DECANATO DE INGENIERÍA E INFORMÁTICA

ESCUELA DE INFORMÁTICA

IMPLEMENTACIÓN DE UNA HERRAMIENTA DE PREVENCIÓN DE PÉRDIDA DE DATOS Y PLAN DE RECUPERACIÓN ANTE DESASTRES EN LA EMPRESA CAM INC, SANTO DOMINGO, 2014.

Sustentado por:

Stephanie Petit Homeis 2010 0551

Luis Ariel Rosario 2010 1542

Raúl Geovanny Peña 2010 1669

Asesores:

Ing. Mitsuteru Nishio

Ing. Santo Rafael Navarro

“Los conceptos expuestos en esta investigación son de la exclusiva responsabilidad de sus autores”.

Monografía para optar por el título de
Ingeniero en Sistemas de Computación

Distrito Nacional, República Dominicana
2014

DECANATO DE INGENIERÍA E INFORMÁTICA

ESCUELA DE INFORMÁTICA

IMPLEMENTACIÓN DE UNA HERRAMIENTA DE PREVENCIÓN DE PÉRDIDA DE DATOS Y PLAN DE RECUPERACIÓN ANTE DESASTRES EN LA EMPRESA CAM INC, SANTO DOMINGO, 2014.

Sustentado por:

Stephanie Petit Homeis 2010 0551

Luis Ariel Rosario 2010 1542

Raúl Geovanny Peña 2010 1669

Asesores:

Ing. Mitsuteru Nishio

Ing. Santo Rafael Navarro

“Los conceptos expuestos en esta investigación son de la exclusiva responsabilidad de sus autores”.

Monografía para optar por el título de
Ingeniero en Sistemas de Computación

Distrito Nacional, República Dominicana
2014

DEDICATORIA

A Dios,

Por darme salud, por guiarme en estos años de estudio, por darme fuerzas para vencer obstáculos y así alcanzar esta meta.

A mis padres,

Jean Petit y Margueta Homeis por ser pilares fundamentales en mi vida, mis modelos a seguir, por todos sus sacrificios para darme lo mejor y por su apoyo. Los amo.

A mis hermanos,

Dasca, Jimmy y Jessica, por su ayuda, por sus consejos, por su aliento y su cariño. Los quiero mucho.

A mi amiga y hermana del alma,

Diana Jiménez Díaz, porque a pesar de que no está en vida para presenciar este logro, siempre fue su sueño verme concluir mi carrera profesional. Siempre te querré.

A mi novio,

Louinel Jeune por su paciencia, ayuda y comprensión. Preferiste sacrificar tu tiempo para que yo pudiera cumplir con el mío. Por tu bondad me inspiraste a ser mejor para ti.

A mi abuela,

Annette por ser como mi segunda madre, gracias a tu sabiduría y dedicación cada vez que te necesité.

Stephanie Petit Homeis

DEDICATORIA

A Dios,

Porque es el único que hace posible las cosas y por darme la sabiduría para culminar un logro más en mi vida.

A mi novia,

Leidy Cepeda por el gran apoyo incondicional y gracias por estar siempre a mi lado y confiar en mí, diciéndome que siempre puedes dar el cien por ciento.

A mis padres,

Yvelisse Alt. Cabrera y Luis Fco. Rosario, que me educaron de la mejor manera posible, dotándome de ricos valores y enseñanzas de la vida. Sin sus guías no hubiese podido lograr mis metas y ser el hombre que soy hoy en día.

A la empresa Airport Team Solution,

Representada por el señor Rafael Reyes, quien ha jugado un papel muy importante en este trayecto, dándome la oportunidad de superación a mi vida en el ámbito laboral.

Luis Ariel Rosario Cabrera

DEDICATORIA

A Dios,

Por haberme dado la sabiduría y las fuerzas para poder llegar a esta etapa de mi vida, por permitirme la oportunidad de cumplir otra de mis metas que tanto le pedí y que ahora estoy alcanzando. Por darme cada día lo que necesito, y por nunca desampararme, aunque haya puesto pruebas en mí camino, que con mi fe en Él eh ido superando.

A mis abuelos,

Sorqui Maldonado y Raúl Antonio Ureña, que amo de una manera especial, porque han sido los mejores padres que una persona puede desear, porque ellos a pesar de las bajas y altas que eh tenido para poder llegar a esta etapa de mi vida, siempre han estado ahí para apoyarme, darme fuerzas y aliento para que no caiga y salga a camino.

A el Hermano Félix Francisco Peña Lora, director de la escuela La Salle,

Por haber confiado en mí y darme la oportunidad de alcanzar esta parte de mi vida, mi formación como profesional, y enseñarme que el que quiere, puede lograr todo lo que se proponga.

Raúl Geovanny Peña Ureña

AGRADECIMIENTOS

A Dios todopoderoso por permitirnos cumplir una más de nuestras metas en la vida, sin Él no hubiese sido posible.

Agradecer hoy y siempre a nuestras familias por el esfuerzo y apoyo en nuestros estudios.

A nuestros asesores Ing. Mitsuteru Nishio e Ing. Santo Navarro, por brindarnos sus conocimientos y trazarnos las pautas para realizar un excelente proyecto.

A los profesores que a lo largo de la carrera nos han traspasado muchos de sus conocimientos y experiencias para que hoy podamos ser los profesionales que somos en especial.

A nuestros compañeros de carrera, por todo el apoyo brindado.

"El agradecimiento es la parte principal del hombre de bien."

Francisco de Quevedo

Stephanie, Luis, Raúl

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En las empresas el objetivo general a menudo va encaminado a garantizar en todo momento la seguridad de la información de sus clientes y la seguridad de sus instalaciones. Según IBM, de las empresas que han tenido una pérdida principal de registros automatizados, el 43% nunca vuelve a abrir, el 51% cierra en menos de dos años y sólo el 6% sobrevivirá a largo plazo.

Esta monografía se centró en la implementación de la herramienta *Symantec Data Loss Prevention* que permite mitigar la pérdida de información dentro de la empresa de servicios de remesas CAM INC, y al mismo tiempo, se diseñó un plan de recuperación ante desastres que garantice que los servicios que ofrece continúen funcionando a un nivel operacionalmente aceptable, en caso de enfrentarse a cualquier eventualidad. De igual modo, durante el proceso de investigación se definieron los conceptos que funcionaron como palabras clave para la elaboración del plan de recuperación ante desastres y se presentaron los controles y medidas necesarios para contrarrestar los efectos de cualquier incidente. Algunos métodos para el desarrollo del estudio fueron la observación, el análisis y método deductivo que permitió partir de premisas generales en base a los lineamientos de la seguridad de la información hasta premisas particulares que concluyeron en el análisis de la situación de la empresa en cuestión.

El alcance final de esta investigación es mejorar la calidad de los servicios y gestionar la seguridad de la información

INTRODUCCIÓN

La gestión de la seguridad de la información es un punto que no siempre se le da la atención e importancia que requiere en muchas empresas. A medida que avanza la globalización, las organizaciones se vuelven más dependientes de la tecnología, y con ello se enfrentan a panoramas complejos para el manejo y gestión de la seguridad de los datos. Se ven obligadas a responder ante acciones que son capaces de penetrar sus vulnerabilidades, amenazando la confidencialidad, integridad y disponibilidad de la información que utilizan para sus operaciones y servicios. Pero, qué pasa cuando dentro de la empresa hay pérdida de datos o, cuando la empresa no cuenta con un plan alternativo que asegure la continuidad de sus operaciones en caso de que ocurran incidentes graves. Las respuestas para ambas preguntas es que al final la empresa tendría que salir de circulación, por no tener el quórum suficiente que demande sus servicios por la falta continua de seguridad de su información o, porque ocurrió un incidente que afectó sus registros de datos o destruyó sus instalaciones y por ende, no pudo recuperarse de la pérdida.

Para contrarrestar las problemáticas mencionadas anteriormente, es necesario contar con herramientas que aseguren la correcta gestión de la seguridad de la información basada en las normas establecidas por la Organización Internacional de Normalización (*siglas en inglés ISO*) y las buenas prácticas, que permita salir a flote durante y después de cualquier contingencia. La herramienta de gestión de la seguridad de la información y el plan de recuperación ante desastres, son los propósitos de esta investigación.

Un plan de recuperación ante desastres (*siglas en inglés DRP*) es un conjunto de procedimientos que tienen como objetivo proteger la infraestructura tecnológica de una empresa en caso de desastre pero, se refiere a todo lo relacionado con la respuesta ante cualquier incidente. Y por su parte la perdida de datos, representa uno de los principales problemas que enfrentan las empresas de hoy en día, lo que se puede traducir a la larga como pérdidas monetarias y de credibilidad organizacional.

Los "estatutos de la seguridad de la información" afirman que se deben verificar que los riesgos y las amenazas de cualquier organización estén correctamente identificados, evaluados y gestionados al momento de brindar sus servicios y ejecuta sus procesos, para protección tanto de la información de los clientes como la información organizacional, en ese orden, este informe detalla todos los conceptos clave relacionados con la gestión y riesgos de la seguridad de la información, aspecto que sigue siendo estudiado por la comunidad tecnológica de la actualidad, llamada en base a sus avances "la era de la información."

CAPÍTULO I. EMPRESA CAM INC.

1.1. Antecedentes de CAM INC

CAM INC fue fundada en 1984 por el empresario Julio P. Hendrickx[1], cuyo propósito era crear una empresa de envío de remesas y valores desde Estados Unidos hacia otros países. En ese mismo año se inauguraron las primeras oficinas en Nueva York y Miami; y a la vez la primera compañía en Haití. También se hizo posible el envío de artículos comestibles y se agregó el servicio de entrega inmediata de remesas para las realizadas antes de la 1:00 p.m.

Hoy, con más de 600,000 clientes CAM INC., es la compañía líder ofreciendo el más rápido y confiable servicio, contando con transporte de paqueterías y valores, remesas y transferencia de fondos a nivel nacional e internacional. Tiene licencia para transferencias de dinero y está acreditada por los departamentos bancarios de Nueva York, Nueva Jersey, Florida, Rhode Island, Washington, Massachusetts, Georgia, Connecticut e Illinois.

Por más de 19 años de trabajo continuo, CAM INC ha brindado una excelencia de servicio para satisfacer a sus clientes, logrando el apoyo de la banca nacional e internacional, lo que le ha permitido trascender fronteras y expandirse a nivel internacional.

[1] Empresario belga, con máster en ciencias económicas. Fundador de CAM INC y socio de Caribe Express en República Dominicana.

1.2. Filosofía Corporativa

La filosofía corporativa le permite a cualquier empresa desarrollar su cultura colectiva. Establece los valores y la ética de la misma y deja en claro cuál es el propósito de la organización. También, le da a la empresa una ventaja competitiva porque con ella se posee una visión clara de cómo se quiere que los clientes y los competidores perciban el negocio.

La filosofía corporativa de CAM INC queda resumida dentro de tres factores primordiales:

1) Misión
2) Visión
3) Valores

1.2.1. Misión

La misión empresarial representa la razón de ser de la existencia de una empresa u organización. Engloba lo que pretende cumplir y para quien lo quiere hacer. Es el marco de referencia para las actividades que realiza.

Lo que cualquier organización hace por sus clientes se clasifica como la misión empresarial. Presenta la necesidad a satisfacer, los clientes a dónde quiere llegar y los servicios a ofrecer. De igual modo, permite definir una identidad corporativa que ayuda a establecer el carácter de la organización.

La misión empresarial de CAM INC es: “Mantenernos a la vanguardia ofreciendo soluciones certeras a las necesidades de nuestros clientes con la satisfacción de sus expectativas en captación, distribución de remesas y entrega de alimentos.”

1.2.2. Visión

La visión define la posición en la que la empresa pretende situarse. En tal sentido, responde a las preguntas: ¿Quiénes queremos ser en los próximos años? y ¿Qué queremos que sea la empresa? Estas respuestas son la mirada hacia un futuro a largo plazo y sirven de rumbo y orientación para el establecimiento de estrategias de crecimiento y desarrollo, las cuales impactaran de forma positiva la elaboración y ejecución de las estrategias de competitividad de la empresa.

En consonancia con lo descrito anteriormente, la visión de CAM INC es: “Continuar siendo líder y referente del mercado de envío de dinero y entrega de alimentos de manera personalizada en la República Dominicana, comprometidos con la excelencia y regidos por estrictos principios éticos.”

1.2.3. Valores

El término valor puede ser aceptado como la importancia o validez de una persona u organización. Es considerado como una cualidad agregada a las cosas que permite darle una estimación positiva o negativa.

Los valores organizaciones de CAM INC son:

2. Excelencia
3. Compromiso
4. Integridad
5. Respeto
6. Colaboración

1.3. Estructura Organizacional

La estructura organizacional es una representación gráfica y modelo de diseño que detalla la forma en que está organizada y dividida una empresa, con la finalidad de cumplir las metas operacionales y organizacionales para llegar a los objetivos deseados. Es un elemento basado fundamentalmente en la jerarquía de subordinación dentro de la organización. Permite hacer las asignaciones de funciones y procesos al personal.

CAM INC es una empresa multinacional con su casa matriz ubicada en la ciudad de Miami, Estados Unidos. Tienen sedes en otros países, que actúan con una estrategia global para obtener el mayor beneficio, por ende, es importante presentar su división organizacional, ya que esta empresa en su conjunto es el objeto de estudio en esta monografía.

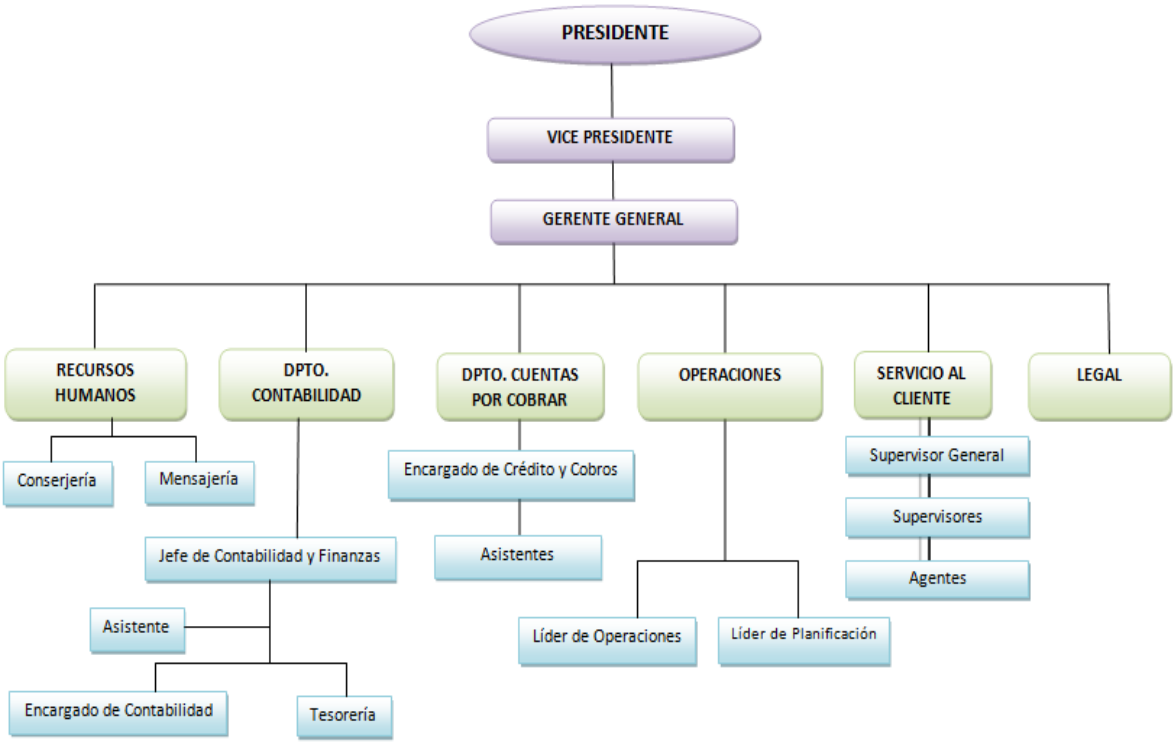

Figura 1. Organigrama de la empresa CAM INC. **Fuente:** CAM INC

1.4. Servicios de CAM INC

Los servicios son utilidades o funciones que llevan a cabo personas, objetos u organizaciones. Dichas funciones buscan responder a las necesidades inmediatas de la gente, agrupando una gran gama de actividades. Son intangibles y pretenden llenar las expectativas de quienes lo demandan e incrementar la satisfacción de los usuarios.

En su conjunto, los servicios son el objeto principal de cualquier transacción, o en última instancia, un valor añadido a la funciones de la empresa.

Los servicios prestados por CAM INC son:

Servicio de Remesas en República Dominicana

- ✓ Servicio al Cliente en horario de 8:00 AM a 10:00 PM
- ✓ Servicios los 365 días del año
- ✓ 100% de pagos en efectivo en dólares o pesos.

Servicio de Envío/Pago de remesas internacionales

Este servicio permite a cualquier persona recibir o enviar dinero desde Estados Unidos, Canadá, Turcos y Caicos, Jamaica, Bahamas y otros países, en cuestión de minutos.

Características:

- ✓ Pago 100% en efectivo en dólares o moneda local.
- ✓ Entrega a domicilio gratis
- ✓ Notificación telefónica

- ✓ El cliente deposita en pesos y el dinero es entregado en la moneda del país destino, para el caso de envío.

Servicio de Envío/Recepción de Alimentos

Este servicio permite a cualquier persona enviar o recibir alimentos.

- ✓ Los alimentos son entregados el mismo día si son enviados desde Estados Unidos o Canadá hacia Haití o República Dominicana, si la transacción fue realizada antes de la 1:00 PM.
- ✓ Entrega a domicilio.
- ✓ Garantía de buen estado de los mismos.

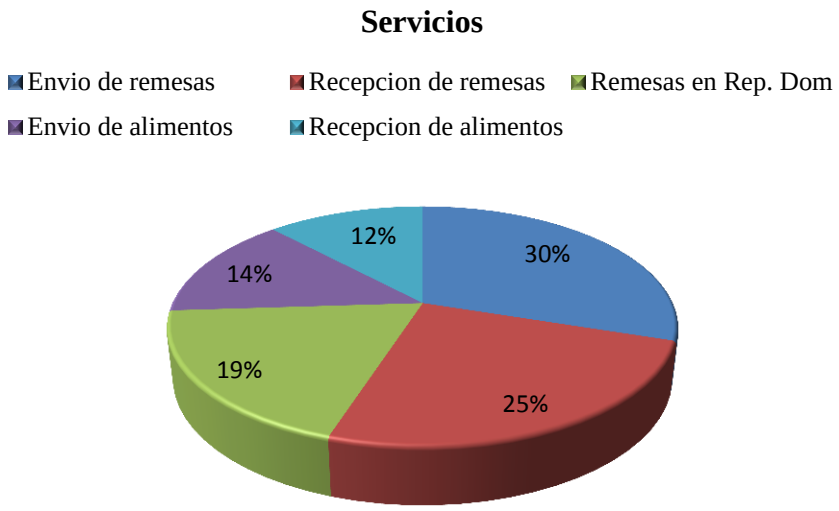

Figura 1.1 Detalle de los servicios de CAM INC. **Fuente:** CAM INC

1.5. Procesos Fundamentales en CAM INC

Un proceso es el conjunto de operaciones o procedimientos que se realizan con la finalidad de realizar una o varias tareas. Está conformado por una serie de elementos de entrada que al interactuar entre sí, se convierten en resultado.

Los procesos se pueden dividir en operativos y de soporte. Siendo los operativos aquellos que guardan una relación directa con el cliente y los de soporte son los que facilitan las bases y recursos para la realización de los procesos operativos.

Los procesos fundamentales de CAM INC son:

1. **Soporte al producto del cliente:** Este proceso se refiere a la capacidad de sostener los niveles de servicio al cliente, contestar teléfonos, correo electrónico y solicitudes de soporte. Se efectúa a diario e involucra el sistema distribuidor automático de llamadas.

Incluye los siguientes sub procesos:

a) Acceso al sistema de CAM INC: Los agentes de servicio al cliente y representantes de contabilidad y cuentas por cobrar deben acceder al sistema interno de CAM INC llamado CAM MT AGENT y Quick Books respectivamente, para poder brindar los servicios pertinentes a los usuarios.

b) Verificación de datos de los clientes: Consiste en comprobar la identidad de los clientes a la hora de demandar cualquier servicio o la revisión del mismo. Las revisiones de identidad permiten visualizar toda la información del cliente, tales como: nombres, domicilio, numero/s de cuenta bancaria, historial crediticio, documentos de identidad, números de contacto, correo electrónico, usuario en el sistema de CAM INC, entre otros.

c) Verificación de historial de transacciones: Permite visualizar las transacciones que han realizado los usuarios. Para verificar cualquier envío se debe dar el número del mismo, si es beneficiario debe suministrar el nombre del remitente, y si es remitente debe suplir el nombre del beneficiario, y el país de origen o destino respectivamente.

2. **Proceso de apoyo:** Este proceso engloba todo lo relacionado con el mantenimiento de las tecnologías y de las telecomunicaciones, se realiza diariamente y abarca el uso de los servidores disponibles en la empresa y sus teléfonos.
3. **Facilidades:** Con este proceso se ejecuta el mantenimiento del sistema del plantel operativo de CAM INC.
4. **Nómina:** Este proceso se encarga de generar y distribuir los pagos correspondientes a los empleados y se realiza de forma quincenal.

CAPÍTULO II. HERRAMIENTA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: *SYMANTEC DATA LOSS PREVENTION* (SDLP).

2.1. Definición de *Symantec Data Loss Prevention* (SDLP)

Symantec Data Loss Prevention (SDLP) es una completa solución de seguridad de datos que detecta, supervisa, protege y administra los datos confidenciales dondequiera que se almacenen o se utilicen. Ayuda a proteger la información de la empresa contra robo y pérdida, para cumplir con la privacidad de datos y al mismo tiempo proteger la reputación de la organización.

La herramienta gira en torno a la administración de flujos de trabajo. Permite la revisión instantánea de incidentes y mide la reducción de riegos desde una plataforma de administración unificada basada en web. Brinda la mayor visibilidad de los procesos empresariales y cuenta con controles de datos establecidos en caso de que se produzca una auditoría.

Symantec Data Loss Prevention tiene la siguiente metodología:

- ✓ **Visibilidad:** El primer paso es comprender donde están almacenados los datos y cuál es su uso en toda la empresa.
- ✓ **Reparación:** Una vez que haya identificado los procesos dañados y los usuarios de alto riesgo podrá comenzar a resolver los incidentes y resolver las fugas de datos.

- ✓ **Notificación:** Educa a los usuarios sobre las políticas de pérdidas de datos a través de notas emergentes en pantalla; esto reduce considerablemente los errores reincidentes.
- ✓ **Prevención:** Por último, somete las comunicaciones salientes a un período de cuarentena, cifrado o bloqueo para evitar que los usuarios filtren la información de forma accidental o maliciosa[2].

En base a esa metodología se puede deducir que el 90% de la prevención contra la pérdida de datos repercute en torno a lo que se hace después de encontrar información confidencial.

La empresa CAM INC viene presentando incidentes de robo y pérdida de información de sus clientes, lo que podría llevar a la realización de abusos en contra de los mismos. Todo esto porque no cuenta con controles para el acceso a los datos y no tiene establecidas políticas eficientes de privacidad y seguridad de la información, controles y políticas que ofrece la herramienta *Symantec Data Loss Prevention.*

Una encuesta reciente realizada por la firma Symantec reveló que el 50% de los empleados envía regularmente archivos de trabajo por correo electrónico a cuentas

[2] Symantec. http://www.symantec.com/es/mx/data-loss-prevention

personales, acción que sucede muy a menudo en CAM INC, dejando claro que los canales más comunes de pérdida de datos son el correo electrónico y la web. Por ende, es importante supervisar y proteger las comunicaciones de red enviadas por los usuarios dentro o fuera de la red de la empresa.

Conocer los datos representa el foco de la protección de la información, se debe saber dónde se almacena la información confidencial y por donde circula para identificar las mejores políticas y procedimientos para protegerlas. Esta es la funciona primordial de *Symantec Data Loss Prevention* y la misma es congruente con el objetivo general de esta monografía: la prevención de la pérdida de información.

2.2. Funcionalidad de *Symantec Data Loss Prevention*

Las funciones de *Symantec Data Loss Prevention* son las siguientes:

a) Detección: Detecta dónde se almacenan los datos en los Endpoint y servidores; identifica a los verdaderos propietarios de los datos y recibe notificaciones de actividades inusuales.
b) Supervisión: Supervisa cómo se usan los datos cuando los usuarios están dentro y fuera de la red corporativa.
c) Protección: Protege los datos mediante el envío de notificaciones a los usuarios acerca de infracciones de políticas, la protección de carpetas y archivos expuestos, y la detención de comunicaciones salientes.

d) Administración: Administra las políticas de pérdida de datos, el flujo de trabajo, las reparaciones, la elaboración de informes y la administración desde una consola de administración eficaz basada en Web.

e) Portal de reparación con autoservicio: Permite a los propietarios de datos de las empresas revisar y reparar infracciones de políticas de archivos de la red directamente desde un portal intuitivo en línea, y optimiza el proceso de reparación de riesgos.

f) Administración de agentes Endpoint: Proporciona capacidades mejoradas de elaboración de informes de estado de los agentes y una implementación más flexible de diferentes configuraciones del grupo de agentes desde un solo servidor de Endpoint.

g) Correlación de documentos indexados de Endpoint: Evalúa documentos en tiempo real en busca de coincidencias exactas de contenido en Endpoint y proporciona mayor control sobre el uso de datos cuando los usuarios están dentro y fuera de la red.

h) Correlación exacta de datos: Detecta con más precisión datos estructurados (por ejemplo, bases de datos y hojas de cálculo) que contienen frases complejas y de varias palabras, de modo que reduce la cantidad de falsos positivos.

i) Supervisión de correo electrónico móvil: Detecta mensajes de correo electrónico confidenciales que los usuarios descargaron en dispositivos Android e iOS mediante el protocolo Microsoft Exchange ActiveSync.

j) Supervisión de red: Detecta datos confidenciales enviados mediante la nueva versión del protocolo de Internet, IPv6.

k) Instalación de un solo servidor: Permite implementar la plataforma de Enforce, los servidores de detección y la base de datos de Oracle en un único servidor físico. reduce los costos de hardware y mantenimiento[3].

2.2.1. Beneficios claves de *Symantec Data Loss Prevention*

Symantec Data Loss Prevention tiene los siguientes beneficios:

- ✓ Aumenta la visibilidad del riesgo de pérdida de datos y reduce los riesgos notablemente.
- ✓ Instruye a los empleados bien intencionados sobre infracciones de políticas y evita filtraciones de datos accidentales.
- ✓ Evita que intrusos maliciosos roben elementos de propiedad intelectual, como diseños de productos e informes financieros.
- ✓ Ayuda a demostrar el cumplimiento de las normas globales de privacidad de datos, como la Ley de Responsabilidad y Transferibilidad de Seguros Médicos (HIPAA) de los Estados Unidos y la Directiva de Protección de Datos de la Unión Europea[4].

[3] Symantec. http://www.symantec.com/es/mx/data-loss-prevention
[4] Symantec. http://www.symantec.com/es/mx/data-loss-prevention

2.2.2. Requisitos de sistema para la utilización de *Symantec Data Loss Prevention*

El software Symantec Data Loss Prevention está compuesto por una plataforma de administración unificada, servidores de detección basados en contenido y agentes Endpoint ligeros. A diferencia de otras soluciones de prevención contra la pérdida de datos, funciona en entornos muy dispersos y escala hasta cientos de miles de empleados.

- ✓ **Plataforma de administración y servidores de detección**

Enforce Plataform y los servidores de detección de Symantec Data Loss Prevention son compatibles con una amplia variedad de sistemas operativos y entornos virtualizados:

- Microsoft Windows Server 2008, 2012[5]
- Red Hat Enterprise Linux 5.7: 5.10, 6.4, 6.5[6]
- VMware ESX 4.0; ESX/ESXi 4.1 y 5.x[7]

Enforce Plataform también cuenta con el soporte de una base de datos interna, Oracle Standard One u Oracle Standard Edition, que almacena todos los datos de incidentes históricos y la información del sistema.

[5] Línea de productos para servidores de Microsoft Corporation en las versiones 2008 y 2012.
[6] Distribución del sistema operativo Linux.
[7] Plataforma de virtualización a nivel de centro de datos producido por VMware, Inc.

- ✓ **Agente Endpoint**

El agente Endpoint de Symantec Data Loss Prevention es compatible con los siguientes sistemas operativos y entornos virtualizados:

- Apple Mac OS X 10.8, 10.9[8]
- Microsoft Windows 7, 8.0, 8.1; Server 2003, Server 2008
- Citrix XenApp[9] 4.5, 6.0, 6.5; XenDesktop 3.0, 4.0, 5.0, 5.6
- Microsoft Hyper-V[10]
- VMware Workstation[11] 6.5; VMware View 4.6

2.3. Módulos de la herramienta *Symantec Data Loss Prevention*

Symantec Data Loss Prevention posee una gama variada de módulos direccionados a los distintos ambientes del área de tecnología de la información.

Los módulos principales de Data Loss Prevention son:

[8] Entorno operativo basado en Unix, desarrollado, comercializado y vendido por Apple Inc., versión 10.
[9] Software que permite a las empresas poner a disposición de sus empleados las aplicaciones que están instalados dentro de la empresa, para ser accesados de manera remota.
[10] Programa de virtualización basado en un hipervisor para los sistemas de 64 bits.
[11] Herramienta que permite virtualizar un sistema operativo dentro de otro.

- **Symantec Backup Exec System Recovery:** Data Loss Prevention se integra con Backup Exec System Recovery para permitir el análisis de imágenes de copia de seguridad de datos confidenciales.

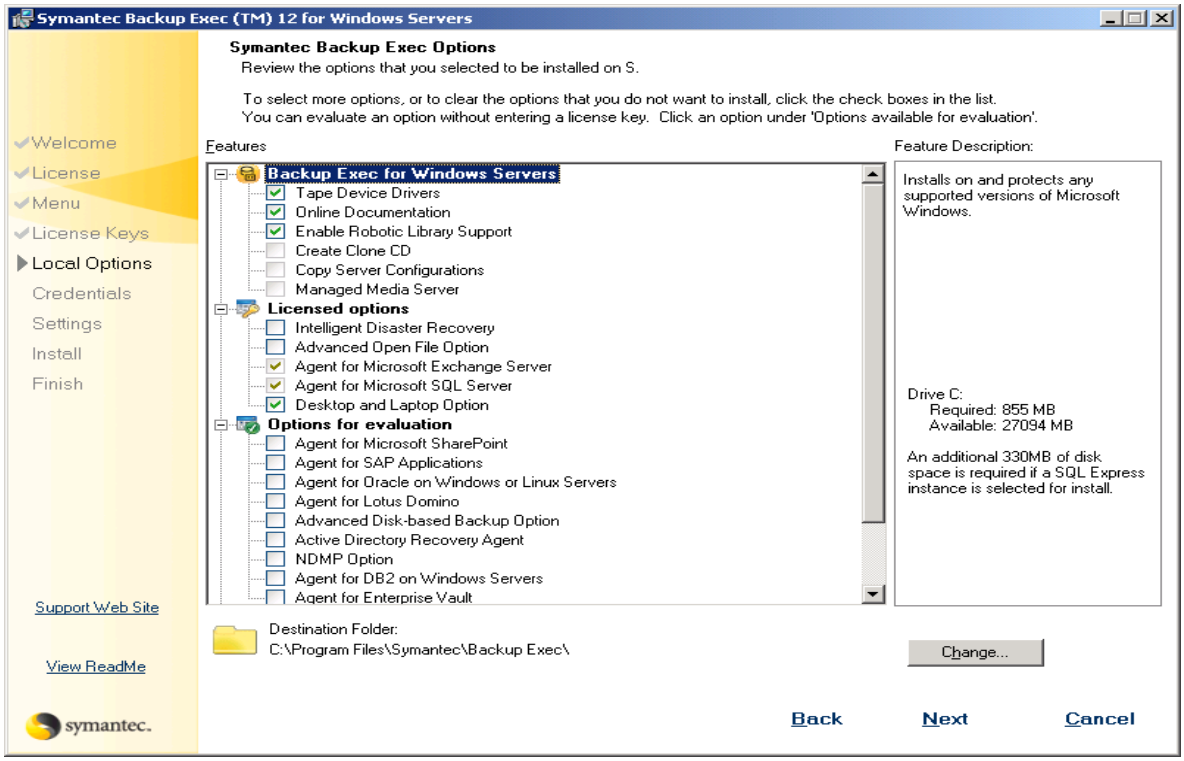

Figura 2. Entorno de Symantec Backup Exec System Recovery. **Fuente:** Symantec

- **Symantec Control Compliance Suite:** Los datos de incidentes de Data Loss Prevention pueden importarse en Control Compliance Suite para identificar los sistemas que pueden estar sujetos a políticas de control técnico en función de los datos almacenados en ellos.

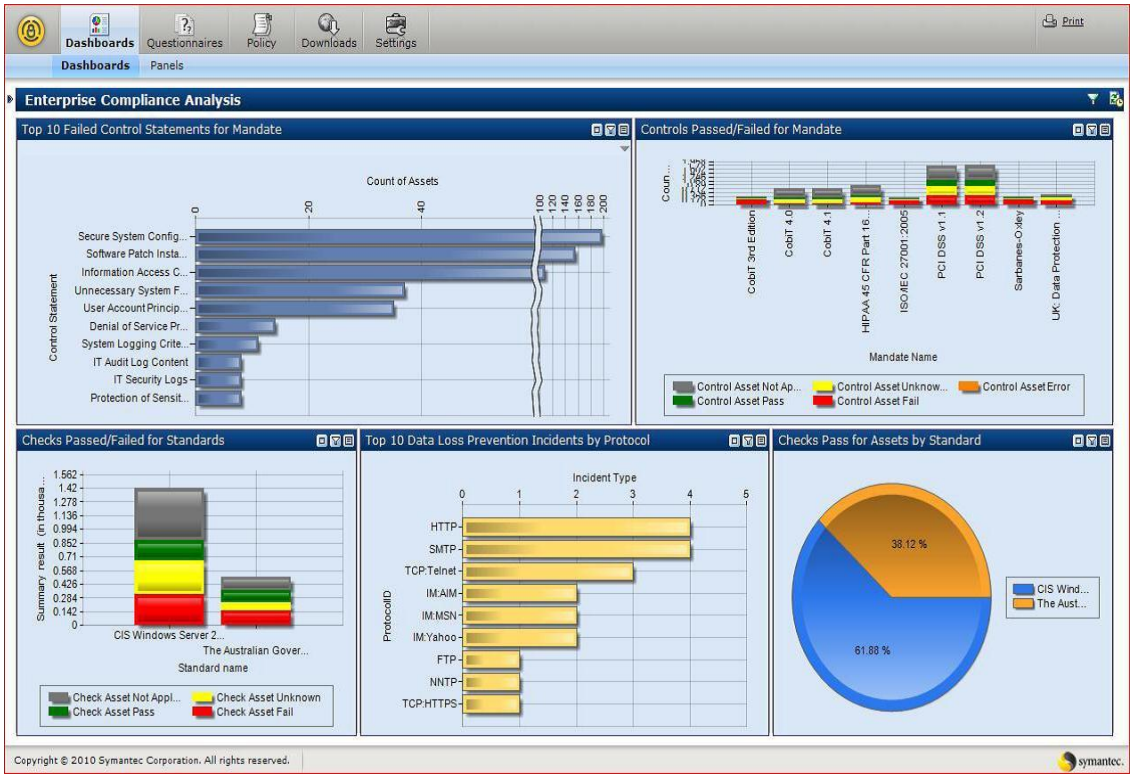

Figura 2.1 Módulo Symantec Control Compliance Suite. **Fuente:** Symantec

- **Symantec Encryption:** Data Loss Prevention se integra con Symantec Endpoint Encryption para aplicar cifrado de archivos basado en políticas a medida que se copian en tiempo real en dispositivos USB; se integra con Symantec File Share Encryption para extraer, descifrar y analizar texto en documentos cifrados en File Share; se integra con Symantec Universal Gateway Email para aplicar cifrado

basado en políticas de correo electrónico y proporcionar confirmación de ciclo cerrado de entrega segura en Enforce Plataform de Data Loss Prevention.

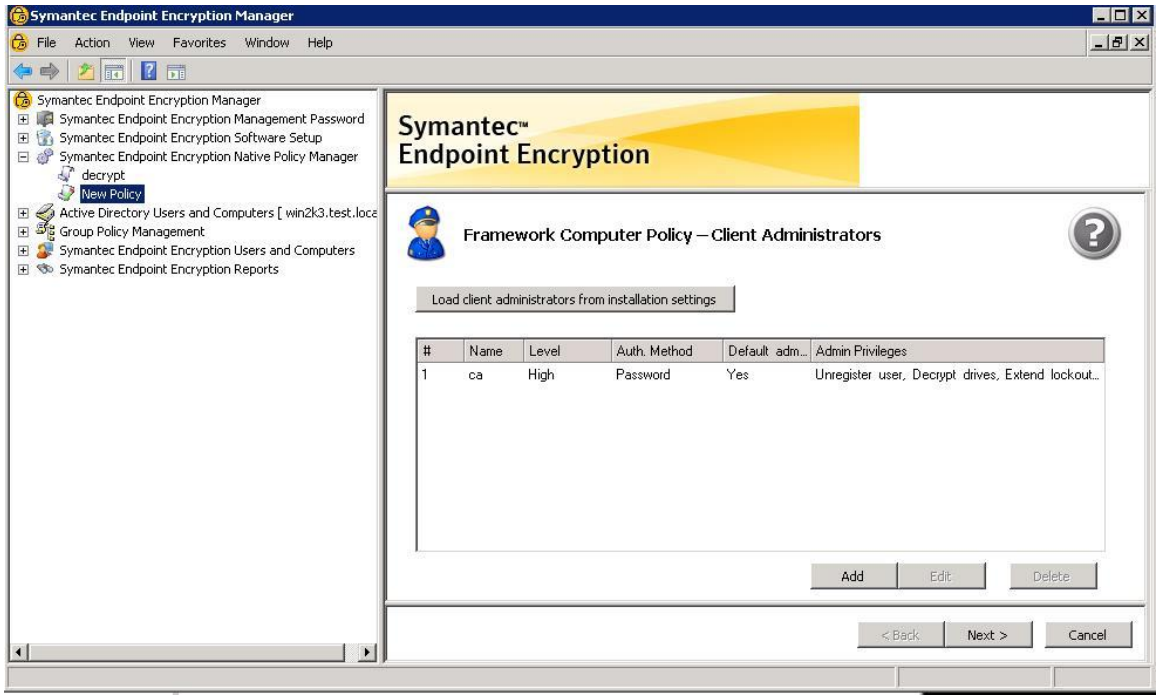

Figura 2.2 Módulo Symantec Endpoint Encryption. **Fuente:** Symantec

- **Symantec Endpoint Protection Manager:** Data Loss Prevention se integra con Endpoint Protection Manager para aplicar bloqueo basado en políticas (por ejemplo, control de aplicaciones, bloqueo de puertos, control de dispositivos) en equipos portátiles y de escritorio.

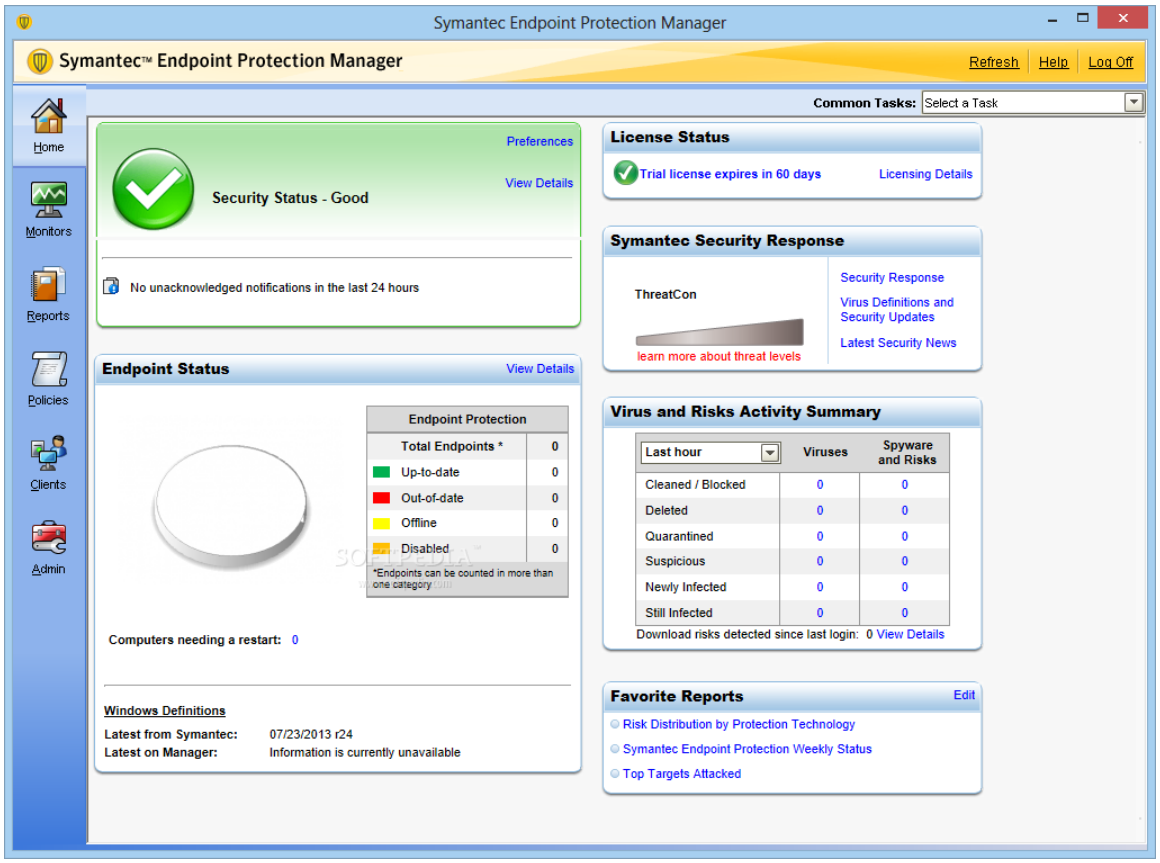

Figura 2.3 Symantec Endpoint Protection Manager. **Fuente:** Symantec

- **Symantec Enterprise Vault:** Con tecnología del motor de detección de contenido de Data Loss Prevention, Enterprise Vault Data Classification Services proporciona servicios de clasificación y etiquetado de datos basados en políticas para el correo electrónico archivado. Symantec Enterprise Vault Compliance Accelerator y Symantec Enterprise Vault Discovery Accelerator aprovechan los resultados de la clasificación para respaldar la retención de registros.

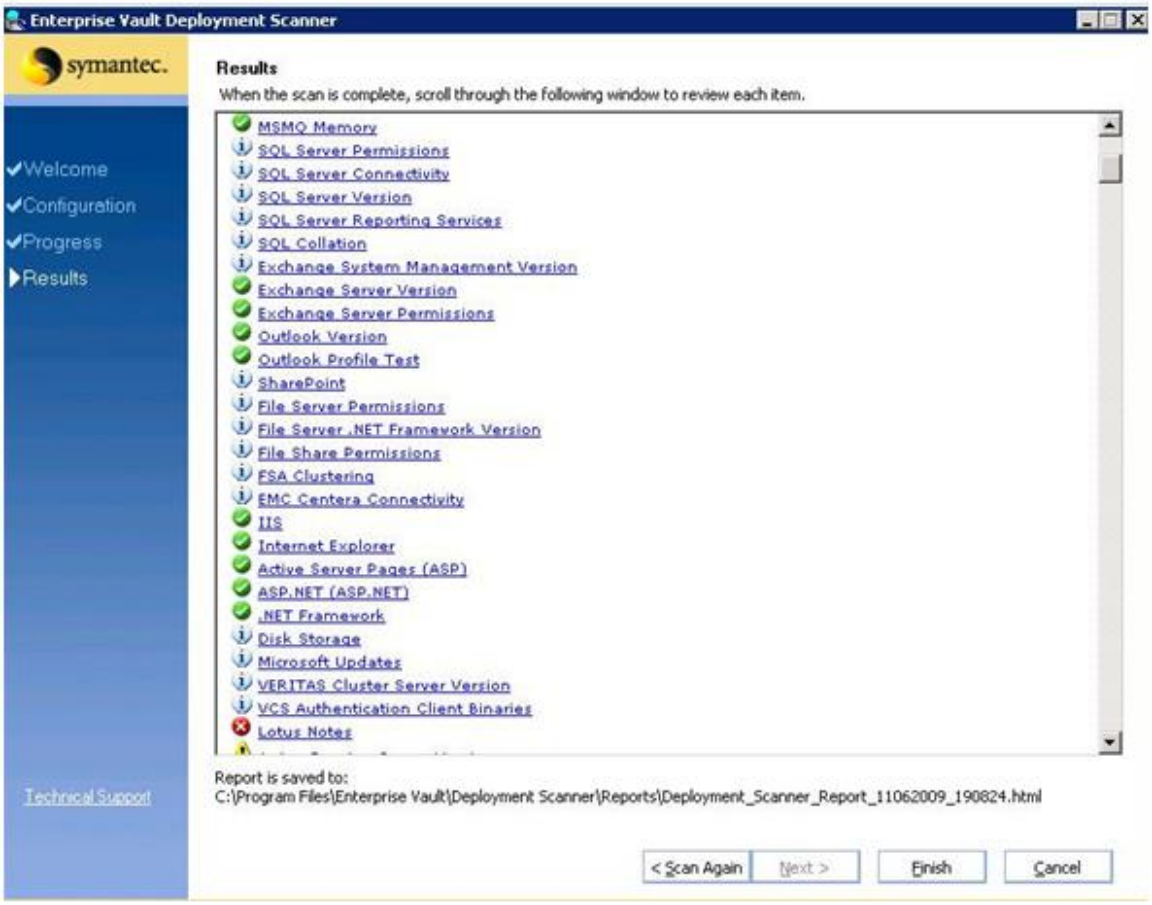

Figura 2.4 Symantec Enterprise Vault Deployment Scanner. **Fuente:** Symantec

- **Symantec Messaging Gateway:** Data Loss Prevention se integra con Messaging Gateway para que pueda revisar, lanzar y dirigir mensajes en cuarentena con facilidad directamente desde Enforce Plataform de Data Loss Prevention.

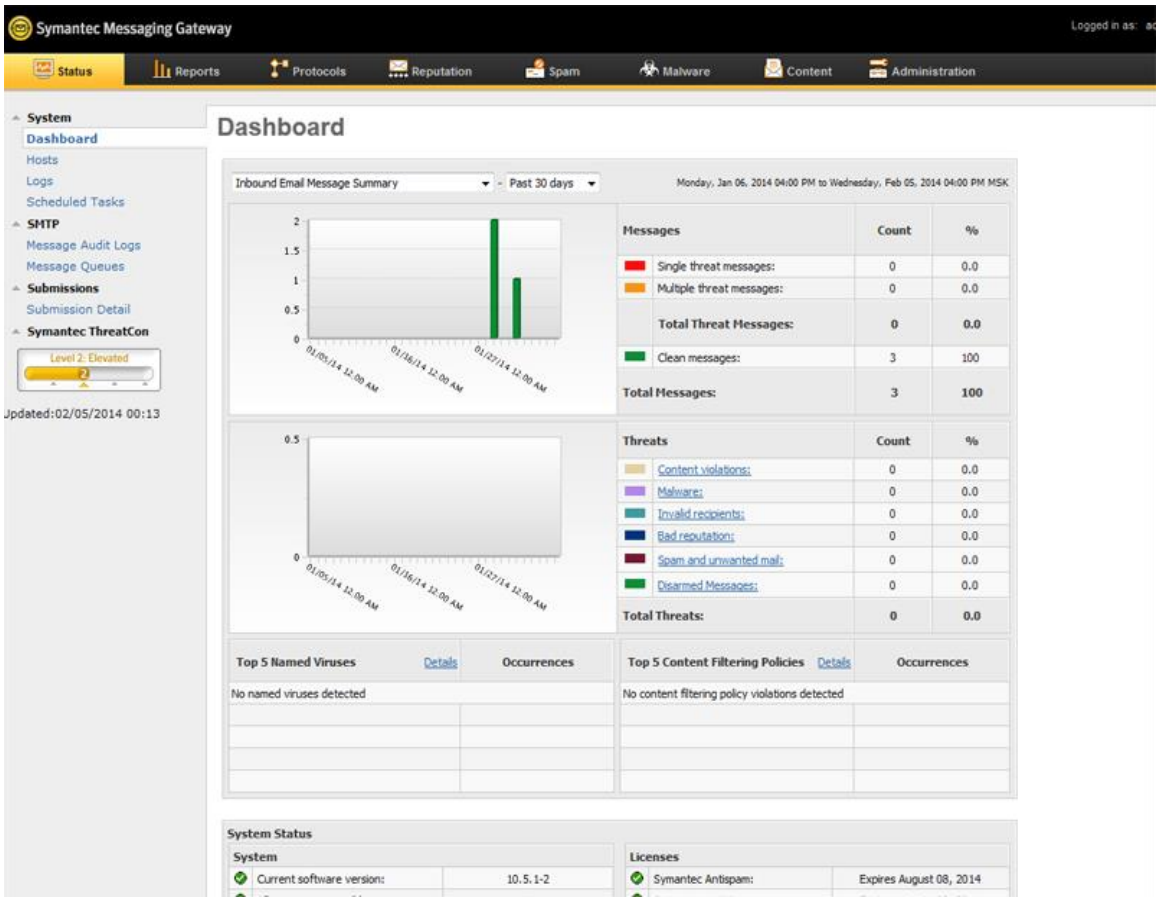

Figura 2.5 Symantec Messaging Gateway. **Fuente:** Symantec

- **Symantec Mobile Management:** Data Loss Prevention se integra con Mobile Management para aplicar configuración de red privada virtual en dispositivos móviles, mostrar notificaciones en pantalla cuando los usuarios intentan manipular perfiles de los dispositivos y aplica borrado remoto basado en políticas en dispositivos.

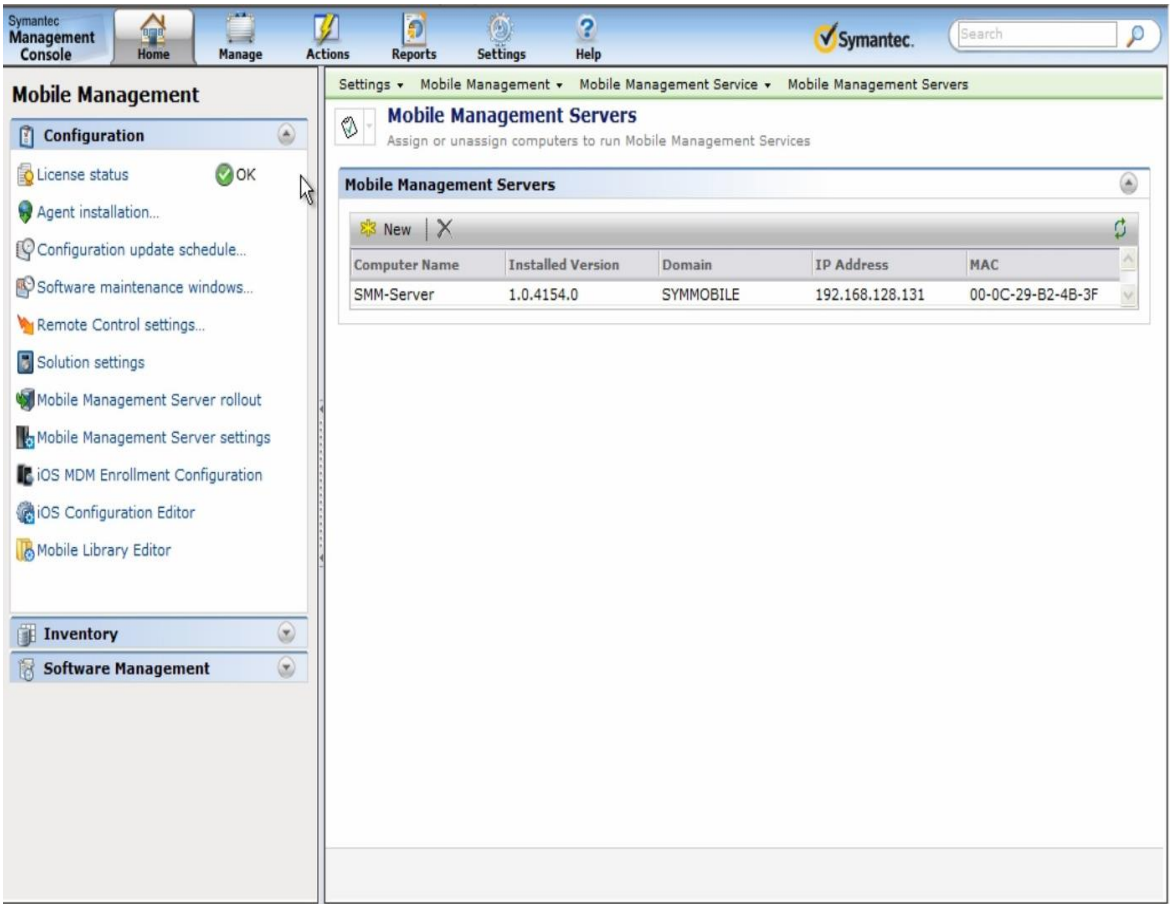

Figura 2.6 Symantec Mobile Management. **Fuente:** Symantec

CAPÍTULO III. SEGURIDAD DE LA INFORMACIÓN.

La información es uno de los activos más valiosos que tiene cualquier organización. Es vital para el funcionamiento y quizá incluso sea decisiva para la supervivencia de la empresa. Por ende, la seguridad de este activo debe ser un proceso continuo de mejoramiento, tanto en la parte concerniente a las políticas, como a los controles establecidos para la protección de la misma.

3.1. Seguridad de la Información

La seguridad es el término que alude al conjunto de soluciones técnicas, métodos y procedimientos que permite resguardar cualquier persona u objeto de los riesgos. Es un concepto asociado a la certeza y la contingencia. De forma específica, la seguridad de la información hace referencia a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos.

La seguridad de la información se encarga de garantizar la disponibilidad y confiabilidad de la información. Para alcanzar tal objetivo se apoya en la seguridad informática que debe responder por la seguridad de la infraestructura tecnológica en las cuales opera la seguridad de la información.

En la seguridad de la información, la información se concibe como el centro de sus operaciones. Su manejo está basado en la tecnología y su valor puede variar ateniendo al

grado de impacto que genera en la empresa. Según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:

- Crítica: Es indispensable para las operaciones de la empresa.
- Valiosa: Es un activo de la empresa.
- Sensible: Debe de ser conocida por las personas autorizadas.[12]

3.2. Bases de la Seguridad de la Información

La seguridad de la información es de forma general la protección de la información y de los sistemas de la información contra acceso, uso, divulgación, interrupción o destrucción no autorizada. A pesar de que la seguridad absoluta de la información no es posible, existen algunos elementos que le dan soporte y le permiten garantizar el mayor nivel de confiabilidad. Dichos elementos son: confidencialidad, autenticación, integridad, disponibilidad, no repudiación, control de acceso, auditabilidad, protección a la réplica y certificación mediante terceros de confianza.

3.2.1. Confidencialidad

Esta es la función de la seguridad de la información que garantiza que cada mensaje que se transmita o sea almacenado en un sistema informático solo podrá ser leído por su destinatario. En caso de que dicho mensaje caiga en manos de terceras personas, estas no

[12] Oficina de Estadística e Informática. Tecnología de la Información y Comunicaciones. http://issuu.com/fmalcap/docs/publicaciontics

podrán acceder al contenido del mensaje. Por lo tanto, esta función busca garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de respaldo y de los datos transmitidos a través de redes de comunicaciones.

3.2.2. Autenticación

La autenticación es la función que le permite al destinatario de un mensaje estar seguro de que su creador es la persona que figura como remitente de dicho mensaje. Esta función garantiza que la identidad del creador de un mensaje o documento sea legítima.

Por otro lado, también se puede hablar de la autenticación de un equipo a una red o intento de acceso a un determinado servicio. En este caso, la autenticación puede efectuarse mediante la identidad del dispositivo o mediante la identificación del servidor y dispositivo mutuamente.

3.2.3. Integridad

La integridad es la función que se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de la red informática. Permite la detección de modificaciones como la añadidura o eliminación de algún dato en el mensaje.

3.2.4. Disponibilidad

La disponibilidad del sistema informático también es factor importante para garantizar el cumplimiento de sus objetivos, debido a que se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de manera que pueda estar siempre a disposición de los usuarios que deseen acceder a sus servicios.

3.2.5. No repudiación

La finalidad de este servicio de seguridad es implementar un mecanismo de prueba que permita demostrar la autoría y envío de un determinado mensaje, de tal manera que el usuario que lo ha creado y enviado a través del sistema no pueda posteriormente negar esta circunstancia, situación que también se aplica al destinatario del envío.

3.2.6. Control de acceso

El control de acceso es el proceso en el que se da permisos a usuarios o a un grupo de usuarios de acceder a distintos objetos tales como ficheros, documentos, mensajes, carpetas o impresoras dentro de la red. El control de acceso se basa en tres conceptos fundamentales, los cuales son: identificación, autenticación y autorización.

También es considerado un mecanismo que, en función de la identificación mediante programas de control de acceso, permite acceder a los datos y/o recursos de la empresa. Los programas o herramientas de control de acceso deberán identificar a los usuarios que tienen autorización para usar determinadas funcionalidades del sistema, con su correspondiente nivel de acceso. En base a esto, se tienen los siguientes niveles de acceso a la información:

- Nivel 1. Consulta de la información no restringida o reservada.
- Nivel 2. Mantenimiento de la información no restringida o reservada.
- Nivel 3. Consulta de la información incluyendo la restringida o reservada.
- Nivel 4. Mantenimiento de la información incluyendo la restringida.[13]

3.2.7. Auditabilidad

La auditabilidad es el servicio que permite registrar y monitorizar la utilización de los distintos recursos del sistema por parte de los usuarios que han sido previamente autenticados y autorizados. De esta forma, se puede detectar situaciones o comportamientos extraños por parte de los usuarios, además de llevar un control del rendimiento del sistema.

[13] Microsoft. Pymes y Autónomos. http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=323

3.2.8. Protección a la réplica

Este es el servicio de seguridad que trata de reprimir la realización de “ataques de repetición” por parte de los usuarios maliciosos, que consisten en la interceptación y posterior reenvío de mensajes para tratar de engañar al sistema y provocar operaciones no deseadas. Para esto, en este servicio se suele utilizar un número de secuencia o sello temporal en todos los mensajes y documentos que necesiten ser protegidos dentro del sistema.

3.2.9. Certificación mediante terceros de confianza

Cuando se realiza cualquier tipo de transacción a través de un medio electrónico se requiere de nuevos requisitos de seguridad, para poder garantizar la autenticación de las partes que interviene, la integridad y el contenido de los mensajes. El organismo que se encarga de certificar la realización y el contenido de las operaciones y de asegurar la identidad de los intervinientes, dotando de esta manera a las transacciones electrónicas de una mayor seguridad jurídica.

3.3. Seguridad Informática

La seguridad informática es una serie de procedimientos, métodos, normas y técnicas, que impiden que se ejecuten operaciones no autorizadas en un sistema o red informática,

cuyos efectos puedan producir daños sobre la información, poner en riesgo su confidencialidad, autenticidad o integridad, reducir el rendimiento de los equipos o prohibir el acceso de usuarios autorizados al sistema.

3.3.1. Objetivos de la Seguridad Informática

Entre los principales objetivos de la seguridad informática se pueden destacar los siguientes:

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad.
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

3.4. Base de Datos

Según Connolly y Begg (2006) y Date (1995), una base de datos es un repositorio para la colección de registros de datos computarizados, integrados y compartidos y debido a que

una base de datos puede ser vista por el usuario como un solo elemento compartido entre todos los usuarios del sistema, satisfaciendo las necesidades de información de una organización. Donde organización es un término genérico que converge para cualquier organización comercial, científica, técnica o de algún otro tipo. Al hablar de bases de datos, nos referimos al almacenamiento de datos.

3.4.1. Definición de Base de Datos

Según Manuel Sierra (2013), una base de datos es un sistema informático a modo de almacén. En este almacén se guardan grandes volúmenes de información. Por ejemplo, imaginemos que somos una compañía telefónica y deseamos tener almacenados los datos personales y los números de teléfono de todos nuestros clientes, que posiblemente sean millones de personas.

"Colección o depósito de datos, donde los datos están lógicamente relacionados entre sí, tienen una definición y descripción comunes y están estructurados de una forma particular. Una base de datos es también un modelo del mundo real y, como tal, debe poder servir para toda una gama de usos y aplicaciones", (*Conference des Statisticiens Européens, 1977*).

De forma general una base de datos no es más que un depósito que permite guardar grandes cantidades de información de manera organizada para que luego ser encontrada y utilizada fácilmente.

3.4.2. Tipos de bases de datos

Las bases de datos están divididas en tres renglones:

- Bases de datos de acuerdo a variabilidad.
- Bases de datos de acuerdo a su contenido.
- Bases de datos de acuerdo a su modelo.

Según la variabilidad de la base de datos, pueden ser:

- **Bases de datos estáticas**

  Este tipo de bases de datos es de solo lectura, es decir, la información no puede ser cambiada, y se utilizan principalmente para guardar información histórica que más adelante se pueden utilizar para estudiar el comportamiento de una serie de datos a través del tiempo, analizar la conducta ya sea de algún lugar o persona, tomar decisiones y realizar proyecciones, debido a que información permanecerá y no hay riesgo de que pueda cambiar.

- **Bases de datos dinámicas**

En este tipo de bases de datos la información que se almacena se puede modificar con el tiempo, permitiendo de esta manera, operaciones como actualización, borrado y adición de datos, a parte de las operaciones fundamentales de consulta. Esta modificación puede ser de manera automática por el mismo ordenador o una persona lo puede actualizar. Un ejemplo de estas puede ser la base de datos que se utiliza en los sistemas de información de una farmacia, una empresa o un supermercado.

Según su contenido, las bases de datos pueden ser:

- **Bases de datos bibliográficas**

Este tipo de bases de datos se utiliza regularmente con documentos o libros, ya que contiene información de un autor, una publicación, editoriales, y todos los datos con los que este cuenta.

- **Bases de datos de texto completo**

Este tipo de base de datos es utilizada para almacenar fuentes primario, por ejemplo, todo el contenido de las ediciones de una colección de revistas.

- **Directorios**

Un ejemplo de este tipo de base de dato son las guías telefónicas en formato electrónico.

Según el modelo, las bases de datos pueden ser:

- **Bases de datos jerárquicas**

  Esta es una base de datos lógica donde se organizan los datos utilizando estructuras de árbol invertido en el cual cada registro se conoce como segmento. Esta se compone de una serie de bases de datos físicas, de forma que cada base de datos física se compone de todas las ocurrencias de un determinado tipo de registro o ficha. Las bases de datos jerárquicas son principalmente utilizadas por aplicaciones que manejan una gran cantidad de información y datos que se comparten de manera seguida permitiendo de esta forma, crear estructuras estables y de gran rendimiento. Una base de datos de este tipo, no permite el acceso directo a las instancias de un segmento hijo, si no es seleccionando previamente las instancias de los padres de los que depende.

- **Base de datos de red**

  A diferencia del modelo jerárquico, el modelo de bases de datos de red permite que un mismo nodo tenga varios padres (evento que no se permite en el modelo jerárquico). Este modelo es una mejora del modelo jerárquico, debido a que ofrece una solución eficiente al problema de la redundancia de datos; no obstante, la dificultad que a la hora de administrar la información en este tipo base de datos, ha hecho que este sea un modelo utilizado en la mayoría de los casos por programadores

más que por usuarios finales. Este modelo está diseñado para representa relaciones complejas de información de manera más efectiva, para que de esta forma, se pueda mejorar el desempeño de la base de datos e imponer estándares.

- **Bases de datos transaccionales**

La finalidad de estas bases de datos es el envío y recepción de datos a grandes velocidades, es decir, recolección y recuperación de datos a la mayor velocidad posible, por consiguiente, la redundancia y duplicación de información no es un problema al igual que con los demás tipos bases de datos. Este tipo bases de datos no son muy comunes y están mayormente dirigidas al entorno de análisis de calidad, datos de producción e industrial.

- **Bases de datos documentales**

Las bases de datos documentales admiten la indexación a texto completo, y en líneas generales la realización búsquedas más potentes.

- **Base de dato relacional**

Una base de datos relacional es un conjunto de tablas ordenadas en registros y campos, que están vinculadas entre sí por un campo en común, en ambos casos tiene las mismas características como por ejemplo el nombre de campo, tipo y longitud; a este campo por lo general se le denomina ID, identificador o clave.

- **Bases de datos orientadas a objetos**

Este tipo de base de datos está enfocado a objetos, este modelo trata de almacenar los objetos completos (estado y comportamiento). Esta base de datos incorpora todos los conceptos importantes del paradigma de objetos: encapsulación, herencia y polimorfismo. En este tipo de base de datos, los usuarios tienen la opción de definir operaciones sobre datos como parte de la definición de esta.

- **Bases de datos deductivas**

Un sistema de base de datos deductiva permite realizar deducciones a través de inferencias. Este se basa especialmente en reglas y hechos que son almacenados en la base de datos. Estas bases de datos llamadas también bases de datos lógicas, a raíz de que se basan en la lógica matemática.

3.4.3. Base de Datos a utilizar para la implementación de la herramienta *Symantec Data Loss Prevention*

Para la implementación de la herramienta de control de pérdida *Symantec Data Loss Prevention* se pretende utilizar bases de datos relacionales. Según Jorge Sánchez (2004), las bases de datos relacionales se basan en el uso de tablas (también se las llama relaciones). Las tablas se representan gráficamente como una estructura rectangular

formada por filas y columnas. Cada columna almacena información sobre una propiedad determinada de la tabla (se le llama también atributo), nombre, apellidos, edad, etc. Cada fila posee una ocurrencia o ejemplar de la instancia o relación representada por la tabla (a las filas se las llama también tuplas).

La base de dato relacional cumple con el modelo relacional, el cual permite establecer inter conexiones o relaciones entre los datos, los cuales están guardados en tablas, y a través de estas conexiones relacionar los datos de ambas tablas. Este modelo busca representar la base de datos como un conjunto de tablas. El modelo de base de datos relacional es el que se utiliza para modelar problemas reales y administrar datos dinámicos.

Características:

- Una base de datos relacional está compuesta por varias tablas o relaciones.
- No se puede tener dos tablas con el mismo nombre.
- Cada tabla es a su vez un conjunto de registros.
- La relación entre una tabla padre y una tabla hijo se realiza por medio de las claves primarias y ajenas.

3.5. Servidores

Cuando se menciona la palabra servidor, se refiere a un ordenador o conjunto de ordenadores, que suministra algún tipo de información o servicio a un cliente final. En las empresas se utilizan diferentes tipos de servidores, ya sea para alojar las aplicaciones que estos utilizaran para el desarrollo de sus funciones, para dar accesos a los empleados, para el manejo de los correos entre otros.

3.5.1. Definición de Servidor

Según Manuel Sierra (2013), un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información.

Un servidor es un computador que forma parte de una red informática y que provee servicios a otros ordenadores, los cuales son llamados clientes. Los servidores suelen ser utilizados para almacenar grandes cantidades de archivos digitales, y a través de la red, los clientes se conectan con el servidor y acceden a dicha información.

3.5.2. Tipos de Servidores

A continuación se listan los tipos de servidores más comunes y utilizados:

- **Servidores de Aplicaciones**

  Este tipo de servidor es el que proporciona los distintos servicios que soportan la ejecución y disponibilidad de las aplicaciones desplegadas. Es el centro de un gran sistema distribuido. El servidor de aplicaciones provee una estructura en tres capas que permite distribuir nuestro sistema de forma más eficiente.

- **Servidores de Audio/Video**

  Los servidores de Audio/Video agregan capacidad de multimedia a los sitios web permitiéndoles de esta forma, mostrar contenido multimedia en forma de flujo continuo desde el servidor.

- **Servidores de Chat**

  Los servidores de chat son los que permiten llevar a cabo discusiones en tiempo real, ya que a través de estos, se intercambian información a una gran cantidad de usuarios.

- **Servidores de Protocolo de Transferencia de Archivos (FTP)**

  Este es uno los servicios más antiguos de Internet, el protocolo de transferencia de archivos (*siglas en inglés File Transfer Protocol*) permite mover uno o más archivos.

Este es el servidor que se utiliza a la hora de hacer una transferencia de una computadora a otra desde cualquier parte del mundo a través de Internet.

- **Servidores Groupware**

Un servidor groupware es un software que se diseña para permitir la colaboración con los usuarios, sin importar el lugar donde se encuentre, vía Internet o vía Intranet corporativo, para así poder trabajar juntos en una atmósfera virtual.

- **Servidores de Listas**

Los servidores de listas son los ofrecen a los usuarios una mejor forma de manejar listas de correo electrónico, ya sean discusiones interactivas abiertas al público o listas unidireccionales de anuncios, publicidad o boletines de noticias.

- **Servidores Proxy**

Los servidores proxy están situados entre un programa del cliente (mayormente un navegador) y un servidor externo (en la mayoría de los casos un servidor web) para filtrar peticiones, compartir conexiones y mejorar el funcionamiento.

- **Servidores Telnet**

Un servidor telnet es el que permite a los usuarios acceder a un ordenador huésped, para que de esta forma, pueda realizar tareas como si estuviera trabajando directamente en dicho ordenador.

- **Servidores Web**

Un servidor web es el que se encarga de servir el contenido estático a un navegador, cargar un archivo y lo servir a través de la red.

- **Servidor DHCP**

Un servidor DHCP es el que se encarga de recibir las peticiones de los clientes que solicitan una configuración de red IP. Este es el que responderá a dichas peticiones suministrando los parámetros que permitan a los clientes auto configurarse. Este tipo de servidor utiliza un modelo cliente-servidor en el que mantiene una administración centralizada de las direcciones IP utilizadas en la red.

- **Servidores de Acceso Remoto**

Un servidor de acceso remoto no es más que la unión de un hardware y un software que permite el acceso de manera remota a herramientas o información que están almacenadas en una red de dispositivos.

3.6. Implementación de los Sistemas de Seguridad

Para implementar un sistema de seguridad se recomienda seguir 7 pasos:

Paso 1: Establecer la política de seguridad de la empresa

Qué debe incluir su política de seguridad de la empresa:

- Responsables del desarrollo, implantación y gestión de la política
- Cree una directiva de uso aceptable: Es un documento en el que se informa a los empleados de lo que pueden y no pueden hacer en los equipos de la empresa.
- Plan de Actuación en caso de alarma de Seguridad.

Paso 2: Proteger los equipos de escritorios y portátiles.

- Protéjase de los virus y el software espía: Los virus, así como los gusanos y los troyanos, son programas maliciosos que se ejecutan en su equipo. Existen herramientas de eliminación de software malintencionado que comprueban infecciones por software malintencionado específico y ayuda a eliminarlas. Instalar software antivirus. Debe disponer de protección antivirus en todos sus equipos de escritorio y portátiles.
- Configure un firewall: Un firewall es un programa encargado de analizar tanto el tráfico entrante como saliente de un equipo, con el fin de bloquear determinados puertos y protocolos que potencialmente podrían ser utilizados por las aplicaciones.
- Evite el correo electrónico no deseado. (Spam): Spam son mensajes de correo electrónico comercial no solicitado. Hay que adoptar medidas de protección frente al correo electrónico no deseado. Como filtros de correo electrónico actualizados.
- Utilice solamente software legal: El uso de software ilegal además de generar riesgos de carácter penal, también puede generar problemas en la seguridad de la

información, lo que lo que conlleva a pérdidas en la rentabilidad y productividad de la organización. El software legal ofrece garantía y soporte del fabricante.

Paso3: Proteger la red

- Utilice contraseñas seguras: Informar a los empleados de la importancia de las contraseñas es el primer paso para convertir las contraseñas en una valiosa herramienta de seguridad de la red, ya que dificultan la suplantación de su usuario. Es decir, no se debe dejar en cualquier parte ni se debe compartir.
- Configure un firewall a nivel de red: Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Un firewall puede ser un dispositivo software o hardware.

Paso 4: Proteger los servidores

- Certificados de servidor: Identifican a los sitios web. Requiere de la existencia de una autoridad certificadora (CA) que afirme, mediante los correspondientes certificados de servidor, que éstos son quienes dicen ser antes del establecimiento del canal seguro. Le permitirá establecer comunicaciones seguras con sus clientes, cifrando la conexión usando la tecnología SSL para que no pueda ser leída por terceros.
- Mantenga sus servidores en un lugar seguro: Las empresas deben asegurarse de que sus servidores no son vulnerables a las catástrofes físicas. Coloque estos

equipos en una sala segura y con buena ventilación. Haga una relación de los empleados que tienen las llaves de la sala de servidores.

- Práctica de menos privilegios: Asigne distintos niveles de permisos a los usuarios. En vez de conceder a todos los usuarios el acceso “Administrador”, debe utilizar los servidores para administrar los equipos cliente. De este modo se garantiza que los usuarios no pueden efectuar cambios que son fundamentales en el funcionamiento del servidor o equipo cliente.

Paso 5: Mantener los datos a salvo

- Copias de seguridad de los datos importantes para el negocio: La realización de copias de seguridad de los datos significa crear una copia de ellos en otro medio. Por ejemplo, puede grabar todos los archivos importantes en un CD-ROM o en otro disco duro. Es recomendable probar las copias de seguridad con frecuencia mediante la restauración real de los datos en una ubicación de prueba.
- Establezca permisos: Se pueden asignar distintos niveles de permisos a los usuarios según su función y responsabilidades en la organización. En vez de conceder a todos los usuarios el acceso "Administrador" (instituya una política de "práctica de menos privilegios”).
- Cifre los datos confidenciales: Cifrar los datos significa convertirlos en un formato que los oculta. El cifrado se utiliza para garantizar la confidencialidad y la integridad de los datos cuando se almacenan o se transmiten por una red.

Utilice el Sistema de archivos cifrados (EFS) para cifrar carpetas y archivos confidenciales.

- Utilice sistemas de alimentación ininterrumpida (SAI): Para evitar que los equipos informáticos no se interrumpan bruscamente en caso de corte del suministro eléctrico y para filtrar los "micro cortes" y picos de intensidad, que resultan imperceptibles, es recomendable el uso de SAI.

Paso 6: Proteger las aplicaciones y recursos

- Valore la instalación del Directorio Activo: La implementación del directorio activo facilita las tareas tanto de seguridad como de funcionalidad.

Ventajas:

- ✓ La propagación de permisos está centralizada desde el Controlador de Dominio.
- ✓ Posibilidad de escalabilidad según las necesidades particulares de la empresa.
- ✓ La integración con un servicio DNS.
- ✓ Sencillez en la estructuración de ficheros y recursos compartidos.
- ✓ Robustez en la seguridad del sistema.
- ✓ Establecimiento de Políticas.

- Gestione las Aplicaciones a través del Directorio Activo:
  - ✓ Políticas
  - ✓ Permisos Usuario
  - ✓ Impresoras
  - ✓ Correo Electrónico

- Preste atención a la base de datos: Instale los últimos Service Packs de la base de datos. Asegúrese de instalar los Service Packs y las actualizaciones más recientes para mejorar la seguridad. Utilice el modo de autenticación de Windows. Aísle el servidor y realice copias de seguridad periódicas del mismo.

Paso 7: Gestión de actualizaciones

- Actualizaciones oportunas: Las revisiones y las actualizaciones de errores, junto con nuevas versiones de software, se pueden implementar desde el servidor en los equipos y portátiles de los usuarios. Así sabe que se han realizado correctamente de forma oportuna y no tiene que depender de que los usuarios no se olviden.
- Configuraciones especiales: Puede impedir que los usuarios instalen programas no autorizados si limita su capacidad para ejecutar programas desde CD-ROM y otras unidades extraíbles o para descargar programas de Internet.
- Supervisión**:** Si se produce un acceso no autorizado en un equipo o si hay un error del sistema de algún tipo en algún equipo, se puede detectar inmediatamente mediante las capacidades de supervisión que están disponibles en un entorno de equipos/portátiles administrado.[14]

[14] Martin, M. (2008). Guía de Seguridad. Seguridad e Iniciativas de Privacidad, Microsoft. Versión 10.

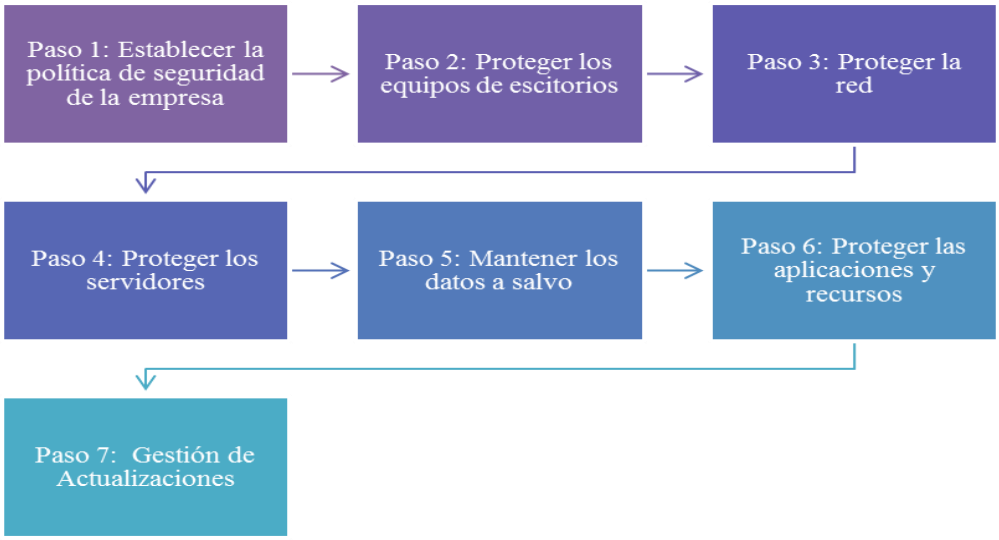

Figura 3.1 Pasos para la implementación de los sistemas de seguridad

CAPÍTULO IV. GESTIÓN DE RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN.

Con el pasar del tiempo, las transacciones comerciales se realizan por medio de redes informáticas. Los acontecimientos que afectan la integridad de la información pueden perturbar la capacidad de la empresa para seguir con sus actividades. Por consiguiente las empresas u organizaciones deben de constar con procesos y procedimientos implantados tanto en asegurar la información como en manifestar su responsabilidad ante las agencias reguladoras y el público.

4.1. Sistema de Gestión de Riesgos de la Información

El riesgo es considerado como cualquier eventualidad que perturbe o imposibilite el cumplimento de los objetivos organizacionales, por consiguiente, surge la administración de riesgos, que vela por garantizar la supervivencia de la empresa y minimizar los costos relacionados con los riesgos.

La gestión de riesgos es el proceso de identificación de las vulnerabilidades de información que utiliza una empresa en sus operaciones. Permite cuantificar las probabilidades de pérdidas en segundo plano que se pudieran generar a partir de un desastre. Tiene como objetivo principal saber cuáles activos de tecnología de la información están propensos a mayores riesgos y cuáles afectarían gravemente la empresa si fuesen afectados.

Por ser la gestión de riesgos un proceso, tiene una serie de pasos que lo conforman. Dichos pasos son:

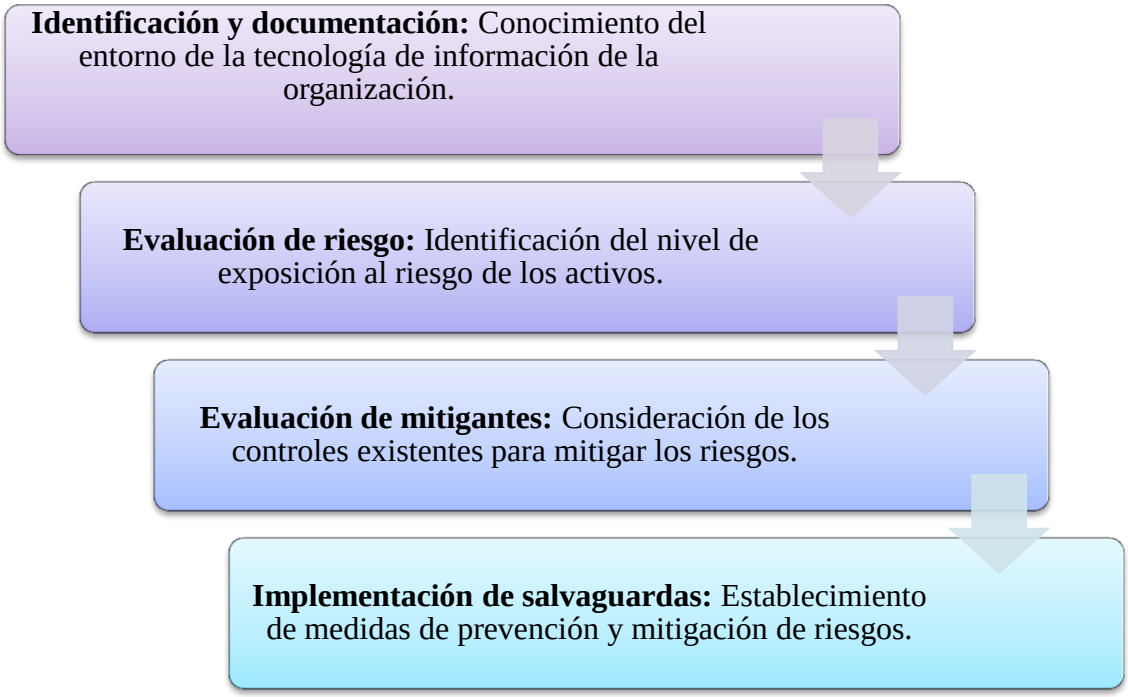

Figura 4.1 Pasos de la gestión de riesgos de la información

En congruencia, un sistema de gestión de riesgos de la información (SGSI) es una herramienta que permite diseñar, implantar y dar mantenimiento al conjunto de políticas y procesos para la administración eficiente de la información. Este conglomerado de políticas están reguladas por la Organización Internacional de Normalización y por la Comisión Electrónica Internacional (*siglas en inglés ISO/IEC*).

Un sistema de gestión de la seguridad de la información debe adaptarse a los cambios internos de la organización y enfrentar los cambios del entorno. Esto se hace mediante un proceso sistemático, documentado y conocido por toda la empresa desde el punto de vista de riesgo empresarial.

4.2. Riesgos

Un riesgo es la probabilidad o vulnerabilidad de que una potencial amenaza o perjuicio se convierta en un desastre. No obstante, a mayor ser la vulnerabilidad mayor es el riesgo, asimismo causando daños o pérdidas financieras a las empresas u organizaciones.

La Organización Internacional por la Normalización (ISO) define riesgo tecnológico (Guías para la gestión de la seguridad de TI /TEC TR 13335-1, 1996) como:

> "*La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generándoles pérdidas o daños.*"

4.2.1. Tipos de Riesgos

a. **Riesgos de integridad:** Este tipo arropa todos los riesgos relacionados con la autoridad, completitud y exactitud de la entrada, procedimiento y reportes de las herramientas o aplicaciones utilizadas en una empresa u organización.

Por consiguiente estos riesgos se manifiestan en los diversos elementos de un sistema, tales como:

- Interface del Usuario
- Procesamiento
- Procesamiento de errores
- Interface
- Administración de cambios
- Información

b. Riesgos de relación: Este riesgo se refiere al uso adecuado de la información creada por una aplicación. También está estrechamente se relaciona a la información de toma de decisiones.

c. Riesgos de acceso: Estos riesgos se orientan al inapropiado acceso a sistema, datos e información. Estos riesgos engloban: los riesgos de segregación inapropiada de trabajo de sistemas de bases de datos y los riegos asociados a la confidencialidad de la información.

d. Riesgos de utilidad: Estos riesgo se centran en tres niveles de riesgos:

1. Los riesgos pueden ser enfrentados por direccionamiento de sistemas antes de los problemas ocurran.

2. Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.

3. Backups y planes de contingencia contralan desastres en el procesamiento de la información.

e. **Riesgos de la infraestructura:** Estos riesgos reseñan a que en las organizaciones no existe una estructura informática tecnológica efectiva, ya sea hardware, software, redes, personas y procesos, para sobrellevar adecuadamente las necesidades futuras y presente de los negocios.

f. **Riesgos de seguridad general:** Los estándares de IEC 950 suministran los requisitos de diseños para lograr una seguridad general, que disminuyen los riesgo de:

- Riesgos de choque de eléctrico: Niveles altos de voltajes.
- Riesgos de incendio: Inflamabilidad de materiales.
- Riesgos de niveles inadecuados de energía eléctrica.
- Riesgos de radiaciones: Ondas de ruido, de láser y ultrasónicas.
- Riegos mecánicos: Inestabilidad de las piezas eléctricas.

4.3. Amenazas

Una amenaza es cualquier situación u ocurrencia que tenga la fuerza suficiente para causarle daños a la infraestructura tecnológica de una empresa o a cualquier sistema. Siendo estas ocurrencias ataques humanos, desastres naturales, fallas internas o externas, entre otras.

Dentro de la seguridad del computador o de un sistema hay que tomar en cuenta una amplia variedad de amenazas. Por lo consiguiente, es importante percatarse del daño que puede llegar a causar y la forma efectiva de contrarrestarlos y mantener dicho computador seguro. Una amenaza se puede materializar de cualquier circunstancia ya sea interna o del ambiente, con el potencial capaz de causar perdida o daños al sistema.

4.3.1. Tipos de Amenazas

Según el tipo de evento o acción en el que se produce un daño (material o inmaterial), las amenazas se pueden dividir en:

1. **Criminalidad:** Esta comprende todas las acciones, causado por la intervención humana, que violan la ley y penada por la misma. Dentro de esta están: los allanamientos, sabotaje, robo/hurto, fraude, espionajes, virus, entre otros.
2. **Sucesos de origen físico:** Estos son todos los hechos naturales y técnicos, en ocasiones eventos indirectamente causados por la intervención humana. Estos comprenden: incendios, inundaciones, sismo, polvo, sobrecarga eléctrica, falta de corriente, entre otros.
3. **Negligencia y decisiones institucionales:** Son todas las decisiones, acciones u omisiones de las personas que poseen poder e influencia sobre el sistema. Dentro de esta están: falta de reglas, falta de capacitaciones, no cifrar datos críticos, mal manejo de contraseñas, entre otros.

4.4. Vulnerabilidades

Si no existe amenaza tampoco existe la vulnerabilidad o quizás esta no fuera de importancia, porque podría causar ningún daño. Por lo tanto, las vulnerabilidades y las amenazas están directamente interrelacionadas. Las vulnerabilidades al ser explotadas por amenazas, afectan la confidencialidad, disponibilidad e integridad de la información de una empresa o individuo. La vulnerabilidad es el punto más débil de seguridad de un sistema que puede explotarse para causar pérdida o daño al sistema.

Según en el VI Informe sobre Seguridad de Internet publicado por la empresa Symantec, se daba a conocer el dato de que durante el primer trimestre de 2004 se habían descubierto cada semana una media de 48 nuevas vulnerabilidades, de las que en un 96% de los casos podrían tener consecuencias moderadas o graves para los sistemas afectados.[15]

4.4.1. Tipos de Vulnerabilidades

1. **Vulnerabilidades físicas:** Son aquellas presentes en los ambientes en los cuales la información se almacena o maneja. Esta afecta directamente a la disponibilidad. Dentro de estas vulnerabilidades se incluye sabotaje, vandalismo, amenazas de bomba, huelgas y atentados terroristas, entre otras.

[15] Enciclopedia de la Seguridad Informática.

2. **Vulnerabilidades naturales:** Estas están ligadas a las condiciones de la naturaleza y su probabilidad de exposición dependerá de su elección y montaje de un ambiente. Dentro de las vulnerabilidades naturales se incluyen terremotos, inundaciones, tormentas, incendios forestales no provocados y huracanes, entre otras.
3. **Vulnerabilidad de hardware:** En este tipo de vulnerabilidad se toma en cuenta los posibles defectos de manufactura o configuración por parte de la empresa, los cuales pudieran permitir ataques de los mismos. Este tipo de vulnerabilidad engloba el robo o pérdida de equipos, fallo de los equipos, desperfectos de fábrica, entre otras.
4. **Vulnerabilidad de software:** Este es el tipo de vulnerabilidad se ha convertido en el objetivo principal de ataques de agentes creadores de amenazas. Estos puntos débiles permiten que personas tengan acceso indebido a los sistemas informáticos y así explotar las amenazas según su fin. Aquí figuran las vulnerabilidades como ataque de virus, malware, troyanos, software no legítimo, entre otras.

4.5. Ataques Informáticos

No solamente los elementos físicos como muebles o utensilios son activos de importancia, la información es considerada por ser uno de los activos más relevantes con los que una empresa puede contar y orientar su misión, visión y valores institucionales.

Cabe destacar el reporte de la agencia norteamericana Agencia de Defensa de Sistemas de Información (*Defense Information Systems Agency*) titulado “Defendiendo la Defensa de la Infraestructura de la Información” del 9 de julio de 1996, en donde se muestra que las corporaciones más grandes de los Estados Unidos reportaron pérdidas estimadas en US$ 800 millones debido a ataques a sus infraestructuras de red.

Dentro de los ataques informáticos se pueden encontrar los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema.

Un ataque de forma general, es cualquier acción que explota una vulnerabilidad.

4.5.1. Tipos de Ataques Informáticos

Los ataques informáticos están basados generalmente en cuatro renglones generales del atacante y del tipo de ataque, dentro de la cuales están:

- Interrupción: En este tipo de ataque la información del sistema se pierde. No está disponible ni utilizable. Un ejemplo de ello sería la destrucción de un disco duro.
- Interceptación: Este ataque está implicado al copiado o al acceso no autorizado a un activo del sistema. Esto puede ser mediante una persona, programa, dispositivo, etc. Un ejemplo de ella puede ser la extracción o copiado de datos.

- Modificación: Este ataque se basa no solamente con el acceso no autorizado, sino, también a la manipulación de la información de los activos del sistema. Un ejemplo de ella sería el cambio de valores de los archivos o modificación de mensajes en una red.
- Generación: En este tipo de ataque se accede al sistema y se crea objetos falsos al sistema sin autorización. Un ejemplo de ello sería la inserción de transacciones un sistema o base de datos.

4.6. Políticas de Gestión de la Seguridad de la Información

Las políticas de seguridad son una "declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran" (RFC´s 1244 y 2196).

Las políticas de gestión de la seguridad de la información establecen el modo como debe actuar el personal entorno a los recursos y servicios informáticos de importancia en la organización y el acceso a la información dentro de la misma. Estas políticas constituyen el conjunto de normas reguladoras y buenas prácticas que determinan la manera en que todos los activos son distribuidos, gestionados y protegidos dentro de la empresa. Es importante tener toda la colaboración y disposición de todos los integrantes de la empresa con el fin de lograr los mejores resultados con respecto al uso de la información.

Para llevar a cabo la implementación de un sistema de gestión de seguridad de la información se debe contemplar los siguientes aspectos:

1. Formalizar la gestión de la seguridad de la información.
2. Analizar y gestionar los riesgos
3. Establecer procesos de gestión de la seguridad siguiendo la metodología PDCA:
    - "*Plan*": selección y definición de medidas y procedimientos.
    - "*Do*": Implementación de medidas y procedimientos de mejora:
    - "*Check*": Comprobación y verificación de las medidas implantadas.
    - "*Act*": Actuación para corregir las deficiencias detectadas en el sistema.[16]
4. Certificación de la gestión de la seguridad.

4.7. Estándares para la Gestión de la Seguridad de la Información

La necesidad de desarrollar la actividades de una organización o empresa se puede ver afectada por diferentes riesgos y amenazas, por lo que es necesario implantar un sistema de gestión de seguridad de la información que permita estar preparado contra cualquier imprevisto y proceder con rapidez y eficacia. Con este sistema se podrá analizar los riesgos e implantar las medidas de seguridad necesarias y controles para evaluar la eficacia de las mismas.

[16] Enciclopedia de la Seguridad Informática.

Para la facilidad de realizar dicho proceso está la familia de estándares y normas internacionales ISO/IEC 27000. Estas normas han sido confeccionadas por la Organización Internacional de Normalización (*siglas en inglés ISO*) y por la Comisión Electrotécnica Internacional (*siglas en inglés IEC*). ISO e IEC están constituidos por los principales organismos de normalización de cada país. Estos se encargan de elaborar las normas internacionales que el mercado requiere y demanda.

Una norma es un documento que proporciona los requisitos, especificaciones, directrices o características que pueden ser utilizadas consistentemente para asegurar que los materiales, productos, procesos y servicios son adecuados para su propósito.[17]

Dentro de los estándares más populares están:

- ✓ ISO 9000 – Gestión de calidad
- ✓ ISO 22000 – Gestión de la seguridad alimentaria
- ✓ ISO 31000 – Gestión del riesgo
- ✓ ISO 20121 – Eventos sostenibles
- ✓ ISO 14000 – Gestión ambiental
- ✓ ISO 26000 – Responsabilidad Social
- ✓ ISO 4217 – Códigos de las monedas
- ✓ ISO 27001 – Seguridad de la información
- ✓ ISO 3166 – Códigos de país
- ✓ ISO 50001 – Gestión de la energía

[17] Organización Internacional de Normalización. http://www.iso.org/iso/home/standards.htm

4.7.1. Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC 27001)

La norma ISO/IEC 27001:2005 cubre todo tipo de organizaciones (empresas comerciales por ejemplo, agencias gubernamentales, organizaciones sin fines de lucro). ISO/IEC 27001:2005 especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información documentado en el contexto de los riesgos globales de negocio de la organización. Especifica los requisitos para la aplicación de los controles de seguridad a medida de las necesidades de las organizaciones individuales o partes de los mismos.

ISO/IEC 27001:2005 está diseñado para garantizar la selección de controles adecuados y proporcionados de seguridad que protegen los activos de información y dar confianza a las partes interesadas.

ISO/IEC 27001:2005 pretende ser adecuado para diferentes tipos de uso, incluyendo los siguientes:

- Utilizar dentro de las organizaciones para formular los requisitos y objetivos de seguridad;
- Utilizar dentro de las organizaciones como una forma de garantizar que los riesgos de seguridad son rentables gestionados eficazmente;

- Utilizar dentro de las organizaciones para asegurar el cumplimiento con las leyes y reglamentos;
- Utilizar dentro de una organización como un marco de proceso de la aplicación y gestión de los controles para garantizar que se cumplan los objetivos específicos de seguridad de una organización;
- Definición de nuevos procesos de gestión de seguridad de la información;
- Identificación y clarificación de los procesos de gestión de seguridad de las informaciones existente;
- Utilizar la gestión de las organizaciones para determinar el estado de las actividades de gestión de seguridad de la información;
- Usar por los auditores internos y externos de las organizaciones para determinar el grado de cumplimiento de las políticas, directrices y normas adoptadas por la organización;
- Utilizar las organizaciones para proporcionar información relevante acerca de las políticas de seguridad de la información, directivas, normas y procedimientos a los socios comerciales y otras organizaciones con las que interactúan por razones operativas o comerciales;
- Implementación de seguridad de la información empresarial propicio;
- Utilizar las organizaciones para proporcionar información relevante sobre seguridad de la información a los clientes.[18]

[18] Organización Internacional de Normalización. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103

4.7.2. Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/IEC 27002)

La Organización Internacional de Normalización con junto con la Comisión Electrotécnica Internacional hacen referencia en la norma ISO/IEC 27002:2013, la cual proporciona directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluida la selección, implementación y gestión de los controles, teniendo en cuenta el medio ambiente de riesgos de seguridad de información de la organización (s).

Está diseñado para ser utilizado por las organizaciones que pretenden:

1. Seleccionar los controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001;
2. Implementar controles de seguridad de la información generalmente aceptadas;
3. Desarrollar sus propias directrices de gestión de seguridad de información.[19]

[19] Organización Internacional de Normalización. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42103

4.7.3. Control de Objetivos para la Información y Tecnologías Relacionadas (COBIT 5)

El Control de Objetivos para la Información y Tecnologías Relacionadas (*siglas en Inglés COBIT 5*) es tipo de marco de gestión y de negocio global para el gobierno y la gestión de las TI de la empresa. En si este ayuda a crear un valor optimo que las empresas u organizaciones necesitan a partir de la TI, y al mantener un balance entre la relación de beneficios y la optimización de los niveles de riesgos y la utilización de los recursos.

Dentro de los principios de COBIT 5 están:

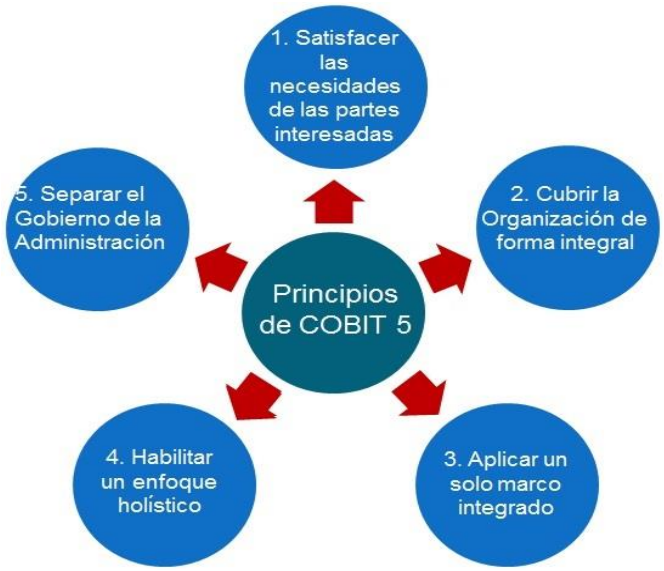

Figura 4.2 Principios de COBIT 5. **Fuente:** COBIT® 5, 2012, ISACA®

Los habilitadores de COBIT 5 son:

Figura 4.3 Habilidades de COBIT 5. **Fuente:** COBIT® 5, 2012®

4.7.4. Comisión del Comité de Organizaciones Patrocinadoras (COSO)

La Comisión del Comité de Organizaciones Patrocinadoras tiene como objetivo primordial de suministrar el liderazgo de pensamiento a través de la confección de marcos y directrices sobre la gestión del riesgo empresarial, el control interno y la disuasión del fraude.

Dicho comité está sustentado por cincos asociaciones profesionales con sede en los Estados Unidos, dentro de las cuales están: el Instituto Americano de Contadores Públicos Certificados (*siglas en inglés AICPA*),el Instituto de Auditores Internos (*siglas*

en inglés IIA), la Asociación Americana de Contabilidad (*siglas en inglés AAA*), Ejecutivos Internacionales Financieros (*siglas en inglés FEI*) y la Asociación Nacional de Contadores (ahora el Instituto de Contadores Administrativos [*siglas en inglés IMA*]).

4.8. Respaldo de la Información

Para referirse al respaldo de la información, está generalmente aceptado el término "backup". Un backup o respaldo de la información es la copia de los datos importantes de un dispositivo u ordenador primario en uno o varios secundarios, para que en caso de que el dispositivo primario sufra una falla o error en su estructura interna o electromecánica, sea posible tener a disposición la mayoría de la información necesaria para seguir operando.

Es de suma importancia tener los datos a salvo, por lo que muchas veces no se toman la medidas o precauciones necesarias para salvaguardar dicha información. En pocas palabras el respaldo de información no es más que el duplicado de los datos más relevantes de un dispositivo, ya sea de forma manual o automática.

Para los servicios de respaldo de información se utilizan los siguientes dispositivos:

1. Cintas de almacenamiento
2. Servidores web o Discos espejo de servidores
3. Discos duros

4.8.1. Tipos de Respaldo de Información

Los respaldos de información o backup pueden ser:

1. **Respaldo o backup completo:** Este tipo de backup consiste en hacer una copia total de los datos en cintas, discos, CD o DVD. La principal ventaja de realizar este tipo de backup radica en que se dispone de la totalidad de los datos en el mismo juego de soportes. De esta manera, se puede restaurar los datos en un mínimo tiempo. No obstante, este tipo de backup requiere de más tiempo y espacio de almacenamiento que los demás backup.
2. **Respaldo o backup incremental:** En este tipo de backup, solo se copian los datos que han sido modificados en la última operación realizada. Para esto se utilizan la fecha y hora en la que se modificó el archivo, la cual esta encriptado en el mismo, y se compara con la fecha y hora del último backup. La principal ventaja de este tipo de backup es que copia una menor cantidad de datos que la que se copia en un backup completo. Por esta razón, esta operación se realiza con mayor rapidez y requieren menor espacio para almacenar el respaldo.
3. **Respaldo o backup diferencial:** Este tipo de backup es parecido al respaldo incremental la primera vez que se realiza, porque se copiaran todos los datos que hayan cambiado desde el último respaldo. No obstante, cada vez que esto se ejecute, volverá a copiar todos los datos que se hayan cambiado desde el anterior completo. Por ende, este tipo de respaldo almacenará una cantidad mayor de datos

que en respaldo incremental, pero menos que el respaldo completo, en las subsiguientes operaciones.

A partir de estos tres tipos de backup principales, se puede definir una estrategia propia para la protección de datos. Normalmente se utiliza uno de los enfoques siguientes:

- ✓ Backup completo diario
- ✓ Backup completo semanal más diferencial diario
- ✓ Backup completo semanal más incremental diario

El respaldo de datos es sin duda el mantenimiento preventivo. El hardware puede ser reemplazado, pero a menudo los datos no pueden ser, por lo menos no con mucha facilidad. Hacer una copia de seguridad de los archivos es una medida de seguridad que asegura que los datos pueden sobrevivir al dispositivo en que se almacena. Una regla de oro de la informática es realizar una copia de seguridad de archivos con regularidad, y luego copia de seguridad de las copias de seguridad.

4.8.2. Almacenamiento en la Nube (*Cloud Storage*)

El almacenamiento en la nube está reemplazando a gran escala los métodos tradicionales para almacenar información. Es un modelo de servicio muy utilizado en la actualidad. En este tipo de servicio los datos del sistema de cualquier institución se almacenan,

gestionan, administran y se respaldan de forma remota, en servidores que están situados en la nube. Los servidores que son utilizados son administrados por un proveedor de servicios de almacenamiento en la nube y los datos se ponen a disposición de los usuarios a través de una red, donde solo requiere conexión a internet.

Existen básicamente tres tipos de servicios de almacenamiento en la nube:

1. **Almacenamiento en la nube público**: En este servicio la nube requiere poco control administrativo y se puede acceder a los datos en línea, siempre y cuando se tenga la autorización. Este tipo de almacenamiento en la nube es alojado externamente, y se puede acceder mediante internet. Usualmente una persona individual puede tener acceso a este servicio por su bajo costo y el bajo requerimiento de mantenimiento.

Entre los servicios que se pueden encontrar como almacenamiento en la nube pública están:

- **Dropbox:** Es uno de los servicios más populares para compartir archivos en la nube.
- **Google Drive**: Es el servicio de almacenamiento en la nube de Google.

2. **Almacenamiento en la nube privado**: Este servicio de almacenamiento en la nube está orientado más a cubrir las necesidades de una empresa. Puede ser presentado en dos formatos: en la misma oficina o casa y alojado externamente.

La empresa que utiliza este tipo de servicio tiene el control administrativo, y por lo tanto le es posible diseñar y operar el sistema de acuerdo a sus necesidades específicas.

3. **Almacenamiento en la nube híbrido**: Este servicio de almacenamiento en la nube ofrece una combinación del almacenamiento en nubes públicas y privadas. Se puede configurar de forma tal que los datos más importantes se almacenen en un sistema de almacenamiento en la nube privada, mientras que los datos menos importantes se pueden almacenar en una nube pública con acceso disponible por una gran cantidad de personas a distancia.

4.8.2.1. Network Access Point (NAP) del Caribe

Es el centro tecnológico de acceso de redes (Network Access Point-NAP) más avanzado del país y de la región del Caribe dotado de los más avanzados estándares de seguridad, confiabilidad y redundancia. Diseñado y operado para ofrecer soluciones de centro de datos, recuperación de desastres y continuidad de negocios utilizando la más avanzada infraestructura de telecomunicaciones en el Caribe.[20]

[20] NAP del Caribe. http://napdelcaribe.net.do/quienes-somos/

El NAP del Caribe es operado por Terremark una compañía Verizon, considerada a nivel global como una de las empresas de mayor experiencia en la operación de NAP's. Terremark es un líder mundial en la provisión de servicios de infraestructura de tecnologías de la información y comunicación a través de una de las plataformas más robustas, modernas y avanzadas de la industria. Con la presencia de sus centros de datos en los Estados Unidos, Europa y América Latina, así como el acceso a una red global de masiva y diversa conectividad Terremark ofrece a clientes de gobierno y empresas del sector privado una serie de completas y sofisticadas soluciones que incluyen, alojamiento de equipos, energía, servicios de conectividad, servicios de Cloud, servicios de seguridad entre otros.

4.8.2.1.1. Servicios de NAP del Caribe para la empresa CAM INC

Para el proceso de almacenamiento y respaldo de los datos en la nube se pretende utilizar los servicios que presta NAP del Caribe en su módulo de servicios gestionados: Cloud Computing. En este servicio NAP del Caribe combina la potencia y flexibilidad de la infraestructura tecnológica, ofreciendo una con experiencia de seguridad y disponibilidad. Tiene una interfaz unificada sobre una arquitectura de computación basada en el almacenamiento en la nube, virtualización y recursos informáticos dedicados. En la actualidad cualquier cliente que quiera alojarse bajo las facilidades de la

del NAP del Caribe puede acceder a facilidades de ancho de banda internacional a través de las empresas prestadoras de telecomunicaciones Tricom, Claro/Codetel, Wind Telecom y Orange las cuales están en capacidad de ofrecer a clientes o a otras empresas de telecomunicaciones parte de la capacidad de ancho de banda que ellas poseen disponibles en los sistemas de cable submarinos que llegan al país Arcos 1 y Antillas 1.[21]

[21] NAP del Caribe. http://napdelcaribe.net.do/conectividad/

CAPÍTULO V. PLAN DE RECUPERACIÓN ANTE DESASTRES.

Para las empresas es de suma importancia garantizarles a sus usuarios el más alto nivel de seguridad, confiabilidad y disponibilidad de sus productos y servicios, pero, en múltiples ocasiones esta disponibilidad se ve afectada por causas accidentales o provocadas. Por tal razón, las empresas se ven en la obligación de diseñar e implementar mecanismos que contrarresten los riesgos a los que se ven expuestas si quieren tener continuidad operacional después de cualquier desastre.

5.1. Concepto de Plan de Recuperación ante Desastres (*Disaster Recovery Planning, DRP*)

Un plan de recuperación ante desastres es la descripción de cómo una empresa enfrenta las posibles contingencias que puedan surgir durante su vida operacional. Está compuesto por las precauciones tomadas para que los efectos de un incidente se reduzcan al mínimo y la organización sea capaz de mantener o reanudar rápidamente sus funciones. Es un proceso documentado que también busca la protección de la infraestructura tecnológica. Por lo general, implica un análisis de los procesos de negocio y las necesidades de continuidad.

Plan de recuperación ante desastres se refiere a la inmediata y temporal restauración de los sistemas computacionales críticos y las operaciones con redes después de un desastre natural o alguna interrupción humana. Una organización documenta como va a responder ante un desastre y restaurar las funciones criticas de negocio dentro de un periodo de tiempo determinado; minimiza la perdida y repara los daños de la localidad para restituir el procesamiento de datos.[22]

5.2. Cuándo aplicar un Plan de Recuperación ante Desastres

Existen muchas razones por el cual se debe de realizar un plan de recuperación ante desastre, entre estas razones están:

- Si llega a colapsar el centro de cómputos de la empresa.
- Por la falta de algún servicio básico.
- Si se llega a presentar fallas generalizadas.
- Si llega a faltar uno de sus proveedores informáticos importantes.
- Si llega a faltar uno de los sistemas de telecomunicaciones o enlaces.
- Si llegara a fallar alguno de los sistemas críticos de la empresa.
- Si se presenta algún incidente medioambiental que afecta las operaciones.

[22] Hansche, S. Berti, J. Hare, C. (2003). Official, (ISC) Guide to the CISSP. Florida.

5.3. Ventajas de un Plan de Recuperación ante Desastres

Dentro de las ventajas de plan de recuperación ante desastres están:

- Previene o reduce las pérdidas que puede tener un negocio en caso que ocurra un desastre.
- Describe los activos para garantizar su protección en caso de un desastre.
- Describe los tiempos críticos de recuperación para volver a la situación anterior al desastre, para de esta forma, el negocio pueda seguir su marcha sin que este se comprometa.
- Da a conocer los diferentes eventos que podrían ocurrir e impactar sobre la continuidad de las operaciones del negocio y su impacto financiero.

5.4. Ciclo de un Plan de Recuperación ante Desastres

El ciclo de vida de un plan de recuperación ante desastres es un conjunto de etapas interrelacionadas de forma cíclica que buscan asegurar la restauración o recuperación de los procesos tecnológicos que apoyan las actividades de una empresa, frente a cual evento no programado.

Las organizaciones se enfrentan a constantes cambios en sus procesos de negocios y de tecnología, buscando ventajas competitivas en respuesta a la competencia. Algunos de estos cambios pueden ser:

- ✓ Cambios de roles o de personal
- ✓ Cambios de activos
- ✓ Cambios en los procesos
- ✓ Cambios operacionales
- ✓ Cambios en el mercado

Un plan de recuperación ante desastres está compuesto por seis fases, las cuales se detallan a continuación:

- **Fase 1. Gestión del Riesgo:** En esta fase se contemplan las actividades de la gestión del riesgo, evalúan las amenazas de un desastre, se detallan las vulnerabilidades existentes, se enumeran los potenciales impactos de un desastre e identifican e implementan los controles necesarios para prevenir o reducir los riesgos de un desastre.
- **Fase 2. Análisis de Impacto al Negocio:** Esta fase reside en identificar los procesos relacionados con apoyar la misión de la empresa y también de analizar los impactos a la gestión comercial del negocio, en caso de que fuesen interrumpidos por un desastre.
- **Fase 3. Desarrollo de Estrategia:** Esta fase se enfoca en evaluar los requerimientos e identificar las opciones para la recuperación de procesos críticos y los recursos necesarios, en el caso que fuesen interrumpidos por un desastre.

- **Fase 4. Desarrollo del Plan:** En esta fase desarrolla un plan para conservar la continuidad del desempeño del negocio, fundamentado en las fases previas, específicamente en la "gestión del riesgo" y en el "análisis de impacto al negocio", así como en los aspectos trazados en el desarrollo de la estrategia DRP.
- **Fase 5. Ensayo del Plan:** En esta fase se efectúa el ensayo del plan, con intenciones a poder determinar su grado de precisión y actualización.
- **Fase 6. Mantenimiento del Plan:** En esta fase se mantiene el plan en un estado de preparación constante para dado un desastre poder ejecutarlo, así minimizar las posibilidades de errores.

Figura 5.1 Ciclo de un plan de Recuperación ante Desastres

CAPÍTULO VI. IMPLEMENTACIÓN DE *SYMANTEC DATA LOSS PREVENTION* Y PLAN DE RECUPERACIÓN ANTE DESASTRES EN LA EMPRESA CAM INC.

Las organizaciones están interesadas en Data Loss Prevention para proteger sus datos más importantes. Según un estudio de Symantec y Ponemon Institute, las actitudes diarias de los empleados y sus opiniones respecto del robo de propiedad intelectual están en conflicto con la gran mayoría de las políticas empresariales[23], por ende, se debe brindar mayor visibilidad de los procesos empresariales como prueba de que se está cumpliendo con las reglamentaciones.

6.1 Symantec Data Loss Prevention en CAM INC

Debido a la importancia que tienen los datos para la vida operacional de cualquier organización, y a causa de los constantes actos de robo y pérdida de información, es necesario implementar herramientas que controlen dicha problemática.

Las siguientes imágenes muestran el proceso de instalación, configuración y prueba de Symantec Data Loss Prevention para el control de acceso y la fuga de datos en CAM INC. Para las pruebas se utilizaron servidores con el sistema operativo Windows Server 2008 y las bases de datos tanto de la empresa como de los clientes son del tipo relacional.

[23] Symantec Corporation. http://www.symantec.com/es/mx/products-solutions/families/advantages.jsp?fid=data-loss-prevention

Acceso a la herramienta: En esta imagen, tras haber instalado correctamente Symantec Data Loss Prevention se debe acceder a la herramienta a través del usuario y la contraseña creada previamente.

Figura 6.1 Acceso a Data Loss Prevention

Luego de acceder como administrador, la herramienta permite visualizar el sumario de las políticas de acceso a los datos, el historial, estado y tipos de incidentes registrados y los atacantes más potenciales en la empresa.

Figura 6.2 Sumario de acceso a los datos en CAM INC

Se visualizan todos los reportes de incidentes de los últimos 30 días, tanto en la red como Endpoint dentro de la empresa para tomar las medidas necesarias. Uno de los incidentes más reportados es la navegación a través de las redes sociales. También permite filtrar los incidentes, detectar quienes representan mayores riesgos de acuerdo al análisis, agrupar las políticas por objetivos y manejar el sumario de objetivos e incidentes.

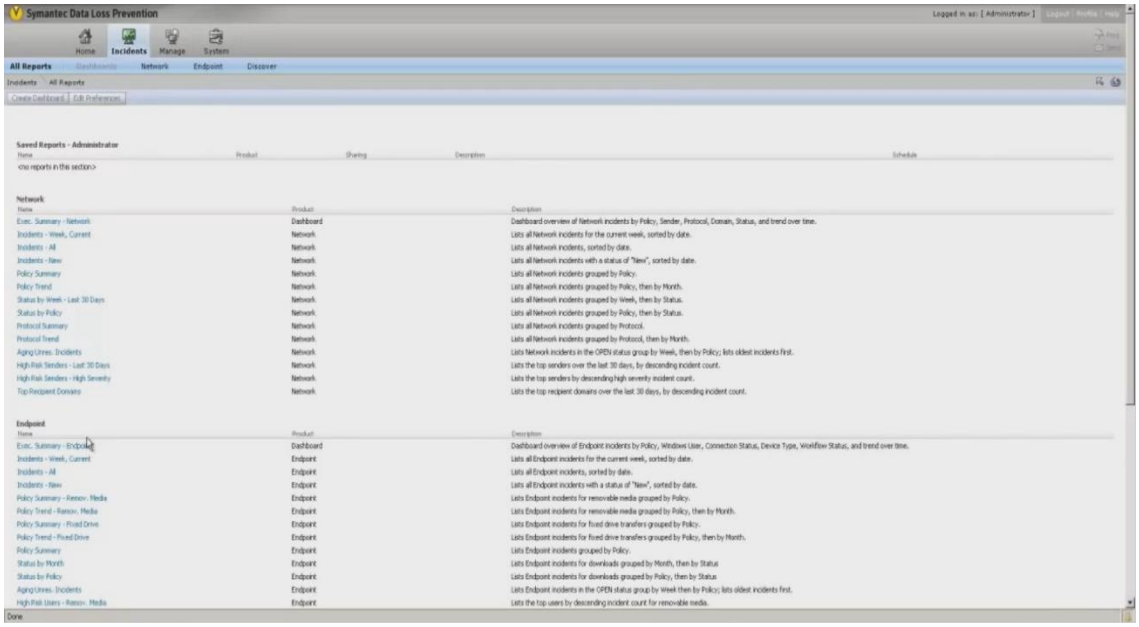

Figura 6.3 Sumario de incidentes en CAM INC

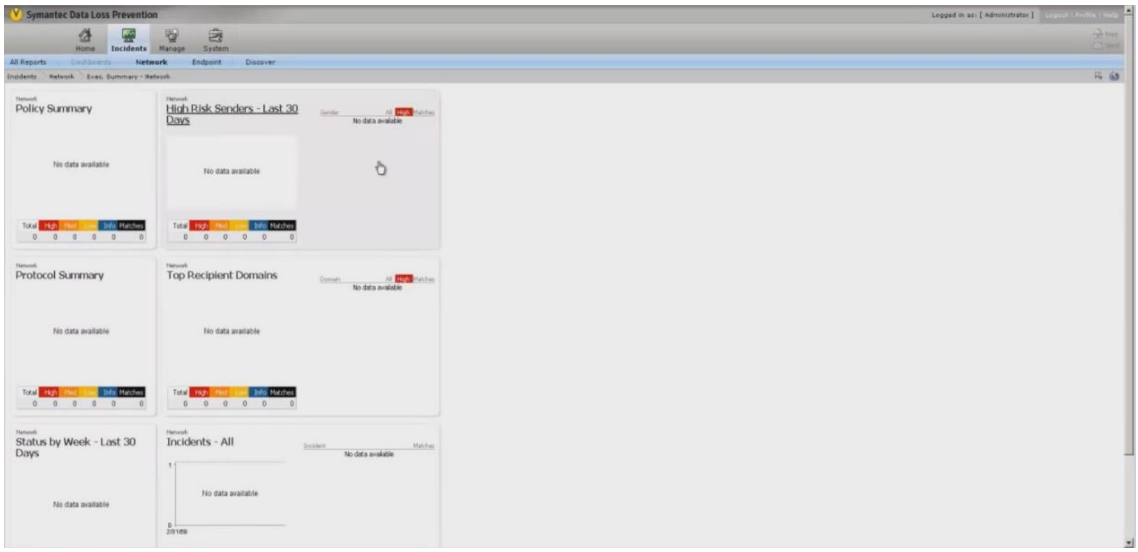

Figura 6.4 Consola de manejo de objetivos e incidentes en CAM INC

En congruencia con el objetivo de Data Loss Prevention, también se instaló el módulo Endpoint Protection Manager que permite identificar eventos críticos casi en tiempo real para crear la solución más rápida y efectiva disponible.

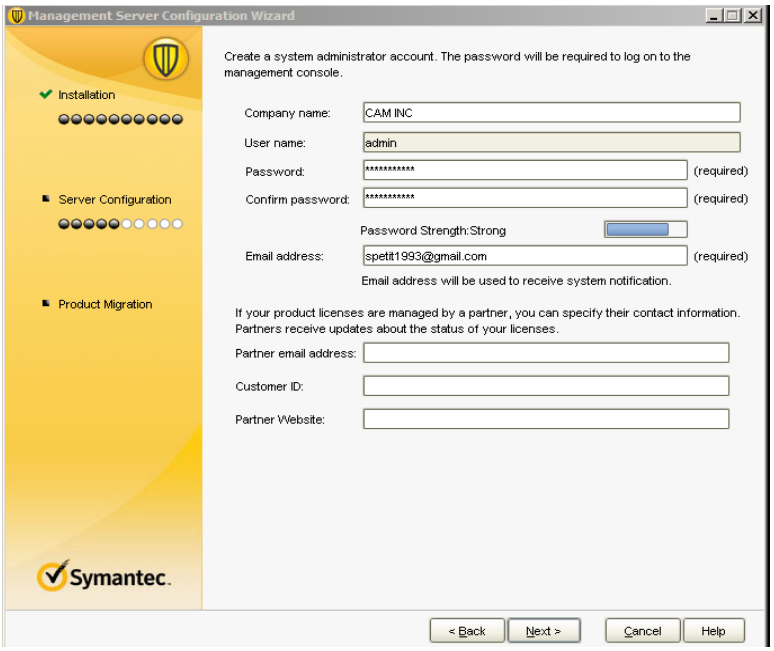

Figura 6.5 Creación de usuario para manejo de Endpoint Protection

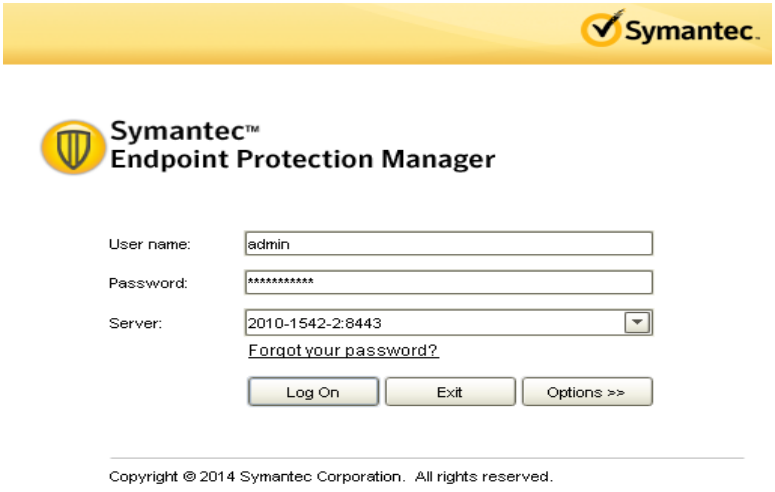

Figura 6.6 Acceso a la consola de Endpoint Protection

La consola de Endpoint Protection Manager presenta un resumen del estado de la seguridad, del servidor y los clientes, los monitores de datos, el listado de reportes y las políticas. Permite a la empresa hacer diferentes grupos de acuerdo a los usuarios y así tener diferentes políticas o configuraciones, tanto de actualización, firewall, bloqueo de páginas web, etc. Muestra el resumen de las acciones de acuerdo a las detecciones, los riesgos por hora, el resumen del estado de la seguridad de acuerdo a cada equipo en la red y el sumario de las aplicaciones de la empresa que están en observación.

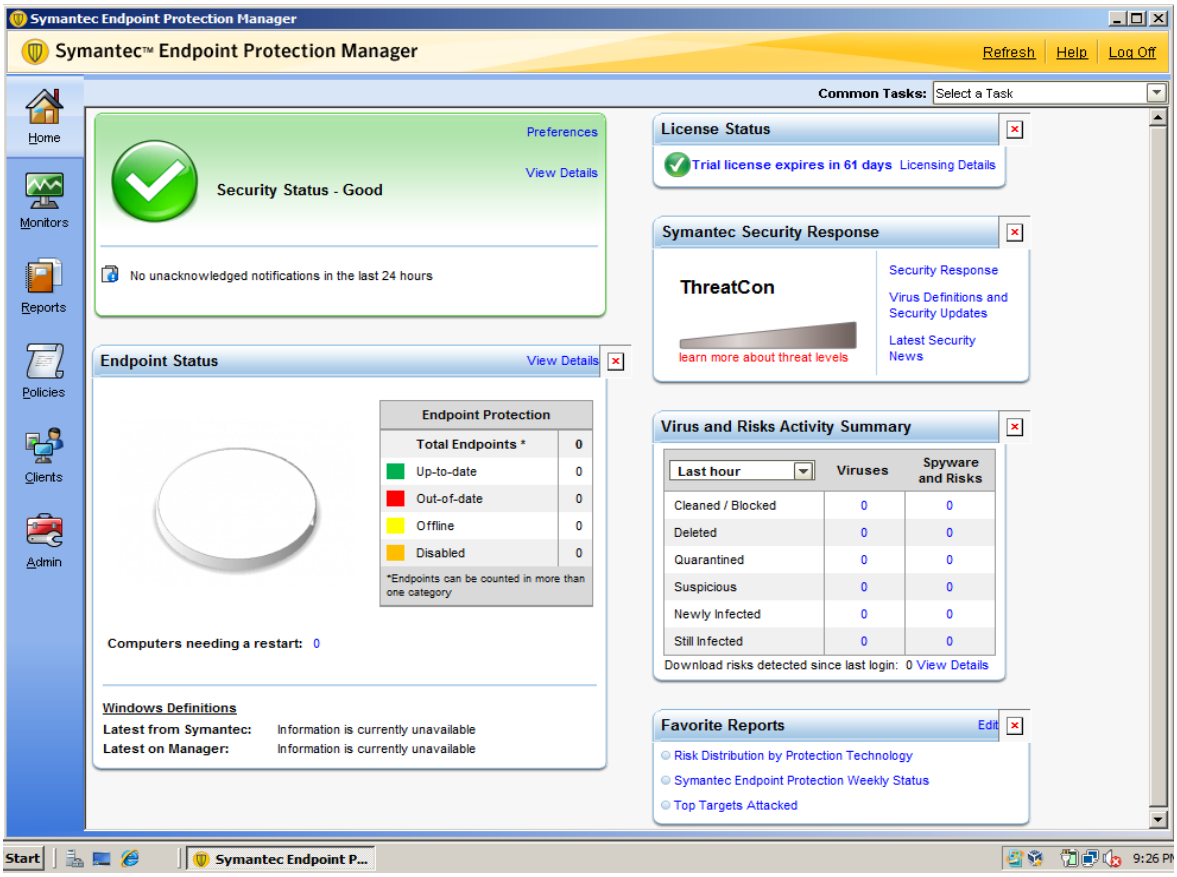

Figura 6.7 Ejecución de Endpoint Protection Manager en CAM INC

Finalmente, la pestaña administrador de la consola de Symantec Endpoint Protection Manager muestra al usuario debidamente autenticado, las informaciones generales del sistema.

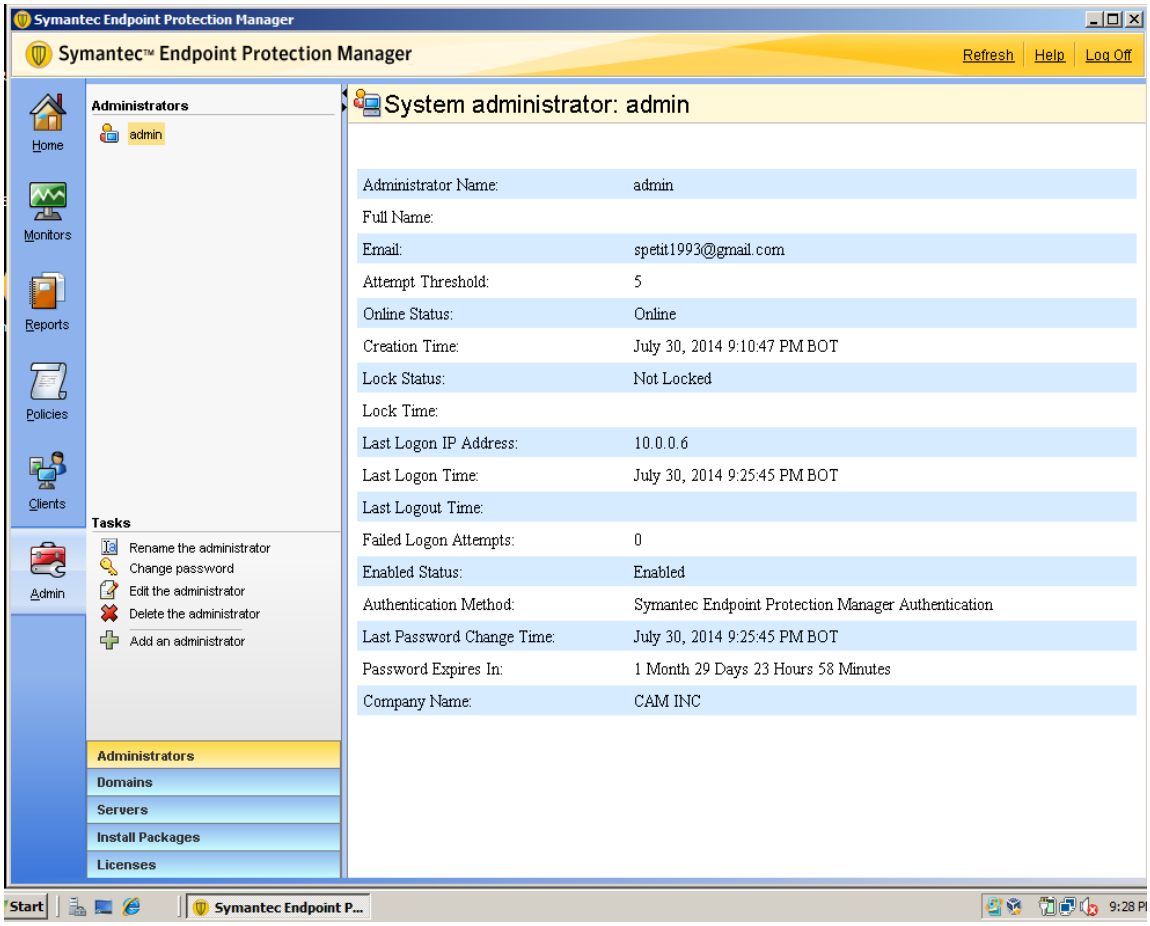

Figura 6.8 Administrador de sistema de Endpoint Protection Manager para CAM INC

La implementación de Symantec Data Loss Prevention o de cualquier otra herramienta eficaz para controlar la fuga de datos le supondrá a la empresa CAM INC beneficios en términos de control de acceso a los datos, protección de la información crítica de sus clientes y buen manejo de políticas de seguridad. Todo lo anterior se refleja en lo siguiente:

- ✓ Disminución en un 75% de los reportes de sus clientes notificando la divulgación no autorizada de su información personal.
- ✓ Aumento de la seguridad de la información a un 98% dentro de la empresa.
- ✓ Mejora en un 25% adicional en la calidad de sus servicios.
- ✓ Disminución de costos monetarios a causa de la pérdida de información.
- ✓ Prevención de daños a la marca, y pérdida de los accionistas.
- ✓ Reducción de costos por monitoreo de créditos y por bienes y servicios para retener clientes en un 80%, lo que representa un ahorro de $25,000 dólares al año.
- ✓ Prevención de la suspensión de sus operaciones por investigaciones de seguridad.
- ✓ Prevención de costos por multas y por notificación a los afectados de robo de información.

6.2. Desarrollo del Plan de Recuperación ante Desastres dentro de CAM INC

El principal objetivo de un plan de recuperación ante desastres es mantener las operaciones y reducir al mínimo el impacto de un incidente de seguridad dentro de cualquier organización. Este plan puede prevenir que los procesos de la empresa se interrumpan y en caso de que lleguen a ser interrumpidos, que la inactividad sea la menor posible. Además, permite mantener el nivel de servicios operando de forma aceptable, estableciendo un periodo de recuperación que garantice la continuidad de las actividades hasta volver a la normalidad.

6.2.1. Objetivos del Plan de Recuperación ante Desastres en CAM INC

Los objetivos que debe cumplir el plan de recuperación ante desastres son los siguientes:

- ✓ Identificar los factores de riesgo a los que se expone la empresa.
- ✓ Identificar las amenazas a las que se enfrenta la organización.
- ✓ Definir los procedimientos de actuación ante incidentes para garantizar una rápida y oportuna respuesta frente al desastre.
- ✓ Establecer la estrategia de vuelta a la normalidad tras cualquier incidente.

6.2.2. Organización de Equipos

En esta etapa se procede con la organización de los equipos formados por el personal de Smart Solutions, empresa de outsourcing que dirige el área de tecnología de la empresa conjuntamente con los empleados de CAM INC, quienes en labor conjunta se encargaran de la activación y desarrollo del plan de recuperación ante desastres.

6.2.2.1. Equipo de Respuesta a Emergencias:

Equipo de Respuesta a Emergencias		
Miembros del equipo	Nombre:	Junior Raccini
	Posición:	Gerente General
	Teléfono móvil:	809-432-3333
	Teléfono residencial:	809-414-3014
	Nombre:	Julio Amador
	Posición:	Líder de Operaciones
	Teléfono móvil:	809-432-3334
	Teléfono residencial:	809-231-5463
	Nombre:	Luis Renato Jerez
	Posición:	IT Manager
	Teléfono móvil:	809-432-3335
	Teléfono residencial:	809-599-4536
	Nombre:	Sophie Méndez
	Posición:	Gerente Recursos Humanos
	Teléfono móvil:	809-432-3336
	Teléfono residencial:	809-231-6732

Tabla 6.1 Equipo de respuesta a emergencias

6.2.2.2. Equipo de Recuperación

Es el equipo autorizado a ejecutar todo lo relacionado con el proceso de recuperación para reponer los servicios en las facilidades del NAP del Caribe.

Equipo de Recuperación		
Miembros del equipo	Nombre:	Edward Tsema
	Posición:	Encargado de TI
	Teléfono móvil:	809-432-3337
	Teléfono residencial:	809-599-6578
	Responsabilidad:	Coordinador de Personal Técnico
	Nombre:	Boris Luxama
	Posición:	Analista de TI
	Teléfono móvil:	809-432-3338
	Teléfono residencial:	809-231-5400
	Responsabilidad:	Encargado de Aplicaciones
	Nombre:	Mariano Meléndez
	Posición:	Técnico de TI
	Teléfono móvil:	809-432-3339
	Teléfono residencial:	809-599-7621
	Responsabilidad:	Encargado de Sistemas Operativos
	Nombre:	Luisa Santana
	Posición:	Técnico de TI
	Teléfono móvil:	809-432-3340
	Teléfono residencial:	809-231-5401
	Responsabilidad:	Encargada de Seguridad Lógica

Tabla 6.2 Equipo de recuperación

6.2.2.3. Equipo de Coordinación Logística

Este equipo deberá atender las necesidades relacionadas con transporte del personal, transporte de los materiales, suministro de alimentos al personal afectado, contacto con los proveedores de CAM INC para solicitar los materiales necesarios que soliciten los encargados de recuperación, y todo lo relacionado con la logística.

Equipo de Coordinación Logística		
Miembros del equipo	Nombre:	Miguel Valenzuela
	Posición:	Encargado de Contabilidad
	Teléfono móvil:	809-432-3341
	Teléfono residencial:	809-599-5768
	Nombre:	Michelle Matos
	Posición:	Encargada de Créditos y Cobros
	Teléfono móvil:	809-432-3342
	Teléfono residencial:	809-596-5400
	Nombre:	Susana Paredes
	Posición:	Encargada de Tesorería
	Teléfono móvil:	809-432-3343
	Teléfono residencial:	809-682-7621

Tabla 6.3 Equipo de coordinación logística

6.2.2.4. Equipo de Relaciones Públicas

Este equipo se encarga de comunicar al resto de la empresa la activación del plan de recuperación ante desastres por los medios pertinentes.

Equipo de Relaciones Públicas		
Miembros del equipo	Nombre:	Patricia Montero
	Posición:	Coordinadora de Recursos Humanos
	Teléfono móvil:	809-432-3344
	Teléfono residencial:	809-599-7852
	Nombre:	Michael Rosario
	Posición:	Asistente de Recursos Humanos
	Teléfono móvil:	809-432-3345
	Teléfono residencial:	809-687-5400

Tabla 6.4 Equipo de relaciones públicas

6.2.2.5. Equipo de Unidades de Negocios

Este equipo se encarga de probar los procesos críticos y reporte de anomalías en caso de que se presenten.

Equipo de Unidades de Negocios		
Miembros del equipo	Nombre:	Joel Pérez
	Posición:	Líder de Planificación
	Teléfono móvil:	809-432-3346
	Teléfono residencial:	809-599-3013
	Nombre:	Juan Cabrera
	Posición:	Líder de Operaciones
	Teléfono móvil:	809-432-3347
	Teléfono residencial:	809-232-9853

Tabla 6.5 Equipo de unidades de negocios

6.2.3. Evaluación de Riesgos y Análisis de Impacto

La fase de evaluación de riesgos y análisis de impacto es una de las etapas más importantes del proceso de elaboración del plan de recuperación ante desastres. Permite identificar la naturaleza y probabilidad de las amenazas que predominan en la organización, al mismo tiempo que, estima las pérdidas más fuertes en bienes y servicios, es decir, de ella depende la correcta toma de decisiones con respecto al tratamiento de los riesgos de la empresa.

El objetivo principal de la evaluación de riesgos y análisis de impacto es la evaluación de lo que ya existe, evitar la duplicación de esfuerzos y aprovechar la información y las capacidades existentes.

6.2.3.1. Gestión y Evaluación de Riesgos

El objetivo de la evaluación de riesgos es identificar y analizar los factores de riesgo que puedan afectar la empresa. Es recomendable que todos los empleados conozcan el impacto que podrían tener estos riesgos, a sabiendas de que ninguna organización está exenta de riesgos, pero sí puede contar con las medidas de seguridad adecuadas que respondan ante los incidentes.

La evaluación de riesgos conlleva a un análisis de los riesgos sobre los activos y también de sus amenazas; estas últimas explotan las vulnerabilidades de la empresa pero pueden ser reducidas con las contramedidas, las cuales al final reducen los riesgos.

Activos de CAM INC		
Hardware		
Tipo	**Distribuidor**	**Ubicación**
Servidor de Aplicaciones	DELL	Centro de Datos
Servidor Web	DELL	Centro de Datos
Servidor de Acceso Remoto	DELL	Centro de Datos
Servidor Proxy	DELL	Centro de Datos
Servidor de Correo	DELL	Centro de Datos
Switches	CISCO	Centro de Datos
Routers	CISCO	Centro de Datos
Computadores	DELL	Oficinas/Servicio al cliente
Teléfonos digitales	LinkSys	Oficinas/Servicio al cliente
UPS	APC	Cuarto eléctrico
Aplicaciones		
Software	**Propietario**	**Uso**
My SQL Server	Microsoft	Administración de base de datos de aplicaciones
CAM MT	Smart Solution	Manejo de transacciones
Sistemas Operativos		
Windows Server 2008 R2	Microsoft	Servidor de archivos y aplicaciones

Tabla 6.6 Listado de activos de CAM INC

La tabla anterior muestra los activos de hardware y software más importantes de CAM INC. Contiene los nombres de los distribuidores y propietarios, ubicación y uso. Estos datos son esenciales para la reacción ante cualquier incidente en CAM INC.

6.2.3.1.1. Identificación de Amenazas

Al momento de analizar los riesgos de la empresa hay que evaluar las diferentes amenazas tanto internas como externas. Para la construcción de la evaluación de riesgos es indispensable la identificación y gestión de dichas amenazas.

La siguiente ilustración muestra la clasificación de las distintas amenazas:

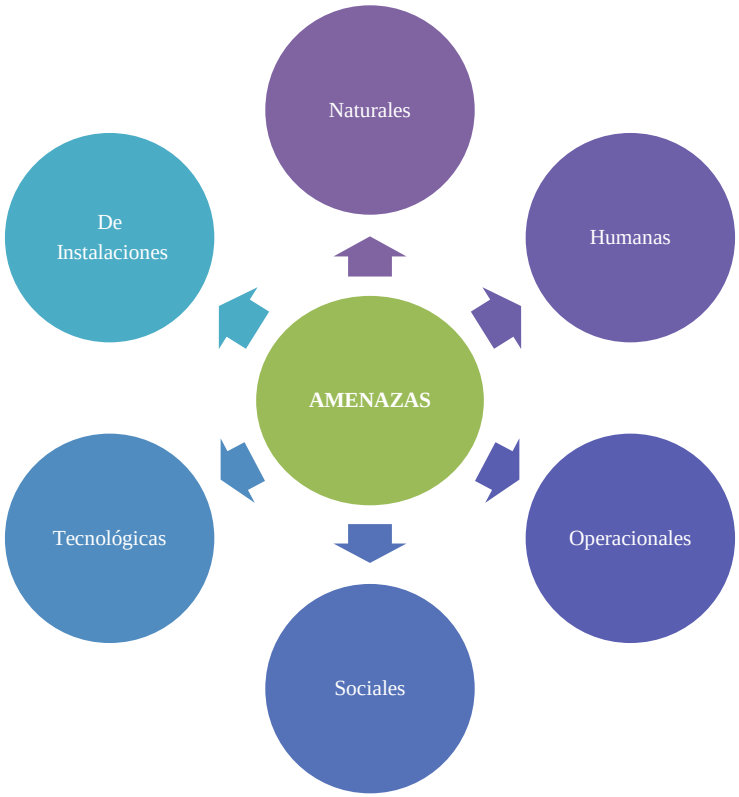

Figura 6.9 Tipos de amenazas

Del listado de amenazas fueron marcadas las que pueden afectar a CAM INC en su situación actual. Para ello se usó la siguiente escala de valoración para la probabilidad y el impacto:

Probabilidad Calificación		*Evaluación de impacto*	
Puntuación	**Nivel**	**Puntuación**	**Nivel**
1	Muy alta	1	Terminal
2	Alto	2	Devastadores
3	Medio	3	Crítica
4	Bajo	4	Controlable
5	Muy baja	5	Muy pequeña

Tabla 6.7 Escala de medición de probabilidad e impacto

- **Evaluación de Desastres Naturales**

Amenazas Naturales	Probabilidad Calificación	Evaluación de impacto	Breve descripción de las posibles consecuencias
Tornado	5	1-5	Tornados no se han producido en esta región
Huracán/ tormenta-huracán Nivel fuertes vientos	4	4-5	Interrupción de energía eléctrica, daños a la propiedad, inundaciones
Inundación	3	4-5	Problemas de transporte, problemas de estacionamiento, daños a la propiedad
Terremoto	3	1-5	Interrupción infraestructura, daños a la propiedad, problemas de transporte, de seguridad para empleados
Tormentas eléctricas	3	4-5	Interrupción de energía eléctrica, daños a la propiedad, seguridad de los empleados
Fuego	4	1-5	Interrupción de energía eléctrica, daños a la propiedad, seguridad de los empleados
Contaminación y los peligros ambientales	3	1-5	Daños a la propiedad, seguridad de los empleados

Epidemia	3	1-5	Personal afectado por una epidemia generalizada, esto tendría consecuencias en los niveles de servicio.

Tabla 6.8 Evaluación de amenazas naturales

- **Evaluación de las amenazas humanas**

En esta parte se evalúan las amenazas pero en el ámbito humano, cuáles son los posibles escenarios donde un proceso de la empresa se puede ver afectado por una interrupción causada en base a una amenaza humana.

Amenazas Humanas	Probabilidad Calificación	Evaluación de impacto	Breve descripción de las posibles consecuencias
Disputas laborales / Acción industrial	5	4-5	No ha habido ninguna actividad laboral en CAM INC. Disputas laborales impactan los niveles de servicio.
Incendio provocado	5	1-5	No han tenido una incidencia de este tipo, pero el impacto dependerá de la intensidad del fuego.
Robo	4	5-5	Los incidentes de robo en CAM INC han variado desde datos hasta pequeños sistemas informáticos. El impacto directo en la empresa ha sido notorio
Acto de guerra	5	1-5	No han tenido un acto de este tipo en la República Dominicana hace ya muchos años. El impacto dependerá de la gravedad.
Acto de sabotaje	5	1-5	Nunca se ha presentado esta situación pero su impacto dependerá de la gravedad.
Acto de terrorismo	5	1-5	El impacto dependerá de la gravedad.

Tabla 6.9 Evaluación de amenazas humanas

- **Evaluación de las amenazas en las instalaciones**

Aquí se examinan y evalúan las amenazas con mayores posibilidades de ocurrencia en el espacio de CAM INC. Los potenciales desastres que pueden ocurrir en caso de la pérdida de las utilidades o servicios de CAM INC.

Amenazas a las Instalaciones	Probabilidad Calificación	Evaluación de impacto	Breve descripción de las posibles consecuencias
Falta de energía eléctrica	1	1-3	Fallo de alimentación en CAM INC solo impacta a la empresa si los generadores de emergencia no entran en funcionamiento inmediatamente al ocurrir el evento. Los niveles de servicio se ven interrumpidos.
Pérdida de suministro de agua	3	4	Cualquier pérdida de agua sería temporal y mejorable, a menos que parta de una mayor escala de desastre (terremotos, etc.).
Interrupción de los servicios de comunicaciones	3	4-3	Pérdida del servicio telefónico impacta de inmediato los niveles de servicio.
Pérdida de drenaje / eliminación de desechos	4	4	Pérdida de drenaje sería temporal y manejable, a menos que parte de una mayor escala de desastre (terremotos, etc.).
Falta de aire acondicionado	3	4	Fracaso de las unidades individuales puede ser compensado por otras unidades en el edificio. Fracaso general de nivel de servicio podría generar interrupciones si el edificio llega a estar demasiado calientes para los agentes trabajar de manera eficaz. Las unidades podrían ser sustituidas o reparadas rápidamente.
Avería de los equipo (con exclusión de hardware de TI)	3	5-4	En función de nivel de impacto a la construcción de infraestructuras. Es improbable que tenga un impacto en los niveles de servicio.

Tabla 6.10 Evaluación de amenazas en las instalaciones

- **Evaluación de incidentes serios con los sistemas de información**

Los escenarios con mayor posibilidad que podrían afectar a la empresa en caso de que suceda un incidente con los sistemas de información son los siguientes:

Potencial de los desastres	Probabilidad Calificación	Evaluación de impacto	Breve descripción de las posibles consecuencias
Crimen Cibernético	3	3	Podría crear interrupción a los sistemas de TI e impactar los niveles de servicios
Pérdida de registros o datos	2	2	Podría crear interrupción a los sistemas de TI e impactar los niveles de servicios
Revelación de información sensible	3	3	Depende de la naturaleza de la información
Fallo del sistema TI	2	1	Impacta los niveles de servicio. No existen copias de seguridad de los sistemas disponibles.

Tabla 6.11 Evaluación de incidentes con los sistemas de información

- **Evaluación de otras amenazas**

Existen otras amenazas que poseen un nivel de impacto considerable en la empresa en caso de ocurrir, ejemplo de dichas amenazas se describen en la tabla a continuación:

Potencial de los desastres	Probabilidad Calificación	Evaluación de impacto	Breve descripción de las posibles consecuencias
Reglamento de Salud y Seguridad	4	5	Sin efecto sobre los niveles de negocios
La moral de los empleados	3	4-5	Podrían tener un impacto en el nivel de personal y el afectar los niveles de servicio
Las fusiones y adquisiciones	4	5	Poco o ningún impacto a nivel de servicios
Publicidad negativa	4	3	Impacto a nivel de demanda de servicios

Tabla 6.12 Evaluación de otras amenazas

6.2.3.1.2. Evaluación de Vulnerabilidades

Las vulnerabilidades son ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen llevan a esos activos a ser vulnerables. Mediante el uso de las debilidades existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.[24]

Vulnerabilidades en CAM INC

Durante el proceso de identificación de las vulnerabilidades de la empresa CAM INC se pudo observar que estas provienen de diferentes fuentes. A continuación la tabla que contiene las vulnerabilidades recopiladas, la evaluación del impacto en caso de que se materialicen y las causas de esas vulnerabilidades.

Vulnerabilidades en CAM INC	***Evaluación de impacto***	***Causa***
Falta de mantenimiento de los equipos	3	No existe un período de tiempo preestablecido para la verificación y mantenimiento de los equipos.
Suministro eléctrico poco eficiente	2	Las unidades de generación de energía no están en capacidad de suministrar energía de forma ininterrumpida.

[24] Sena L., Tenser S. Introducción a Riesgo Informático. Catedra Introducción a la Computación-FCEA. Agosto 2004.

Ausencia de sistema de extinción de fuegos	3	No tienen un sistema contra incendios instalados
Educación inapropiada de los empleados en virus y troyanos	3	La empresa no capacita ni provee ningún tipo de información sobre las consecuencias de los virus y troyanos
Política de seguridad de la información deficiente	3	No tienen políticas de control de acceso a la información y tampoco existe una clasificación de la información a nivel de confidencialidad.
Ausencia de copias de respaldo	2	No tienen políticas de copias de seguridad de los datos
Descarga incontrolada y mal uso de software	4	No existen controles para el uso de internet y descargas de software
Deterioro de cableado y dispositivos de trabajo.	3	No se hacen revisiones periódicas de los cableados

Tabla 6.13 Evaluación de vulnerabilidades

6.2.3.1.3. Evaluación de Riesgos

Riesgo es aquella eventualidad que imposibilita el cumplimiento de un objetivo. Es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado.[25]

La siguiente tabla muestra una relación entre las diferentes amenazas que pueden sufrir los activos tomando en cuenta el impacto y la probabilidad de que ocurran, y de esta forma medir el nivel de priorización del riesgo.

[25] Sena L., Tenser S. Introducción a Riesgo Informático. Catedra Introducción a la Computación-FCEA. Agosto 2004.

Activo	Amenaza	Vulnerabilidades	Impacto	Probabilidad	Medición	Priorización
Central telefónica	Falla de hardware, fallas del proveedor de servicios, vandalismo.	Suministro eléctrico ineficiente, seguridad débil.	3	3	9	B
Teléfonos	Error humano, falla de la red, vandalismo.	Suministro eléctrico ineficiente.	3	4	12	A
Servidor de aplicaciones	Virus, troyanos, inundaciones, corte de energía, hackers.	Suministro eléctrico ineficiente, seguridad lógica débil, falta de antivirus.	2	2	4	C
Servidor de correo	Virus, troyanos, inundaciones, corte de energía, hackers.	Suministro eléctrico ineficiente, seguridad lógica débil, falta de antivirus.	2	2	4	C
Servidor Proxy	Virus, troyanos, inundaciones, corte de energía, hackers.	Suministro eléctrico ineficiente, seguridad lógica débil, falta de antivirus.	2	2	4	C
Base de datos de la empresa	Falla en el software, pérdida o robo de datos, manipulación, divulgación.	Falta de copias de respaldo, seguridad lógica débil, falta de antivirus.	1	2	2	D
Base de datos de clientes	Falla en el software, pérdida o robo de datos, manipulación, divulgación.	Falta de copias de respaldo, seguridad lógica débil, falta de antivirus, falta de controles de acceso.	1	2	2	D
Software de aplicaciones	Falla de software, fallas en la red, falla de integridad de datos.	Falta de copias de respaldo, seguridad lógica débil, falta de antivirus.	4	3	12	A
Sistemas Operativos	Falla de red, hackers, virus, error humano.	Falta de copias de respaldo, seguridad lógica débil, falta de antivirus.	4	3	12	A
Computadoras	Falla del hardware, virus, vandalismo, corte de energía, inundaciones.	Suministro eléctrico ineficiente, seguridad lógica débil, falta de antivirus.	3	3	9	B
Routers	Virus, troyanos, inundaciones, corte de energía, hackers.	Suministro eléctrico ineficiente, seguridad lógica débil, falta de antivirus.	3	2	6	C

Switches	Virus, troyanos, inundaciones, corte de energía, hackers.	Suministro eléctrico ineficiente, seguridad lógica débil, falta de antivirus.	3	2	6	C
UPS	Falla del hardware, fuego, inundaciones, vandalismo.	Falta de extintores automáticos, falta de mantenimiento de los equipos, falta de señalización y extintores manuales.	2	3	6	C
Personal	Epidemias, huelgas, problemas de transporte, falta de capacitación, desmotivación.	Falta de motivación, falta de dispensario médico, falta de tolerancia.	4	4	16	A

Tabla 6.14 Evaluación de riesgos

6.2.3.1.4. Evaluación de Contramedidas

Para reducir los niveles de riesgos se deben utilizar los siguientes controles o medidas de seguridad:

Controles para acceso a la información

- ✓ Crear perfiles de seguridad para todos los usuarios de acuerdo a sus responsabilidades.
- ✓ Limitar el acceso de los diferentes usuarios dependiendo de las tareas que deba realizar en su puesto.
- ✓ Limitar los servicios de Internet y del correo electrónico de la empresa para uso exclusivamente laborales
- ✓ Establecer revisiones periódicas sobre la administración de las cuentas.
- ✓ Revalidación anual de usuarios y grupos dentro del sistema.

- ✓ Detección y bloqueo de cuentas inactivas.
- ✓ Redacción de un acuerdo de uso apropiado de los datos y equipos para los empleados.
- ✓ Utilización de contraseñas de encendido para los servidores.

Medidas para garantizar las copias de seguridad

- ✓ Establecer políticas de copias de seguridad para los datos.
- ✓ Salvaguardar los medios y soportes utilizados para las copias de seguridad en lugares seguros.
- ✓ Asignar el personal técnico especializado para la supervisión de los datos y ficheros de las copias de seguridad.
- ✓ Desarrollar un procedimiento para realizar pruebas a las copias de seguridad.
- ✓ Probar las copias de seguridad con frecuencia mediante la restauración real de los datos en una ubicación de prueba.

Controles para evitar virus y troyanos

- ✓ Tener un antivirus potente y actualizado.
- ✓ Actualizar los sistemas operativos y programas con los sitios oficiales.
- ✓ Instalar un firewall para el bloqueo de los sitios web no autorizados.
- ✓ Establecer políticas sobre el uso de software y aplicaciones no autorizadas en la empresa.

- ✓ Bloquear los archivos ejecutables que sean descargados en la red.
- ✓ Capacitar a los usuarios con respecto a los virus y troyanos y sus consecuencias.

Medidas para suministro de energía redundante

- ✓ Priorizar los servicios que requieran el uso de energía redundantes
- ✓ Verificar la adecuada conexión de los equipos a la toma de tierra.
- ✓ Implementación del uso de sistemas de alimentación ininterrumpida (SAI).
- ✓ Analizar los requerimientos de potencia actuales y futuros de los equipos.
- ✓ Diseñar políticas de mantenimiento para las unidades de generación de energía redundante.
- ✓ Mantenimiento correctivo y preventivo para los UPS.
- ✓ Instalación de generadores eléctricos.

Otras medidas

- ✓ Realizar revisiones periódicas en las instalaciones físicas, cableados y dispositivos de las empresa.
- ✓ Colocar señalizaciones para casos de evacuación de emergencia.
- ✓ Proveer orientación al personal con respecto al plan de recuperación ante desastres.

6.2.3.2. Análisis de Impacto en CAM INC

Una vez se tiene el análisis de riesgos, se realiza el análisis de impacto de negocios o *Business Impact Analysis (BIA).* El BIA es la guía que determina qué necesita ser recuperado y el tiempo que tarda dicha recuperación. En esta fase del plan de recuperación ante desastres se analiza el impacto a los procesos de la empresa en caso de que fueran interrumpidos por un incidente.

El objetivo principal de la evaluación de riesgos y análisis de impacto es la evaluación de lo que ya existe, evitar la duplicación de esfuerzos y aprovechar la información y las capacidades existentes.

En el análisis de impacto se incluye la relación de los procesos, la relación de las aplicaciones, la relación de departamentos y usuarios, se determinan los procesos críticos, se establece el tiempo objetivo de recuperación (RTO), el objetivo de punto de recuperación (RPO) y el tiempo máximo de interrupción (MTO).

Proceso	Descripción	Frecuencia de uso	Sistema con que interactúa	Equipo necesario	Personal Crítico	Suplidores	MTD	RTO	RPO	Costo impacto por H/D/M	Nivel de Criticidad
Soporte al Producto del Cliente	Capacidad de sostener los niveles de servicios al cliente.	Diario	Distribuidor Automatico de Llamadas	Servidores	Agentes de Servicio al Cliente, Representante de TI	LinkSys	< 2 horas	1 hora	2 horas	2800 dólares por hora en promedio	1
Proceso de Apoyo	Mantenimiento de las tecnologías y telecomunicaciones.	Diario	Windows Server 2008, SQL Server	Servidores y teléfonos	Representantes de TI	N/A	2-4 horas	< 1 hora	2 horas	1700 dólares por hora	2
Facilidades	Mantenimiento del sistema del plantel operacional de CAM INC.	Diario, Semanal, Mensual	Mantenimiento TI	Servidores de aplicaciones, UPS.	Personal de mantenimiento	N/A	2 horas a 2 días	<2 horas a 1 día	2 horas	500 dólares	2
Nómina	Generar la nómina	Quincenal	SAP	Servidores y computadores	Representantes de finanzas	CAM INC	24 a 48 horas	< 24 horas	2 a 6 días	170 dólares por hora	3

Tabla 6.15 Análisis de impacto en CAM INC

6.2.4. Desarrollo de Estrategias

Las estrategias de recuperación permiten el diseño de iniciativas viables para recuperar los sistemas de información de mayor importancia que soportan los procesos críticos antes identificados. Dichas estrategias contemplarán el hardware, capital humano, localización geográfica, software, comunicaciones y servicio eléctrico.

6.2.4.1. Estrategia de procesamiento de la información mediante computación y almacenamiento en la nube (Cloud Computing and Storage Computing).

Esta estrategia se basa en la contratación de los servicios de la empresa NAP del Caribe para el procesamiento, almacenamiento y respaldo de los datos en la nube, en su módulo de servicios gestionados: Cloud Computing.

La estrategia de computación en la nube disminuye la redundancia en la transmisión, lo que se reflejara en los costos, pero tiene dependencia en cuanto a los acuerdos de uso y contrataciones con los suplidores.

6.2.4.2. Estrategia de Preparación de un Warm Site

Esta estrategia pretende crear un duplicado del sitio original de la empresa CAM INC en donde se pueda seguir operando en caso de desastre.

El Warm Site estará ubicado en el segundo piso en un área preparada, con las condiciones necesarias. Dicho centro secundario contara con los siguientes equipos y tecnologías:

- Servidor de Aplicaciones DELL
- Servidor de Base de Datos
- Servidos Web DELL
- Switches CISCO
- Routers CISCO
- Cableado
- UPS
- Planta de energía eléctrica
- Teléfonos
- Computadores
- Windows Server 2008
- Base de datos Oracle

En el Warm Site se deberá hacer un backup incremental cada 30 minutos y un backup completo semanal. Los backup deberán ser encriptados para garantizar la confidencialidad.

6.2.4.3. Costes Financieros de Implementación de Estrategias

Los costos para implementar cualquiera de las estrategias anteriores se detallan en la siguiente tabla:

		Computación y Almacenamiento en la Nube	***Warm Site***
Cant	***Componentes***	***US$ Costo***	***US$ Costo***
8	Mantenimiento y personal	40568.32	58218.32
12	(8x1.6GHz CPU, 16 GB RAM, 2,040 GB Almacenamiento) 250 GB Ancho de Banda	1500	N/A
4	Servidores 2.4 GHz 8GB RAM	N/A	12580
2	Servidores de Base de datos	7000	7000
2	Servidor Web	N/A	5900
2	Servidor de Aplicaciones	N/A	4700
1	Switches	400	400
1	Routers	500	600
5	Caja de cables 1000 pies	N/A	9000
1	Planta de Energía Eléctrica 1200KW	25000	35000
2	UPS	20000	32000
1	Sistema de enfriamiento	12000	15900
1	Sistema de detección de incendio	5500	6200
		112,468.32	**187,498.32**

Tabla 6.16 Costos de implementación de estrategias

6.2.5. Acciones del Plan de Recuperación ante Desastres

En esta sección se muestran las acciones a tomar por parte de los equipos durante la ejecución del plan de recuperación ante desastre. La siguiente grafica describe las etapas que se llevaran a cabo:

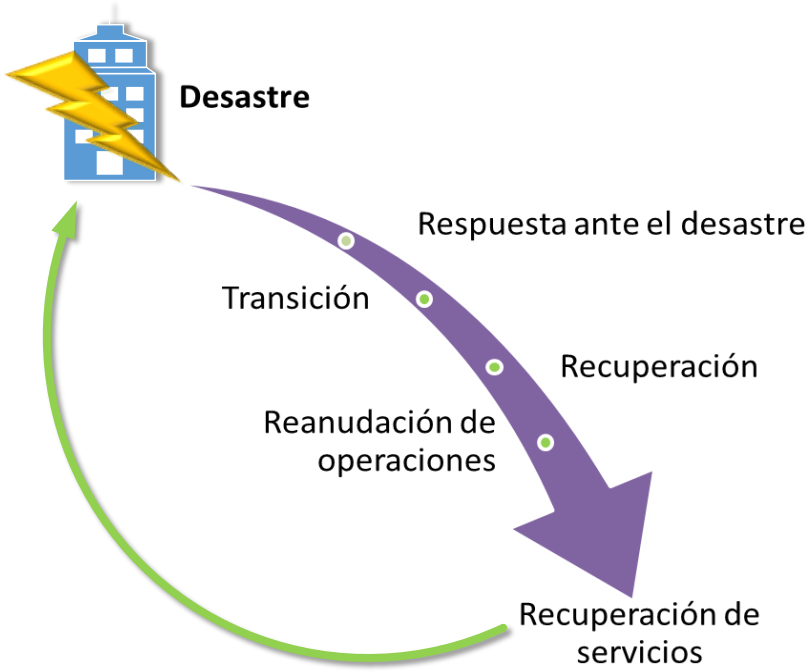

Figura 6.10 Acciones del plan de recuperación ante desastres

6.2.5.1. Respuestas ante Desastres

Una vez haya ocurrido el desastre el equipo de respuesta a emergencias deberá evaluar la situación con toda la información del incidente y luego, decidirán si se activa o no el plan de recuperación ante desastre.

La siguiente tabla muestras las actividades que se realizaran durante este proceso:

Acciones	a. Coordinar la respuesta inicial y la utilización de procedimientos establecidos para proteger la vida y minimizar los daños. b. Calcular los daños. c. Evaluar posible activación del plan de recuperación. d. Proporcionar un aviso oficial a la empresa en general. e. Comenzar la recuperación de desastre de la forma establecida. f. Suministrar las informaciones pertinentes correspondientes sobre la situación por los canales correspondientes. g. Establecer un informe de la evaluación de las perdidas.

Tabla 6.17 Acciones de respuesta ante desastre

6.2.5.2. Transición

La transición es el término que se utiliza normalmente para definir el cambio, el traspaso, la evolución progresiva de un estado a otro.[26] En esta etapa del DRP se convoca el personal y los equipos necesarios para poner en acción el plan, y se designa un equipo de logística para coordinar el traslado del personal correspondiente a las instalaciones del NAP del Caribe para gestionar todo el material necesario para poner en funcionamiento el centro de recuperación a través de las cintas de backup, la documentación y el almacenamiento realizado en la nube.

[26] Definición ABC. http://www.definicionabc.com/general/transicion.php#ixzz38obAPdHH

6.2.5.3. Recuperación

Cuando el equipo designado para la recuperación llegue al NAP del Caribe y los materiales estén listos, deben verificar rápidamente el estado de los equipos y luego iniciar con la instalación de las aplicaciones.

Una vez instaladas las aplicaciones, se procederá a cargar el backup más reciente de la data y verificar que dicha información este correcta. Luego quien se encargue de la seguridad lógica verificará que toda la data se esté procesando en este nuevo sitio, que tenga las garantías necesarias y que los equipos tengan un alto nivel de seguridad establecidos para no ser atacado por hackers y otros.

La siguiente tabla muestra las actividades a realizar:

Acciones de Recuperación	a. Recibir notificación del equipo de respuesta a emergencia. b. Comenzar las actividades de recuperación. c. Iniciar los preparativos del Warm Site. d. Confirmar condiciones del Warm Site. e. Verificar servidores y sistemas operativos. f. Instalar aplicaciones correspondientes g. Cargar base de datos y restaurar el último backup. h. Verificar si la información es correcta. i. Verificar la seguridad lógica del Warm Site. j. Activar el Warm Site.

Tabla 6.18 Acciones de recuperación ante el desastre

6.2.5.4. Restauración

El orden de recuperación de las aplicaciones se hará de acuerdo a la criticidad de los sistemas: soporte a los servicios del cliente, sistemas de apoyo, tecnología informática y telecomunicaciones.

Una vez los sistemas restaurados, el equipo de unidades de negocio realizará las comprobaciones necesarias que certificaran que dicho sistema funcionan de manera satisfactoria y así continuar prestando los servicios.

6.2.5.5. Vuelta a la Normalidad

En esta parte se plantearán las diferentes estrategias y acciones para recuperar la normalidad total del funcionamiento de la organización.

Se efectuaran las siguientes actividades:

- Asegurar que todos los equipos estén en su estado normal para su funcionamiento.
- Iniciar los preparativos para regresar las instalaciones de CAM INC.
- Activar el centro de datos de la empresa.
- Desactivar el Warm Site del NAP del Caribe.
- Emitir un comunicado general.

6.3. Ensayo o Diseño de Pruebas del Plan de Recuperación ante Desastres

La experiencia indica que los planes de recuperación deben ser probados en su totalidad por lo menos una vez al año. La documentación debe especificar los procedimientos y la frecuencia con que se realizan las pruebas. Las razones principales para probar el plan son: verificar la validez y funcionalidad del plan, determinar la compatibilidad de los procedimientos e instalaciones, identificar áreas que necesiten cambios, entrenar a los empleados y demostrar la habilidad de la organización de recuperarse de un desastre.[27]

Los objetivos del plan de prueba del DRP se fundamentan en los resultados que se quieren obtener. En base a esto, los objetivos de la prueba del plan de recuperación de desastres diseñado para CAM INC son los siguientes:

- ✓ Verificar que las acciones de recuperación son viables.
- ✓ Examinar todos los componentes del plan: software, hardware, data, telecomunicaciones, documentación, procedimientos, transportación, sitios de procesamiento alternos y el personal.
- ✓ Probar el rendimiento de los sistemas de respaldo de los datos y de las redes.
- ✓ Actualizar el plan para cubrir los nuevos requerimientos de la empresa.
- ✓ Capacitar los líderes operacionales en los procedimientos de la ejecución del plan.

[27] Search Data Center en Español. http://searchdatacenter.techtarget.com/es/cronica/Pasos-para-un-Plan-de-Recuperacion-de-Desastres-DRP.

Después de realizar las pruebas el plan de recuperación debe ser actualizado. Es recomendable que la prueba original se realice en horas que minimicen trastornos en los servicios que brinda la empresa, y una vez demostrada la funcionalidad del plan, se debe hacer pruebas adicionales donde todos los empleados tengan acceso virtual y remoto a estas posiciones y funciones en el caso de un desastre. Un plan de recuperación ante desastres sin haber sido probado es equivalente a no tener un ningún plan.

6.3.1. Tipos de Pruebas

Previo a realizar la prueba del plan es necesario saber qué tipo de prueba se va a realizar. Los tipos de pruebas más conocidas y aceptadas generalmente son:

- Pruebas sobre papel (*Structure Walk-Trough Test*): Las diferentes áreas de la empresa se reúnen y "caminan" a través del plan, evaluando diversos escenarios desde el principio al fin.
- Prueba de lista de verificación (*CheckList Test*): Representantes de las diferentes áreas de la organización revisan el plan y hacen sus comentarios para asegurarse de que nada falte.
- Prueba de Simulación (*Simulation Test*): Esta toma más gente y planeación, se revisa un escenario específico y se ejecutan los pasos que indican en el plan, simulando incluso la relocalización hacia un sitio alterno.

- Prueba Paralela (*Parallel Test*): Se hace para asegurarse de que los sistemas trabajen de acuerdo a lo esperado en el sitio alterno. Se procesa en el sitio alterno y se comparan los resultados con lo que se obtiene en el sitio de producción.
- Prueba de Interrupción Completa (*Full Interruption Test*): Esta es una prueba real donde el sitio de producción es detenido y se debe trabajar en las instalaciones y facilidades alternas.[28]

6.4. Mantenimiento del Plan

Se puede asegurar que periódicamente toda organización recluta nuevo personal, modifica sus procesos y adquiere nuevos equipos. Por ende, actualizar la documentación del plan es fundamental para la recuperación satisfactoria tras cualquier eventualidad.

CAM INC debe modificar y mantener su plan de recuperación ante desastres por lo menos una vez al año, para conservarlo actualizado, debido a que asegura que las áreas permanezcan preparadas para el manejo de incidentes relacionados a la continuidad del negocio a pesar de los cambios a las personas, los procesos y la tecnología.

[28] ISACA.org
http://www.isaca.org/chapters7/Monterrey/Events/Documents/20050920%20Cobit%20para%20asegurar%20continuidad%20operaciones.pdf

Los principales disparadores de mantenimiento al plan de recuperación ante desastres en CAM INC son:

- ✓ Revisiones periódicas al DRP (mantenimiento programado).
- ✓ Adecuaciones identificadas por el control de cambios.
- ✓ Adecuaciones identificadas como resultado de pruebas o ejercicios.

El plan debe ser mejorado continuamente, aprendiendo de los errores cometidos, a sabiendas de que contiene mucha información sensitiva, por lo que debe ser distribuido solo a las personas autorizadas para actualizarlo.

CONCLUSIONES

La pérdida o robo de datos y los eventos catastróficos que ocurren en las empresas demuestran la necesidad de contar con métodos de control de acceso a la información y plan de recuperación ante desastres. Es importante identificar los riesgos y amenazas a los que se encuentra expuesta una organización, ya que al menos para un 60% de las empresas el impacto económico de la pérdida de datos representa una cifra igual o superior a 50.000 dólares al año y la respuesta tardía ante incidentes no programados ha dejado fuera de servicio a un 15%.

En el estudio realizado se demostró el hecho de que la empresa CAM INC actualmente necesitaba implementar una herramienta que mitigue la pérdida de datos al igual que diseñar un plan de recuperación efectivo para garantizar la continuidad de sus procesos durante una eventualidad o desastre. Dicha empresa en caso de no seguir las recomendaciones realizadas podría mermar en sus operaciones de manera definitiva, pero con el seguimiento de las pautas presentadas, el poder de reacción y sobrevivencia ante cualquier desastre incrementa y disminuyen los efectos causados por estos. Del mismo modo, se realizaron estudios que ayudan a la solución óptima en lo referente a costos, eficacia y prontitud, ya que se analizaron los procesos que representan la vida misma de la empresa.

Finalmente, los mecanismos de prevención de pérdida de datos y plan de recuperación antes desastres deben ser parte esencial de cualquier organización, ya que se implementan con la finalidad de garantizar la confidencialidad de los datos, la credibilidad de la organización y de sus operaciones apoyadas en tecnologías, ante cualquier problemática de origen humano o natural, provocadas o no.

RECOMENDACIONES

A partir de los resultados obtenidos tras la implementación de la herramienta de prevención de pérdida de datos y diseño de plan de recuperación ante desastres, se sugiere lo siguiente para CAM INC:

- ✓ Establecer controles de acceso a la información.
- ✓ Asignar permisos de acceso a los recursos de la red en función de los diferentes perfiles de los usuarios.
- ✓ Utilizar distintas tecnologías de filtrado de contenido, para evitar los virus, malware y troyanos.
- ✓ Respaldar la información en distintos lugares.
- ✓ Implementar herramientas para el control y vigilancia del acceso a los servicios de internet.
- ✓ Motivar, capacitar y concientizar a los usuarios sobre el buen manejo de los recursos de la empresa.
- ✓ Diseñar políticas de seguridad eficientes.
- ✓ Aplicar el plan de recuperación ante desastres en los diferentes procesos existentes, para garantizar la sobrevivencia ante un desastre.
- ✓ Poner en práctica evaluaciones periódicas de los diferentes factores que podrían fungir como amenazas contra el desenvolvimiento de la empresa.
- ✓ Plantear escenarios de desastres que servirán de base al momento de determinar las alternativas viables de recuperación.

GLOSARIO

Almacenamiento en la nube: Es un modelo de servicio en el cual los datos de un sistema de cómputo se almacenan, se administran, y se respaldan de forma remota, típicamente en servidores que están en la nube y que son administrados por un proveedor del servicio. Estos datos se ponen a disposición de los usuarios a través de una red, como lo es Internet.

Amenaza: Todo elemento o acción capaz de atentar contra la seguridad de la información.

Base de Datos: Sistema computarizado para llevar registros. Es posible considerar a la propia base de datos como una especie de armario electrónico para archivar, es decir, es un depósito o contenedor de archivos de datos computarizados.

Centro de datos: Centro de almacenaje de datos, que provee servicios de negocio y entrega de forma segura aplicaciones y datos a usuarios remotos a través de Internet.

Cold Site: Es un duplicado del sitio original de la organización Este sitio es el más barato de operar. No incluye copias de backup ni tampoco hardware. La falta de hardware

contribuye con los costos mínimos de mantenimiento que tiene este tipo de sitios pero requiere un mayor tiempo para que la organización se recupere luego de un desastre.

Confidencialidad: Servicio de seguridad o condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. También puede verse como la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

Dato: Un dato es una información breve y concreta que representa una condición o situación de un sujeto o idea más amplia. El dato es una representación simbólica (numérica, alfabética, algorítmica, etc.) de un atributo o variable cuantitativa. Los datos describen hechos empíricos, sucesos y entidades.

Hot Site: Es un duplicado del sitio original de la organización. Mantiene la completitud de los sistemas informáticos como también los backups más recientes. Puede haber sincronización en tiempo real.

Información: La información es un conjunto de datos acerca de algún suceso, hecho, fenómeno o situación, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo.

Informática: Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.

Integridad*:* Cualidad de la información que se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores de esos datos. Esta cualidad se obtiene cuando se impide eficazmente la inserción, modificación o destrucción no autorizada, sea accidental o intencional del contenido de una base de datos. La integridad de los datos es uno de los seis componentes fundamentales de la seguridad de la información.

Objetivo de Punto de Recuperación: *"*Recovery Point Objective*"* o *"*RPO*"*. Define la pérdida de datos máxima tolerable que se acepta ante una situación de desastre.

Respaldo de Información: "Backup". Es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una avería electromecánica o un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar perdida generalizada de datos.

Riesgo: Incertidumbre existente por la posible realización de un suceso relacionado con una amenaza de daño respecto a los bienes o servicios informáticos, como equipos, periféricos, instalaciones, programas, etc.

Seguridad Informática: Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Seguridad de la Información: Es la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Sistema: Conjunto de componentes que interaccionan entre sí para lograr un objetivo común. Aunque existe una gran variedad de sistemas, la mayoría de ellos pueden representarse a través de un modelo formado por cinco bloques básicos: elementos de entrada, elementos de salida, sección de transformación, mecanismos de control y objetivos.

Tecnología: Conjunto de conocimientos y técnicas aplicadas de forma lógica y ordenada que le permiten al ser humano cambiar su entorno material o virtual para satisfacer sus necesidades. Es un proceso combinado de pensamiento y acción con la finalidad de generar soluciones que sean útiles.

Tecnología de la Información: Es toda herramienta y método empleado para recabar, retener, manipular o distribuir información. La tecnología de la información se encuentra

generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.

Tiempo Objetivo de Recuperación: "Recovery Time Objective" o "RTO". Se refiere a cuánto tiempo puede permanecer la organización sin ejecutar una actividad, el uso de una aplicación (hardware y/o software) o información relevante.

Tiempo Máximo de Interrupción: "Maximum Tolerable Outage" o "MTO". Es el tiempo máximo de inactividad que la organización puede tolerar la ausencia o no disponibilidad de una función o proceso.

Virtualización: Es el concepto que describe cómo en un solo computador físico se coordina el uso de los recursos para que varios sistemas operativos puedan funcionar al mismo tiempo de forma independiente y sin que ellos sepan que están compartiendo recursos con otros sistemas operativos.

Vulnerabilidad: Debilidad en un sistema que permite a los atacantes violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

VMWare: Es el nombre que lleva el software de virtualización de servidores (Virtual Machine), por extensión de la marca de la empresa que lo facilita. Se trata de un sistema de virtualización por software, en el que se emula un sistema físico (ordenador) con unas características de hardware determinadas. VMware permite ejecutar varios sistemas operativos de forma independiente sobre una infraestructura física.

Warm Site: Es un duplicado del sitio original de la organización intermedio entre el hot y el cold site. Estos sitios tendrán hardware y conectividad operativos, aunque en una escala menor al sitio original. Tendrán backups a mano pero estos no serán completos y pueden no ser tan recientes.

BIBLIOGRAFÍA

- Asociación de Auditoría y Control de Sistemas de Información (ISACA). (2014). Consultado el 21 de julio de 2014, en http://www.isaca.org/chapters7/Monterrey/Events/Documents/20050920%20Cobit%20para%20asegurar%20continuidad%20operaciones.pdf
- Basualdo, Cristian (2011). Delitos informáticos. Consultado el 27 de junio de 2014, en http://crimenescyberneticos.blogspot.com/p/pericia-informatica.html
- Cappiello, Hernán (2012). La invisibilidad de las pruebas de corrupción. Consultado el 25 de junio de 2014 en http://www.lanacion.com.ar/1450864-la-invisibilidad-de-las-pruebas-de-corrupcion
- Daltabuit, E. (2007).La seguridad de la información. México, Limusa.
- Date, C. (1995). An Introduction to database System 6th edition. Addison Wesley.
- E., C. T. (2006). Sistemas de Bases de Datos 4ta Edición. Addison Wesley.
- Guess (2009). El Cibercrimen y delitos informáticos. Consultado el 22 de julio de 2014, en http://www.slideshare.net/guest225f3bd/el-cibercrimen-y-delitos-informaticos
- J, R. (2005). Cibersociedad, Tecnologia de la Informacion y La Comunicacion. Consultado el 16 de junio de 2014, en http://www.cibersociedad.net/archivo/articulo.php?art=218

- Pérez Cleto, Cristian Ariel (2009). Implementación de un plan de recuperación de desastres para las empresas de Call Center en la República Dominicana Caso: Stream Global Services. Universidad UNAPEC.
- Rodríguez Prieto, A. (2006). Protección de la información. Diseño de criptosistemas informáticos. Madrid, Paraninfo. ISBN 84-283-1434-9.
- Salazar, C. (2008). Cibermundos, La TIC como herramienta a la gestion empresarial. Recuperado de http://cibermundos.bligoo.com/content/view/145501/Las-TIC-como-herramienta-a-la-gestion-empresarial.html
- Santiago Quevedo, Carlos María (2007, 16 de diciembre). Tecnología y algo más. Recuperado de http://csantiagoeljurista.blogspot.com/2007/12/realidad-de-los-delitos-informticos-en.html
- Sosa González, Gregorys José (2012). Plan de recuperación ante desastres aplicado al área de tecnología del Ministerio de Educación de la República Dominicana (MINERD) en el periodo enero-abril 2012. Universidad UNAPEC.
- Vásquez, M. R. (2008). Crimines y Delitos de Computadoras y Alta Tecnología en la era de los convergentes. Santo Domingo.
- Vieites Gómez, A. Enciclopedia de la Seguridad Informática. Editorial Alfaomega. México. ISBN 978-970-15-1266-1.

Fuentes electrónicas:

- Symantec. http://www.symantec.com/products-solutions/
- ISACA.org. https://www.isaca.org/Pages/default.aspx
- ISO.org. http://www.iso.org/iso/home/standards.htm
- Asociación Española para la Calidad. http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion
- Universidad Nacional Autónoma de México. http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ServConfidencialidad.php
- YourDictionary.com. http://computer.yourdictionary.com/dataintegrity
- Galeon.com. Riegos Informáticos. http://auditoriadesistemas.galeon.com/productos2223863.html
- Diccionario de informática. http://www.alegsa.com.ar/Dic/vulnerabilidad.php
- About.com. http://aprenderinternet.about.com/od/La_nube/g/Almacenamiento-en-la-nube.htm
- Seguridad de la Información en Colombia. http://seguridadinformacioncolombia.blogspot.com/2010/05/analisis-de-impacto-de-negocios.html

ANEXO I

ANTEPROYECTO DE TRABAJO DE GRADO

Decanato de Ingeniería e Informática

Escuela de Informática

Implementación de una herramienta de prevención de pérdida de datos y plan de recuperación ante desastres en la empresa CAM INC, Santo Domingo, 2014.

Autores

Stephanie Petit H.	**2010 0551**
Luis Ariel Rosario	**2010 1542**
Raúl G. Peña	**2010 1669**

Asesores:

Ing. Mitsuteru Nishio

Ing. Santo Rafael Navarro

Anteproyecto de la monografía para optar por el título de:

Ingeniero en Sistemas de Computación.

Distrito Nacional, República Dominicana

2014

IMPLEMENTACIÓN DE UNA HERRAMIENTA DE PREVENCIÓN DE PÉRDIDA DE DATOS Y PLAN DE RECUPERACIÓN ANTE DESASTRES EN LA EMPRESA CAM INC, SANTO DOMINGO, 2014.

2. Selección del Título y Definición del Tema

2.1 Título: Implementación de una herramienta de prevención de pérdida de datos y plan de recuperación ante desastres en la empresa CAM INC, Santo Domingo, 2014.

2.1 Definición del Tema

La pérdida de datos en las empresas puede atribuirse a errores humanos o del sistema, fallos en los equipos, ataques externos o condiciones adversas. La información es uno de los componentes claves para que las instituciones puedan enfrentarse a la competencia y satisfacer las necesidades del mercado. Es indudable lo difícil que puede llegar a ser prevenir y controlar todos los riesgos a los que se enfrenta la seguridad de la información. Siguiendo ese orden, en esta investigación se plantea la implementación de una herramienta para la gestión de la seguridad informática en la empresa CAM Inc., que permita la prevención de pérdida de información y administración de la misma. Es menester estudiar, y en su caso, introducir o implementar todo un sistema o herramienta que permita reducir al mínimo estos riesgos.

3. Planteamiento del Problema

En vista de los avances de la tecnología en la actualidad se puede afirmar que es imposible concebir la idea de manejar una empresa sin utilizar medios informáticos (hardware y software). Las instituciones se ven obligadas a implementar y utilizar las nuevas tecnologías para satisfacer las necesidades del mercado, ser más eficientes, proveerles más facilidades a sus clientes, gestionar y almacenar sus datos y transacciones, entre otras actividades.

El crecimiento sostenido del mercado negro de la información[29], funciona como motor que impulsa una importante masa de ataques informáticos, principalmente destinados a obtener bases de datos con información personal o empresarial. En tal sentido, y de forma específica, los ataques informáticos se han filtrado en la empresa CAM Inc., institución privada dedicada a brindar servicios de envío de dinero y alimentos hacia Haití, y envío de dinero hacia República Dominicana, Canadá, Estados Unidos y otros países. La problemática que afecta a la empresa consiste en perdida y robo de información crítica de sus clientes y agentes autorizados, tales como: número de cuenta bancaria, historial de transacciones, situación domiciliaria, límite de crédito, historial crediticio, en general, información sensible de sus clientes que podrían llevar a serios abusos.

[29] Panda Security. *The Cyber Crime Black Market*. (2011). Recuperado el 28 de mayo de 2014, desde http://cybercrime.pandasecurity.com

La empresa no cuenta con controles para el acceso a los datos, agravante que se hace mayor teniendo en cuenta que manejan una cartera de más de seiscientos mil clientes y un volumen de datos de 2.5 terabytes al mes, con un tráfico de 0.964 gigabytes por segundo.

Desde su órbita interna no tiene políticas de privacidad, procedimientos de respaldo y recuperación de datos, ni almacenamiento externo de información, lo que significa que cualquier fallo en su sistema o alguna incidencia intencional o no, les representaría una perdida cuantiosa, a sabiendas de que cuentan con un capital de activos de alrededor de diez millones de dólares.

Por todas las razones mencionadas anteriormente la fuga de información, y plagio de datos en CAM Inc. se ha vuelto el pan de cada día y es necesario contrarrestar estas incidencias, realizando un monitoreo de datos con una herramienta eficaz que permita detectar, supervisar y proteger los datos confidenciales, al igual que descubrir el flujo anormal de datos, la extracción o duplicación de información, o cualquier modalidad de ataque contra la seguridad informática de la empresa, de forma tal que sea posible la identificación de los diferentes riesgos que constituyen una amenaza para sus operaciones.

4. Objetivos

4.1. Objetivo General

Implementar la herramienta de gestión de seguridad de la información Symantec Prevención de Perdida de Datos (*Data Loss Prevention*) y diseñar un plan de recuperación ante desastres en la empresa CAM Inc.

4.2. Objetivos Específicos

a. Prevenir la perdida y robo de datos en la empresa CAM Inc., mediante el uso de una herramienta de monitoreo y administración de datos.
b. Implementar controles lógicos y físicos de acceso a la información en las distintas áreas de CAM Inc.
c. Analizar los tipos de bases de datos con las que se va a trabajar.
d. Diseñar políticas de respaldo de datos en los servidores.
e. Asegurar los metadatos a través del servicio de almacenamiento en la nube que ofrece NAP del Caribe.
f. Implementar un plan de recuperación ante desastres.

Esquematización de la Investigación

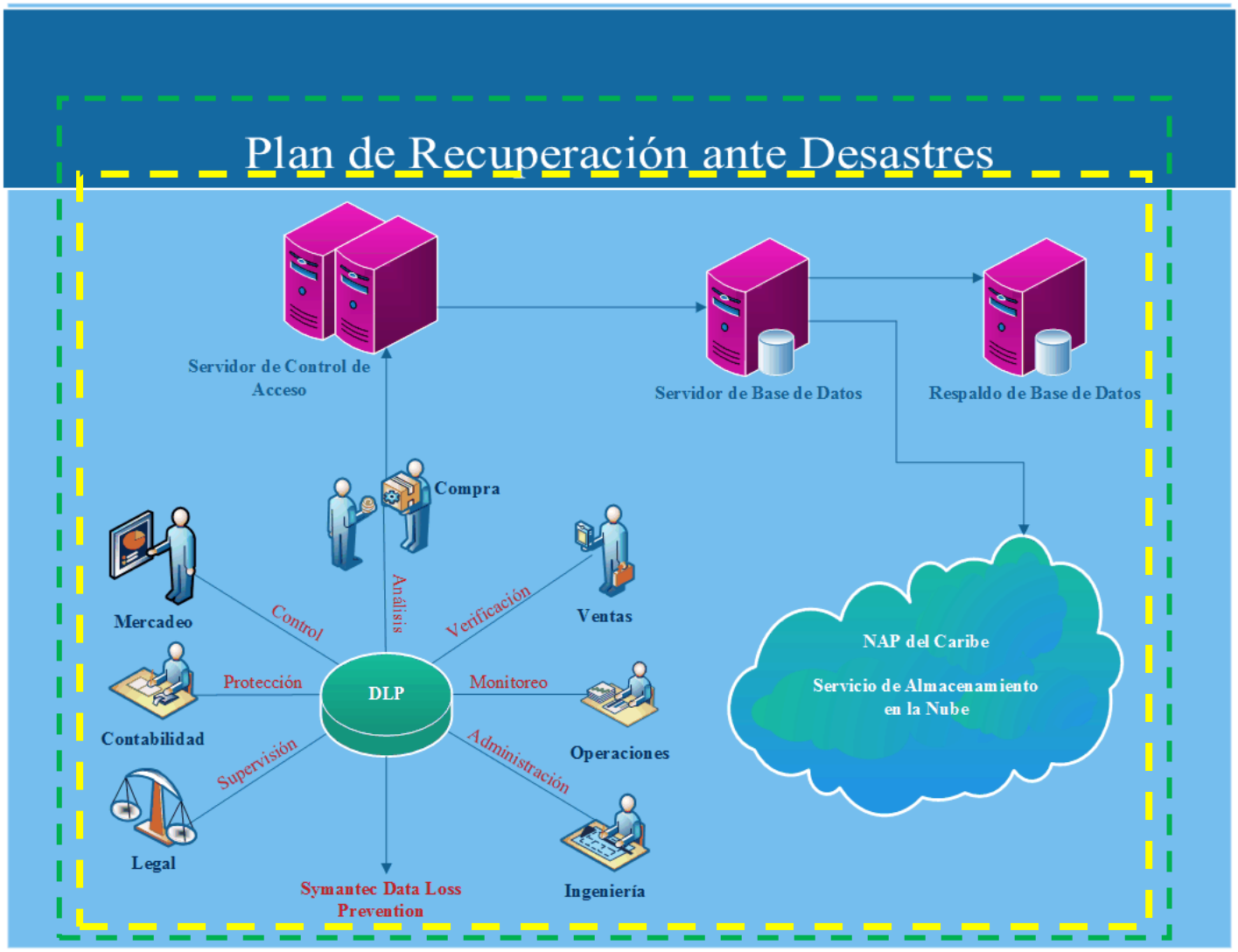

Figura 1.1 Esquematización de la investigación. Fuente: Fuente Propia

5. Justificación

De acuerdo con el más reciente Informe Global sobre Fraude de Kroll 2011, la mitad de las compañías se sienten muy vulnerables al robo de información, y en aquellas que tienen más pérdidas por fraude, los autores más probables fueron ejecutivos de alto nivel o ejecutivos menores. Afirman que la mayor incidencia en el robo de información y datos electrónicos ocurre en las empresas financieras (29%); de tecnología, medios y telecomunicaciones (29%); salud, farmacéuticas y biotecnología (26%); y servicios profesionales (23%). Asimismo, en 28% de las compañías afectadas por fraude, los autores más probables de estos fueron ejecutivos menores, en tanto que en otro 21% fueron empleados de nivel gerencial.

En CAM INC, se han recibido reportes por parte del 12% de los clientes donde el denominador común es que sus datos están siendo usados y divulgados sin autorización previa, lo que podría dar paso al phishing, fraude u hostigamiento, todos estos, delitos informáticos que consisten en aprovechar fallas en la protección de información confidencial para fines delictivos. Además, la organización mensualmente pierde el 14,4% de la información almacenada, lo que representa pérdidas monetarias y pone en cuestionamiento su reputación.

5.1. Justificación Teórica

Mediante la aplicación teórica y procedimental de una herramienta que ofrezca soluciones para la gestión de datos, esta investigación busca supervisar y administrar la pérdida de información en CAM INC, y a su vez establecer controles de acceso para la obtención de la misma.

De igual modo, se busca describir los procesos que soportan el manejo de la información, cómo garantizar su integridad y de qué forma responder ante cualquier contingencia.

5.2. Justificación Metodológica

Para realizar los objetivos de dicha investigación se agotaran técnicas que apoyen el análisis de la problemática que presenta la empresa CAM INC, y luego se suministrarán soluciones de gestión, protección y recuperación de datos de forma satisfactoria.

Por otra parte, permitirá la recolección de datos, se procesarán y se obtendrá la información pertinente para la redacción de informes.

5.3. Justificación Práctica

La utilización de medios informáticos en la actualidad representa un recurso imprescindible para las empresas y su desarrollo. Este recurso a medida que avanzan los tiempos se ha convertido en una necesidad inherente del mundo organizacional.

El fin práctico fundamental de la investigación es la implementación de una herramienta de gestión de seguridad que les permita a los encargados de la tecnología de información proteger y controlar toda la información vital que maneja la empresa.

La implementación de dicha herramienta, le brindara a CAM INC, los siguientes beneficios:

- ✓ Una plataforma para la administración de flujo de trabajo, de reparación y políticas, y revisión de incidentes.
- ✓ Supervisión de los puntos de salida, Endpoint y dispositivos, para evitar poner en peligro los datos confidenciales.
- ✓ Protección de los datos confidenciales mientras se transfieren del recinto de la organización a la nube.
- ✓ Supervisión y protección de los datos utilizados en equipos portátiles y escritorios cuando los usuarios están dentro y fuera de la red.

6. Tipo de Investigación

Según la naturaleza de la información que va a presentar en la investigación y a fin de llevar a cabo el desarrollo de esta monografía, serán utilizados los siguientes tipos de investigación:

a) **Explicativa:** Busca mostrar las relaciones de causa-efecto de los problemas que pueden presentarse al no poseer una logística adecuada para la protección de la información ante la ausencia de un sistema de seguridad informática.

b) **Cualitativa:** La investigación se define como cualitativa debido a que responde al proceso y fases establecidas para la misma. Dichas fases son: definición del problema, diseño del trabajo, análisis e informe.

c) **De Campo:** El estudio está delimitado como investigación de campo, debido a que constituye un proceso sistemático, riguroso y racional de recolección, tratamiento, análisis y presentación de datos, basado en una estrategia de recolección directa de la realidad de las informaciones necesarias para la investigación, con enfoque cualitativo y perspectiva descriptiva.

7. Marcos de Referencia

7.1. Marco Teórico

La seguridad de la información tiene como fin la protección de la información y de los sistemas de una amplia variedad de amenazas, como por ejemplo: acceso, uso, divulgación, interrupción o destrucción no autorizada. Su protección tiene como objeto asegurar la continuidad del negocio, minimizar los riesgos (combinación de la probabilidad de ocurrencia de un evento y sus consecuencias) y maximizar el retorno de la inversión y las oportunidades (Leonardo Ramos, 2009).

La seguridad de la información es una secuencia de pasos continuos de mejora donde intervienen factores como las políticas de privacidad y seguridad, confidencialidad y controles establecidos para proteger la información de cualquier riesgo de pérdida, robo o alteración. Dichos factores deberán revisarse, modificarse y adecuarse ante las nuevas amenazas que se puedan generar, con el objetivo de tomar las medidas necesarias para reducirlas y en el mejor de los casos eliminar por completo los riesgos.

Es así como las medidas de prevención ante pérdida de información y acceso a los datos han cobrado mucho más importancia en las organizaciones.

McAfee publicó recientemente un análisis sobre la problemática de la pérdida de datos de empresas causada por la violación de sistemas de seguridad informáticos. De acuerdo al estudio, Pérdida de Datos por los Números *(*siglas en inglés: *Data Loss by the Numbers*), la persistencia del problema del robo de datos está garantizada por el hecho de que la información es valiosa para propósitos legítimos, en este caso la actividad empresarial.

Entre los severos perjuicios económicos que significan para las empresas la pérdida o destrucción de datos se destacan:

- Daño a la marca y pérdida de confianza de los accionistas.
- Costos legales, demandas colectivas y costos de relaciones públicas.
- Costos por multas y por notificación a los afectados.
- Costos por monitoreo de créditos y por bienes y servicios para retener a clientes.
- Suspensión de los servicios, investigaciones de seguridad y pérdida de clientes e ingresos.

La pérdida de datos es una de las problemáticas más importantes en una empresa. Día tras día se crean y modifican muchos datos, archivos y ficheros como parte de los procedimientos que dan soporte a las actividades. La vulnerabilidad ante la pérdida de datos es un riesgo al que se está expuesto de forma inevitable.

7.2. Marco Conceptual

Informática

Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.[30]

Sistema

Un sistema es un conjunto de componentes que interaccionan entre sí para lograr un objetivo común. Aunque existe una gran variedad de sistemas, la mayoría de ellos pueden representarse a través de un modelo formado por cinco bloques básicos: elementos de entrada, elementos de salida, sección de transformación, mecanismos de control y objetivos.[31]

Dato

Un dato es una información breve y concreta que representa una condición o situación de un sujeto o idea más amplia. El dato es una representación simbólica (numérica, alfabética, algorítmica, etc.) de un atributo o variable cuantitativa. Los datos describen hechos empíricos, sucesos y entidades.[32]

---

[30] Definición de informática en el Diccionario Real Academia de la Lengua Española.
[31] Alarcón, Vicenc Fernández. Desarrollo de Sistemas De Información. 2006. Universidad Politécnica de Catalunya, SL.
[32] Corrales, Juan Desongles. Conocimientos Básicos de Informática. 2006. España. Mad, S.L.

Información

La información es un conjunto de datos acerca de algún suceso, hecho, fenómeno o situación, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo.[33]

Base de Datos

Un sistema de bases de datos es básicamente un sistema computarizado para llevar registros. Es posible considerar a la propia base de datos como una especie de armario electrónico para archivar, es decir, es un depósito o contenedor de archivos de datos computarizados.[34]

Tecnología

Conjunto de conocimientos y técnicas aplicadas de forma lógica y ordenada que le permiten al ser humano cambiar su entorno material o virtual para satisfacer sus necesidades. Es un proceso combinado de pensamiento y acción con la finalidad de generar soluciones que sean útiles.35

[33] Promonegocios. (2008). http://www.promonegocios.net/mercadotecnia/que-es-informacion.html
[34] Date & Ruiz Faudón. (2001).
[35] Que es la tecnología? http://quees.la/tecnologia/

Tecnología de la Información

Es toda herramienta y método empleado para recabar, retener, manipular o distribuir información. La tecnología de la información se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.[36]

Seguridad Informática

Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.[37]

Seguridad de la Información

La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.[38]

---

[36] Tecnología de información. http://www.tuobra.unam.mx/publicadas/040702105342-__191_Qu.html
[37] Gestión de riesgo en la seguridad de la informática. http://protejete.wordpress.com/gdr_principal/definicion_si/
[38] Asociación Española para la Calidad. http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

Confidencialidad

Servicio de seguridad o condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. También puede verse como la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.[39]

Privacidad

Derecho de mantener de forma reservada o confidencial los datos de la computadora y los que intercambia con su red.[40]

Integridad

Cualidad de la información que se considera exacta, completa, homogénea, sólida y coherente con la intención de los creadores de esos datos. Esta cualidad se obtiene cuando se impide eficazmente la inserción, modificación o destrucción no autorizada, sea accidental o intencional del contenido de una base de datos. La integridad de los datos es uno de los seis componentes fundamentales de la seguridad de la información.[41]

---

[39] Universidad Nacional Autónoma de México. http://redyseguridad.fip.unam.mx/proyectos/seguridad/ServConfidencialidad.php

[40] Privacidad y seguridad informática. http://www.slideshare.net/alu4albertde/privacidad-y-seguridad-informtica

[41] YourDictionary.com, http://computer.yourdictionary.com/dataintegrity

Amenaza

Todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.[42]

Riesgo

Incertidumbre existente por la posible realización de un suceso relacionado con una amenaza de daño respecto a los bienes o servicios informáticos, como equipos, periféricos, instalaciones, programas, etc.[43]

Vulnerabilidad

Debilidad en un sistema que permite a los atacantes violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.[44]

Respaldo de Información

[42] Universidad Nacional de Lujan. Departamento de Seguridad Informática. http://www.seguridadinformatica.unlu.edu.ar/?q=node/12
[43] Galeon.com. Riegos Informáticos. http://auditoriadesistemas.galeon.com/productos2223863.html
[44] Diccionario de informática. http://www.alegsa.com.ar/Dic/vulnerabilidad.php

Es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una avería electromecánica o un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar perdida generalizada de datos.

Almacenamiento en la Nube

Es un modelo de servicio en el cual los datos de un sistema de cómputo se almacenan, se administran, y se respaldan de forma remota, típicamente en servidores que están en la nube y que son administrados por un proveedor del servicio. Estos datos se ponen a disposición de los usuarios a través de una red, como lo es Internet.[45]

7.3. Marco Espacial

[45] About.com. http://aprenderinternet.about.com/od/La_nube/g/Almacenamiento-en-la-nube.htm

Este trabajo se llevara a cabo en la empresa de envío de valores y alimentos CAM INC, Santo Domingo, República Dominicana. Se ha tomado dicha empresa por las siguientes razones:

- Tiene pérdida de información.
- Tiene reportes de sus clientes con respecto a la duplicación y divulgación de sus datos sin autorización.
- No tienen una herramienta que les permita monitorear los ataques a su sistema y contrarrestarlos.
- No tienen control de acceso a sus datos.

Todas estas razones hacen más cómoda la plataforma para llevar a cabo delitos informáticos.

7.4. Marco Temporal

La investigación será realizada en un periodo aproximado de cuatro meses; iniciando en mayo y culminando en agosto 2014. Dicho periodo fue seleccionado porque coincide con la selección y entrega de los trabajos de grado.

8. Aspectos Metodológicos

8.1. Método

Para recolectar las informaciones necesarias en el desarrollo de la investigación se utilizaran los siguientes métodos:

a) **Método de Observación:** Se utilizará para visualizar de forma continua la situación actual en lo que respecta a la seguridad de la información, específicamente la perdida de datos dentro de la empresa a investigar.

b) **Método Deductivo:** Se partirá de premisas generales (lineamientos en los que se basa la seguridad de la información) hasta llegar a premisas particulares (implementación de una herramienta para prevención de pérdida de información).

c) **Método de Análisis:** Se utilizará este método para identificar cada una de las partes que se deben llevar a cabo al momento de asegurar la información que maneja la empresa.

8.2. Procedimientos

Luego de obtener las informaciones sobre el objeto de estudio aplicando los métodos ya mencionados anteriormente se procederá a definir los conceptos teóricos necesarios para conocer los fundamentos y características de los temas. Las definiciones se realizarán a partir de libros, sitios webs y documentos académicos en línea.

8.3. Técnicas

Las técnicas predominantes a lo largo de esta investigación serán la entrevista y los cuestionarios, usando como instrumento auxiliar, el fichaje.

Las entrevistas permitirán recopilar información de mano directa del gerente general y del encargado de TI de la empresa.

Los cuestionarios servirán para hacer una recopilación mixta de los datos y el fichaje permitirá tomar notas extras de forma informal de la información obtenida.

9. Tabla de Contenido

6.2. Desarrollo del Plan de Recuperación ante Desastres dentro de la empresa CAM INC.

6.2.1. Objetivos del Plan de Recuperación ante Desastres dentro de CAM INC.

6.2.2. Organización de equipos

6.2.2.1. Equipo de Respuesta a Emergencias

6.2.2.2. Equipo de Recuperación

6.2.2.3. Equipo de Coordinación Logística

6.2.2.4. Equipo de Relaciones Públicas

6.2.2.5. Equipo de Unidades de Negocios

6.2.3. Evaluación de Riesgos y Análisis de Impacto

6.2.3.1. Gestión y Evaluación de Riesgos

6.2.3.1.1. Identificación de Amenazas

6.2.3.1.2. Evaluación de Vulnerabilidades

6.2.3.1.3. Evaluación de Riesgos

6.2.3.1.4. Evaluación de Contramedidas

6.2.3.2. Análisis de Impacto en CAM INC

6.2.4. Desarrollo de Estrategias

6.2.4.1. Estrategia de procesamiento de la información mediante computación y almacenamiento en la nube (Cloud Computing and Storage Computing).

6.2.4.2. Estrategia de Preparación de un Warm Site

6.2.4.3. Costes Financieros de Implementación de Estrategias

6.2.5. Acciones del Plan de Recuperación ante Desastres

6.2.5.1. Respuesta ante Desastres

6.2.5.2. Transición

6.2.5.3. Recuperación

6.2.5.4. Restauración

6.2.5.5. Vuelta a la normalidad

6.3. Ensayo o diseño de pruebas del Plan de Recuperación ante Desastres

6.3.1. Tipos de Pruebas

6.4. Mantenimiento del Plan de Recuperación ante Desastres

- **CONCLUSIONES**
- **RECOMENDACIONES**
- **GLOSARIO**
- **BIBLIOGRAFÍA**
- **ANEXOS**

10. Fuentes de Documentación

10.1. Fuentes Primarias

- ✓ Entrevista al gerente general de CAM INC: Ing. Junior Raccini

- ✓ Entrevista al encargado de TI de CAM INC: Ing. Edward TSema

10.2. Fuentes Secundarias

Libros especializados:

- Rodríguez Prieto, A. (2006). Protección de la información. Diseño de criptosistemas informáticos. Madrid, Paraninfo. ISBN 84-283-1434-9.

- Vieites Gómez, A. Enciclopedia de la Seguridad Informática. Editorial Alfaomega. México. ISBN 978-970-15-1266-1.

- Pérez Cleto, C. A & De los Santos, M. (2009). Implementación de un plan de recuperación de desastres. Tesis de Grado No Publicada, Universidad APEC.

- Daltabuit, E. (2007). La seguridad de la información. México, Limusa.

10.3. Otras fuentes:

- Cappiello, Hernán (23 de Febrero 2012). La invisibilidad de las pruebas de corrupción. Recuperado de http://www.lanacion.com.ar/1450864-la-invisibilidad-de-las-pruebas-de-corrupcion

- Santiago Quevedo, Carlos María (2007, 16 de diciembre). Tecnología y algo más. Recuperado de http://csantiagoeljurista.blogspot.com/2007/12/realidad-de-los-delitos-informticos-en.html

- Antigua, magnolia (2011, 12 0ctubre). Departamento de investigación de crímenes de alta tecnología. Recuperado de http://www.slideshare.net/magnoliaantigua/departamento-investigaciones-de-crimenes-de-alta-tecnologia-5ta

- Basualdo, Cristian (2011). Delitos informáticos. Recuperado de http://crimenescyberneticos.blogspot.com/p/pericia-informatica.html

- Guess (2009, 19 de junio). El Cibercrimen y delitos informáticos. Recuperado de http://www.slideshare.net/guest225f3bd/el-cibercrimen-y-delitos-informaticos

- J, R. (2005). Cibersociedad, Tecnologia de la Informacion y La Comunicacion. Recuperado de http://www.cibersociedad.net/archivo/articulo.php?art=218

- Salazar, C. (2008). Cibermundos, La TIC como herramienta a la gestion empresarial. Recuperado de http://cibermundos.bligoo.com/content/view/145501/Las-TIC-como-herramienta-a-la-gestion-empresarial.html.

ANEXO II

Cuestionario Seguridad de la Información

1. ¿Están sufriendo pérdidas de datos en la empresa?
2. En caso de tener, ¿Con qué frecuencia ocurren estas pérdidas de datos?
3. ¿Quiénes tienen acceso a los datos?
4. ¿Qué políticas de acceso a la información tiene la empresa?
5. ¿Qué políticas de seguridad de la información tiene la empresa?
6. ¿Tienen respaldo de datos?
7. En caso de tener, ¿Con qué frecuencia se hacen dichos respaldos?
8. ¿Tienen plan de recuperación ante desastres?
9. ¿Tienen equipos de emergencia?
10. ¿Cuándo fue la última vez que la empresa se vio afectada por una de las siguientes amenazas? Asigne un valor del 1 al 5 para las frecuencias.

    Donde 1 = casi nunca 5 = muy frecuente

    - Terrorismo
    - Terremotos
    - Inundaciones
    - Ataques Humanos/Huelgas
    - Incendio
    - Virus

ANEXO III

Cuestionario BIA

1. ¿Cuáles son los procesos de negocio de CAM INC?
2. ¿Cuánto tarda en horas recuperar el trabajo atrasado?
3. ¿Cuál es el plazo en horas para la recuperación de los procesos que se han interrumpido?
4. Haga una valoración del impacto operacional de la interrupción de esos procesos.
5. ¿Cuáles son las dependencias internas y externas?
6. ¿Cuáles son las aplicaciones informáticas que soportan dichas dependencias?
7. ¿Cuáles son los procedimientos alternos o sugeridos que tienen?
8. ¿Tienen registros de cada proceso?
9. ¿Cuáles son los recursos mínimos para la recuperación de cada dependencia?

ANEXO IV

Nombre	
Departamento	
Puesto	
Correo electrónico	
Fecha	

En la siguiente tabla, complete la información solicitada según los procesos que usted maneja:

Proceso	***Subproceso***	***Descripción***	***Frecuencia de uso***	***Nombre de responsable y puesto***