemas de información, redes y datos.

- Mantener las máquinas actualizadas y seguras físicamente
- Mantener personal especializado en cuestiones de seguridad (o subcontratarlo).
- Aunque una máquina no contenga información valiosa, hay que tener en cuenta que puede resultar útil para un atacante, a la hora de ser empleada en un DoS coordinado o para ocultar su verdadera dirección.
- No permitir el tráfico ‘broadcast’ desde fuera de nuestra red. De esta forma evitamos ser empleados como ‘multiplicadores’ durante un ataque Smurf.
- Filtrar el tráfico IP Spoof.
- Auditorias de seguridad y sistemas de detección.
- Mantenerse informado constantemente sobre cada una de las vulnerabilidades encontradas y parches lanzados. Para esto es recomendable estar suscripto a listas que brinden este servicio de información.
- Realizar capacitaciones continuas con cada uno de los usuarios.
- Asegurar los servidores basándose en el concepto de privilegio mínimo, esto es, configurarlos para que proporcionen un número limitado de servicios y con un nivel de acceso restringido según el tipo de usuario. Además deben evitarse configuraciones por defecto, como claves predefinidas, recursos compartidos, entre otros. También sería interesante disponer de medios de notificación al administrador cuando se produzcan accesos a niveles de privilegio no autorizados.

- Mantener la seguridad de la red, configurando un filtro perimetral en modo ‘paranoico’, esto es, denegando cualquier tipo de acceso no autorizado expresamente, y manteniendo sólo el tráfico necesario para la actividad diaria normal. Esto incluirá instalación de cortafuegos, detectores de intrusos (IDS), monitores de red, uso de redes privadas virtuales (VPNs), uso de protocolos seguros (IPSec, SSL).
- Prevenir la ejecución de código malicioso (malware), utilizando programas antivirus capaces de parar este tipo de código como virus, caballos de Troya, gusanos, entre otros.
- Formar e informar a sus usuarios para que conozcan, acepten y sean capaces de aplicar las directrices de su política de seguridad. Hágales ver lo que ha ocurrido en otras organizaciones o entidades, cómo han ‘aprendido la lección’, cómo ha afectado un incidente a sus actividades. Informando y formando a los usuarios reducirá la frecuencia de los incidentes, sobre todo aquellos que impliquen la ejecución de código malicioso, o el saltarse la política de uso adecuado de los sistemas.

Teniendo en cuenta las anteriores recomendaciones, es necesario preparar y dar respuesta a los incidentes y es por esto que, se debe incluir dentro de la política de seguridad un Plan de Respuesta ante Incidentes.

7.2.5 Plan de respuesta ante incidentes

Estos planes dependerán en gran medida de las características de la organización, y de su política, a continuación se describen algunas bases que deberían contener dicho plan.

- Alcance, propósitos y objetivos del plan de acción.

- Estructura organizativa del equipo de respuesta a incidentes, responsabilidades, autoridad, departamentos implicados.
- Actuaciones para la contención del problema.
- Procedimientos de recuperación y restauración de sistemas SIN eliminación de posibles evidencias del ataque.
- Índices para la valoración de los daños, tanto desde el punto de vista económico como de imagen corporativa.
- Determinar en qué casos se tratará el incidente internamente y en qué casos se dará aviso a las Autoridades.
- Sopesar la contratación de personal externo para llevar a cabo la investigación.
- Establecer las fases de la investigación.
- Elaboración de informes y formularios tipo para comunicación del incidente tanto dentro como fuera de la organización si fuese necesario.

7.2.6 Recopilación de evidencias

La recopilación de evidencias digitales puede llegar a ser una tarea bastante difícil, entonces será necesario, preparar los sistemas para obtener buenos datos forenses. La implantación de procedimientos adecuados en la gestión de archivos, registros y copias de seguridad puede ayudar al equipo de ingenieros en esta labor.

- Conocer y monitorizar los parámetros de funcionamiento normal de los sistemas, tales como tráfico IP usual, carga de transacciones, ancho de banda consumido, usuarios conectados, entre otros.

- Utilizar un servidor de registros central y establecer una política de mantenimiento y retención de esos registros que permitan su estudio pasado el tiempo.
- Activar al máximo de detalle la información que contendrán los archivos de registro, lo que permitirá facilitar el proceso de reconstrucción de lo sucedido.
- Sincronizar todos los relojes de los servidores mediante, por ejemplo, el protocolo NTP (Network Time Protocol), permitiendo que los registros contengan todos la misma hora.
- Disponer de una base de conocimientos sobre incidentes, basta algo tan sencillo como páginas de software antivirus, o empresas y organizaciones especializadas en seguridad informática, así como suscribirse a sus listas e-mail de notificaciones de alertas y vulnerabilidades.
- Considere la experiencia como un factor irremplazable, esto le permitirá distinguir rápidamente un ataque de un simple problema técnico.

7.2.7 Tipos de pruebas

Las pruebas digitales o pruebas electrónicas son cualquier información probatoria almacenada o transmitida en la forma digital que se puede usar en un proceso judicial. El empleo de pruebas digitales ha aumentado en las pocas décadas pasadas, como los tribunales han permitido el empleo de los correos electrónicos, fotografías digitales, troncos de transacción de ATM (de cajero automático), documentos de procesamiento de textos, historias de mensaje inmediatas, archivos salvados (ahorrados) de programas de la contabilidad, hojas de cálculos, historias de catálogo del Internet, bases de datos, el contenido de memoria de ordenador, reservas de ordenador, listados del ordenador, el sistema rastreador de colocación global, troncos de las cerraduras de la puerta electrónicas de un hotel, y archivos digitales de vídeo o de audio. Ahora es más fácil poder resolver

casos con toda esta información, siempre y cuando esta información no haya sido cambiada o alterada.

La evidencia electrónica se puede recolectar de una infinidad de fuentes. Dentro de la red de la organización, la evidencia se va a encontrar en cualquier forma de tecnología que permita la transmisión o el almacenamiento de datos. La evidencia deberá ser recolectada por tres diferentes partes de la red del delincuente una es el área de trabajo del delincuente, otra sería el servidor accesado por el infractor o por la red que conecta a los dos. Después los ingenieros podrán usar tres diferentes fuentes para confirmar el origen de la información.

Como cualquier otra pieza de evidencia usada en un caso, la información del resultado de una investigación informática forense deberá seguir con los estándares de evidencia admisible. Se deberá tener mucho cuidado con la información que se ha recolectado, ya sea peligros de virus, daños electromagnéticos o mecánicos, trampas, entre otros. Hay ciertas reglas que nos permiten que la evidencia nos sea destruida o comprometida, éstas se describen a continuación:

- Usar la información original lo menos posible para evitar algún tipo de cambio de información.
- Establecer y mantener la cadena de custodia.
- Documentar todo lo que hemos hecho.
- Nunca excederse en el conocimiento personal.

Si estos pasos no se siguen, la información original puede ser cambiada, arruinada o puede ser corrompida y aquellos resultados no podrán ser válidos en un proceso judicial. Estas preguntas son muy importantes y deben tenerse en cuenta ¿los tiempos de las operaciones de la empresa son inconvenientes? y ¿cómo la información que se descubre involuntariamente será manejada?

En cualquier investigación donde el dueño de las pruebas digitales no ha dado el consentimiento de tener los medios de comunicación examinados, como en la mayoría de los casos criminales, se deberá tener un cuidado especial para asegurar que el investigador tenga la autoridad legal para agarrar, y examinar cada dispositivo.

7.2.8 Pasos para identificar un incidente informático

Hay ciertos pasos que un informático forense debe tener en cuenta para identificar y poder juntar información suficiente que pueda existir en un sistema de computadora:

- Proteger el sistema del ordenador sustancial durante la investigación de cualquier posible alteración, daño, corrupción de datos o introducción de virus.
- Descubrir todos los archivos que existan en el sistema. Esto incluye archivos normales, archivos eliminados, archivos ocultos, archivos protegidos con claves y archivos encriptados.
- Recuperar todos o todos los posibles de los documentos encontrados que fueron eliminados.
- Revelar(al grado posible) el contenido de los archivos ocultos o archivos de cambio usados por ambos, los programas de aplicaciones como por el sistema de operaciones.
- Acceso (si es posible y es apropiadamente legal) al contenido de los archivos protegidos y encriptados.

- Analizar todo la información posible que sea relevante encontrada en especial aquellas áreas de un disco. Esto incluye, pero no es limitado a lo que llaman el espacio ‘in-asignado’ en un disco (actualmente no es usado, pero posiblemente el depósito de los datos anteriores que pueden ser pruebas relevantes), así como el espacio ‘Slack’ en un archivo (el área restante al final de un archivo, en el último espacio de disco asignado, que no es usado por datos de archivos corrientes, pero otra vez puede ser sitio posible para pruebas antes creadas y relevantes.
- Imprimir un análisis general del sistema, así como una lista de los posibles documentos relevantes e información descubierta. Después, proporciona una opinión de la disposición del sistema, las estructuras de los archivos descubiertos, cualquier dato descubierto y la información del creador, cualquier tentativa para ocultar algo, eliminar, proteger, encriptar la información y cualquier otra cosa que haya sido descubierta y aparezca ser relevante al sistema de examinación.
- Proveer una consultaría por medio de un experto y/o un testimonia, así sea necesario.

7.2.9 Aplicaciones de pruebas en procesos judiciales

En el Décimo Congreso de las Naciones Unidas, sobre la prevención del crimen y el tratamiento de los delincuentes, se definieron dos categorías de Crímenes Informáticos, a saber:

- Crimen informático en sentido estricto: Cualquier comportamiento ilegal, dirigido por medio de operaciones electrónicas que tengan como objetivo la seguridad de sistemas informáticos y de los datos que procesan.

- Crimen Informático en sentido amplio (Crímenes Relacionados Con La Informática): Cualquier comportamiento ilegal cometido por medio o en relación con un sistema informático o una red, incluyendo crímenes como la posesión ilegal, la oferta y la distribución de información por medio de un sistema informático o de una red.

Estas definiciones no son completamente definitivas pero proporcionan un buen punto de inicio que además tiene reconocimiento y acuerdo internacional, si bien el asunto es más complejo pues una acción puede ser ilegal en un país y no serlo en otro.

Atendiendo a las definiciones expuestas anteriormente, los ordenadores y las redes pueden verse involucrados en un crimen informático de varias formas:

- El ordenador o la red pueden ser las herramientas utilizadas para cometer el crimen.
- El ordenador o la red pueden ser los objetivos o víctimas del crimen.
- El ordenador o la red pueden ser utilizadas para propósitos incidentales relacionados con el crimen.

Muchos de los procedimientos criminales y civiles pueden y deben hacer uso de la evidencia revelada por los especialistas en informática forense, algunas de las aplicaciones serán las siguientes:

- Los acusadores criminales usan evidencia encontrada en las computadoras en la variedad de crímenes donde se encuentras documentos que pueden incriminar gente ya sean de: homicidios, fraudes financieros, drogas, pornografía infantil, entre otros.

- Litigaciones civiles pueden hacer uso de información personal o de empresas encontradas en los sistemas computacionales que hablar sobre: fraudes, divorcios, discriminación y casos de hostigamiento.
- Las compañías de seguros será posible que puedan reducir costos en casos donde se encuentren fraudes de accidentes, compensaciones en casos de trabajadores, entre otros.
- Algunas corporaciones contratan gente para que busquen evidencia relacionado con: hostigamiento sexual, robos, el mal uso de secretos y el uso de información interna e información confidencial.
- Los oficiales en la ejecución de derecho con frecuencia requieren la ayuda en preparativos de autorización y en el manejo de equipo computacional.

7.2.10 Herramientas para una investigación de informática forense

Para realizar una investigación informática forense se cuenta con dos herramientas:

1. Los instrumentos de forenses de línea de mando. Hay ciertas ventajas para las herramientas de línea de comando ya que pueden entrar en disquete y usan muy pocos recursos. Sin embargo también tienen sus desventajas, entre las que destacan que no pueden buscar archivos con .zip o .cab. Además algunos son limitados a los archivos MS-DOS FAT del sistema.

2. Los de Interfaz de Usuario Gráfico (GUI). Las herramientas GUI no necesitan mucho conocimiento como herramientas de línea de comando. Algunas de estas herramientas GUI son simplificadas para que los principiantes pueden empezar a trabajar con ellas.

Los investigadores forenses deben siempre recordar que ninguna herramienta puede hacer todo el trabajo o puede hacer el trabajo por sí sola. Un ingeniero informático debe tener al menos más de una herramienta en su set de herramientas.

Se dice que un ingeniero debe evitar alterar un disco en cualquier manera, ya que si se le pasa algo o se pierde información es como estar perdiendo una evidencia importante. Para prevenir esto se recomienda usar instrumentos que permitan bloquear la información, ya que de esta manera estamos seguros que no le va a pasar nada a la información. Debido a que al prender el computador se causa que el sistema operativo escriba cierta información, es necesario que estos equipos de bloqueo de información estén conectados desde el principio antes de que se prenda el computador. La única cosa que el ingeniero informático debe de hacer con el disco es crear una copia normal del disco duro y después asegurar el disco original en el estante de la evidencia. Cualquier análisis deberá hacerse en la copia que se hizo, ya que si algo sale mal durante el análisis, la evidencia como quiera sigue estando a salvo guardada en el disco original.

Uno de los mayores problemas que se enfrenta en la Informática Forense, es que hace falta mucho personal capacitado en este campo. El mayor reto que enfrentan los ingenieros informáticos es encontrar y proteger cualquier evidencia, para que de esta manera la evidencia pueda estar a salvo y pueda ser presentada en los procesos judiciales y sea válida, ya que si tiene algunos cambios es posible que no sea tomada como evidencia válida.

Como los forenses tradicionales que su evidencia se basa en huella digitales, estudios de la dentadura y lo más reciente el ADN, la evidencia digital requiere más cuidado a la hora de estar recolectando todos los datos, una documentación, un acceso restringido a la información, y prestar mucha atención a todo lo que se hace para que nada vaya a salir mal. A diferencia de los forenses

tradicionales, los forenses de la evidencia digital requiere un conocimiento especializado en las uso de la tecnología ya sea usando hardware y software, incluyendo varios sistema operativos, técnicas de almacenaje de archivos, y técnicas para recuperar archivos. Esto representa que se tengan que hacer ciertos ajustes en la aplicación de las leyes.

Para los aplicadores de la ley, el reto es encontrar gente capaz y que tenga las habilidades para poder hacer este tipo de análisis. Ya cuando se encuentran a las personas indicadas es necesario que se entrenen y se les de toda las herramientas necesarias para que puedan realizar su análisis. La mayor parte de los ingenieros que trabajan en este ámbito dicen que lo más importante que deben de tener es educación, entrenamiento y certificación. Hoy en día hay una falta de certificaciones para los profesionales que ya tienen mucha experiencia en este ámbito.

7.2.11 Pasos para recolectar las evidencias

A continuación se describen los pasos necesarios para llevar a cabo un excelente análisis de incidentes informáticos:

1. **Preparación:** En la preparación de las pruebas es muy importante tener en cuenta el recurso humano, la logística, los dispositivos, las herramientas para su manejo y los documentos, como lo vemos a continuación:
   - Recurso Humano. Aunque puede sonar muy evidente es importante que la o las personas que van a ser los responsables de realizar los análisis de incidentes en una organización deben tener algunas consideraciones tanto de privacidad como de legalidad.

- Privacidad: Dentro de las consideraciones de privacidad se enmarcan las Políticas y Reglamentación con respecto al uso de los recursos tecnológicos, la privacidad de la información de las personas (Archivos personales) influye al no poder ser recolectados sin la suficiente indicación que es un incidente real.
- Legalidad: En Colombia el artículo 236 del Código de Procedimiento Penal Ley 906 de 2004 puede servir como marco de legalidad frente a este punto. Las políticas deben seguirse en el contexto de una investigación para no infringir alguna política y/o regla al momento de fijar la escena o recolectar la evidencia.
- Con respecto a las consideraciones legales un analista forense debe conocer que la evidencia debe ser admisible o aceptable, autentica, completa, confiable y creíble.

Se puede incluso pensar que esta persona debería estar en capacidad de realizar un levantamiento dactiloscópico en la escena del incidente, este tipo de evidencia que en principio puede ser vista como extrema, en algún momento se puede constituir como elemento importante dentro de la vinculación de la videncia digital con algún sospechoso.

2. **Logística:** Cuando se realiza la recolección de la evidencia digital generalmente la preocupación es solo del espacio y del dispositivo en donde vamos a guardar la información y como se va a realizar; pero no se piensa que tan válidas pueden ser esas pruebas sino se realizan los procedimientos adecuados para el manejo de los elementos físicos (Disco Duro, CD, entre otros.).

   A continuación se enumeran algunos componentes que se deben tener al alcance:

- Bolsas antiestáticas, que permitan la correcta manipulación de medios de almacenamiento.
- Bolsas de seguridad, para guardar los elementos físicos, que permitan garantizar que una vez guardados se tenga la certeza que la bolsa no ha sido abierta.
- Embalaje, para guardar los Discos Duros y evitar que una eventual caída o maltrato al elemento ocasione una pérdida de información, que en este caso sería perdida de la evidencia.
- Etiquetas o Rótulos, para marcar los elementos físicos, con el fin de identificarlos.
- Esta etiqueta debe tener la información necesaria que identifique al elemento. Por ejemplo si se habla de un Disco Duro, se debería incluir por lo menos la siguiente información:
  - Un consecutivo
  - Número del incidente
  - Descripción del elemento (Marca, Modelo, Serial, Capacidad, tipo de conector (IDE, SCSI, ATA), configuración física, particiones, Sistema Operativo).
  - Fecha y Hora
  - Lugar
  - Nombre y firma de quien recolecta el elemento. Si es posible nombre y firma de un testigo.

También se debe marcar el elemento físico directamente, siempre y cuando no altere la autenticidad de la evidencia teniendo en cuenta las características del elemento. No realizar este tipo de procedimientos puede acarrear una desventaja para la defensa en un proceso legal, ya que sencillamente se puede llegar a romper la cadena de custodia.

3. **Dispositivos:** Cuando se piensa en una investigación forense, se debe tener conocimiento de las características de los equipos con que se cuentan, es decir se debería tener un inventario completo de todos los dispositivos de la organización, resaltando aquellos que de alguna forma permitan algún tipo de almacenamiento como pueden ser: memorias USB, Tarjetas SD, CD, DVD, disquetes, PDA, entre otros.

   Los medios de almacenamiento que se vayan a utilizar en una investigación forense deben estar libres de contaminación, lo cual se puede hacer con un proceso de sanación de datos.

   Igualmente, es necesario pensar donde vamos a guardar la evidencia una vez se esté recolectando, teniendo en cuenta que cualquier cambio que haga a la configuración del sistema afecta el estado original de la evidencia. La mejor manera de extraer los datos de una maquina comprometida es a través de la red, pero también se debe pensar que muchas veces los incidentes ocurren por medio de las conexiones de red. Se debe pensar en varias estrategias y escenarios que permitan recolectar la evidencia tratando de no contaminarla, a continuación veremos algunos escenarios comunes:

   - Con acceso a la red: Partimos de la idea que el destino de la recolección de la evidencia no está contaminado, se debe tener una máquina que tiene que configurarse en el mismo ambiente de la maquina afectada, es necesario tener un disco duro adicional con la suficiente capacidad y libre de contaminación, en la maquina destino.
   - Sin acceso a la red: Si de alguna manera la cantidad de datos que necesitamos recolectar es pequeña, podemos utilizar CD´s, que es la forma más económica de recolección de evidencia. Pero muchas veces nos enfrentamos a grandes cantidades de datos que no

pueden ser almacenados en estos dispositivos; pensaríamos en varias estrategias que permitan realizar la transferencia de los datos recolectados.

- Colocar un Disco Duro: Normalmente no se puede realizar sin apagar la máquina, y se puede hacer siempre y cuando los datos volátiles del sistema han sido recuperados anteriormente. Colocar dispositivos de almacenamiento removibles (USB o Firewire): No es recomendable por que cambia el estado original del sistema. Pero se puede pensar en utilizarlos si los datos volátiles del sistema ya se tienen.

Teniendo en cuenta los comentarios anteriores se recomienda pensar en los siguientes elementos o dispositivos básicos, al momento de una investigación forense.

- Un computador disponible para las investigaciones forenses.
- Un disco duro libre de contaminación.
- Medios de almacenamiento libres de contaminación (CDs, DVDs, Memorias USB, disquetes).
- Inventario de todo el hardware y software de la organización

En cualquiera de los casos es indispensable realizar la respectiva documentación de lo que se tiene y de los procedimientos que se han aplicado para dejarlos libres de contaminación.

4. **Herramientas:** Se debe crear un perfil forense de todas las herramientas que se tengan previstas a utilizar en un incidente de seguridad. Para cada herramienta debe identificar y documentar las siguientes características: adquisición, descripción, funcionabilidad, dependencias y en que afecta el sistema. A continuación se describirán de forma concisa:

- Adquisición: Documente como se adquirió la herramienta, si fue bajada de Internet, desarrollada, o comprada. Documente como se verifico la integridad de la herramienta cuando la adquirió. (Verificando el hash MD58 para las herramientas bajadas de Internet, o las validaciones y/o pruebas realizadas las herramientas desarrolladas o compradas).

- Descripción: Documente los detalles de la herramienta, incluyendo para que tipo de sistema operativo es compatible, como se utiliza y si tiene interfaz gráfica o línea de comandos.

- Funcionabilidad: Documente tanto como pueda, si aplica, la salida esperada generada, la información volátil que pueda ser recolectada, parámetros de la línea de comandos o sintaxis.

- Dependencias y en que afecta el sistema: Estos dos puntos quizás son los más importantes dentro de las características de la herramienta y se deben documentar. Para determinarlos se debe probar la herramienta y ver el efecto que esta produce en el sistema. Es preferible tener las herramientas forenses en diferentes dispositivos de almacenamiento como memorias USB, CD, disquetes, entre otros.

5. **Documentos:** Cuando utilizamos los procedimientos para hacer una investigación forense, se debe documentar absolutamente todo lo que se realice, desde el mismo momento en que el incidente es detectado hasta que finaliza la investigación. Esto nos ofrece una línea de tiempo que puede ser auditada y comprobada con cada una de las acciones tomadas durante el proceso.

Dentro de los documentos necesarios podemos destacar los siguientes:

- Procedimientos, bien documentados y en lo posible probados.
- Inventarios de hardware y software, detallados.
- Formatos con la historia del caso, donde se registre cada movimiento hecho en la investigación.
- Formatos de levantamiento de la información. (Recolección de datos)
- Formatos de entrega de custodia de la evidencia.

7.2.12 Las pruebas

En este paso debemos ser conscientes que para poder tener los dispositivos, las herramientas, los procedimientos y los investigadores a punto, se deben realizar pruebas sobre cada uno de ellos. Cualquier fallo de alguno de ellos en una investigación puede dañar todo o parte del proceso. Por eso es importante evaluarlos y tener en cuenta los siguientes elementos:

- Dispositivos: El estado de cada uno de los elementos debe ser óptimo, para comprobarlo se deben realizar pruebas, en el caso de los dispositivos de almacenamiento deben quedar completamente saneados para que queden listos como medios de almacenamiento de evidencia digital.

- Herramientas: Se deben realizar pruebas de cada una de las herramientas, para saber el alcance de cada una, el nivel de confiabilidad, la estabilidad, el impacto que pueden causar al sistema, las dependencias que generan, el tipo de reporte que generan, el formato de salida de los datos, la portabilidad entre Sistemas operativos y el desempeño.

- Procedimientos: Las pruebas de cada uno de los procedimientos deben ser efectivas y bien documentadas, ya que de esto depende que se haga una correcta recolección de la evidencia sin contaminarla y sobre todo dentro de los parámetros establecidos para ello. No se puede llegar a improvisar en el momento de manejar un incidente, aunque nunca podremos predecir de qué manera será un incidente, se pueden tener procedimientos estándares que nos ayuden a mitigar el impacto.

- Recurso Humano: Punto crítico que debe ser muy bien probado, pues la inexperiencia en la mayoría de los casos, puede acabar con cualquier investigación; es por eso que este elemento dentro de la cadena de un proceso de investigación es la parte fundamental, pues de la capacidad, la experiencia y la recursividad depende en gran medida una recolección válida y no contaminada de la evidencia digital. Por lo anterior, las pruebas son muy importantes como parte del conocimiento del investigador, además sirven para afinar los procedimientos.

7.2.13 La documentación

Mientras más se pueda documentar como se procedió con el incidente, existen más posibilidades de demostrar la validez de la evidencia digital. En este se recolecta toda la información de lo que se preparó, se hizo, se dejó de hacer. Empezando desde la preparación del hardware y las herramientas a utilizar, pasando por cómo se detectó el incidente, qué acciones se tomaron y por qué. Se deben mostrar todos los detalles y acciones de la recolección de la evidencia digital y

posteriormente como se realizó la custodia de la evidencia. No se puede pasar por alto ningún detalle.

La documentación es importante para lograr establecer la línea de tiempo de los sucesos alrededor del incidente.

Los puntos que podemos destacar en el proceso de documentación son:

- Recolectar las pruebas realizadas a los dispositivos disponibles para una posible investigación.
- Las herramientas que se van a utilizar se deben documentar completamente, incluso las pruebas realizadas sobre cada una de las herramientas.
- Cualquier procedimiento se debe documentar, pues de ello depende la reutilización de procesos y técnicas logradas con la experiencia.
- Se deben documentar las pruebas realizadas a los procedimientos y anotar observaciones al respecto. De tal forma que nos sirvan para afinar los procedimientos.

7.3 Marco legal

Si tras la realización de un primer análisis existen sospechas de que el incidente se ha provocado desde el interior de la red, tendrá que plantearse la posibilidad de llevar a cabo un análisis interno a la organización para depurar responsabilidades, bastará para este propósito recopilar información suficiente tanto en cantidad como calidad para poder tomar acciones disciplinarias posteriores, sin llegar a los juzgados. En esta situación además del equipo técnico de respuesta a incidentes, tendrá que contar con otros departamentos como el de Recursos Humanos e incluso con la Sección

Sindical, pues no puede permitirse que por una mala gestión del caso, el incidente se vuelva contra usted y acabe siendo acusado, por ejemplo, de despido improcedente.

Si los indicios llevan a su equipo forense a un ataque externo, habitualmente no merece la pena llevar a cabo acciones legales cuando los daños producidos son mínimos debido al alto costo económico que esto puede ocasionar. Por ejemplo una deformación de su página Web corporativa que se subsana rápidamente o intentos de intrusión sin mayores consecuencias que genera algunas molestias para sus usuarios, pueden resolverse enviando un aviso de uso inapropiado al proveedor o proveedores de los servicios de conexión de los presuntos atacantes.

Si documenta suficientemente bien su queja adjuntando históricos detallados de conexiones, del escaneado de sus equipos, entre otros, puede conseguir que el proveedor de servicios de Internet 'ISP', desconecte o anule las cuentas de sus atacantes. La mayoría de los proveedores tienen direcciones de e-mail para estos casos y los más importantes suelen ser muy estrictos en cuanto a la política de uso de sus servicios.

Pero si el incidente realizado por atacantes internos o externos, ha provocado daños importantes a su organización ya sean económicos, de imagen corporativa o su reputación ha quedado en entredicho, puede considerar abrir un proceso judicial contra sus atacantes. En este caso la investigación técnica deberá ser tratada como una investigación pericial técnica, incorporando procedimientos en materia de probatoria judicial, pues una evidencia digital no será considerada como prueba en un proceso judicial hasta que el juez así lo determine. Por lo anteriormente descrito, tendremos que convencerle de que hemos actuado de forma profesional, científica, veraz, con

cautela e imparcial, y además explicárselo para que lo entienda pues es muy probable que el juez no tenga conocimientos avanzados en estos temas.

Dentro de las muchas leyes que hacen referencia a los delitos informáticos tenemos dentro de la legislación tres frentes importantes: legislación informática, legislación penal y legislación civil[1].

- La legislación civil permite responder a personas y a sus bienes si es de carácter patrimonial o moral.
- La legislación penal vela por los daños a los bienes jurídicos protegidos por el estado. El análisis de la evidencia digital deberá cumplir con los requisitos de admisibilidad, pertinencia, suficiencia y legalidad establecidas por la ley, los documentos electrónicos deben ser aceptados por el juez sin valorar antes su autenticidad y seguridad. Para que los documentos digitales sean admitidos como evidencias se deben de tener en cuenta las siguientes leyes:
    - Ley 527 de 1999 conocida como la ley del comercio electrónico y su decreto reglamentario 1747 de 2000, reconoció fuerza probatoria como documentos a los mensajes de datos.
    - El artículo 10º de la Ley 527/99 regla: "Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de procedimiento Civil. Lo anterior satisface el requisito de que la información conste por escrito, equiparándolo así al documento escrito tradicional.

[1] Álvarez Serna, Andrés. (Julio- Diciembre 2012). Framework para la computación forense en Colombia. Recuperado de: http://web.usbmed.edu.co/usbmed/fing/v3n2/v3n2a8.pdf

- La Corte Constitucional en sentencia C-662 de junio 8 de 2000, con ponencia del Magistrado Fabio Morón Díaz, al pronunciarse sobre la constitucionalidad de la Ley 527 de 1999, hizo las siguientes consideraciones: (...) "El mensaje de datos como tal debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento.
- Con la promulgación de la ley 1273 de 2009 se da mayor admisibilidad a las evidencias digitales, en esta ley se modifica el código penal buscando la preservación integral de los sistemas de información y las comunicaciones.
- La ley 1273 de 2009 "De la Protección de la información y de los datos"

7.3.1 Referencias de ataques según el nuevo código penal[2]

1. **Legislación que plantea el código penal[3]:** Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

   - **Artículo 192:** Violación ilícita de comunicaciones. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a

[2] Bogotá Prieto, Diana. (2007). Evidencia Digital en Colombia. Recuperado de: file:///C:/Users/mosoral/Downloads/EJUS_BOGOTA_2007_EVIDENCIA_DIGITAL_EN_COLOMBIA.pdf
[3] Canedo Estrada, Alex. (Enero-Junio 2010). Recuperado de: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/98/93

otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya delito sancionado con pena mayor. Si el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro, la pena será prisión de dos (2) a cuatro (4) años.

- **Artículo 193:** Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. El que sin permiso de autoridad competente, ofrezca, venda o compre instrumentos aptos para interceptar la comunicación privada entre personas, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor[4].

- **Artículo 194:** Divulgación y empleo de documentos reservados. El que en provecho propio o ajeno o con perjuicio de otro divulgue o emplee el contenido de un documento que deba permanecer en reserva, incurrirá en multa, siempre que la conducta no constituya delito sancionado con pena mayor.

- **Artículo 195:** Acceso abusivo a un sistema informático. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.

[4] Recuperado de: http://www.acnur.org/biblioteca/pdf/0848.pdf.

- **Artículo 196:** Violación ilícita de comunicaciones o correspondencia de carácter oficial. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida comunicación o correspondencia de carácter oficial, incurrirá en prisión de tres (3) a seis (6) años. La pena descrita en el inciso anterior se aumentará hasta en una tercera parte cuando la comunicación o la correspondencia estén destinadas o remitidas a la Rama Judicial o a los organismos de control o de seguridad del Estado.

- **Artículo 199:** Sabotaje. El que con el fin de suspender o paralizar el trabajo destruya, inutilice, haga desaparecer o de cualquier otro modo dañe herramientas, bases de datos, soportes lógicos, instalaciones, equipos o materias primas, incurrirá en prisión de uno (1) a seis (6) años y multa de cinco (5) a veinte (20) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor.

  Si como consecuencia de la conducta descrita en el inciso anterior sobreviniere la suspensión o cesación colectiva del trabajo, la pena se aumentará hasta en una tercera parte.

- **Artículo 218:** Pornografía con menores. El que fotografíe, filme, venda, compre, exhiba o de cualquier manera comercialice material pornográfico en el que participen menores de edad, incurrirá en prisión de seis (6) a ocho (8) años y multa de cien (100) a mil (1.000) salarios mínimos legales mensuales vigentes.

  La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima.

- **Artículo 257:** Del acceso ilegal o prestación ilegal de los servicios de telecomunicaciones. El que acceda o use el servicio de telefonía móvil celular u otro servicio de comunicaciones mediante la copia o reproducción no autorizada por la autoridad competente de señales de identificación de equipos terminales de éstos servicios, derivaciones, o uso de líneas de telefonía pública básica conmutada local, local extendida o de larga distancia no autorizadas, o preste servicios o actividades de telecomunicaciones con ánimo de lucro no autorizados, incurrirá en prisión de dos (2) a ocho (8) años y multa de quinientos (500) a mil (1.000) salarios mínimos legales mensuales vigentes[5].

  La pena anterior se aumentará de una tercera parte a la mitad, para quien hubiese explotado comercialmente por sí o por interpuesta persona, dicho acceso, uso o prestación de servicios de telecomunicaciones no autorizados.

  Igual aumento de pena sufrirá quien facilite a terceras personas el acceso, uso ilegítimo o prestación no autorizada del servicio de qué trata este artículo.

- **Artículo 258:** Utilización indebida de información privilegiada. El que como empleado o directivo o miembro de una junta u órgano de administración de cualquier entidad privada, con el fin de obtener provecho para sí o para un tercero, haga uso indebido de información que haya conocido por razón o con ocasión de su cargo o función y que no sea objeto de conocimiento público, incurrirá en multa.

[5] Recuperado de: URL http://www.acnur.org/biblioteca/pdf/0848.pdf

> En la misma pena incurrirá el que utilice información conocida por razón de su profesión u oficio, para obtener para sí o para un tercero, provecho mediante la negociación de determinada acción, valor o instrumento registrado en el Registro Nacional de Valores, siempre que dicha información no sea de conocimiento público.
>
> La ausencia de una legislación específica sobre la materia, el desarrollo doctrinal en relación con la delincuencia informática ha sido abundante; la razón de ello, en nuestro criterio, es que la amplitud e importancia del tema permite su estudio desde distintas perspectivas y a partir de diferentes conductas ilícitas, cuyos modos de ejecución evolucionan al ritmo de la tecnología y del ingenio humano.
>
> En este escrito enfocaremos nuestra atención en el derecho a la información, como bien jurídico que resulta afectado con los delitos informáticos. A partir de allí, analizaremos las conductas ilícitas que lo afectan y la forma como el citado derecho fue protegido en el nuevo código penal.

El propósito de este trabajo, es precisamente analizar el estado con el cual se encuentra la legislación colombiana respecto de la protección del derecho a la información; y por otro lado, realizar aportes que sean útiles para la aplicación de las normas jurídico penales que existen sobre la materia.

- **Ley 906 de 2004 Código penal:** Se aplica a partir del 1° de enero de 2005, de acuerdo al Régimen de Implementación establecido en el Libro VII de la misma.

2. Acceso Abusivo a un Sistema Informático:

- **Artículo 195 C.P**. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.

- **Artículo 246**: Estafa. El que tenga provecho ilícito para sí o para un tercero, con perjuicio ajeno, induciendo o manteniendo otro en error por medio de artificios o engaños, incurrirá en prisión de 32 a 144 meses y multa de 66.66 a 1500 salarios mínimos legales mensuales vigentes.

- **Artículo 239:** Hurto. El que se apodere de una cosa ajena, con el propósito de obtener provecho para sí o para otro, incurrirá en prisión de 32 a 108 meses.
  La pena será de prisión de 16 a 36 meses cuando la cuantía no excede de 10 salarios mínimos legales mensuales vigentes.

- **Artículo 240:** Hurto calificado. La pena será de prisión de 48 a 144 meses, si el hurto se cometiere: Parágrafo 4. Con escalamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes.

- **Ley 1153 de 2007, Ley de pequeñas causas.** Las siguientes conductas contra el patrimonio económico cuya cuantía no supere los 10 salarios mínimos mensuales vigentes[6]:
    - Hurto
    - Hurto calificado
    - Hurto agravado
    - Hurto atenuado
    - Estafa
    - Emisión y transferencia ilegal de cheque
    - Abuso de confianza
    - Abuso de confianza calificado
    - Aprovechamiento de error ajeno o caso fortuito
    - Alzamiento de bienes
    - Disposición de bien propio gravado con prenda
    - Defraudación de fluidos
    - Perturbación de la posesión sobre inmuebles
    - Daño en bien ajeno

3. Normatividad

La siguiente es una compilación única de normatividad Colombiana relevante en materia de internet, comercio electrónico, contratación electrónica, privacidad, pornografía infantil, documento electrónico y delitos informáticos.

[6] Recuperado de: http://www.elabedul.net/Documentos/Leyes/2007/Ley_1153.pdf

- **Ley 692 de 2005**:

  Objetivo: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

- **Ley 794 de 2003**:

  Objetivo: Por la cual se modifica el Código de Procedimiento Civil, se regula el proceso ejecutivo y se dictan otras disposiciones.

- **Ley 788 de 2002:**

  Objetivo: Por la cual se expiden normas en materia tributaria y penal del orden nacional y territorial; y se dictan otras disposiciones.

- **Ley 765 de 2002:**

  Objetivo: Por medio de la cual se aprueba el 'Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de los niños en la pornografía', adoptado en Nueva York, el veinticinco (25) de mayo de dos mil (2000).

- **Ley 679 de 2001:**

  Objetivo: Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44.

- **Ley 599 de 2000:**

Objetivo: Por la cual se expide el Código Penal.

- **Ley 598 de 2000:**

Objetivo: Por la cual se crean el Sistema de Información para la Vigilancia de la Contratación Estatal, SICE, el Catálogo único de Bienes y Servicios, CUBS, y el Registro Único de Precios de Referencia, RUPR, de los bienes y servicios de uso común en la administración pública y se dictan otras disposiciones[7].

- **Ley 588 de 2000:**

Objetivo: Por la cual se reglamenta el ejercicio de la actividad notarial.

- **Ley 527 de 1999:**

Objetivo: Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- **Ley 1273 de 2009[8]:**

[7] Archivo General de la Nación. Recuperado de: http://archivogeneral.gov.co/?idcategoria=2040
[8] Recuperado de: http://www.informaticaforense.com.co/index.php/leyes/61-ley-1273-de-2009.

Esta ley creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273"Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos,

a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

El capítulo primero adiciona el siguiente articulado (subrayado fuera del texto):

- **Artículo 269A:** ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269B:** OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

- **Artículo 269C:** INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema

informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

- **Artículo 269D:** DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269E:** USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- **Artículo 269F:** VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien ‘sustraiga’ e ‘intercepte’ dichos datos a pedir autorización al titular de los mismos.

- **Artículo 269G:** SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

  En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

  La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

  Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “phishing”, modalidad de estafa que usualmente utiliza como medio el correo electrónico

pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de Delitos Informáticos de la Policía Judicial (Dijín) con esta modalidad se robaron más de 3.500 millones de pesos de usuarios del sistema financiero en el 2006.

Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala "por quien tuviere un vínculo contractual con el poseedor de la información".

Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal.

Por su parte, el capítulo segundo establece:

- **Artículo 269I:** HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.
- **Artículo 269J:** TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos o telemáticos.

Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea.

En este sentido y desde un punto de vista empresarial, la nueva ley pone de presente la necesidad para los empleadores de crear mecanismos idóneos para la protección de uno de sus activos más valiosos como lo es la información.

Las empresas deben aprovechar la expedición de esta ley para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información.

Por otra parte, es necesario regular aspectos de las nuevas modalidades laborales tales como el teletrabajo o los trabajos desde la residencia de los trabajadores los cuales exigen un nivel más alto de supervisión al manejo de la información.

Así mismo, resulta conveniente dictar charlas y seminarios al interior de las organizaciones con el fin de que los trabajadores sean conscientes del nuevo rol que les corresponde en el nuevo mundo de la informática.

Lo anterior, teniendo en cuenta los perjuicios patrimoniales a los que se pueden enfrentar los empleadores debido al uso inadecuado de la información por parte de sus trabajadores y demás contratistas.

Pero más allá de ese importante factor, con la promulgación de esta ley se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.

4. Decretos

- **Decreto 2926 de 2005:**

  Objetivo: Por el cual se modifica el Decreto 2542 de 1997.

- **Decreto 4149 de 2004:**

  Objetivo: Por el cual se racionalizan algunos trámites y procedimientos de comercio exterior, se crea la Ventanilla Única de Comercio Exterior.

- **Decreto 3055 de 2003:**

  Objetivo: Por el cual se modifica el decreto 600 de 2003.

- **Decreto 866 de 2003:**

  Objetivo: Por el cual se modifica el artículo 14 del decreto 2170 de 2002.

- **Decreto 600 de 2003:**

  Objetivo: Por medio del cual se expiden normas sobre los servicios de valor agregado y telemáticos y se reglamente el decreto-ley 1900 de 1990.

- **Decreto 067 de 2003:**

  Objetivo: Por el cual se prorroga el plazo previsto en el primer inciso del artículo 8 del Decreto 1524 de 2002.

- **Decreto 2170 de 2002:**

  Objetivo: Por el cual se reglamenta la ley 80 de 1 9 93, se modifica el decreto 8 55 de 1 9 94 y se dictan otras disposiciones en aplicación de la Ley 52 7 de 1999.

- **Decreto 1524 de 2002:**

  Objetivo: Por el cual se reglamenta el artículo 5 de la Ley 679 de 2001.

- **Decreto 898 de 2002:**

Objetivo: Por el cual se reglamenta el Título VI del Libro Primero del Código de Comercio y se dictan otras disposiciones reglamentarias.

- **Decreto 408 de 2001:**

  Objetivo: Por medio del cual se reglamenta el artículo 579-2 del Estatuto Tributario.

- **Decreto 1747 de 2000:**

  Objetivo: Por el cual se reglamenta parcialmente la Ley 527 de 1999 en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

- **Decreto 726 de 2000:**

  Objetivo: Por el cual se reglamenta la elección de directivos de las Cámaras de Comercio y se dictan otras disposiciones.

- **Decreto 266 de 2000:**

  Objetivo: Normas para suprimir y reformar las regulaciones, trámites y procedimientos.

5. **Resoluciones**

- **Resolución 1271 de 2005:**

  Objetivo: Por la cual se fija el precio de los aplicativos informáticos para su transmisión a la Ventanilla Única de Comercio Exterior – Vuce[9].

[9] Archivo General de la Nación. Recuperado de: http://archivogeneral.gov.co/?idcategoria=2040

- **Resolución 01455 de 2003:**

  Objetivo: Por medio de la cual se regula la administración de registros del dominio .co.

- **Resolución 000020 de 2003:**

  Objetivo: Por medio de la cual se establece el procedimiento a seguir por el Ministerio de Comunicaciones para la fijación de las condiciones de administración del dominio .co.

- **Resolución 600 de 2002:**

  Objetivo: Por medio de la cual se regula parcialmente la administración del dominio punto co = .co.

- **Resolución 05339 de 2002:**

  Objetivo: Por la cual se modifican las Resoluciones 05313 y 05314 de febrero 28 de 2002.

- **Resolución 36904 de 2001:**

  Objetivo: Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.

- **Resolución 26930 de 2000:**

Objetivo: Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.

- **Resolución 307 de 2000:**

  Objetivo: Por la cual se promueve el acceso a Internet a través de planes tarifarías para el servicio de TPBLC y se dictan otras disposiciones.

- **Resolución 7652 de 2000:**

  Objetivo: Por la cual se reglamenta la administración, publicación y uso de la información electrónica vía Intranet e Internet en la Dirección de Impuestos y Aduanas Nacionales.

6. Proyectos de normatividad

- **Proyecto de ley 166 de 2003 (Cámara de representantes):**

  Objetivo: Por el cual se regulan las comunicaciones Vía Internet y mediante el uso de Fax que se realicen desde lugares habilitados para brindar al público esos servicios.

- **Proyecto de ley 71 de 2002(Senado de la república):**

  Objetivo: Por la cual se reglamentan los bancos de datos financieros o de solvencia patrimonial y crediticia y se dictan otras disposiciones[10].

[10] Archivo General de la Nación. Recuperado de: http://archivogeneral.gov.co/?idcategoria=2040

8. Diseño metodológico

A continuación se realizará una descripción de cómo se llevará a cabo la investigación, indicando la estrategia para obtener la información, puntualizando las actividades necesarias para darle respuesta a los objetivos planteados.

8.1 Enfoque

"La metodología cualitativa, tiene como objetivo la descripción de las cualidades de un fenómeno, se trata de hablar de un entendimiento en profundidad del problema en cuestión. Este tipo de investigación busca analizar exhaustivamente el asunto o actividad particular y se interesa más en saber cómo se da la dinámica o como ocurre el proceso en que se da la determinada situación o problema de estudio".[11]

Los investigadores cualitativos participan en la investigación a través de la interacción con los sujetos que estudian, analizan y comprenden estos sujetos y su problemática para entender el problema como un todo.

Por lo anterior, es que la investigación de este documento es de tipo cualitativa, puesto que dentro de sus características más relevantes evidencia paso a paso la estrategia para conocer los procesos y la estructura de cada área de HGM, los investigadores conocen y están involucrados en el proceso a investigar y entienden la problemática presentada. Además, se tiene un conocimiento importante del proceso a profundidad como principal insumo para el estudio y análisis de ataques, penetración

[11] Recuperado de: http://www.ponce.inter.edu/cai/Comite-investigacion/investigacion-cualitativa.html

de intrusos y acceso no autorizado en sistemas operativos Windows, AIX y bases de DB2 tomando en consideración aquellos elementos que aporten criterios con los cuales se puedan realizar juicios valorativos respecto al papel que juega la forénsica digital ante éste tipo de hechos. Además porque el cliente Hospital General de Medellín tiene esta plataforma tecnológica.

8.2 Tipo de estudio

En la elaboración de la investigación de metodologías para manejo de incidentes en TI mediante actividades de forénsica digital se optó por un tipo de investigación descriptivo.

El estudio se adapta en una investigación de tipo descriptivo, porque recoge sistemáticamente, la información sobre los hechos, las situaciones y características de una población o área de interés. Por lo que permite informarse como es una determinada situación, señalar su naturaleza y el tipo de condiciones existentes en un momento determinado.

El trabajo de investigación tiene como propósito identificar el procedimiento que puede ser utilizado para determinar metodologías para manejo de incidentes en TI mediante actividades de forénsica digital. Permitiendo obtener información sobre la situación que presenta una determinada organización aun conociendo cual es la naturaleza del problema.

8.3 Método de estudio

El método de investigación que se utilizara en este análisis es el deductivo, porque partir de los incidentes en TI se investigara sobre metodologías para el manejo de dichos incidentes por medio de actividades de forénsica digital.

8.4 Población y muestra

Se realizaron encuestas a través de correo electrónico a los Analistas de sistemas, Ingenieros Informáticos y de Sistemas que laboran en el área de sistemas del Hospital General de Medellín.

Dentro del área de sistemas existen varias áreas de atención a las que son escalados los incidentes o requerimientos informáticos provenientes de las áreas de usuarios finales, estas son:

- Mesa de ayuda nivel 1: Soporte en sitio
- Mesa de ayuda nivel 1 especializado: Redes
- Mesa de ayuda nivel 1 especializado: Servidores
- Mesa de ayuda nivel 2 SAP: Nivel básico de atención
- Mesa de ayuda nivel 2 SAP: Nivel especializado de atención
- Mesa de ayuda nivel 2 SAP: Soporte servidores, plataforma, canal de comunicación, bases de datos.

Para este ejercicio, se tomaron encuestados de cada una de las áreas de atención descritas anteriormente, y así poder tener una muestra representativa para establecer las casuísticas de los incidentes o requerimientos que se presentan relacionados con la seguridad de la información.

A. Espacial: La ubicación donde se va a realizar la investigación será en la ciudad de Medellín, específicamente para el Hospital General de Medellín.

El espacio geográfico está constituido por los sitios en los cuales se encuentra el material bibliográfico, documentos, escenarios virtuales y físicos donde se llevarán a cabo las

asesorías técnicas y metodológicas, se recolectará y analizará la información pertinente para esta investigación.

B. Temporal: El estudio se llevará a cabo durante todo el 2014 comenzando desde octubre y terminando en mayo de 2015.

8.5 Categorías de análisis

Se analizarán los riesgos y vulnerabilidades existentes actualmente dentro del área de sistemas del Hospital General de Medellín, así como de los aplicativos y plataformas usadas para la centralización de los datos; reflejado esto en las variables técnicas propias de la plataforma tales como:

- Almacenamiento disponible: esta variable indica si existe el espacio suficiente para el crecimiento de los filesystem tanto para los servicios SAP como base de datos.

- Crecimiento de almacenamiento base de datos: este indicador muestra el porcentaje de crecimiento mensual de la base de datos, después de realizar la depuración de los datos.

- Eficiencia backup mensual: en esta variable se espera observar el cumplimiento mensual de la ejecución del backup a disco y a cinta para cada uno de los ambientes implementados dentro de la plataforma.

- Eficiencia backup histórico: esta variable muestra el comportamiento del backup mensual y su comportamiento histórico.

- Disponibilidad de la plataforma mensual: esta variable indica la cantidad de indisponibilidades que ha sufrido la plataforma ya sea por inconvenientes en el servicio del canal de comunicaciones o la falla del fluido eléctrico del HGM.

- Disponibilidad de la plataforma histórica: esta variable indica la cantidad de indisponibilidades que ha sufrido la plataforma a lo largo de todos los meses.

- Performance tiempo de respuesta: esta variable muestra el incremento/disminución en los tiempos de respuesta del ambiente de producción con relación al número de usuarios concurrentes que acceden al sistema.

- Consumo CPU: este indicador evidencia el consumo de CPU y el efecto de la paginación[12].

- Memoria buffer pool: esta variable muestra el comportamiento de la extensión de la capacidad de la memoria. Lo recomendado como buena práctica es que esté indicador esté por encima del 96%.

- Parámetros de configuración de base de datos: el indicador catalog cache muestra la cantidad máxima de espacio de almacenamiento dinámico de base de datos que el caché del catálogo[13] puede usar y el indicador de package cache muestra la cantidad de memoria heap que se usa para el almacenamiento en caché de sentencias SQL estáticas y dinámicas

[12] Paginación: los programas dividen la memoria en partes (páginas), de este modo la cantidad de memoria desperdiciada por un proceso está en la última página.
[13] Caché de catálogo: se refiere a la cantidad de veces que una tabla, vista o alias se procesa durante la compilación de una sentencia SQL.

de un paquete. Lo recomendado como buena práctica es que esté indicador esté por encima del 98%.

- Tiempo promedio lectura/escritura: este indicador muestra dos tipos de variables: la de lectura/escritura asíncrona física y la de lectura/escritura directa. Los tiempos recomendados para las dos variables son: lectura 5ms y escritura 2ms.

- Bloqueos en base de datos: esta variable muestra la cantidad de bloqueos deadlocks y lock timeouts[14] en la base de datos.

- Tiempo promedio del sort: este indicador muestra los ahorros significativos en tiempo de ejecución de procesos de carga, reorganización y reconstrucción de índices a nivel de bases de datos. Lo recomendado como buena práctica es que esté indicador sea menor a 1ms.

- Transacciones más usadas: este indicador muestra las 5 transacciones SAP más usadas.

8.6 Técnicas e instrumentos de recolección y análisis de la información

Se realizarán revisiones de los informes de la plataforma, tanto de los servidores como de la base de datos para verificar los mayores puntos de mejora de esta y así identificar los incidentes más comunes. Adicionalmente, se realizarán entrevistas con los analistas del área de sistemas de HGM para verificar que interrupción de la plataforma les han reportado los usuarios finales o que otro

[14] Deadlock y lock timeouts: DB2 usa este tipo de bloqueos en objetos de datos. Tipos de bloqueos que se pueden colocar en filas, tablas y bases de datos.

tipo de inconvenientes son de su conocimiento y que estén dentro de alguna de las categorías anteriormente mencionadas.

También se realizarán entrevistas al DBA y BASIS que son las personas encargadas de generar los informes de desempeño de la plataforma y de alertar sobre los hallazgos de la misma. (Ver Anexo 1).

9. Análisis de la información

Al realizar el análisis de la situación actual de la plataforma del Hospital General de Medellín, se ha identificado el resultado para cada una de las categorías establecidas dentro de este estudio, las cuales son:

- Almacenamiento disponible:

Filesystem	GB	Usado	Disponible	Free	%Iused
/dev/hd4	8,38	4,22	4,16	51%	/
/dev/hd9var	2,75	0,82	1,93	30%	/var
/dev/hd3	5	4,41	0,59	89%	/tmp
/dev/hd1	3	2,56	0,44	86%	/home
/dev/hd11admin	0,12	0	0,12	1%	/admin
/proc	-		-	-	/proc
/dev/hd10opt	2	0,2	1,8	11%	/opt
/dev/livedump	0,25	0	0,25	1%	/var/adm/ras/livedump
/dev/sapcd_lv	350	287,99	62,01	83%	/sapcd
/dev/backup_lv	9200	5786,95	3413,05	63%	/backup
/aha	-		-	-	/aha
/dev/db2prd_lv	3	0,12	2,88	5%	/db2/PRD
/dev/db2dump_lv	1	0,15	0,85	15%	/db2/PRD/db2dump
/dev/logarchive_lv	3	0	3	1%	/db2/PRD/log_archive
/dev/logdir_lv	50	13,76	36,24	28%	/db2/PRD/log_dir
/dev/sapddata1_lv	**449,75**	**147,09**	**302,66**	**33%**	**/db2/PRD/sapdata1**
/dev/sapddata2_lv	**449,75**	**147,09**	**302,66**	**33%**	**/db2/PRD/sapdata2**
/dev/sapddata3_lv	**449,75**	**147,09**	**302,66**	**33%**	**/db2/PRD/sapdata3**
/dev/sapddata4_lv	**449,75**	**163,83**	**285,9**	**37%**	**/db2/PRD/sapdata4**
/dev/saptemp_lv	5	0	5	1%	/db2/PRD/saptemp1
/dev/db2db2prd_lv	6	3,34	2,66	56%	/db2/db2prd
/dev/usrsap_lv	15	1,57	13,43	11%	/usr/sap
/dev/usrsapprd_lv	57,75	3,8	53,95	7%	/usr/sap/PRD
/dev/sapmntprd_lv	5	2,38	2,62	48%	/sapmnt/PRD
hgmsapdev01:/usr/sap/trans	99,75	35,51	64,24	36%	/usr/sap/trans
Total	**2063,75**	**677,74**	**1386,01**		
		33%	**67%**		

Filesystem	GB	Usado	Disponible	Free	%Iused
/dev/sapddata1_lv	449,75	147,09	302,66	33%	/db2/PRD/sapdata1
/dev/sapddata2_lv	449,75	147,09	302,66	33%	/db2/PRD/sapdata2
/dev/sapddata3_lv	449,75	147,09	302,66	33%	/db2/PRD/sapdata3
/dev/sapddata4_lv	449,75	163,83	285,92	37%	/db2/PRD/sapdata4
TOTAL	**1799**	**605,1**	**1193,9**		
		36%	**64%**		

Figura 4. Disposición espacio filesystem SAP.

RESULTADOS: se detectó que el espacio disponible para el crecimiento de los filesystem de los servidores de bases de datos del ambiente de desarrollo de SAP tiene un porcentaje muy bajo de crecimiento (33%) lo que implicaría aumento en el hardware físico disponible del servidor o una redistribución de los componentes de hardware para evitar sobrepasar el límite adecuado para este tipo de servidores que debe estar alrededor del 45%. Adicional, pueden realizarse actividades de mantenimiento a nivel de bases de datos como comprimir la información o re indexar.

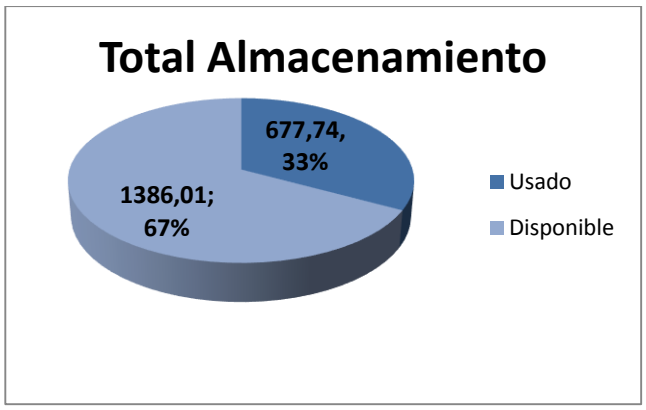


Figura 5. Porcentaje total almacenamiento SAP.

RESULTADOS: se detectó que en general el porcentaje de espacio disponible de los servidores de aplicación SAP, es el adecuado para la cantidad de información que posee el HGM.

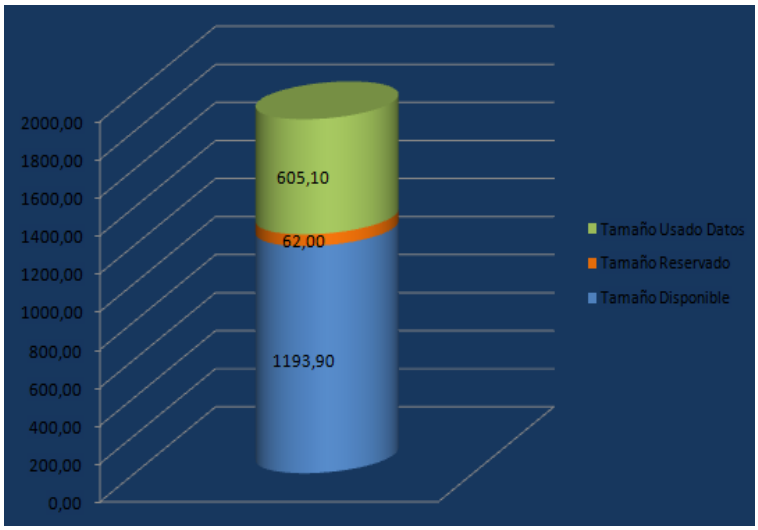


Figura 6. Porcentaje total almacenamiento base de datos.

RESULTADOS: en general, el total de almacenamiento con respecto al tamaño de datos usados, el tamaño reservado y el tamaño disponible es el adecuado para este tipo de plataforma de información.

- Crecimiento de almacenamiento base de datos:

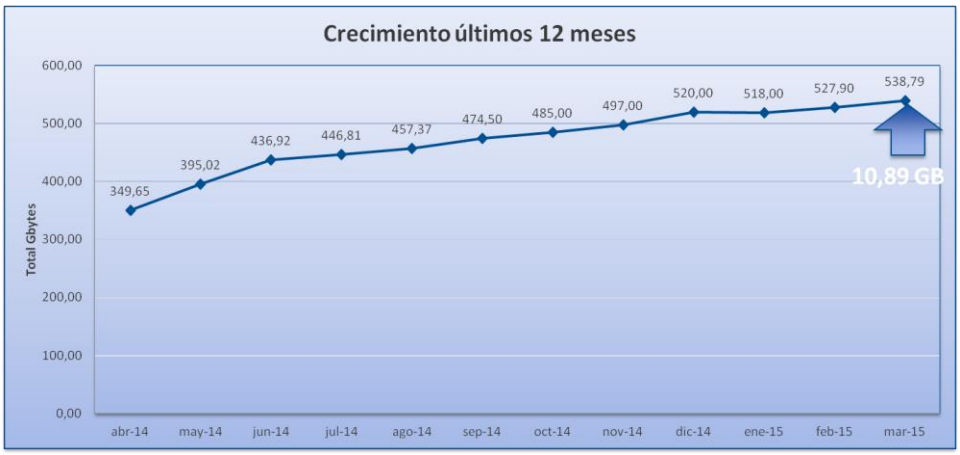


Figura 7. Porcentaje crecimiento base de datos.

RESULTADOS: se detectó que el porcentaje de crecimiento mensual de la base de datos ha estado en aumento, esto se debe a la habilitación de nuevas funcionalidades de SAP como el monitor IQ, Solman, FIORI, BI y BO.

- Eficiencia backup mensual:

PLAN DE BACKUP ERP SAP						
Marzo - 2015						
AMBIENTE	Eficiencia	Diarios	Fallidos	Correctos	Total/Fecha	Totales/Mes
Desarrollo - DEV	100%	1	0	31	31	31
Calidad - QAS	100%	1	0	31	31	31
Productivo - PRD	100%	1	0	31	31	31
SandBox - SBX	100%	1	0	31	31	31
SOLMAN	100%	1	0	31	31	31

Figura 8. Plan de backup mensual.

RESULTADOS: se muestra el plan de backup de los servidores de SAP, mostrando la cantidad de backups fallidos o ejecutados con éxito.

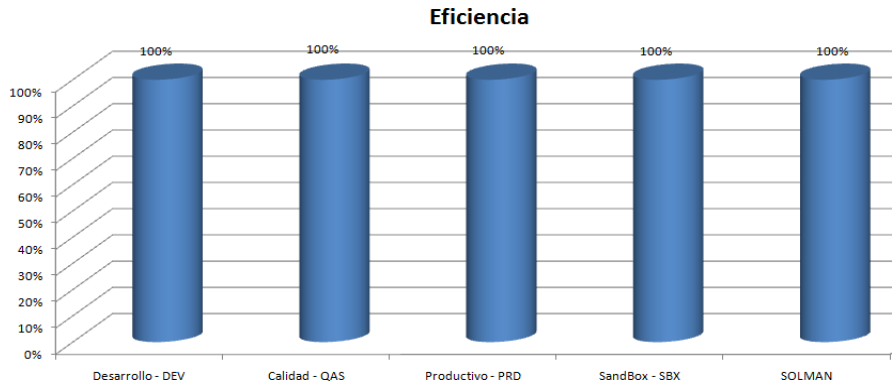


Figura 9. Gráfica de eficiencia.

RESULTADOS: se muestra la eficiencia en utilización de recursos usados del servidor para la ejecución del plan de backup de los servidores de SAP, evidenciando que esta ha sido óptima.

- Eficiencia backup histórico:

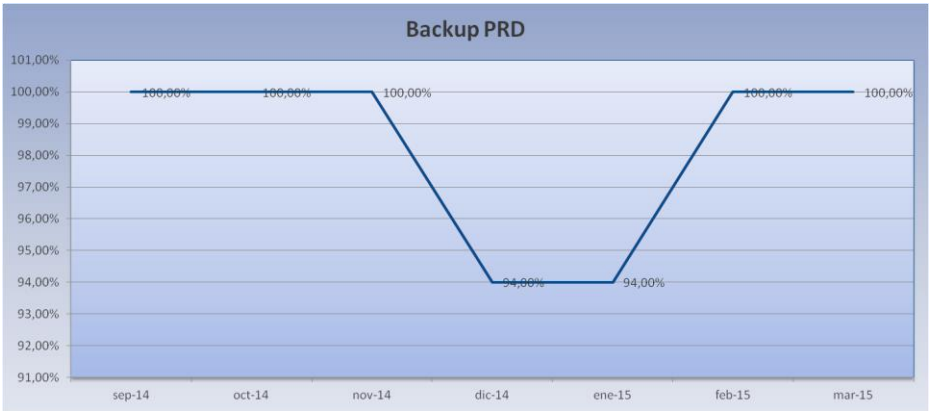


Figura 10. Gráfica de eficiencia backup histórica.

RESULTADOS: se muestra la eficiencia histórica en utilización de recursos usados del servidor para la ejecución del plan de backup de los servidores de SAP, evidenciando que esta ha sido óptima a excepción de los meses de diciembre y enero donde se realizaron ventanas de mantenimiento para redistribuir los recursos físicos de hardware de los servidores.

- Disponibilidad de la plataforma mensual:

DISPONIBILIDAD ERP SAP Marzo - 2015								
AMBIENTE	Disponibilidad Total Mes (Horas)	Ventana	Horas Mes Disponible Con Ventana	% Disponible Con Ventana	Disponibilidad Comprometida	Indisponibilidad Sin Ventana	Horas Mes Disponible SIN Ventana	% Disponible SIN Ventana
Desarrollo - DEV	744	0	744,0	100,00%		0	744,0	100,00%
Calidad - QAS	744	0	744,0	100,00%		0	744,0	100,00%
Productivo - PRD	744	0	744,0	100,00%		0,38	743,6	99,95%
SandBox - SBX	744	0	744,0	100,00%		0	744,0	100,00%
SOLMAN	744	0	744,0	100,00%		0	744,0	100,00%

Figura 11. Gráfica de disponibilidades SAP mensual.

RESULTADOS: se muestra la cantidad de indisponibilidades que se han presentado en la plataforma, mostrando una indisponibilidad de 24 minutos en el ambiente de producción debido a la intermitencia del canal de comunicación entre la sede del Hospital General de Medellín y el lugar donde se alojan los servidores (DATACENTER UNE).

- Disponibilidad de la plataforma histórica:

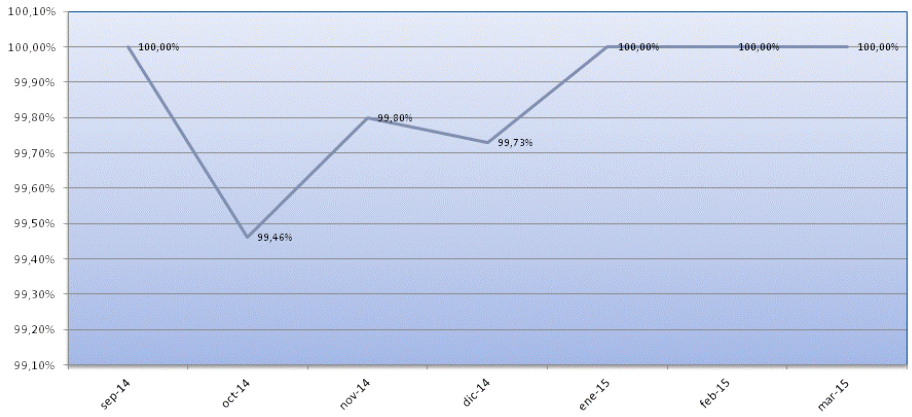


Figura 12. Gráfica de disponibilidades SAP histórico.

RESULTADOS: se muestra la cantidad de indisponibilidades históricas que se han presentado en la plataforma, evidenciando que en los meses de octubre y noviembre se presentaron indisponibilidades del servicio debido a ventanas de mantenimiento realizadas por redistribución del componente físico de hardware del servidor y en el mes de diciembre por problemas con el canal de comunicación entre la sede de HGM y el DATACENTER de Une.

- Performance tiempo de respuesta:

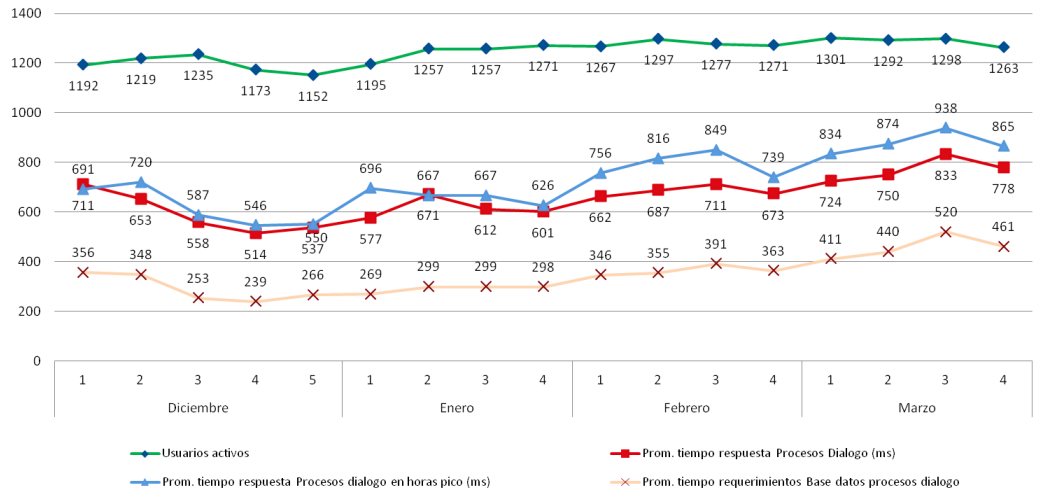


Figura 13. Relación tiempos de respuesta del sistema.

RESULTADOS: se muestra el incremento/disminución en los tiempos de respuesta del ambiente de producción con relación al número de usuarios concurrentes que acceden al sistema, evidenciando que en el mes de marzo se presenta un aumento del tiempo de respuesta de los procesos tanto a nivel de aplicación como de bases de datos.

- Consumo CPU:

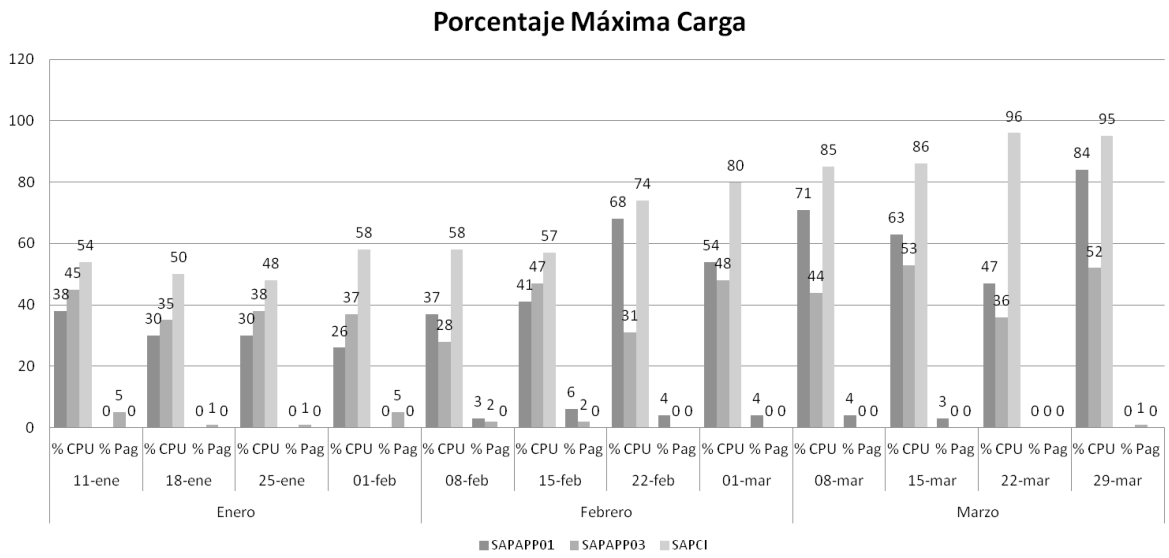


Figura 14. Porcentaje de consumo (carga).

RESULTADOS: se muestra el consumo de CPU y el efecto de la paginación, observando que desde el mes de febrero se viene presentando un consumo de CPU mayor al de los meses anteriores y sobre todo en el ambiente de producción, esto debido a la habilitación de las nuevas funcionalidades de SAP: Monitor IQ, Fiori, BI, BO y Solman.

- Memoria buffer pool:

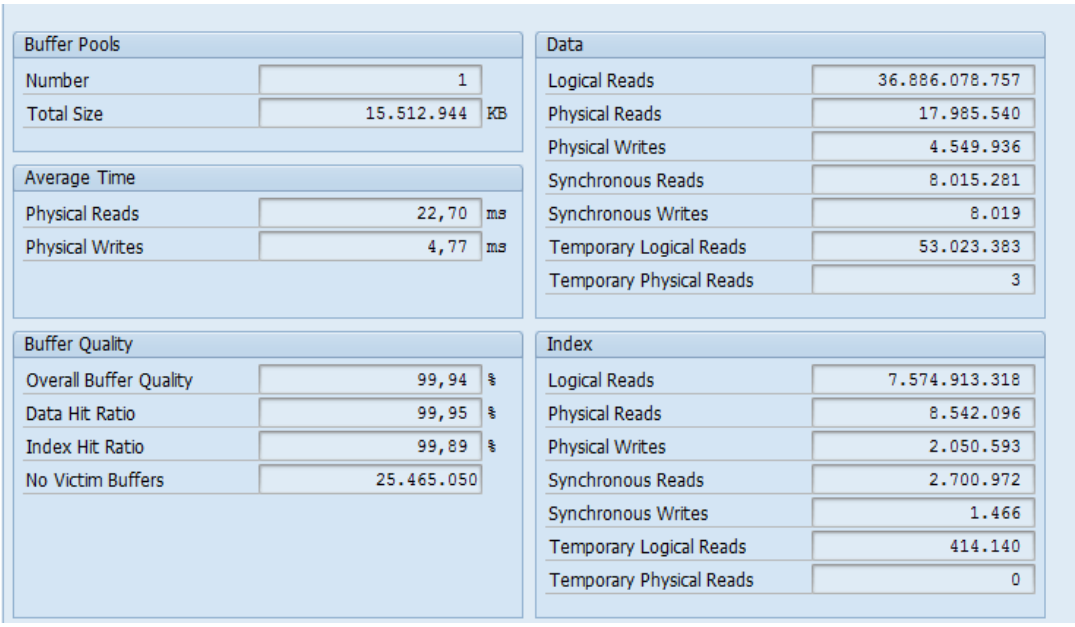


*Figura 15.*Indicador performance buffer pools.

RESULTADOS: se muestra el comportamiento de la extensión de la capacidad de la memoria, evidenciando que el valor está conforme a lo recomendado como buena práctica y es que esté por encima del 96%.

- Parámetros de configuración de base de datos:

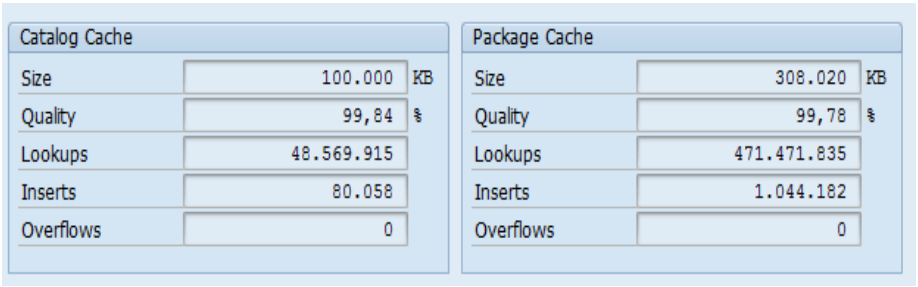


*Figura 16.*Parámetros de configuración BD.

RESULTADOS: se detecta que el indicador catalog cache que muestra la cantidad máxima de espacio de almacenamiento dinámico de base de datos que el caché del catálogo puede usar está acorde al valor recomendado y es que esté por encima del 98%. Adicional, se evidencia que el indicador de package cache que muestra la cantidad de memoria heap que se usa para el almacenamiento en caché de sentencias SQL estáticas y dinámicas de un paquete está acorde a lo recomendado y es que esté por encima del 98%.

- Tiempo promedio lectura/escritura:

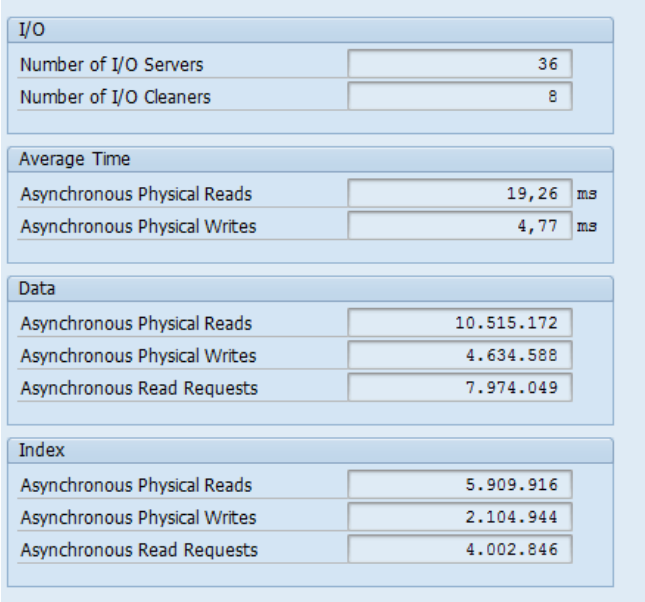


Figura 17 .Tiempos de lectura/escritura física.

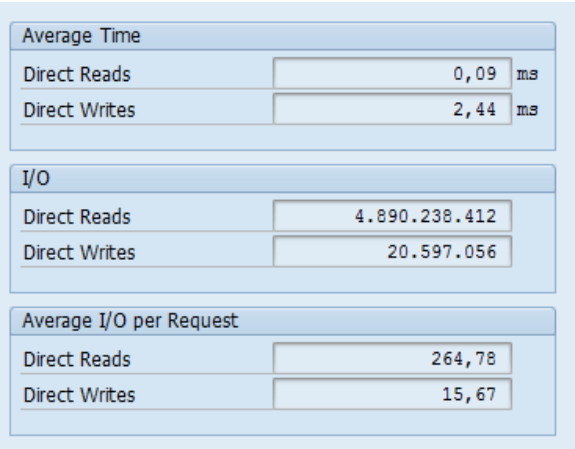


Figura 18 .Tiempos de lectura/escritura directa.

RESULTADOS: se detecta que los indicadores de lectura/escritura asíncrona física están por fuera de los niveles recomendados como buena práctica. Adicional, el indicador de lectura/escritura directa están bajo los valores recomendados. Para los dos casos, los valores recomendados son de lectura 5ms y escritura 2ms.

- Bloqueos en base de datos:

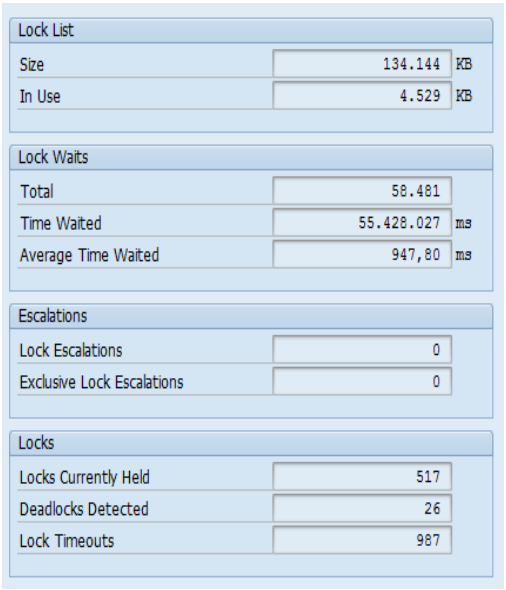


Figura 19. Deadlock y lock timeout.

RESULTADOS: se muestra la cantidad de bloqueos deadlocks y lock timeouts en la base de datos, evidenciando que se siguen presentando bloqueos entre los objetos reservados de la base de datos.

- Tiempo promedio del sort:

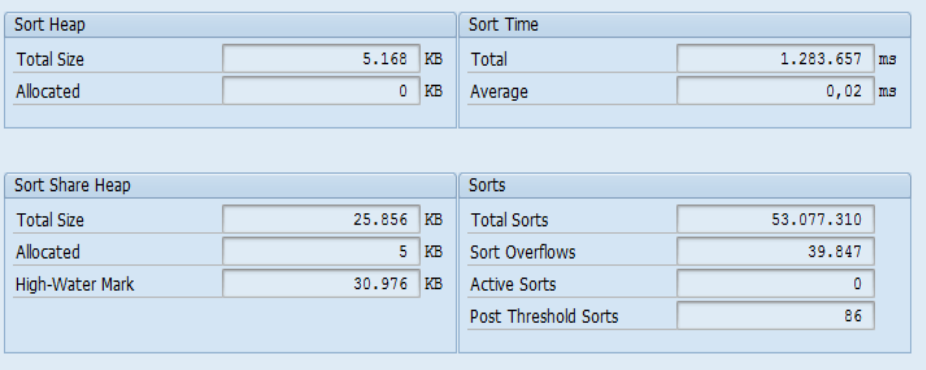
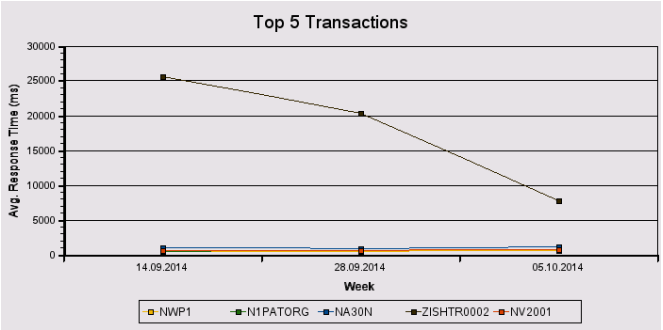


Figura 20. Tiempo promedio sort.

RESULTADOS: se muestran los ahorros significativos en tiempo de ejecución de procesos de carga, reorganización y reconstrucción de índices a nivel de bases de datos, evidenciando que este tiempo está acorde con lo recomendado y es que esté indicador sea menor a 1ms.

- Transacciones más usadas:



Transaction Code	Load (%)	Nombre Transacción
NWP1	66.1	Puestos de Trabajo
N1PATORG	3.6	Organizador de Pacientes
NA30N	3.0	Facturación
ZISHTR0002	2.9	Pedidos clte.prontos a envío
NV2001	2.2	Creación Episodios

Figura 21. Top 5 transacciones más usadas.

RESULTADOS: se muestran las 5 transacciones SAP más usadas por las áreas usuarias, evidenciando que el mayor número de transacciones se reconcentra en las áreas de la vertical de salud.

10. Metodología de forénsica digital para el Hospital General de Medellín

Dentro de cualquier investigación es necesario contar con un método que permita dar credibilidad a la misma, a través de un cuidadoso manejo de las evidencias recolectadas para no afectar la credibilidad de toda la investigación. Es así, como para el Hospital General de Medellín, se propone implantar la metodología que se describirá a continuación para el manejo de los incidentes que deben ser tratados bajo la lupa de la forénsica digital.

Dentro de la metodología que se propone, lo inicial es conocer las fases y las actividades comprendidas dentro de cada una de ellas:

Figura 22. Fases metodología forénsica digital HGM.

Para comenzar con la implementación de la metodología es importante tener claro el concepto de Incidente de seguridad informática, puesto que no todos los incidentes informáticos están relacionados con una vulneración de la información en donde sea necesario realizar una investigación detallada de un posible ataque informático.

Un incidente de seguridad informática se entiende como una violación o intento de violación de la política de seguridad de uso adecuado de utilización de los sistemas informáticos. Es entonces allí cuando entra la puesta en marcha de la metodología que se definiría a continuación.

10.1.1 Fases de recolección

Dentro de esta fase existen dos actividades primordiales que deben realizarse:

1. Identificación del incidente: lo primero es que se debe descartar fallas de hardware o software de la red o el servidor. Una vez esto sea descartado, el siguiente paso deberá ser realizar listas de comprobación del sistema para estar seguros de que se trata de un incidente de seguridad informática.

   Las comprobaciones básicas que deben realizarse son:

   - Comandos en modo consola (cmd, bash)
   - Listar direcciones IP del sistema y mapear las direcciones físicas MAC con las IP
   - Buscar archivos ocultos o eliminados
   - Verificar las bitácoras (logs) del sistema
   - Verificar la configuración de seguridad del sistema
   - Generar funciones hash de ficheros
   - Leer, copiar y escribir a través de la red
   - Realizar copias bit a bit de discos duros y particiones
   - Analizar el tráfico de la red

2. Recopilación de la evidencia: una vez se está seguro del incidente, se procede a realizar una bitácora detallada al realizar la inspección de los archivos, sistemas o dispositivos atacados. Para la recopilación de estas evidencias lo principal es desconectar el equipo de la red eléctrica, si bien podrán perderse datos de la memoria RAM, micro, etc es información volátil, pero aún se tendrá suficiente información que recuperar para dar tratamiento al incidente.

Supongamos entonces, que se puede mantener activo el sistema por medio de una UPS o algún otro mecanismo, lo primero que se deberá realizar es una imagen del disco bit a bit en CD, DVD o un ambiente paralelo de la información para recrear la escena, además de recolectar esta información en tiempo real:

- ✓ Registros y contenidos de la caché
- ✓ Contenidos de la memoria
- ✓ Estado de las conexiones de red
- ✓ Listar procesos activos, recursos que usa, usuarios o aplicaciones que lanzaron dichos procesos
- ✓ Contenido de archivos o discos duros
- ✓ Contenido de otros dispositivos de almacenamiento
- ✓ Fecha y hora del sistema
- ✓ Puertos TCP/UDP abiertos y las aplicaciones que los usan
- ✓ Usuarios conectados local y remotamente

10.1.2 Fases de evaluación

Dentro de esta fase es primordial preservar la evidencia para no perder las huellas digitales del ataque. Como primera medida se deberán realizar dos copias de las evidencias y sobre estas comenzar a realizar el análisis exhaustivo de la información.

Estas copias pueden realizarse mediante el empleo de funciones hash como MD5[15] o SHA3[16]. Una vez realizadas estas copias se deberán etiquetar con la fecha y hora de creación y el nombre de cada copia.

A continuación, se debe establecer la cadena de custodia, estableciendo los responsables con sus datos básicos y controles de las personas que manipularán la evidencia, es decir:

- Dónde, cuándo y quién manipuló la evidencia con nombres, cargo, identificación, fechas y horas, etc.
- Quién estuvo custodiando la evidencia, durante cuánto tiempo y dónde se almacenó.
- Cuándo se cambie la custodia de la evidencia también deberá dejarse el registro correspondiente.

10.1.3 Fases de análisis

Dentro de esta fase es necesario realizar las siguientes actividades:

1. Preparación del entorno: es indispensable contar con un ambiente para recrear el escenario en el que se presentó el ataque y poder observar las evidencias recolectadas en la fase anterior. Para esto, es importante disponer dos estaciones de trabajo, ya sean físicas o virtuales para cargar las imágenes de disco y reconstruir la secuencia del ataque.

[15] Algoritmo de reducción criptográfico de 128 bits
[16] Algoritmo de hash seguro que produce una salida resumen de 160 bits (20 bytes), similar a MD5

2. Reconstrucción de la secuencia del ataque: una vez las imágenes del disco están implementadas, se debe proceder a establecer la línea de tiempo con los sucesos que dieron evidencia del ataque, teniendo en cuenta:

    - Marcas de tiempo MACD (fecha y hora de modificación, acceso, creación y borrado)
    - Ruta completa
    - Tamaño en bytes y tipos de archivos
    - Usuarios y/o grupos a los que pertenece
    - Permisos de acceso
    - Archivos borrados o no

    Una vez el sistema tenga recreados los datos, se procede a establecer cómo se realizó el ataque, identificando la vía de acceso al sistema a través de la cual se presentó la vulnerabilidad o el agujero de seguridad.

    El punto de partida para esta reconstrucción es verificar los procesos y servicios que estaban ejecutándose en ese momento y que aparecen dentro de la evidencia recolectada, verificar los aplicativos, las peticiones de servicios, en fin, es importante fortalecer cada hipótesis estableciendo causa-efecto para descartar una a una todas las posibilidades.

3. Identificación de los autores: con la reconstrucción de la secuencia del ataque, es importante establecer ahora los autores de este además si el caso es establecer acciones legales o investigaciones internas dentro de la organización.

   Para esto es necesario revisar las evidencias volátiles recopiladas tales como los puertos y direcciones IP desde las que se realizaron solicitudes y los log's de conexiones.

   Lo principal es averiguar la dirección IP del atacante, por lo que deben revisarse los registros de conexiones de red, procesos y servicios que estaban cargados, archivos de la memoria virtual, conexiones fallidas, etc. Si se detecta una dirección IP sospechosa, el siguiente paso es buscar en el registro RIPE NCC (www.ripe.net) a quien pertenece. Una vez detectada la dirección IP, se debe descartar que no se haya usado desde ordenadores "espejo" empleados para la suplantación de identidad, esto mediante la aplicación de mapeadores de red.

4. Evaluación del impacto: para establecer el impacto causado por el atacante, hay que reconocer si se trata de un ataque pasivo o activo. Los ataques pasivos son en los que no se altera la información ni la operación normal de los sistemas, sólo se fisgonea por ellos. Los ataques activos son en los que la información y la operación son alteradas.

   Una vez establecido el tipo de ataque, se deberán valorar los riesgos e impactos surgidos del ataque y que han sido materializados para poder establecer los daños

monetarios, afectación de la imagen, etc todo lo que se pueda presentar dentro de esta valoración del ataque.

10.1.4 Fases de reportes

Dentro de esta fase es importante establecer la generación de los informes para explicar en detalle la situación presentada.

Para esto, es indispensable presentar dos tipos de informes: uno técnico y uno ejecutivo.

Informe técnico: este informe deberá incluir todo el detalle del análisis realizado, como:

- Antecedentes del incidente.
- Recolección de los datos.
- Descripción de la evidencia.
- Entorno del análisis.
- Análisis de la evidencia.
- Descripción de los hallazgos.
- Cronología de la intrusión.
- Conclusiones.
- Recomendaciones

Informe ejecutivo: este informe debe ser en un lenguaje común y no técnico que pueda ser entendido por las personas no técnicas ni especializadas en el tema y donde se incluya.

- Motivos de la intrusión.
- Desarrollo de la intrusión
- Resultados del análisis.
- Recomendaciones.

Para el desarrollo de la metodología anteriormente descrita, se debe tener en cuenta que el proceso y flujo que deben seguirse para el registro y seguimiento de este tipo de solicitudes de servicio son los establecidos para HGM desde el sistema de gestión de calidad (SGC).

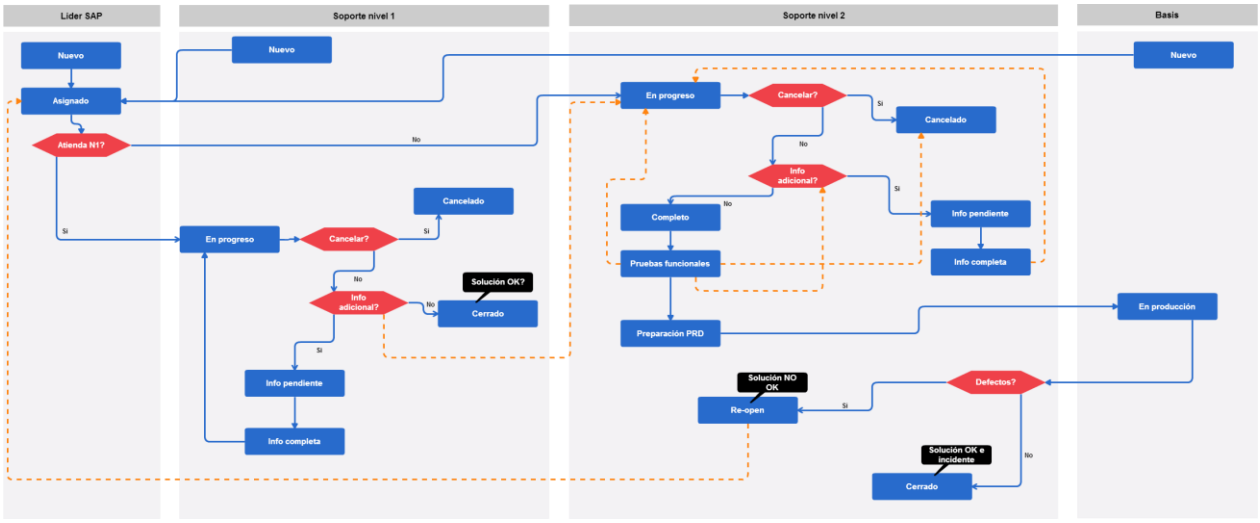


Figura 23. Flujo de atención de incidentes.

11. Cronograma de actividades

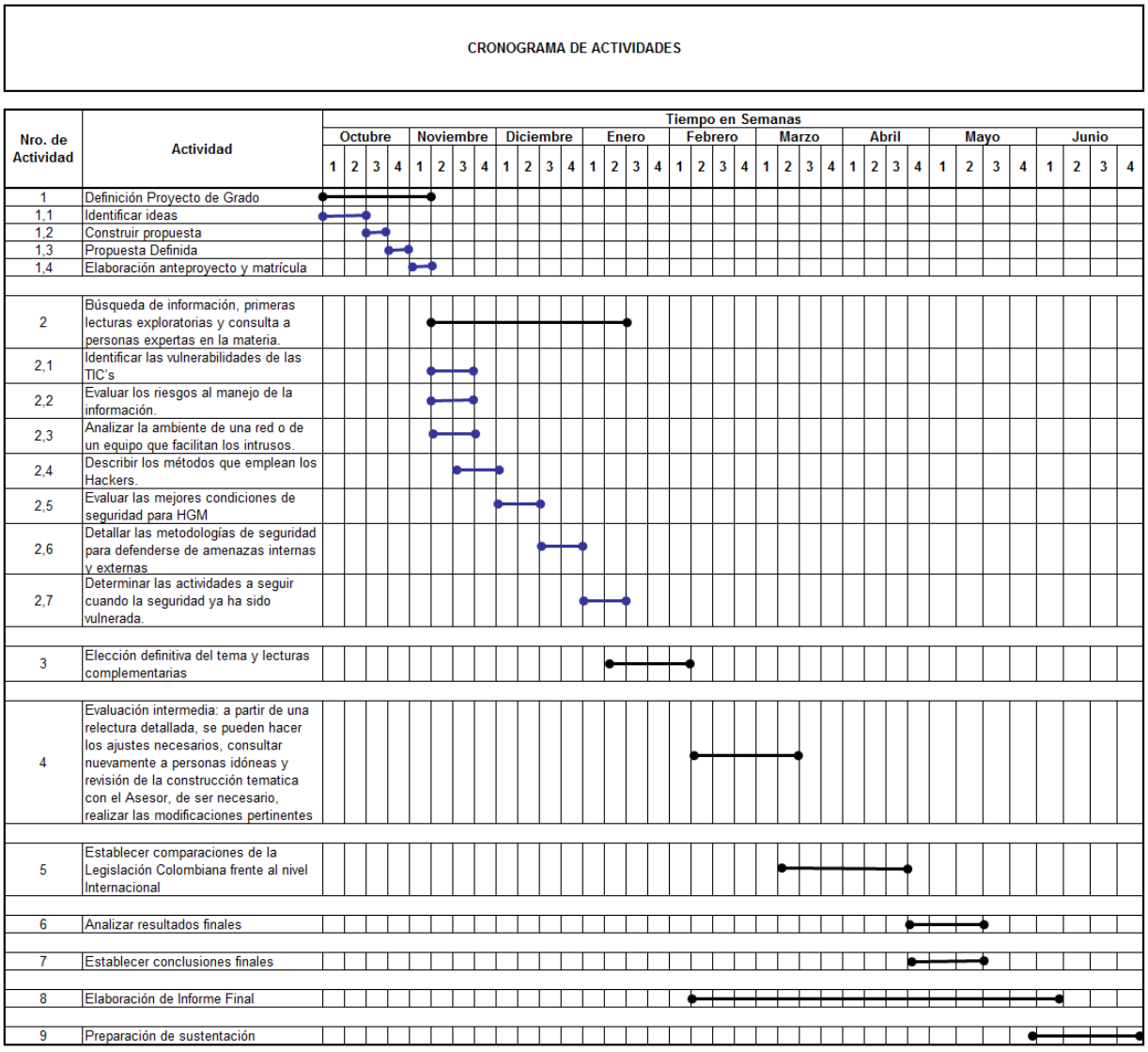


Figura 24. Cronograma actividades.

Conclusiones

- Debido a que las tecnologías crecen día con día cada vez se tendrán que capacitar más y más las personas del área de sistemas de HGM que se dediquen a investigar casos en la informática forense. Se tendrán que enseñar y capacitar a personas, del como investigar y poder utilizar todas las herramientas necesarias para poder encontrar todo la información necesaria y poder resolver un caso.
- Una investigación informática forense empieza desde el momento en que un evento ha ocurrido. Es importantísimo durante una investigación tener mucho cuidado con las evidencias que se encuentran ya que son una clave importantísima a la hora de tratar de resolver un caso.
- Por ninguna razón se recomienda que a la hora de estar investigando algún caso se trabaje con la información original, ya que si algo sale mal todo esta información se puede perder y no podría ser tomada como evidencia en caso de querer emprender acciones legales. Hay que seguir todos los pasos necesarios para que la información no vaya a ser cambiada, alterada o pueda ser afectada por otros factores.
- La informática forense nace a raíz de proteger la información de una compañía, buscando tanto la prevención como la reacción y corrección a problemas que puedan afectar los sistemas de información.
- Para la buena aplicación preventiva de la informática forense es necesaria la realización de auditorías continuas en los sistemas, y la corrección de los errores encontrados en los mismos. También se necesita establecer políticas de seguridad para usuarios y para el uso

de los sistemas de información, con el fin de minimizar la posibilidad de infiltraciones por alguna negligencia por parte de los usuarios o alguna falla en los procedimientos.

- Para la informática forense se necesita el uso de programas para la detección de la intrusión en el sistema de información y los cambios realizados a la información (manipulación o borrado). Así como un equipo multidisciplinario para poder cubrir de manera efectiva las áreas que traspasadas durante el ataque y poder rastrear los daños y al atacante.
- En el HGM, es necesario establecer la planificación de las auditorías internas a través del área de control interno para verificar que cada una de las áreas de usuarios finales esté protegiendo y suministrando la información adecuada al sistema y bajo las políticas de seguridad establecidas para el tratamiento de esta información.
- En el área de sistemas de HGM es necesario involucrar más a los empleados directos del Hospital para que se apropien del conocimiento y del seguimiento que debe realizarse del tema de seguridad informática, porque la mayoría de analistas del área son contratistas y cada empresa por nivel contractual está en la potestad de cambiar recursos entre los proyectos, lo que haría que se perdiera el conocimiento adquirido y verse afectada la continuidad de seguimiento y control del tema.
- En general, los servidores que se encuentran en el DATACENTER de Une cumplen con el estándar y están certificados en el tema de la seguridad de la información, caso contrario para los servidores que se encuentran en las instalaciones de HGM porque no se tiene el control adecuado para el manejo de estos servidores así como el grado de seguridad suficiente para el tratamiento de la información y la transaccionalidad de estos.

Bibliografía

- Asensio, Gonzalo, (2006). Seguridad en internet, 318 páginas, Editorial Nowtilus. ISBN: 84-9763-293-5.

- Babbin, Jacob y Kleiman, Dave, entre otros, (2006). Security log management: Identifying patterns in the chaos, 334 páginas, Editorial Syngress Publishing, Inc. ISBN: 1-59749-042-3.

- Ballesteros Moffa, Luis Ángel, (2005). La privacidad electrónica: Internet en el centro de protección, 348 páginas, Editorial Tirant Lo Blanch. ISBN: 84-8456-490-8.

- Calero, JL, (2000). Investigación cualitativa y cuantitativa. Problemas no resueltos en los debates actuales.

- Cano, Jeimy. Admisibilidad de la Evidencia Digital: De los conceptos legales a las características técnicas. Derecho de Internet y Telecomunicaciones. Facultad de Derecho. Universidad de Los Andes. Editorial Legis. 2003. Bogotá. Pag. 195.

- Código de Procedimiento Civil. Artículos 174, 178 y 187.

- Computer Forensics, Cybercrime, and Steganography Resources (2006). Recuperado de http://www.forensics.nl/.

- Computer forensic world (2014). Recuperado de http://www.computerforensicsworld.com/modules.php?name=News&new_topic.

- Mella, Orlando, (1998). Naturaleza y orientación teórico-Metodologías de la investigación cualitativa. Disponible en: http://www.reduc.cl/reduc/mella.pdf

- DFRWS (2008 y 2014). Recuperado de http://www.dfrws.org/2008/index.shtml.

- Fiscalía General de la Nación. Manual de procedimientos para cadena de custodia, Fiscalía General de la Nación, p. 23, ISBN 958-97542-8-7.

- G. Zucarddi & J. D. Gutiérrez, (2006). "Informática Forense".

- IBM Knowledge center. Recuperado de http://www-01.ibm.com/support/knowledgecenter/SSEPEK_10.0.0/com.ibm.db2z10.doc.perf/src/tpc/db2z_lockcontention.dita.

- J. Cano, (2009). Computación forense descubriendo los rastros Informáticos.

- J. E. Bonilla, (Noviembre 2009). Computación Forense.

- Jones, Keith J y Bejtlich, Richard, (2006). Real digital forensics: Computer security and incident Response, 650 páginas, Editorial Addison- Wesley. ISBN: 0-321-24069-3.

- K. Kent, S. Chevalier, T. Grance & H. Dang, (Agosto 2006). National Institute of Standards And Technology. “Guide to Integrating Forensic Techniques into Incident Response. NIST SP 800-86”.

- Norma técnica Colombiana NTC-ISO/IEC 27001. Online (Julio 2006).

- Real digital forensics . Recuperado de: http://www.revistasic.com/revista70/pdf_70/sic70_bibliografia.pdf.

- Tecnológico de Monterrey (2009 y 2014). Recuperado de http://biblioteca.itesm.mx/nav/contenidos_salta2.php?col_id=acm.

Anexo 1

A continuación se muestran las entrevistas realizadas aleatoriamente al personal de sistemas, que permitió identificar el conocimiento del tema o las falencias en cuanto al tema de seguridad de la información se presentan en el área de sistemas de HGM.

Hospital General de Medellín
Luz Castro de Gutiérrez E.S.E.

Encuesta de seguridad informática

Nombre co Liliana Sánchez
Cargo. Líder Sistemas

	ENTREVISTA DE SEGURIDAD INFORMÁTICA		
N°	Documento	Respuestas	
1	Cuántos empleados interactúan en la actualidad en el área de sistemas de HGM ?	100 a 200	
		200 a 500	
		500 a 900	
		Más de 900	X
		No sabe	
2	En HGM, se ha implementado algún sistema de Backup que garantice el respaldo de la información de estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
3	En HGM existen políticas de seguridad implementadas que garanticen que todo el flujo de información se ha manejado de la manera adecuada y que esta no caiga en manos inescrupulosas ?	Si	
		No	X
		No sabe	
4	En HGM cuentan con personal calificado para darle un buen uso a cada uno de los recursos tanto humanos como físicos que operan ?	Si	
		No	X
		No sabe	
5	En HGM, cuentan con un sistema de antivirus lo suficientemente eficiente como para poder bloquear el acceso de Spam, Troyanos y/o cualquier tipo de acceso dañino o software malicioso a cada una de las estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
6	En HGM, cuentan con personal certificado en el manejo de seguridad informática ?	Si	
		No	X
		No sabe	
7	Si por alguna razón la información del departamento financiero o contable cayera en manos de un Analista de sistemas de HGM, que no tiene porque saber nada de esta información, existe algún medio o mecanismo con el cual se pueda identificar este suceso, bien sea mediante registros de Logs o sistemas de Monitoreo ?	Si	X
		No	
		No sabe	
8	En HGM, se han llegado a presentar casos de violaciones de seguridad a nivel informático ?	Si	X
		No	
		No sabe	
9	En caso de presentarse violaciones de seguridad o fraudes a nivel informático, cuáles son las acciones a tomar en este caso por el personal de seguridad y de sistemas de HGM ?	Solamente confiscan el equipo y lo despiden	
		Confiscan el equipo y lo interrogan	X
		No confiscan el equipo y lo despiden	
		Confiscan el equipo y presentan acusaciones legales contra este	
		Confiscan el equipo y toman represarías físicas contra este	
		No hacen nada	
		Otras	
		No sabe	

10	Alguna persona de la organización asiste a conferencias Nacionales o Internacionales sobre temas de Seguridad Informática ?	Si	
		No	X
		No sabe	
11	HGM cuenta con servidores de archivos que garanticen que toda la información legal de la organización, tanto contable como administrativa se encuentra segura y no al alcance de personal ?	Si	X
		No	
		No sabe	
12	En las políticas de seguridad manejadas en HGM, si es considerado seguro el enviar información tanto a través de la red como de internet a otros destinatarios sin que esta sea interceptada por terceros ?	Si	
		No	X
		No sabe	
13	En HGM poseen contactos o relaciones con autoridades nacionales e internacionales para colaborar y recibir asistencia en casos de un robo o delito informático ?	Si	
		No	X
		No sabe	
14	Cuáles de los siguientes incidentes son los más frecuentes en HGM?	Infección por virus	X
		Fuga de Información	X
		No disponibilidad de los sistemas	X
		Violación de la seguridad física	X
		Sistemas Inaccesibles	
		Lentitud con el acceso a Internet	X
		Lentitud con el acceso a la Intranet	X
15	Qué percepción tienen de la seguridad de la información en HGM ?	Como una tendencia	
		Como una necesidad	X
		Como un factor estratégico	
		Como una evaluación de vulnerabilidades	X
		Como una practica a conducir para la protección de la información	X
		Como una moda	
		Ninguna	
		No sabe	
16	Han proporcionado a los empleados de HGM formación en temas de seguridad y controles sobre el manejo de la información ?	Si	X
		No	
		No sabe	
17	En algún momento dentro de HGM, se han realizado pruebas de seguridad con el fin de poder detectar las vulnerabilidades que se puedan llegar a tener ?	Si	X
		No	
		No sabe	
18	Dentro de HGM cuáles de las tecnologías de mayor preocupación en el área de seguridad informática ?	Informática móvil	
		Memoria extraíble	X
		Redes inalámbricas	X
		Telefonía voz sobre IP	
		Código de libre distribución	X
		Servidores virtuales	X
		Otros	
		Ninguno	
19	Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación ?	Si	
		No	X
		No sabe	

Hospital General de Medellín
Luz Castro de Gutiérrez E.S.E.

Encuesta de seguridad informática

Nombre co Dora Elena Zapata
Cargo. Profesional Universitario

	ENTREVISTA DE SEGURIDAD INFORMÁTICA		
N°	Documento	Respuestas	
1	Cuántos empleados interactúan en la actualidad en el área de sistemas de HGM ?	100 a 200	
		200 a 500	
		500 a 900	
		Más de 900	X
		No sabe	
2	En HGM, se ha implementado algún sistema de Backup que garantice el respaldo de la información de estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
3	En HGM existen políticas de seguridad implementadas que garanticen que todo el flujo de información se ha manejado de la manera adecuada y que esta no caiga en manos inescrupulosas ?	Si	X
		No	
		No sabe	
4	En HGM cuentan con personal calificado para darle un buen uso a cada uno de los recursos tanto humanos como físicos que operan ?	Si	X
		No	
		No sabe	
5	En HGM, cuentan con un sistema de antivirus lo suficientemente eficiente como para poder bloquear el acceso de Spam, Troyanos y/o cualquier tipo de acceso dañino o software malicioso a cada una de las estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
6	En HGM, cuentan con personal certificado en el manejo de seguridad informática ?	Si	
		No	X
		No sabe	
7	Si por alguna razón la información del departamento financiero o contable cayera en manos de un Analista de sistemas de HGM, que no tiene porque saber nada de esta información, existe algún medio o mecanismo con el cual se pueda identificar este suceso, bien sea mediante registros de Logs o sistemas de Monitoreo ?	Si	X
		No	
		No sabe	
8	En HGM, se han llegado a presentar casos de violaciones de seguridad a nivel informático ?	Si	X
		No	
		No sabe	
9	En caso de presentarse violaciones de seguridad o fraudes a nivel informático, cuáles son las acciones a tomar en este caso por el personal de seguridad y de sistemas de HGM ?	Solamente confiscan el equipo y lo despiden	
		Confiscan el equipo y lo interrogan	X
		No confiscan el equipo y lo despiden	
		Confiscan el equipo y presentan acusaciones legales contra este	
		Confiscan el equipo y toman represarías físicas contra este	
		No hacen nada	
		Otras	
		No sabe	

10	Alguna persona de la organización asiste a conferencias Nacionales o Internacionales sobre temas de Seguridad Informática ?	Si	
		No	X
		No sabe	
11	HGM cuenta con servidores de archivos que garanticen que toda la información legal de la organización, tanto contable como administrativa se encuentra segura y no al alcance de personal ?	Si	X
		No	
		No sabe	
12	En las políticas de seguridad manejadas en HGM, si es considerado seguro el enviar información tanto a través de la red como de internet a otros destinatarios sin que esta sea interceptada por terceros ?	Si	
		No	X
		No sabe	
13	En HGM poseen contactos o relaciones con autoridades nacionales e internacionales para colaborar y recibir asistencia en casos de un robo o delito informático ?	Si	
		No	X
		No sabe	
14	Cuáles de los siguientes incidentes son los más frecuentes en HGM?	Infección por virus	X
		Fuga de Información	X
		No disponibilidad de los sistemas	X
		Violación de la seguridad física	X
		Sistemas Inaccesibles	
		Lentitud con el acceso a Internet	X
		Lentitud con el acceso a la Intranet	X
15	Qué percepción tienen de la seguridad de la información en HGM ?	Como una tendencia	
		Como una necesidad	X
		Como un factor estratégico	
		Como una evaluación de vulnerabilidades	X
		Como una practica a conducir para la protección de la información	X
		Como una moda	
		Ninguna	
		No sabe	
16	Han proporcionado a los empleados de HGM formación en temas de seguridad y controles sobre el manejo de la información ?	Si	X
		No	
		No sabe	
17	En algún momento dentro de HGM, se han realizado pruebas de seguridad con el fin de poder detectar las vulnerabilidades que se puedan llegar a tener ?	Si	X
		No	
		No sabe	
18	Dentro de HGM cuáles de las tecnologías de mayor preocupación en el área de seguridad informática ?	Informática móvil	
		Memoria extraíble	X
		Redes inalámbricas	X
		Telefonía voz sobre IP	
		Código de libre distribución	X
		Servidores virtuales	X
		Otros	
		Ninguno	
19	Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación ?	Si	
		No	X
		No sabe	

Hospital General de Medellín
Luz Castro de Gutiérrez E.S.E.

Encuesta de seguridad informática

Nombre co Cesar Rodas
Cargo. Líder SAP

	ENTREVISTA DE SEGURIDAD INFORMÁTICA		
N°	Documento	Respuestas	
1	Cuántos empleados interactúan en la actualidad en el área de sistemas de HGM ?	100 a 200	
		200 a 500	
		500 a 900	
		Más de 900	X
		No sabe	
2	En HGM, se ha implementado algún sistema de Backup que garantice el respaldo de la información de estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
3	En HGM existen políticas de seguridad implementadas que garanticen que todo el flujo de información se ha manejado de la manera adecuada y que esta no caiga en manos inescrupulosas ?	Si	X
		No	
		No sabe	
4	En HGM cuentan con personal calificado para darle un buen uso a cada uno de los recursos tanto humanos como físicos que operan ?	Si	X
		No	
		No sabe	
5	En HGM, cuentan con un sistema de antivirus lo suficientemente eficiente como para poder bloquear el acceso de Spam, Troyanos y/o cualquier tipo de acceso dañino o software malicioso a cada una de las estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
6	En HGM, cuentan con personal certificado en el manejo de seguridad informática ?	Si	
		No	X
		No sabe	
7	Si por alguna razón la información del departamento financiero o contable cayera en manos de un Analista de sistemas de HGM, que no tiene porque saber nada de esta información, existe algún medio o mecanismo con el cual se pueda identificar este suceso, bien sea mediante registros de Logs o sistemas de Monitoreo ?	Si	X
		No	
		No sabe	
8	En HGM, se han llegado a presentar casos de violaciones de seguridad a nivel informático ?	Si	X
		No	
		No sabe	
9	En caso de presentarse violaciones de seguridad o fraudes a nivel informático, cuáles son las acciones a tomar en este caso por el personal de seguridad y de sistemas de HGM ?	Solamente confiscan el equipo y lo despiden	
		Confiscan el equipo y lo interrogan	X
		No confiscan el equipo y lo despiden	
		Confiscan el equipo y presentan acusaciones legales contra este	
		Confiscan el equipo y toman represarías físicas contra este	
		No hacen nada	
		Otras	
		No sabe	

10	Alguna persona de la organización asiste a conferencias Nacionales o Internacionales sobre temas de Seguridad Informática ?	Si	
		No	X
		No sabe	
11	HGM cuenta con servidores de archivos que garanticen que toda la información legal de la organización, tanto contable como administrativa se encuentra segura y no al alcance de personal ?	Si	X
		No	
		No sabe	
12	En las políticas de seguridad manejadas en HGM, si es considerado seguro el enviar información tanto a través de la red como de internet a otros destinatarios sin que esta sea interceptada por terceros ?	Si	
		No	X
		No sabe	
13	En HGM poseen contactos o relaciones con autoridades nacionales e internacionales para colaborar y recibir asistencia en casos de un robo o delito informático ?	Si	
		No	X
		No sabe	
14	Cuáles de los siguientes incidentes son los más frecuentes en HGM?	Infección por virus	X
		Fuga de Información	X
		No disponibilidad de los sistemas	X
		Violación de la seguridad física	X
		Sistemas Inaccesibles	X
		Lentitud con el acceso a Internet	X
		Lentitud con el acceso a la Intranet	X
15	Qué percepción tienen de la seguridad de la información en HGM ?	Como una tendencia	
		Como una necesidad	X
		Como un factor estratégico	
		Como una evaluación de vulnerabilidades	X
		Como una practica a conducir para la protección de la información	X
		Como una moda	
		Ninguna	
		No sabe	
16	Han proporcionado a los empleados de HGM formación en temas de seguridad y controles sobre el manejo de la información ?	Si	X
		No	
		No sabe	
17	En algún momento dentro de HGM, se han realizado pruebas de seguridad con el fin de poder detectar las vulnerabilidades que se puedan llegar a tener ?	Si	X
		No	
		No sabe	
18	Dentro de HGM cuáles de las tecnologías de mayor preocupación en el área de seguridad informática ?	Informática móvil	X
		Memoria extraíble	X
		Redes inalámbricas	X
		Telefonía voz sobre IP	
		Código de libre distribución	X
		Servidores virtuales	X
		Otros	
		Ninguno	
19	Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación ?	Si	
		No	X
		No sabe	

Hospital General de Medellín
Luz Castro de Gutiérrez E.S.E.

Encuesta de seguridad informática

Nombre co Ramón Parra
Cargo. Basis

	ENTREVISTA DE SEGURIDAD INFORMÁTICA		
N°	Documento	Respuestas	
1	Cuántos empleados interactúan en la actualidad en el área de sistemas de HGM ?	100 a 200	
		200 a 500	
		500 a 900	
		Más de 900	X
		No sabe	
2	En HGM, se ha implementado algún sistema de Backup que garantice el respaldo de la información de estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
3	En HGM existen políticas de seguridad implementadas que garanticen que todo el flujo de información se ha manejado de la manera adecuada y que esta no caiga en manos inescrupulosas ?	Si	
		No	X
		No sabe	
4	En HGM cuentan con personal calificado para darle un buen uso a cada uno de los recursos tanto humanos como físicos que operan ?	Si	X
		No	
		No sabe	
5	En HGM, cuentan con un sistema de antivirus lo suficientemente eficiente como para poder bloquear el acceso de Spam, Troyanos y/o cualquier tipo de acceso dañino o software malicioso a cada una de las estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
6	En HGM, cuentan con personal certificado en el manejo de seguridad informática ?	Si	
		No	X
		No sabe	
7	Si por alguna razón la información del departamento financiero o contable cayera en manos de un Analista de sistemas de HGM, que no tiene porque saber nada de esta información, existe algún medio o mecanismo con el cual se pueda identificar este suceso, bien sea mediante registros de Logs o sistemas de Monitoreo ?	Si	X
		No	
		No sabe	
8	En HGM, se han llegado a presentar casos de violaciones de seguridad a nivel informático ?	Si	X
		No	
		No sabe	
9	En caso de presentarse violaciones de seguridad o fraudes a nivel informático, cuáles son las acciones a tomar en este caso por el personal de seguridad y de sistemas de HGM ?	Solamente confiscan el equipo y lo despiden	
		Confiscan el equipo y lo interrogan	X
		No confiscan el equipo y lo despiden	
		Confiscan el equipo y presentan acusaciones legales contra este	
		Confiscan el equipo y toman represarías físicas contra este	
		No hacen nada	
		Otras	
		No sabe	

10	Alguna persona de la organización asiste a conferencias Nacionales o Internacionales sobre temas de Seguridad Informática ?	Si	
		No	X
		No sabe	
11	HGM cuenta con servidores de archivos que garanticen que toda la información legal de la organización, tanto contable como administrativa se encuentra segura y no al alcance de personal ?	Si	X
		No	
		No sabe	
12	En las políticas de seguridad manejadas en HGM, si es considerado seguro el enviar información tanto a través de la red como de internet a otros destinatarios sin que esta sea interceptada por terceros ?	Si	
		No	X
		No sabe	
13	En HGM poseen contactos o relaciones con autoridades nacionales e internacionales para colaborar y recibir asistencia en casos de un robo o delito informático ?	Si	
		No	X
		No sabe	
14	Cuáles de los siguientes incidentes son los más frecuentes en HGM?	Infección por virus	X
		Fuga de Información	X
		No disponibilidad de los sistemas	X
		Violación de la seguridad física	X
		Sistemas Inaccesibles	X
		Lentitud con el acceso a Internet	X
		Lentitud con el acceso a la Intranet	X
15	Qué percepción tienen de la seguridad de la información en HGM ?	Como una tendencia	
		Como una necesidad	X
		Como un factor estratégico	
		Como una evaluación de vulnerabilidades	X
		Como una practica a conducir para la protección de la información	X
		Como una moda	
		Ninguna	
		No sabe	
16	Han proporcionado a los empleados de HGM formación en temas de seguridad y controles sobre el manejo de la información ?	Si	X
		No	
		No sabe	
17	En algún momento dentro de HGM, se han realizado pruebas de seguridad con el fin de poder detectar las vulnerabilidades que se puedan llegar a tener ?	Si	X
		No	
		No sabe	
18	Dentro de HGM cuáles de las tecnologías de mayor preocupación en el área de seguridad informática ?	Informática móvil	
		Memoria extraíble	X
		Redes inalámbricas	X
		Telefonía voz sobre IP	
		Código de libre distribución	X
		Servidores virtuales	X
		Otros	X
		Ninguno	
19	Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación ?	Si	
		No	X
		No sabe	

Hospital General de Medellín
Luz Castro de Gutiérrez E.S.E

Encuesta de seguridad informática

Nombre co Luz Stella González
Cargo. Analista de sistemas

	ENTREVISTA DE SEGURIDAD INFORMÁTICA		
N°	Documento	Respuestas	
1	Cuántos empleados interactúan en la actualidad en el área de sistemas de HGM ?	100 a 200	
		200 a 500	
		500 a 900	
		Más de 900	X
		No sabe	
2	En HGM, se ha implementado algún sistema de Backup que garantice el respaldo de la información de estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
3	En HGM existen políticas de seguridad implementadas que garanticen que todo el flujo de información se ha manejado de la manera adecuada y que esta no caiga en manos inescrupulosas ?	Si	X
		No	
		No sabe	
4	En HGM cuentan con personal calificado para darle un buen uso a cada uno de los recursos tanto humanos como físicos que operan ?	Si	X
		No	
		No sabe	
5	En HGM, cuentan con un sistema de antivirus lo suficientemente eficiente como para poder bloquear el acceso de Spam, Troyanos y/o cualquier tipo de acceso dañino o software malicioso a cada una de las estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
6	En HGM, cuentan con personal certificado en el manejo de seguridad informática ?	Si	
		No	
		No sabe	X
7	Si por alguna razón la información del departamento financiero o contable cayera en manos de un Analista de sistemas de HGM, que no tiene porque saber nada de esta información, existe algún medio o mecanismo con el cual se pueda identificar este suceso, bien sea mediante registros de Logs o sistemas de Monitoreo ?	Si	
		No	
		No sabe	X
8	En HGM, se han llegado a presentar casos de violaciones de seguridad a nivel informático ?	Si	
		No	
		No sabe	X
9	En caso de presentarse violaciones de seguridad o fraudes a nivel informático, cuáles son las acciones a tomar en este caso por el personal de seguridad y de sistemas de HGM ?	Solamente confiscan el equipo y lo despiden	
		Confiscan el equipo y lo interrogan	
		No confiscan el equipo y lo despiden	
		Confiscan el equipo y presentan acusaciones legales contra este	
		Confiscan el equipo y toman represarías físicas contra este	
		No hacen nada	
		Otras	
		No sabe	X

10	Alguna persona de la organización asiste a conferencias Nacionales o Internacionales sobre temas de Seguridad Informática ?	Si	
		No	
		No sabe	X
11	HGM cuenta con servidores de archivos que garanticen que toda la información legal de la organización, tanto contable como administrativa se encuentra segura y no al alcance de personal ?	Si	X
		No	
		No sabe	
12	En las políticas de seguridad manejadas en HGM, si es considerado seguro el enviar información tanto a través de la red como de internet a otros destinatarios sin que esta sea interceptada por terceros ?	Si	
		No	
		No sabe	X
13	En HGM poseen contactos o relaciones con autoridades nacionales e internacionales para colaborar y recibir asistencia en casos de un robo o delito informático ?	Si	
		No	
		No sabe	X
14	Cuáles de los siguientes incidentes son los más frecuentes en HGM?	Infección por virus	X
		Fuga de Información	X
		No disponibilidad de los sistemas	X
		Violación de la seguridad física	
		Sistemas Inaccesibles	
		Lentitud con el acceso a Internet	X
		Lentitud con el acceso a la Intranet	X
15	Qué percepción tienen de la seguridad de la información en HGM ?	Como una tendencia	
		Como una necesidad	X
		Como un factor estratégico	
		Como una evaluación de vulnerabilidades	
		Como una practica a conducir para la protección de la información	X
		Como una moda	
		Ninguna	
		No sabe	
16	Han proporcionado a los empleados de HGM formación en temas de seguridad y controles sobre el manejo de la información ?	Si	X
		No	
		No sabe	
17	En algún momento dentro de HGM, se han realizado pruebas de seguridad con el fin de poder detectar las vulnerabilidades que se puedan llegar a tener ?	Si	
		No	
		No sabe	X
18	Dentro de HGM cuáles de las tecnologías de mayor preocupación en el área de seguridad informática ?	Informática móvil	
		Memoria extraíble	X
		Redes inalámbricas	X
		Telefonía voz sobre IP	
		Código de libre distribución	X
		Servidores virtuales	X
		Otros	
		Ninguno	
19	Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación ?	Si	
		No	X
		No sabe	

Hospital General de Medellín
Luz Castro de Gutiérrez E.S.E.

Encuesta de seguridad informática

Nombre co Edith Andrade
Cargo. Consultora SAP

	ENTREVISTA DE SEGURIDAD INFORMÁTICA		
N°	Documento	Respuestas	
1	Cuántos empleados interactúan en la actualidad en el área de sistemas de HGM ?	100 a 200	
		200 a 500	
		500 a 900	
		Más de 900	X
		No sabe	
2	En HGM, se ha implementado algún sistema de Backup que garantice el respaldo de la información de estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
3	En HGM existen políticas de seguridad implementadas que garanticen que todo el flujo de información se ha manejado de la manera adecuada y que esta no caiga en manos inescrupulosas ?	Si	X
		No	
		No sabe	
4	En HGM cuentan con personal calificado para darle un buen uso a cada uno de los recursos tanto humanos como físicos que operan ?	Si	X
		No	
		No sabe	
5	En HGM, cuentan con un sistema de antivirus lo suficientemente eficiente como para poder bloquear el acceso de Spam, Troyanos y/o cualquier tipo de acceso dañino o software malicioso a cada una de las estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
6	En HGM, cuentan con personal certificado en el manejo de seguridad informática ?	Si	
		No	X
		No sabe	
7	Si por alguna razón la información del departamento financiero o contable cayera en manos de un Analista de sistemas de HGM, que no tiene porque saber nada de esta información, existe algún medio o mecanismo con el cual se pueda identificar este suceso, bien sea mediante registros de Logs o sistemas de Monitoreo ?	Si	X
		No	
		No sabe	
8	En HGM, se han llegado a presentar casos de violaciones de seguridad a nivel informático ?	Si	X
		No	
		No sabe	
9	En caso de presentarse violaciones de seguridad o fraudes a nivel informático, cuáles son las acciones a tomar en este caso por el personal de seguridad y de sistemas de HGM ?	Solamente confiscan el equipo y lo despiden	
		Confiscan el equipo y lo interrogan	X
		No confiscan el equipo y lo despiden	
		Confiscan el equipo y presentan acusaciones legales contra este	
		Confiscan el equipo y toman represarías físicas contra este	
		No hacen nada	
		Otras	
		No sabe	

10	Alguna persona de la organización asiste a conferencias Nacionales o Internacionales sobre temas de Seguridad Informática ?	Si	
		No	X
		No sabe	
11	HGM cuenta con servidores de archivos que garanticen que toda la información legal de la organización, tanto contable como administrativa se encuentra segura y no al alcance de personal ?	Si	X
		No	
		No sabe	
12	En las políticas de seguridad manejadas en HGM, si es considerado seguro el enviar información tanto a través de la red como de internet a otros destinatarios sin que esta sea interceptada por terceros ?	Si	
		No	X
		No sabe	
13	En HGM poseen contactos o relaciones con autoridades nacionales e internacionales para colaborar y recibir asistencia en casos de un robo o delito informático ?	Si	
		No	X
		No sabe	
14	Cuáles de los siguientes incidentes son los más frecuentes en HGM?	Infección por virus	X
		Fuga de Información	X
		No disponibilidad de los sistemas	X
		Violación de la seguridad física	X
		Sistemas Inaccesibles	X
		Lentitud con el acceso a Internet	X
		Lentitud con el acceso a la Intranet	X
15	Qué percepción tienen de la seguridad de la información en HGM ?	Como una tendencia	
		Como una necesidad	X
		Como un factor estratégico	
		Como una evaluación de vulnerabilidades	
		Como una practica a conducir para la protección de la información	
		Como una moda	
		Ninguna	
		No sabe	
16	Han proporcionado a los empleados de HGM formación en temas de seguridad y controles sobre el manejo de la información ?	Si	X
		No	
		No sabe	
17	En algún momento dentro de HGM, se han realizado pruebas de seguridad con el fin de poder detectar las vulnerabilidades que se puedan llegar a tener ?	Si	
		No	
		No sabe	X
18	Dentro de HGM cuáles de las tecnologías de mayor preocupación en el área de seguridad informática ?	Informática móvil	
		Memoria extraíble	X
		Redes inalámbricas	X
		Telefonía voz sobre IP	
		Código de libre distribución	X
		Servidores virtuales	X
		Otros	X
		Ninguno	
19	Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación ?	Si	
		No	X
		No sabe	

Hospital General de Medellín
Luz Castro de Gutiérrez E.S.E.

Encuesta de seguridad informática

Nombre co Diego Sossa
Cargo. Gerente de negocio MDA

	ENTREVISTA DE SEGURIDAD INFORMÁTICA		
N°	Documento	Respuestas	
1	Cuántos empleados interactúan en la actualidad en el área de sistemas de HGM ?	100 a 200	
		200 a 500	
		500 a 900	
		Más de 900	X
		No sabe	
2	En HGM, se ha implementado algún sistema de Backup que garantice el respaldo de la información de estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
3	En HGM existen políticas de seguridad implementadas que garanticen que todo el flujo de información se ha manejado de la manera adecuada y que esta no caiga en manos inescrupulosas ?	Si	X
		No	
		No sabe	
4	En HGM cuentan con personal calificado para darle un buen uso a cada uno de los recursos tanto humanos como físicos que operan ?	Si	X
		No	
		No sabe	
5	En HGM, cuentan con un sistema de antivirus lo suficientemente eficiente como para poder bloquear el acceso de Spam, Troyanos y/o cualquier tipo de acceso dañino o software malicioso a cada una de las estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
6	En HGM, cuentan con personal certificado en el manejo de seguridad informática ?	Si	
		No	X
		No sabe	
7	Si por alguna razón la información del departamento financiero o contable cayera en manos de un Analista de sistemas de HGM, que no tiene porque saber nada de esta información, existe algún medio o mecanismo con el cual se pueda identificar este suceso, bien sea mediante registros de Logs o sistemas de Monitoreo ?	Si	X
		No	
		No sabe	
8	En HGM, se han llegado a presentar casos de violaciones de seguridad a nivel informático ?	Si	X
		No	
		No sabe	
9	En caso de presentarse violaciones de seguridad o fraudes a nivel informático, cuáles son las acciones a tomar en este caso por el personal de seguridad y de sistemas de HGM ?	Solamente confiscan el equipo y lo despiden	
		Confiscan el equipo y lo interrogan	X
		No confiscan el equipo y lo despiden	
		Confiscan el equipo y presentan acusaciones legales contra este	
		Confiscan el equipo y toman represarías físicas contra este	
		No hacen nada	
		Otras	
		No sabe	

10	Alguna persona de la organización asiste a conferencias Nacionales o Internacionales sobre temas de Seguridad Informática ?	Si	
		No	X
		No sabe	
11	HGM cuenta con servidores de archivos que garanticen que toda la información legal de la organización, tanto contable como administrativa se encuentra segura y no al alcance de personal ?	Si	X
		No	
		No sabe	
12	En las políticas de seguridad manejadas en HGM, si es considerado seguro el enviar información tanto a través de la red como de internet a otros destinatarios sin que esta sea interceptada por terceros ?	Si	
		No	X
		No sabe	
13	En HGM poseen contactos o relaciones con autoridades nacionales e internacionales para colaborar y recibir asistencia en casos de un robo o delito informático ?	Si	
		No	X
		No sabe	
14	Cuáles de los siguientes incidentes son los más frecuentes en HGM?	Infección por virus	X
		Fuga de Información	X
		No disponibilidad de los sistemas	X
		Violación de la seguridad física	X
		Sistemas Inaccesibles	X
		Lentitud con el acceso a Internet	X
		Lentitud con el acceso a la Intranet	X
15	Qué percepción tienen de la seguridad de la información en HGM ?	Como una tendencia	
		Como una necesidad	X
		Como un factor estratégico	
		Como una evaluación de vulnerabilidades	X
		Como una practica a conducir para la protección de la información	
		Como una moda	
		Ninguna	
		No sabe	
16	Han proporcionado a los empleados de HGM formación en temas de seguridad y controles sobre el manejo de la información ?	Si	X
		No	
		No sabe	
17	En algún momento dentro de HGM, se han realizado pruebas de seguridad con el fin de poder detectar las vulnerabilidades que se puedan llegar a tener ?	Si	X
		No	
		No sabe	
18	Dentro de HGM cuáles de las tecnologías de mayor preocupación en el área de seguridad informática ?	Informática móvil	X
		Memoria extraíble	X
		Redes inalámbricas	X
		Telefonía voz sobre IP	
		Código de libre distribución	X
		Servidores virtuales	X
		Otros	X
		Ninguno	
19	Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación ?	Si	
		No	X
		No sabe	

Hospital General de Medellín
Luz Castro de Gutiérrez E.S.E.

Encuesta de seguridad informática

Nombre co Jorge Iván Sánchez
Cargo. Líder Arquitectura

	ENTREVISTA DE SEGURIDAD INFORMÁTICA		
N°	Documento	Respuestas	
1	Cuántos empleados interactúan en la actualidad en el área de sistemas de HGM ?	100 a 200	
		200 a 500	
		500 a 900	
		Más de 900	X
		No sabe	
2	En HGM, se ha implementado algún sistema de Backup que garantice el respaldo de la información de estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
3	En HGM existen políticas de seguridad implementadas que garanticen que todo el flujo de información se ha manejado de la manera adecuada y que esta no caiga en manos inescrupulosas ?	Si	X
		No	
		No sabe	
4	En HGM cuentan con personal calificado para darle un buen uso a cada uno de los recursos tanto humanos como físicos que operan ?	Si	X
		No	
		No sabe	
5	En HGM, cuentan con un sistema de antivirus lo suficientemente eficiente como para poder bloquear el acceso de Spam, Troyanos y/o cualquier tipo de acceso dañino o software malicioso a cada una de las estaciones de trabajo y servidores ?	Si	X
		No	
		No sabe	
6	En HGM, cuentan con personal certificado en el manejo de seguridad informática ?	Si	
		No	X
		No sabe	
7	Si por alguna razón la información del departamento financiero o contable cayera en manos de un Analista de sistemas de HGM, que no tiene porque saber nada de esta información, existe algún medio o mecanismo con el cual se pueda identificar este suceso, bien sea mediante registros de Logs o sistemas de Monitoreo ?	Si	X
		No	
		No sabe	
8	En HGM, se han llegado a presentar casos de violaciones de seguridad a nivel informático ?	Si	X
		No	
		No sabe	
9	En caso de presentarse violaciones de seguridad o fraudes a nivel informático, cuáles son las acciones a tomar en este caso por el personal de seguridad y de sistemas de HGM ?	Solamente confiscan el equipo y lo despiden	
		Confiscan el equipo y lo interrogan	X
		No confiscan el equipo y lo despiden	
		Confiscan el equipo y presentan acusaciones legales contra este	
		Confiscan el equipo y toman represarías físicas contra este	
		No hacen nada	
		Otras	
		No sabe	

10	Alguna persona de la organización asiste a conferencias Nacionales o Internacionales sobre temas de Seguridad Informática ?	Si	
		No	X
		No sabe	
11	HGM cuenta con servidores de archivos que garanticen que toda la información legal de la organización, tanto contable como administrativa se encuentra segura y no al alcance de personal ?	Si	X
		No	
		No sabe	
12	En las políticas de seguridad manejadas en HGM, si es considerado seguro el enviar información tanto a través de la red como de internet a otros destinatarios sin que esta sea interceptada por terceros ?	Si	
		No	X
		No sabe	
13	En HGM poseen contactos o relaciones con autoridades nacionales e internacionales para colaborar y recibir asistencia en casos de un robo o delito informático ?	Si	
		No	X
		No sabe	
14	Cuáles de los siguientes incidentes son los más frecuentes en HGM?	Infección por virus	X
		Fuga de Información	X
		No disponibilidad de los sistemas	X
		Violación de la seguridad física	X
		Sistemas Inaccesibles	X
		Lentitud con el acceso a Internet	X
		Lentitud con el acceso a la Intranet	X
15	Qué percepción tienen de la seguridad de la información en HGM ?	Como una tendencia	
		Como una necesidad	X
		Como un factor estratégico	
		Como una evaluación de vulnerabilidades	X
		Como una practica a conducir para la protección de la información	X
		Como una moda	
		Ninguna	
		No sabe	
16	Han proporcionado a los empleados de HGM formación en temas de seguridad y controles sobre el manejo de la información ?	Si	X
		No	
		No sabe	
17	En algún momento dentro de HGM, se han realizado pruebas de seguridad con el fin de poder detectar las vulnerabilidades que se puedan llegar a tener ?	Si	X
		No	
		No sabe	
18	Dentro de HGM cuáles de las tecnologías de mayor preocupación en el área de seguridad informática ?	Informática móvil	
		Memoria extraíble	X
		Redes inalámbricas	X
		Telefonía voz sobre IP	
		Código de libre distribución	X
		Servidores virtuales	X
		Otros	X
		Ninguno	
19	Es capaz de identificar los sistemas infectados y proceder a su desconexión y recuperación ?	Si	
		No	X
		No sabe	