|INTRODUCCIÓN

Se analizara la problemática de Lutexsa Ind. Com. Cía. Ltda., con los repetidos eventos delincuenciales que han sido victima los funcionarios y las oficinas remotas ubicadas en todo el Ecuador. Se ven en la imperiosa necesidad de diseñar un plan tecnológico y aseguramiento de la información que permita que estos eventos tengan el menor impacto en el negocio.

El presente análisis se lleva a cabo tomando en consideración el aspecto tecnológico, seguridad de la información, intereses de la compañía, servicios, crecimiento, clientes, problemas y situaciones de riesgo identificadas partiendo de eventos ocurridos y reportados a las autoridades policiales.

La aplicación de Normas ISO, ITIL, COBIT entre otras más conlleva a realizar un análisis de políticas que deben ser implantadas en la organización previo análisis vialidad, factibilidad, pruebas de laboratorio, borradores, toma de tiempos de procesos en otros procesos adicionales que serán detallados en el desarrollo del presente.

Para este fin se debe de analizar la problemática que ataca a nivel país, empresas nacionales, empresas multinacionales, empresas públicas, empresas privadas y sus distintas variantes que podrían ser violentadas y lo que esto acarrea a las mismas.

Actualmente las leyes Ecuatorianas están tomando en consideración a los crímenes informáticos y se suman artículos en el COIP para estos casos que tienen connotación legal y considerado delitos graves.

CAPITULO I

1. DISEÑO DE LA INVESTIGACIÓN

1.1. ANTECEDENTES DE LA INVESTIGACIÓN

El presente análisis se lleva a cabo tomando en consideración el aspecto tecnológico, seguridad de la información, intereses de la compañía, servicios, crecimiento, clientes, problemas y situaciones de riesgo.

Para este fin se debe de analizar la problemática que ataca a nivel país, empresas nacionales, empresas multinacionales, empresas públicas, empresas privadas y sus distintas variantes que podrían ser violentadas y lo que esto acarrea a las mismas.

Actualmente las leyes Ecuatorianas están tomando en consideración a los crímenes informáticos y se suman artículos en el COIP para estos casos que tienen connotación legal y considerado delitos graves.

Se analiza los casos suscitados para iniciar un detallado análisis, en donde se podrá determinar los niveles críticos de la información que manejan los usuarios en sus equipos tomar acciones que permitan que la información confidencial tenga la respectiva seguridad, integridad, disponibilidad que la información necesita, para esto se debe realizar cuadros de diagnóstico que guía a realizar procesos, políticas y procedimientos.

Realizar las respectivas pruebas de laboratorio, antes de su puesta en producción, determinar responsabilidades para llegar al fin del proceso sin dejar a un lado la retroalimentación. En la actualidad es primordial para las empresas asegurar la continuidad de sus negocios, almacenando toda la información clave en un ambiente que proporcione las condiciones tecnológicas para su seguridad, recuperabilidad y para operar sin interrupciones, ni pérdidas de tiempo.

Por tal motivo, las empresas están cada día más interesadas en los Centros de Procesamiento de Datos (CPD). El tener la información y las aplicaciones más

esenciales siempre disponibles se convierte entonces en la principal función de los Centros de Datos, por lo tanto, ya no son sólo un centro de recolección donde se acumulan cientos de megas de datos, sino que su misión es tener dicha información en constante funcionamiento.

Es preciso señalar, que la información es el activo más importante con que cuentan las compañías, ya que sin ella, éstas no pueden funcionar.

Asegurar a información que permanece en los centros de datos va más allá de protegerla ante posibles amenazas externas. Se trata más bien, de garantizar niveles de servicio que permitan obtener información cuando se necesite, es decir, que esté disponible las 24 horas del día durante los 7 días de la semana.

Hoy, un aspecto relevante para certificar la disponibilidad de los datos, es contar con planes de continuidad correctos, como por ejemplo, los de recuperación de desastres, ya que pueden facilitar la solución a dificultades para que las organizaciones puedan seguir funcionando ante cualquier amenaza, manteniendo así su continuidad y evitando cuantiosas pérdidas.

A esto se suma, el factor humano que es esencial para el resguardo de la información, es decir, contar con personal capacitado y con procedimientos establecidos basados en las normas internacionales, como por ejemplo,

La ISO 17799 y la ISO 27001, que son una guía empresarial para mantener de forma segura la información de los Centros de Datos.

La aplicación de Normas ISO, ITIL, COBIT entre otras más conlleva a realizar un análisis de políticas que deben ser implantadas en la organización previo análisis vialidad, factibilidad, pruebas de laboratorio, borradores, toma de tiempos de procesos en otros procesos adicionales que serán detallados en el desarrollo del presente.

Se analizará la problemática de Lutexsa Ind. Com. Cía. Ltda. con los repetidos eventos delincuenciales que han sido victima los funcionarios y las oficinas remotas ubicadas en todo el Ecuador. Se ven en la imperiosa necesidad de diseñar un plan tecnológico y aseguramiento de la información que permita que estos eventos tengan el menor impacto en el negocio.

En la empresa LUTEXSA IND. COM. CIA. LTDA teniendo en cuenta el auge que ha tenido los centros de datos y la importancia que representa tener su información almacenada en un lugar seguro.

Surge la necesidad, de describir un procedimiento que brinde una idea de las etapas por las cuales se debe transitar para garantizar de forma adecuada un almacenamiento y salva de la información en un CPD.

Teniendo en cuenta lo anteriormente planteado surge como **problema científico** la siguiente interrogante: ¿Cómo garantizar un adecuado proceso de almacenamiento y salvas en los Centros de Procesamiento de Datos?

El **Objeto de Estudio** de esta investigación está dirigido a los procesos de almacenamiento y salvas de la información.

El **Campo de Acción** queda enmarcado en los procedimientos y técnicas utilizadas para el almacenamiento y salvas en los centros de procesamiento de datos.

Se persigue como **Objetivo General** elaborar un procedimiento que brinde una guía para llevar a cabo los procesos de almacenamiento y salva de la información en centros de procesamiento de datos.

1.2. PROBLEMA DE LA INVESTIGACIÓN

1.2.1. PLANTEAMIENTO DEL PROBLEMA

El incremento de pérdida de información es un hecho real y es reflejada en pérdida de eficacia al momento de requerirla.

El descontrol de flujo de información que no cumple con sus respectivas regularizaciones afecta a la disponibilidad e integridad de toda la información que se maneja en la empresa.

El robo de los equipos tecnológicos portátiles son los hechos más relevantes y continuos, en las oficinas remotas que no cuenta con un sistema de respaldo de información todo nos conlleva a solucionar el problema

No se cuenta con la información debidamente resguardad y con la debida integridad que debe tener la data de la empresa.

Actualmente no existe información que sea correctamente segregada, diferenciada llamando a problemas de orden al momento de poner criterios de respaldo, se respalda información no relevante para la empresa.

No se cuenta con el debido aseguramiento de la información tomando en cuentas los diversos eventos delincuenciales que podrían darse con los equipos que tienen información valiosa, critica, confidencial.

Conllevaría a no poder ser productivos al momento de contar con la información que permita tomar las decisiones correctas en los momentos correctos.

No se podría tener la disponibilidad de poder rescatar la data de los usuarios y mucho peor no contar con la información de los usuarios críticos de la compañía.

1.2.2. FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN.

¿Cómo incide la falta de seguridad de la información en las sedes remotas en Lutexsa Com. Cía. Ltda.?

1.2.3. SISTEMATIZACIÓN DEL PROBLEMA DE INVESTIGACIÓN.

¿Afecta a la organización no contar con la información?

¿Está expuesto al no tener precautelada la información crítica de la empresa?

¿Pierde la empresa por la información de la empresa que no fue debidamente respalda en caso de un evento no controlado?

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. OBJETIVO GENERAL

Proponer la mejor practica informática para salvaguardar la información en las sedes de la organización considerando su criticidad.

1.3.2. OBJETIVOS ESPECÍFICOS

- ✓ Analizar las mejores prácticas para realizar respaldos de información de la empresa Lutexsa Ind. Com. Cia. Ltda.
- ✓ Establecer mediante pruebas de éxito de laboratorio los procesos correctos para realizar los respaldos de las sedes remotas de la empresa.
- ✓ Proponer políticas de tecnología para el respaldo de la información de la sedes determinando de manera efectiva las personas involucradas en el procedimiento, documentar, dejar por aprobado la documentación para su divulgación.
- ✓ Plantear procedimientos para realzar el exitoso respaldo hasta llegar al final del proceso y registrarlo para evidenciar lo realizado por el responsable en los procesos documentados.

1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN.

Se propone el aseguramiento de la información de la compañía que conlleva a realizar todos los análisis necesarios, el aseguramiento mitiga problemas a tan ínfimos como tan críticos en la continuidad de la operación sin dejar a un costado la salud económica de una empresa de comercialización de combustibles ya que toda la información vital es digitalizada y responde a procesos de automatizaciones que no deben de dejarse de asegurar.

Debido a la falta de procedimiento de salva o resguardo de información que no es actualizados, renovados y sobre todo certificados.

Porque cada proceso debe tener su continua modificación por los entes correspondientes para que sea efectivo el mismo, llámense departamento de control, departamento de calidad, departamento de aseguramiento, departamento de auditoria.

Para contar con todo el aseguramiento y poder cumplir con las características necesarias que debe tener toda información en una organización que desea tener asegurada y en buen recauda lo más crítico, la información.

1.5. MARCO DE REFERENCIA DE LA INVESTIGACIÓN

1.5.1. MARCO TEÓRICO

En su forma más simple un plan estratégico es una herramienta que recoge lo que la organización quiere conseguir para cumplir su misión y alcanzar su propia visión. Entonces ofrece el diseño y la construcción del futuro para una organización, aunque éste futuro sea imprevisible (Gestion empresarial, 2013).

El plan estratégico define también las acciones necesarias para lograr ese futuro. Entonces dicho plan es una apuesta de futuro y por eso, se adecua a un postulado de Ackoff R (1981), un gurú de planificación estratégica: El futuro no hay que preverlo sino crearlo. El objetivo de la planificación debería ser diseñar un futuro deseable e inventar el camino para conseguirlo.

Según el autor Sainz De Vicuña (2012), al hablar del plan estratégico de la organización, nos estamos refiriendo al plan maestro en el que la alta dirección recoge las decisiones estratégicas corporativas que ha adaptado “hoy” en referencia a lo que hará en los tres próximos años (horizonte más habitual del plan estratégico), para lograr una organización más competitiva que le permita satisfacer las expectativas de sus diferentes grupos de intereses (stakeholders).

Lumpkin y Dess (2003) entienden por plan estratégico el conjunto de análisis, decisiones y acciones que una organización lleva a cabo para crear y mantener ventajas comparativas sostenibles a lo largo del tiempo. Brenes Bonilla (2003) define el plan estratégico de manera similar considerándolo como el proyecto que incluye un diagnóstico de la posición actual de una entidad, la(s) estrategia(s) y la organización en el tiempo de las acciones y los recursos que permitan alcanzar la posición deseada.

Para Martínez Pedrós y Milla Gutiérre (2005) un plan estratégico es un documento que sintetiza a nivel económico-financiero, estratégico y organizativo el posicionamiento actual y futuro de la empresa y cuya elaboración nos obligará a plantearnos dudas acerca de nuestra organización,

de nuestra forma de hacer las cosas y a marcarnos una estrategia en función de nuestro posicionamiento actual y del deseado.

Haciendo un recorrido por definiciones de diversos autores, nos encontramos con elementos comunes que nos acercan en mayor medida a la idea de plan estratégico. Estos elementos son: está el concepto de un entorno, es decir, una serie de condiciones ajenas a la organización, a las que ésta debe responder. Algunas de estas condiciones son negativas (amenazas) y otras positivas (oportunidades). Para conocer estas condiciones, se debe llevar a cabo un análisis del entorno. También la gerencia debe realizar un análisis de la situación actual, con el fin de determinar su posición en el entorno y su cantidad de recursos y reconocer sus debilidades y fuerzas. Además, la organización debe poseer la imagen de su futuro (visión) y establecer metas u objetivos estratégicos básicos. El objetivo de más alto nivel se suele conocer como la misión. Por último la organización proyecta como aplicar sus recursos y describe los programas de acción a largo plazo (estrategias), que determinan los objetivos estratégicos de desarrollo de dicha organización y que muestran cómo lograrlos en forma de objetivos operacionales y tareas a realizar específicas.

¿Por qué desarrollar un plan estratégico?

La respuesta a esta pregunta, aparentemente fácil, ha creado bastante controversia entre los autores.

Una de las opiniones más extendidas es que el desarrollo de un plan estratégico produce beneficios relacionados con la capacidad de realizar una gestión más eficiente, liberando recursos humanos y materiales, lo que redunda en eficiencia productiva y en una mejor calidad de vida y de trabajo para los miembros de la organización (Lopez, 2000).

La finalidad del plan estratégico consiste en definir los objetivos y cuáles son las mejores acciones que deben llevarse a cabo para alcanzar dichos objetivos. De esta manera se facilita la gestión de la organización al hacerla más transparente, asignar políticas concretas a los diversos sectores implicados y

permitir la evaluación en función del cumplimiento de las actuaciones especificadas. Esto genera coherencia entre las acciones que se realizan y las expectativas de la dirección, poniendo a la organización en relación con las necesidades del entorno.

En concreto, el asunto más importante para llevar a cabo un plan estratégico está muy directamente relacionado con la mejora de resultados de la organización. Además, el plan estratégico permite a la organización una gestión más profesional y menos basada en improvisaciones porque:

1. Permite conocer mejor la realidad de la organización.
2. Permite identificar los cambios y desarrollar que se puede esperar.
3. Permite pensar en el futuro, visualizar nuevas oportunidades y amenazas.
4. Permite preparar al futuro, aunque sea impredecible.
5. Permite enfocar la misión de la organización y orientar de manera efectiva su rumbo.
6. Permite plantear la estrategia y pilotarla y evaluarla correctamente.
7. Permite mejorar la coordinación de las actividades.
8. Permite mejorar manejo de recursos.
9. Permite medir el impacto futuro de las decisiones estratégicas que se toma hoy.
10. Permite mantener un enfoque sistémico.

Un plan estratégico debe ser congruente con la cultura de la organización. Estos dos conceptos no deben ser analizados de forma independiente, sino recogiendo en todo momento su interrelación, ya que el éxito o fracaso de un plan estratégico puede depender en gran medida de la relación entre la cultura y el plan estratégico.

Los dos elementos constituyen un sistema de las relaciones dependientes uno de otro. Por un lado, el plan estratégico destaca las direcciones de desarrollo de la cultura organizacional, que significa que la cultura organizacional está estratégicamente orientada (cultura estratégica). Por otro lado, la cultura que ya está el plan estratégico está culturalmente orientado. Además, el plan

estratégico para ser realizado y lograr sus objetivos, depende de que la cultura lo favorezca o lo permita, si el plan estratégico no permite desarrollar y potenciar a la cultura resulta imposible que se logren los resultados esperados.

Otras ventajas derivadas de la concordancia entre el plan estratégico y la cultura organizacional pueden ser las siguientes:

- los miembros de la organización comprenden la misión y la estrategia y se sienten identificados con ellas y, además, identifican los objetivos básicos de la organización; se involucran más en la realización del plan estratégico,
- existe mayor integración con los objetivos de la organización,
- se pueden pre-formular los objetivos y la cultura si es necesario cambiarlos.

Estos y otros efectos que pueden ser directos o indirectos en cualquier caso necesitan ser comprendidos y administrados a los efectos de conducir un proceso de planificación estratégica exitoso y asegurar que de ese proceso surja un plan estratégico útil. Pero esto requiere que dicho plan tenga en cuenta la cultura y los elementos estratégicos que la componen.

LA INFORMACIÓN ES MUY VALIOSA PARA LAS EMPRESAS (Symantec Corporation, 2012)**.**

Los encuestados dicen que Información = 50% la del valor total de una organización

¿Qué tan valiosa es la información? de acuerdo con las respuestas que dieron 500 profesionales de ti en américa latina, aproximadamente 50 por ciento del valor de sus organizaciones deriva de la información que poseen.

Las consecuencias de perder toda o parte de su información podría ser devastador para las empresas. Cuando se les preguntó a los encuestados qué ocurriría si la información de su empresa se perdiera irremediablemente sin posibilidad de recuperarla, las respuestas incluyeron pérdida de clientes (55 por ciento), daño a la marca (50 por ciento), menores ingresos (40 por ciento) y multas (32 por ciento).

A pesar de la importancia de la información para las organizaciones de todos los tamaños y el dinero que gastan en Administrarla, los ejecutivos de TI aún enfrentan múltiples desafíos.

Por un lado, está la cuestión de los datos duplicados. Las empresas en América Latina estiman que en promedio hasta 45 por ciento de su información está duplicada.

Otro desafío es que, de acuerdo con la encuesta, las organizaciones tienen índices de uso de almacenamiento bastante bajos — 32 por ciento dentro del firewall y aún menos (20 por ciento) fuera de él.

Quizás una preocupación mayor en este sentido sea la pérdida de datos. Cuatro de cinco empresas en América Latina manifestaron haber perdido información importante en los últimos 12 meses por causas tales como errores humanos, falla de hardware o software y pérdida o robo de dispositivos móviles.

Casi tres cuartos han experimentado la exposición de información confidencial importante fuera de la organización, y un tercio ha enfrentado cuestiones de cumplimiento normativo en el último año. Una de cada tres organizaciones señaló que el crecimiento de la información es un factor importante cuando sucede algún imprevisto o pérdida de datos.

CUIDANDO LA INFORMACIÓN

Afortunadamente, las organizaciones pueden atender estos desafíos tomando medidas para construir un modelo de TI centrado en la información. Symantec sugiere un enfoque basado en cinco aspectos.

Enfocarse en la información, no en el dispositivo o centro de datos:

El primer paso es enfocarse en construir una infraestructura de información que optimice la capacidad de la organización de encontrar, acceder y consumir

Información crítica del negocio. Hoy, muchas empresas están en esta fase, adoptando tecnologías tales como la virtualización, el cómputo en nube y los dispositivos y aplicaciones móviles.

Para completar el proceso, las empresas deben integrar soluciones de protección de información que funcionen en toda la infraestructura, desde entornos físicos y virtuales hasta la nube y dispositivos móviles. Esto incluye disposiciones de seguridad, respaldo, administración de almacenamiento, disponibilidad y gestión de endpoints.

No toda la información es igual:

Las organizaciones deben entender completamente su información. La encuesta arrojó que muchas organizaciones carecen incluso de conocimientos básicos tales como quién posee determinada información, cuán importantes son los datos o incluso si su naturaleza es personal o comercial. Mediante el mapeo y clasificación de la información, las organizaciones pueden descubrir su valor relativo. Esto facilita priorizar los recursos de seguridad,

Protección y manejo de modo que las empresas puedan hacer foco en la información que realmente les importa.

Ser eficiente: La deduplicación y el archivado ayudan a las empresas a proteger más pero almacenar menos para seguirle el ritmo al crecimiento exponencial de datos.

Mantener coherencia: Es importante establecer políticas de información coherente y consistente que puedan cumplirse sin fracasar dondequiera que los datos se encuentren... en entornos físicos, virtuales y/o en la nube. Tal esfuerzo unifica la clasificación de información, automatiza el descubrimiento de quién posee y utiliza determinada información, controla el acceso y la distribución, automatiza la retención y eliminación de información, y acelera el proceso de eDiscovery.

Ser ágil: Finalmente, hay que mantenerse ágiles y planear futuras necesidades de información implementando una infraestructura flexible que soporte el continuo crecimiento.

Implementando estas recomendaciones, las organizaciones pueden moverse hacia a un modelo de TI centrado en la información para proteger su información valiosa con la mejor relación costo-beneficio.

Reporte sobre el costo y manejo de la información empresarial 2012 (SYMANTEC, 2012)

El Reporte sobre el Costo y Manejo de la Información Empresarial 2012 es el primer estudio de Symantec que cubre desde la seguridad hasta el almacenamiento en la nube, virtualización y movilidad. Hoy en día la información es vital para las organizaciones y así lo confirmaron las empresas y los ejecutivos de TI de 4,506 organizaciones en 36 países, 500 de ellos de América Latina que participaron en el estudio y respondieron una serie de preguntas sobre este tema.

El Reporte sobre el Costo y Manejo de la Información Empresarial estará dividido en tres capítulos. El primero de ellos se enfoca en el verdadero valor, el costo y el crecimiento de la información digital. Las siguientes secciones se centrarán más en el comportamiento de la información y las personas. La tecnología evoluciona y también la forma en que la información está protegida, lo invitamos a que consulte en este espacio las principales conclusiones y conozca más sobre el mundo de la información digital.

Capítulo 1: El costo de la información

La información digital es más valiosa que nunca para las organizaciones. Piense en cuántas transacciones se realizan en línea, o la forma en que la colaboración virtual se lleva a cabo. Considere los grandes volúmenes de almacenamiento de datos de las empresas y cómo los datos se han vuelto fundamentales en las operaciones diarias.

Sin embargo, a pesar de la importancia de la información, muchas empresas y organizaciones se quedan cortas cuando se trata del manejo eficaz de este valioso recurso. Actualmente, es necesario que las empresas desarrollen un modelo "centrado en la información" que les ayude a resolver los retos actuales como el crecimiento exponencial de datos, la pérdida de información y el alto costo de almacenamiento.

Ecuador y Brasil firman memorando para luchar contra el crimen organizado (El universo, 2015)**.**

Representantes de los Ministerios Públicos de Brasil y Ecuador firmaron hoy en Brasilia un memorando para enfrentar el crimen organizado, en particular el tráfico ilegal de personas, de drogas, el lavado de activos y los ciberdelitos, informó hoy la Fiscalía General de Ecuador.

La Fiscalía ecuatoriana y la Procuraduría General de Brasil ratificaron también con este acuerdo su responsabilidad a la hora de luchar para evitar la impunidad en graves violaciones a los derechos humanos.

El fiscal general ecuatoriano y presidente de la Asociación Iberoamericana de Ministerios Públicos, Galo Chiriboga, agradeció la apertura de su homólogo brasileño para colaborar y fortalecer las investigaciones de los delitos trasnacionales y de casos en los que se requiera una asistencia internacional directa.

El procurador general brasileño, Rodrigo Janot, ratificó por su parte su colaboración con Ecuador a través del intercambio de experiencias positivas.

El memorando se basa en el Acuerdo para Incentivar la Cooperación y Asistencia Legal Mutua entre los Integrantes de la Asociación Iberoamericana de Ministerios Públicos, suscrito en diciembre del 2003, según un comunicado de la Fiscalía General de Ecuador.

Chiriboga aprovechó la ocasión para reiterar la invitación a su par brasileño para la XXIII Asamblea General Ordinaria de la AIAMP, que se celebrará en Santa Cruz de la Sierra, Bolivia, entre el 28 y 30 de octubre. (I)

El ciberdelito ataca al sector público, (El comercio, 2010)**.**

La página web de la Policía Nacional del Ecuador fue profanada por un grupo de hackers de Oriente Medio. En el portal inscribieron un mensaje: “Lo hicimos”. Gonzalo Arias, jefe de la Unidad de Investigación de Delitos de Tecnología de la Policía Judicial (PJ), refiere que los hackers querían dar a

conocer su capacidad para acceder, de forma ilegal, en páginas web institucionales. “Para ellos fue como un trofeo”. Ocurrió hace cinco años.

La intervención del portal es una de las ocho modalidades de delitos informáticos que se registran en el Ecuador. Los portales de la Presidencia de la República, el del desaparecido Tribunal Supremo Electoral y el del Ministerio de Energía también fueron intervenidos años atrás. Un estudio de la Escuela de Sistemas de la Universidad Católica del Ecuador (PUCE) revela que, entre mayo y junio de este año, 50 sitios fueron atacados: 15 eran de entidades públicas,12 de educativas, 15 de empresas privadas y ocho de otras organizaciones. Entre las instituciones oficiales vulneradas están los municipios de Nueva Loja, en Sucumbíos, y de Otavalo, en Imbabura. También el proyecto Yasuní ITT y el Psiquiátrico San Lázaro. Francisco Rodríguez, director de la Facultad de Sistemas de la Universidad Católica, dice que en Guayaquil fue identificado un grupo de hackers: los Latin Hack Team. El seguimiento hecho a esa mafia muestra que modifican sitios web de instituciones públicas y privadas; manipulan datos, y envían correos ‘maliciosos’.

La técnica que utilizan se llama desfiguración. Consiste en aprovechar la vulnerabilidad de los portales. “Reemplazan información de un sitio por la de otro. Ponen mensajes que en muchos casos son políticos”, dice Rodríguez. Santiago Acurio, director de Tecnologías de la Información de la Fiscalía, asegura que el ‘phishing’ también se incluye en esta lista de ataques y es la segunda modalidad del cibercrimen. Con esta técnica se suplanta la identidad de un sitio web por otro para extraer información de forma fraudulenta.

Ocurre con frecuencia con las cuentas bancarias. Los perjudicados por esta clase de delito ingresan a páginas similares a las originales, creadas por hackers, donde digitan toda la información personal. Se utilizan como enganche los correos electrónicos masivos. La página incluso muestra el diseño de las instituciones, con sus logos, para confundir a los usuarios. Según un estudio del laboratorio ruso Kaspersky, el 72% de servidores vulnerados por ‘phishing’ en Ecuador pertenece al sector público, el 21% al comercial y el 7%

al educativo. La tercera manifestación del ciberdelito en el país apunta a las transacciones financieras. El 11 de junio, el quiteño Wilmer S. hizo una transferencia bancaria de 2 800 dólares, vía Internet; pagó el alquiler de un local. Al finalizar la operación, verificó que en su cuenta había un saldo de 1 200 dólares, pero dos horas después acudió al cajero y se percató de que esa cifra había desaparecido: fue transferido a otra cuenta sin su autorización. “Esta es la forma típica de fraude informático”, dice Acurio. A esta se suma la alteración de bases de datos de bancos: personas que tienen acceso a información confidencial de cuentas de personas naturales y jurídicas y crean datos inexistentes en la información almacenada para robar (cuarta forma de delito). “Esa metodología es usada para cambiar contabilidad en empresas”, manifiesta Arias. “Hemos encontrado casos en los que la gente que trabaja en la institución hace un mal uso de las bases de datos. Hacemos peritajes de la alteración”. Acurio precisa que las personas que cometen este ilícito se llaman ‘insiders’. La quinta modalidad es la duplicación de tarjetas de crédito y débito (‘skiming’). “Hay dos clases: la falsificación electrónica (clonación) y el uso no consentido de una tarjeta”. Con la primera estrategia se duplica la información de la banda magnética de una tarjeta. Para la otra, se colocan dispositivos de lectura de las claves personales en los cajeros automáticos de los bancos. Los índices de delitos en línea se triplicaron en este año con relación al 2009 (ver cuadro adjunto). Desde enero hasta abril, la Fiscalía registró 146 denuncias de apropiación ilícita utilizando medios tecnológicos. El año pasado se registraron 168 (12 casos cada 30 días). La Policía detectó que el ciberdelito también encuentra réditos en la pornografía infantil (sexta manifestación), donde están involucradas organizaciones criminales internacionales. Un caso -refiere Arias- se dio con un grupo español que se suministraba pornografía infantil en Galápagos. La promoción del sicariato, de préstamos o de viajes (trata) en Internet es la séptima cara del cibercrimen. Interpol investiga estos casos, aunque agentes que operan en Ecuador reconocen dificultades, porque los grupos delictivos utilizan plataformas gratuitas como Yahoo!, Hotmail, Gmail, redes sociales (Facebook o MSN), blogs, etc. “Estos servidores están en el extranjero y es muy complicado concluir una investigación”, dice el jefe policial. La PJ coordina acciones con el personal de empresas como Microsoft. Frente

al incremento del delito, hace seis meses la Policía creó la Unidad de Investigación de Delitos de Tecnología de la PJ. Esta indaga, con 30 agentes, los orígenes, móviles y consecuencias de estos delitos. Rodríguez explica que la octava modalidad de ciberdelito es la compra de programas piratas. “Al adquirir un disco de juegos o paquetes informáticos, este regularmente tiene programas maliciosos. Eso provoca que en las máquinas se abran puertos por los que ingresan virus para extraer datos y contraseñas de la persona que instaló el software”. Para Acurio, el combate a estos ilícitos debe complementarse con una reforma al Código Penal. La propuesta -agrega- es adecuar la legislación de acuerdo con el Convenio del Cibercrimen de la Unión Europea, suscrito en el 2001. “Con esto se lograría estandarizar los tipos penales y el sistema procesal”. Además, acceder a las plataformas gratuitas para detectar a los infractores. El caso de Wilmer S. está en la Fiscalía. Tras la estafa de la que fue víctima, asegura que perdió la confianza en la entidad bancaria. Según la Policía, para evitar ser una cibervíctima, nunca se debe entregar información personal (como claves o números de tarjetas) por teléfono, por correo electrónico o en formularios abiertos en Internet. Solo deben usarse las cuentas encriptadas oficiales.

El crecimiento del cibercrimen en Ecuador es de un 130% (Freire, 2013)

Kaspersky Lab realizó una reunión de varios expertos de Argentina, Ecuador, Brasil, y México para revisar los avances y las nuevas tendencias o tecnologías utilizados por cibercriminales en Latinoamérica y el mundo.

Los principales temas abordados por expertos de Kaspersky Lab fueron las nuevas formas de ataque cibernético y como protegerse de las mismas. Adicionalmente se analiza como los nuevos proyectos de la empresa enfrentan dichas amenazas y como difundir de mejor manera las tecnologías de protección disponibles actualmente.

Dmitry Bestuzhev, Jefe del equipo de GReAT (Global Research and Analysis Team) para Latinoamérica y experto de Kaspersky, destacó que Brasil, Chile, Colombia y Panamá son los países con mayores cantidades de víctimas de ciberataques. "Lo interesante es que estos países son caracterizados en la

región por su creciente y estable economía. Esto comprueba una vez más que el objetivo de los atacantes en América Latina en este momento es el dinero", señaló.

Bestuzhev manifestó que el crimen cibernético se podría comparar como una plaga mundial, que está creciendo de una manera espantosa y sin control. Las estadísticas muestran que tan solo en Brasil, de cada 100 reales robados, 95 se roban a través de la banca en línea, es decir a través del Internet.

El experto indicó que en Ecuador, en particular, lo que Kaspersky ha observado es que los cibercriminales locales están aprendiendo tácticas de países desarrollados y esto ayuda a que cada año, el crecimiento de este tipo de delitos se de en un 130%.

"Podemos estimar que este año el crecimiento será similar. En Ecuador ya se está desarrollando este tipo de delitos. Desde hace cuatro años atrás investigué un código malicioso en una institución del Gobierno, después de extraer la evidencia constante que quién programó el virus era ecuatoriano y trabajaba en otras dependencia del Gobierno", señaló.

Además, Bestuzhev informó que se encontró otro tipo de virus en un banco ecuatoriano. El virus fue elaborado y utilizado en la provincia de Pichincha. "Estos ataques no fueron investigados porque muchas empresas no quieren dar a conocer que fueron atacadas y ver reflejadas sus debilidades en los medios de comunicación", detalló.

Según consignó la empresa de seguridad, Chile junto a Colombia concentran el 39% de los ataques vía web a usuarios. Son seguidos por Panamá (38%), Brasil, Honduras y Perú (37%) y luego Guatemala (36%), México, Uruguay y Argentina (35%), y bajo este porcentaje Ecuador.

Para Bestuzhev, existen dos factores para el creciente índice de delitos financiero: 1. En poco tiempo se puede llegar a ganar grandes sumas de dinero que en ningún otro lado podrían ganarlo. 2. La impunidad. Lamentablemente muchos países no tiene una legislación específica para la lucha contra el

crimen cibernético. Otros países no tienen organismos con personas capacitadas con las herramientas tecnológicas y judiciales para procesar a los criminales encontrados.

"Chile actualmente está realizando un mejor trabajo para combatir esta realidad. Ellos aprobaron hace mucho tiempo atrás leyes para luchar contra este delito, tienen brigadas dentro de la Policía y ellos tienen el cribercrimen tipificado y los delincuentes si reciben castigo", señaló.

El impacto económico de los ataques de seguridad (Isaac Forés)

Todas las empresas son conscientes de que la seguridad de la red es un asunto prioritario. Pero, ¿cómo pueden cuantificar el valor de negocio que aporta una red segura? ¿Y cómo pueden evaluar y justificar la inversión en productos de seguridad de red, como firewalls de próxima generación, sistemas de prevención de intrusiones y dispositivos de gestión unificada de amenazas?

No existe una fórmula exacta ni una herramienta para calcular el "coste de los ataques". Sin embargo, hay una serie de directrices y estudios de investigación muy útiles que pueden proporcionar a los administradores de TI las técnicas y los recursos necesarios para desarrollar su propio modelo de costes. A la hora de evaluar el impacto de los ataques basados en la red y el "valor preventivo" de las tecnologías de firewalls de próxima generación, deben tenerse en cuenta tres áreas principales:

La definición de los diferentes tipos de ataques basados en la red.

La comprensión del modo en que esos ataques pueden afectar al negocio de su empresa.

Los métodos para cuantificar el impacto de dichos ataques.

Tipos de ataques basados en la red

Existen cientos de tipos de ataques basados en la red que pueden dañar su organización. Entre los más comunes se encuentran los siguientes:

- Virus, troyanos, gusanos y otros tipos de malware que pueden poner fuera de servicio servidores y estaciones de trabajo o robar datos.
- Amenazas avanzadas persistentes, diseñadas para penetrar las redes y robar propiedad intelectual e información confidencial de forma desapercibida.
- Ataques distribuidos de denegación de servicio (DDoS) y flooding, que pueden sobrecargar los servidores y poner páginas web fuera de servicio.

Repercusión en el negocio

Los daños causados por los ataques, independientemente de la fuente, se dividen en dos categorías principales: la filtración de datos y la pérdida de servicio.

La filtración de datos siempre da lugar a noticias sensacionalistas, pues la extracción de información corporativa confidencial va a parar a manos de criminales o competidores. Los daños causados por las filtraciones de datos son visibles y muy graves. Pueden ser daños de carácter financiero (pérdida de ingresos, costes legales y normativos, costes derivados de procesos judiciales y multas), costes 'blandos' (pérdida de la confianza y fidelidad de los clientes) y pérdida de competitividad (como resultado de la pérdida de propiedad intelectual).

Después de sufrir filtraciones de información, las empresas se gastan cantidades enormes de tiempo y dinero en tareas de detección y corrección técnica, en la identificación y el bloqueo de ataques, así como en la valoración de los daños causados y en la aplicación de medidas correctivas. Además, los casos de filtración de datos generan una publicidad negativa que dura mucho más que el ataque en sí.

Los ataques por denegación de servicio resultan en la degradación o en la total inoperatividad de los sistemas informáticos, tanto de estaciones de trabajo como de servidores web, de aplicaciones o de bases de datos. Pero los daños colaterales en el ámbito financiero de estos daños también pueden ser catastróficos. El comercio se ralentiza o se detiene por completo, lo cual repercute directamente en los ingresos. Los procesos cotidianos se interrumpen o los empleados no pueden desempeñar sus tareas porque la red está fuera de servicio.

Al igual que ocurre con las filtraciones de datos, se produce un coste real relacionado con el departamento de TI y el personal de soporte, que tienen que diagnosticar los problemas, ayudar a los empleados, reiniciar los servicios y restablecer la imagen inicial de los PC.

¿Cómo se estiman los costes?

En realidad, no existe un modelo de costes universal aplicable a todos los casos. Un estudio de Ponemon Institute, realizado en marzo de 2012, y el estudio de NetDiligence, titulado Cyber Liability & Data Breach Insurance Claims (Reclamaciones de seguros por responsabilidad cibernética y filtración de datos), publicado en octubre de 2012, proporcionan dos fuentes independientes que pueden ayudar a los responsables de TI a cuantificar el impacto de los ataques basados en la red.

El Ponemon Institute realizó entrevistas detalladas a finales de 2011 a 49 empresas pertenecientes a 14 industrias diferentes, que habían sufrido casos de pérdida o robo de datos personales de cliente y extrajo como principales conclusiones que:

- El coste total medio de la filtración de datos asciende a los 4,16 millones de euros (valor en la divisa local utilizando Xe.com).
- Los ingresos perdidos por la filtración son de 2,26 millones de euros.
- Y, los costes posteriores a la filtración alcanzan los 1,13 millones de euros (asistencia técnica, medidas correctivas, descuentos a clientes, etc.).

Las cifras por registro -basadas en cantidades considerablemente grandes (normalmente 100.000+registros)- pueden proporcionar a los administradores de TI por lo menos una idea del coste asociado a la filtración de datos, en función del tamaño de la empresa y de la cantidad de amenazas a las que suele hacer frente. NetDiligence publicó un estudio con 137 eventos sucedidos entre 2009 y 2011, que llevaron a las compañías de seguros a realizar pagos por reclamaciones de responsabilidad cibernética. Pagos medios:

- Acuerdo legal por evento: 1.589.000 euros.
- Defensa legal por filtración: 440.549 euros.
- Pago total medio del seguro por evento: 2,8 millones de euros.

Aunque estos dos estudios miden diferentes elementos de los costes relacionados con los ataques basados en la red, ambos ilustran lo costosos que resultan estos ataques para los resultados, la reputación y la competitividad de las empresas.

Además de estas cifras, existen una serie de cálculos rápidos y aproximados que pueden ayudar a justificar la inversión requerida para las tecnologías de firewalls de red de próxima generación:

- La pérdida de ingresos por cada hora que su página web está fuera de servicio o seriamente impedida a causa de un ataque DDoS.
- La pérdida de productividad por cada hora que un proceso de negocio crítico está fuera de servicio debido a un malware que inhabilita el servidor.
- El precio por hora del personal del servicio técnico para diagnosticar infecciones de malware en los PC y del grupo de soporte para restablecer los PC infectados.
- El coste por registro para informar a los clientes o empleados en caso de filtración de datos y proporcionarles servicios de monitorización crediticia durante un año.

Existen asimismo dos técnicas adicionales que pueden resultar de utilidad a la hora de calcular los costes de los ataques. Algunas organizaciones han hecho

estimaciones detalladas de posibles repercusiones futuras mediante la realización de simulaciones. Para ello, reúnen a un grupo de empleados de diferentes departamentos -TI, marketing, RRHH, legal, etc.- y simulan un ataque. Estos ejercicios no solo ayudan a cuantificar los costes, sino que a menudo además desvelan efectos inesperados, como por ejemplo las obligaciones contractuales o el impacto de las filtraciones de datos asociado a las normas.

Tomar medidas

¿Cuáles son las consecuencias para los administradores de TI? La mala noticia es que los ataques basados en la red son costosos, interrumpen la actividad del negocio y pueden resultar catastróficos a muchos niveles, por lo que deben evitarse a toda costa. La buena noticia es que hay disponible una amplia variedad de herramientas y servicios que le ayudarán a comprender exactamente cómo la filtración de datos y la pérdida de servicio pueden repercutir en el negocio de su empresa. Si compara estos costes con los costes preventivos de las tecnologías de protección de próxima generación, estará mejor preparado para entender y articular el valor financiero y estratégico de incrementar la inversión en la seguridad de su red corporativa. No se trata simplemente de un ejercicio académico, sino de una necesidad de negocio.

El verdadero costo de los ciberataques para las empresas, (Grundvig, 2014)

Un cliente utiliza un terminal para tarjeta de crédito en una tienda Target de Miami, Florida, el 13 de diciembre 2013. Entre el 27 de noviembre y 15 de diciembre se robó la información de más de 40 millones de tarjetas de crédito del gigante minorista en lo que fue una de las mayores violaciones de datos de la historia de las corporaciones. La Gran Época

Compradores saliendo de una tienda Target, una tarde lluviosa, en Alhambra, California, el 13 de diciembre 2013. (La Gran Época)

La empresa Target ahora está aprendiendo el verdadero costo de la fuga de la información, lo que dejó al descubierto los datos de las tarjetas de crédito de 40 millones de clientes.

Las consecuencias del incumplimiento incluyen tres demandas colectivas, una investigación formal, la pérdida de confianza de los consumidores, y una caída del tres por ciento en las ventas en comparación con el mismo período del año pasado. Y tal vez la más grande está por venir: un golpe a su reputación.

Midiendo el impacto

¿Cómo puede una gran marca como Target medir los daños en su reputación?

La respuesta es el sondeo de opiniones, la cual se desarrolló durante la Segunda Guerra Mundial. Después de la guerra, los gigantes industriales alemanes como Volkswagen lo usaron para mejorar la eficiencia del flujo de trabajo para impulsar el "milagro económico alemán".

Durante la última década, el sondeo de opiniones se implementó en muchos sectores, inclusive se buscan opiniones de los consumidores sobre películas, alimentos y bebidas. Internet ha estimulado las encuestas en línea desarrolladas con plataformas de medios sociales.

En 2014 el sondeo de opiniones será reutilizado por las empresas con el propósito de conocer las reacciones de los accionistas acerca de las violaciones de datos, así como para medir la confianza pública sobre la capacidad de una empresa para ejecutar un plan de gestión de crisis, y para medir como la mala reputación repercute negativamente en el precio de las acciones.

El ejemplo del Citigroup

Uno de estos eventos le ocurrió al Citigroup hace dos años.

“El 10 de mayo de 2011, Citigroup descubrió que unos hackers robaron 2,7 millones de dólares de las tarjetas de crédito de 3.400 clientes del Citi, pero el

costo en la valoración de mercado de la entidad fue mucho mayor", según las estimaciones proporcionadas por Corr Analytics.

"El ataque trajo como consecuencia una caída del 17 por ciento en la rentabilidad de mercado de la compañía entre el día del incumplimiento y un mes más tarde, el 8 de junio", dijo el Dr. Anders Corr, un graduado de Harvard y fundador de Corr Analytics.

"La violación de datos del Citi tuvo un efecto contagio en el sector financiero en general. La pérdida durante ese período de la valoración pública de mercado de la empresa fue de aproximadamente $21.6 mil millones de dólares. La pérdida fue más pronunciada a partir del 3 de junio, cuando la compañía anunció esta violación a sus clientes".

Los números de los ciberataques

El costo de los ciberataques supera el de los datos robados. Los costos de legales, relaciones públicas, comunicaciones, y la disminución del precio de las acciones se pueden cuantificar.

Más problemático es el deterioro de la reputación de una empresa. El daño colateral que provoca una empresa, que ha sufrido un robo de datos, sobre las demás empresas también es importante aunque sea difícil de cuantificar. Una semana después del anuncio del robo en Target, JP Morgan Chase anunció que producto de ese robo las tarjetas de dos millones de sus clientes quedaron expuestas. Chase es ahora parte del campo de escombros del hackeo a Target.

En un artículo del Business News Daily, el periodista Chad Brooks señaló: "Sólo el 10 por ciento de las organizaciones tienen confianza en su capacidad para analizar de forma eficaz la seguridad de los datos".

"Kroll, una empresa dedicada a investigaciones corporativas y consultoría de riesgos, predice que los nuevos problemas de seguridad cibernética para 2014

serán los siguientes: el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), y otros marcos de seguridad similares, se convertirán en los estándares de facto de las mejores prácticas para todas las empresas", dijo Brooks.

El marco del NIST estará finalizado para febrero de 2014 coincidiendo con la iniciativa de seguridad cibernética del presidente Obama. ¿Qué recomendará?

“La seguridad cibernética es de vital importancia para inversores, bancos y fondos de cobertura. Las intrusiones pueden causar la pérdida de datos que comprometen las estrategias comerciales, la seguridad de los fondos, la exposición de los datos de los clientes, y el daño físico a los activos reales. Los costos de reputación suelen ser más significativos que la pérdida real”, dijo el Dr. Corr de Corr Analytics, una firma de análisis de riesgo político que atiende a clientes que invierten a nivel mundial.

El Dr. Doug Bond, fundador y presidente de Virtual Research Associates, explicó a través de un correo electrónico: “Los que utilizan las grandes herramientas de datos de hoy en día a veces no pueden reconocer los fundamentos teóricos sobre los que se están construyendo. El análisis del código operacional ha sido utilizado para anticipar las decisiones de los líderes y está basado en las percepciones de un líder acerca de cómo fluirán los acontecimientos políticos. Esta línea de investigación de actitudes, creencias y valores, y cómo estas dan forma a nuestras interacciones y toma de decisiones se inició hace más de 65 años justo después de la segunda guerra mundial”.

Redefiniendo la Ley de Seguridad

“Los países con altos niveles de corrupción, junto con robustas comunidades de hackers, representan el riesgo de ciberdelincuencia de mayor grado, para los inversores. Desde una perspectiva puramente de ciberriesgo, algunos de los peores países para invertir son Rusia, China, Brasil, Turquía, Rumania, India, Hungría, Ucrania, Argentina y Polonia”,

¿Cómo pueden las empresas reducir el riesgo y la exposición a las violaciones cibernéticas?

Parte de la respuesta está en la Ley de Seguridad que ya tiene 12 años. En el marco del Departamento de Seguridad Nacional, la misión de la Ley de Seguridad es “apoyar la lucha contra el terrorismo promoviendo la Ley de Tecnologías Efectivas de 2002”.

La Ley de Seguridad, que podrá ser modificada para tener un ciberlenguaje más fuerte, ofrece un camino claro a las empresas para prepararse mejor contra los ataques cibernéticos, así como para tranquilizar las opiniones de las partes interesadas evitando que se vuelvan negativas, y poder responder a estas de manera anticipada.

El problema del 90 por ciento de las empresas que no saben cómo reducir la exposición y responder ante la opinión pública, comienza con la gestión de datos. La mayoría de las empresas no tiene una visión completa de sus ecosistemas de Tecnología de la Información.

Más problemática ha sido la expansión del correo electrónico, el flujo de datos, y la multiplicación de las terminales de usuarios. Cuando una empresa se ve obligada a actualizar los sistemas de bases de datos, o a migrar datos a un entorno de nube, a menudo lo hace con poca planificación.

La exposición a los ciberataques

Así le ocurrió al Knight Capital Group. Cuando el mercado se abrió el 1 de agosto de 2012, Knight cambió los sistemas de información, pero lo hizo sin tener los controles adecuados. Durante los siguientes 45 minutos, millones de operaciones erróneas significaron 460 millones de dólares en pérdidas.

Este año, la Comisión de Bolsa y Valores (SEC, por sus siglas en inglés), que impuso un acuerdo de 12 millones de dólares, escribió en sus procedimientos administrativos del 16 de octubre, “Knight no tenía controles de gobernanza de tecnología ni mecanismos de control suficientes para garantizar el despliegue

ordenado de un nuevo código, o para evitar la activación de un código que ya no estaba destinado a ser utilizado en las operaciones actuales y que a pesar de esto permaneció en los servidores".

Joe Buonomo, director general de Direct Computer Resources (DCR), fue uno de los primeros en adoptar la Ley de Seguridad para productos de información de privacidad. En una entrevista con Buonomo, le pregunté qué podía hacer por una empresa la tecnología del enmascaramiento de datos.

"Piensa en el cifrado como si fuera buena información en movimiento. Una vez que los datos llegan a destino, se descifran. Esa terminal está expuesta", dijo Buonomo, un agradable veterano con 40 años de experiencia.

"El enmascaramiento o encubrimiento de datos elimina la información que apunta a archivos, nombres, direcciones y archivos de transferencia. Todos ellos tienen una referencia, a diferencia de los sistemas de cinta del pasado", dijo. "Hay muchas maneras para que los hackers sigan estas referencias, o ciclos del CPU. Algunos de los desafíos para el encubrimiento de datos son el tamaño y el tiempo que se necesita para llevar a cabo el enmascaramiento. Tomemos como ejemplo un gran banco de Inglaterra. ¿Cuál era su problema? Necesitaba miles de millones de registros para cifrar las 26 unidades de negocio. Les dijimos déjennos primero hacer tres unidades de negocio. Esto fue justo antes de la crisis financiera de 2008".

Se detuvo con una sonrisa, y añadió: "Tomamos los miles de millones de registros bancarios, lo que llevaría 500 días de tiempo de CPU con un software de la India, y les mostramos cómo hacerlo en ocho horas. Habíamos enmascarado su transacción. Si era hackeado, la información no coincidiría, así que el enmascaramiento de datos no se trata sólo de la encriptación, sino del enmascaramiento al momento de descifrar los datos enviados. Cuando los combinas, son casi imposibles de manipular".

Con un pensamiento final de Corregir sobre la importancia de la Ley de Seguridad y la búsqueda de datos de la NSA, agregó que, "las revelaciones de

la NSA nos confirmaron que las verificaciones de antecedentes son insuficientes, y es necesario un mayor grado de división de la información.

Esto se aplica no sólo al sector público, sino también al sector privado.

La información comercial confidencial es altamente vulnerable al robo por parte de los empleados. Se deben implementar medidas de seguridad de la información mejoradas, para proteger internamente, información empresarial de alta sensibilidad de cualquier persona que no necesite conocerla".

Sean Singleton, director general de Oglethorpe Capital, una empresa dedicada a organizar la financiación y a facilitar la transferencia de tecnología para nuevas empresas cibernéticas, declaró: "Nos centramos en empresas que entienden que la seguridad cibernética es un problema empresarial de riesgo que, además de traer consecuencias financieras, puede traer incertidumbre legal y un daño a su reputación".

Una compañía combina estas y otras herramientas para cuantificar la exposición de la empresa ante el ciberriesgo.

New World Technology Partners, en la cual Singleton es un asesor, emplea métodos de análisis del sistema para medir y totalizar las consecuencias financieras, de reputación, políticas, legales y reglamentarias de los ciberataques de alto impacto, en un balance de ciberriesgo.

Cuantos menos datos se enmascaran, ofuscan, o dividen, más se invita a los piratas informáticos y aumenta la exposición.

La Ley de Seguridad y el plan de ciberseguridad NIST nos mostrarán el camino. Pero las empresas necesitan ver la amenaza y la oportunidad de mantenerse un paso adelante de los cibercriminales.

James O. Grundvig es un columnista y periodista independiente de Nueva York quien colabora frecuentemente con La Gran Época.

Perfil Sobre los Delitos Informáticos en el Ecuador, (Pino, 2009)

Desde que en 1999 en el Ecuador se puso en el tapete de la discusión el proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, desde ese tiempo se puso de moda el tema, se realizaron cursos, seminarios, encuentros. También se conformo comisiones para la discusión de la Ley y para que formulen observaciones a la misma porparte de los organismos directamente interesados en el tema como el CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio y otros, que ven el Comercio Telemático una buena oportunidad de hacer negocios y de paso hacer que nuestro país entre en el boom de la llamada Nueva Economía.

Cuando la ley se presento en un principio, tenía una serie de falencias, que con el tiempo se fueron puliendo, una de ellas era la parte penal de dicha ley, ya que las infracciones a la misma es decir los llamados Delitos Informáticos, como se los conoce, se sancionarían de conformidad a lo dispuesto en nuestro Código Penal, situación como comprenderán era un tanto forzada, esto si tomamos en cuenta los 70 años de dicho Código, en resumen los tipos penales ahí existentes, no tomaban en cuenta los novísimos adelantos de la informática y la telemática por tanto les hacía inútiles por decirlo menos, para dar seguridad al Comercio Telemático ante el posible asedio de la criminalidad informática.

Por fin en abril del 2002 y luego de largas discusiones los honorables diputados por fin aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados Delitos Informáticos.

De acuerdo a la Constitución Política de la República, en su Título IV, Capitulo 4to, en la sección décima al hablar de la Fiscalía General del Estado, en su Art. 195 señala que: "**La Fiscalía dirigirá, de oficio o a petición de parte la investigación pre procesal y procesal penal……"**. Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que "**el ejercicio de la**

acción pública corresponde exclusivamente al fiscal". De lo dicho podemos concluir que el dueño de la acción penal y de la investigación tanto pre procesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal. Es por tanto el Fiscal quien deberá llevar como quien dice la voz cantante dentro de la investigación de esta clase de infracciones de tipo informático para lo cual contara como señala el Art. 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control de la Fiscalía, en tal virtud cualquier resultado de dichas investigaciones se incorporaran en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudaran posteriormente al representante de la Fiscalía a emitir su dictamen correspondiente.

Ahora bien el problema que se advierte por parte de las instituciones llamadas a perseguir las llamadas infracciones informáticas es la falta de preparación en el orden técnico tanto de la Fiscalía como de la Policía Judicial, esto en razón de la falta por un lado de la infraestructura necesaria, como centros de vigilancia computarizada, las modernas herramientas de software y todos los demás implementos tecnológicos necesarios para la persecución de los llamados Delitos Informáticos, de igual manera falta la suficiente formación tanto de los Fiscales que dirigirán la investigación como del cuerpo policial que lo auxiliara en dicha tarea, dado que no existe hasta ahora en nuestra policía una Unidad Especializada, como existe en otros países como en Estados Unidos donde el FBI cuenta conel Computer Crime Unit, o en España la Guardia Civil cuenta con un departamento especializado en esta clase de infracciones.

De otro lado también por parte de la Función Judicial falta la suficiente preparación por parte de Jueces y Magistrados en tratándose de estos temas, ya que en algunas ocasiones por no decirlo en la mayoría de los casos los llamados a impartir justicia se ven confundidos con la especial particularidad de estos delitos y los confunden con delitos tradicionales que por su estructura

típica son incapaces de subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin.

Por tanto es esencial que se formen unidades Investigativas tanto policiales como de la Fiscalía especializadas en abordar cuestiones de la delincuencia informática trasnacional y también a nivel nacional. Estas unidades pueden servir también de base tanto para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. Lo cual es posible aplicando la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos.

La cooperación multilateral de los grupos especiales multinacionales pueden resultar ser particularmente útiles - y ya hay casos en que la cooperación internacional ha sido muy efectiva. De hecho, la cooperación puede engendrar emulación y éxitos adicionales.

De otro lado en los últimos tiempos la masificación de virus informáticos globales, la difusión de la pornografía infantil e incluso actividades terroristas son algunos ejemplos de los nuevos delitos informáticos y sin fronteras que presentan una realidad difícil de controlar.

Con el avance de la tecnología digital en los últimos años, ha surgido una nueva generación de delincuentes que expone a los gobiernos, las empresas y los individuos a estos peligros.
Es por tanto como manifiesta **PHIL WILLIAMS** Profesor de Estudios de Seguridad Internacional, Universidad de Pittsbugh**2**, Es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la Delincuencia Informática, sino también con la infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a este nuevo tipo de delitos transnacionales.

Es por estas razones el Fiscal General Del Estado creo mediante Acuerdo 104-FGE-2008 el Departamento de Investigación y Análisis Forense de la Fiscalía

General Del Estado, dando el primer paso para poseer un cuerpo especializado para combatir esta clase de criminalidad a fin de precautelar los derechos de las víctimas y llevar a los responsables a juicio, terminando así con la cifra negra de esta clase de infracciones.

La norma ISO/IEC 17799 como base para Gestionar la Seguridad de la Información

La información y los procesos que apoyan los sistemas y las redes son los activos más importantes para cualquier organización (Dhillon, 2000).

Estos activos están sometidos a riesgos de una gran variedad, que pueden afectar de forma crítica a la empresa.

Actualmente, el cambio social producido por Internet y la rapidez en el intercambio de información, ha producido que las empresas empiecen a tomar conciencia del valor que tiene la información para sus organizaciones y se preocupen de proteger sus datos.

La entrada de las nuevas tecnologías y en especial Internet en las empresas, produjo un cambio radical en las empresas, ya que ahora éstas disponían de nuevas herramientas para mejorar su nivel de competitividad y la velocidad con la que se realizaban los negocios. Para proteger la información que generaban, algunas empresas se adaptaron mediante la implantación de sistemas de seguridad, que básicamente se basaban en la implantación de medidas de seguridad, pero sin llevar a cabo una adecuada gestión de esos controles. Con el tiempo, al no disponer de una gestión adecuada, esos controles dejaban de mantenerse y se convertían en controles pasivos, que en lugar de ayudar a mejorar la seguridad contribuían a despistar ofreciendo importación errónea en muchos casos. Así, en (Tsujii, 2004) se destacaba que para la construcción de un sistema de seguridad no bastan los aspectos tecnológicos, sino que también son necesarios los aspectos de gestión, y también los aspectos legales y éticos.

Una vez que las empresas han empezado a tener una concienciación mínima en materia de seguridad, se encuentran con el problema que no saben cómo afrontar el problema. La mayor parte de las empresas, tienen sistemas

caóticos, creados sin unas guías adecuadas, sin documentación, y con recursos insuficientes. Los controles clásicos se muestran por sí solos insuficientes y la diversidad de herramientas de seguridad existentes en el mercado ayuda a solucionar parte de los problemas de seguridad, pero nunca afrontan el problema de una manera global e integrada.

Algunas cifras que nos muestran la magnitud de los problemas ocasionados por falta de unas medidas de seguridad adecuadas aparecen por ejemplo en (CSI, 2002) , que indican que sobre una muestra de 257 empresas, el 90% de las empresas detectó fallos de seguridad, el 70% fueron fallos graves de seguridad(robo de portátiles, robo de información, fraude financiero, acceso al sistema por intrusos, sabotaje de datos o redes) y el 74% reconocieron pérdidas financieras debido a fallos de la seguridad. Otros informes aseguran que las pérdidas totales en los Estados Unidos en 2004 como resultado de fallos de seguridad en los ordenadores alcanzaron los $141.496.560.

A pesar de lo negativas que resultan las cifras anteriores, la situación es mucho más dramática en muchos países de Europa, y sobre todo en América Latina.

Las empresas en los tiempos actuales se enfrentan a los retos de garantizar que las tecnologías para los activos informáticos y de información sean seguras, rápidas y de fácil interacción, pero para cumplir estos objetivos, los gerentes de sistemas se encontraron con dos problemas básicos, la falta de herramientas que permitan afrontar la gestión de la seguridad de los sistemas de información de una forma centralizada, sencilla y dimensionada al tamaño de las compañías, y la falta de guías de seguridad de la información, que permitan responder a las preguntas de ¿dónde tengo que buscar? y de ¿Que tengo que controlar y cómo?.

El primer problema sigue sin resolver, pero creemos que puede ser resuelto cuando se dé solución al segundo. Con respecto al segundo problema, las organizaciones tanto nacionales como internacionales se han preocupado p

or elaborar un conjunto de normas y especificaciones relativas a la seguridad en las tecnologías de la información y las comunicaciones, sobre todo centradas en la definición de controles de seguridad mediante códigos de buenas prácticas, normas que definen sistemas de gestión de seguridad, y normas con criterios para certificar la seguridad. No obstante, el panorama es

complejo, y para una empresa pequeña o mediana, abordar la implantación de un sistema de gestión de seguridad, con la posibilidad de tener varios niveles de exigencia y con unos recursos limitados se convierte en una tarea muy compleja.

En este artículo presentamos una aproximación a la implantación de sistemas de gestión de seguridad, basado en la norma ISO/IEC 17799, que estamos desarrollando y mejorando continuamente gracias a la retroalimentación recibida directamente de los clientes de SICAMAN.

Esquema de Implantación de Sistemas de Gestión de Seguridad

A pesar de la relevancia de la norma ISO/IEC 17799, tanto en el ámbito nacional como internacional, no podemos decir que proporcione un sistema de gestión de seguridad de la información sino un conjunto de controles que nos sirven de guía para realizar una revisión detallada de la situación de nuestros sistemas en cuanto a seguridad.

No obstante, y aunque no todos los controles que podemos encontrar en la norma son aplicables en todas las empresas, es recomendable que las organizaciones se preparen para esta norma, al menos como punto de partida (Peltier, 2003) Así, por ejemplo la universidad de Pittsburgh está emprendiendo el desarrollo y la puesta en práctica de un estándar comprensivo de la seguridad basado en las guías proporcionadas por el estándar de la seguridad de la ISO/IEC 17799 (Walton, 2002)aunque como se indica (Eloff, 2003) se sugiere ir realizando una implantación progresiva de controles, que permita que la empresa pueda irse adaptando a la evolución de la seguridad de la empresa de una forma no traumática. Otros estudios consideran importante la norma, pero la complementan de alguna forma con otros aspectos, como es el caso de (Geffert, 2004) que incorpora los requisitos de la HIPAA norteamericana a un programa de seguridad complementando la ISO/IEC 17799, (Von Solms B. , 2005), que considera una aplicación conjunta y complementaria de los COBIT y la norma, o incluso (Masacci, 2005) que además de la norma considera controles relativos al cumplimiento de la legislación italiana en materia de protección de datos y privacidad. Otros, insisten en utilizar la 17799 en modelos de gestión de seguridad, pero siempre haciéndolo de manera incremental,

considerando las necesidades particulares de seguridad (Von Solms B. y., 2001).

Por lo tanto, aunque la norma no sea un sistema de gestión de la seguridad propiamente dicho, hay muchos autores que manifiestan su interés en desarrollar sistemas de gestión de la seguridad basados en ella.

La Gestión de la seguridad de la información puede ser implantada desde varias perspectivas: Una forma de establecer un SGSI es desde una perspectiva estratégica, afrontándolo mediante el gobierno corporativo y las políticas. Otro acercamiento puede ser desde el punto de vista "humano", intentando implantar una cultura de la seguridad, formación, aspectos éticos, etc. (Eloff, 2003).

Así, nos hemos planteado llevar a cabo un enfoque sistemático para abordar la Implantación de sistemas de gestión de la seguridad de la información, considerando como núcleo principal la 17799, pero sin renunciar a otro tipo de estándares y recomendaciones en materia de seguridad y de gestión de seguridad.

Respaldos en empresas: enfoque normativo de los respaldos de información

Indica (Mendoza, 2015), últimamente, la práctica de respaldo de información ha cobrado relevancia tanto en los hogares como a nivel corporativo, y esto tiene sentido si pensamos en el escenario actual de riesgos informáticos relacionados a la pérdida de información, así como la proliferación de nuevas amenazas de seguridad, con el ransomware a la cabeza.

Además, cuando se presenta un incidente o una interrupción que requiera la activación de un plan de recuperación y continuidad, generalmente, una de las actividades primordiales está relacionada con el uso de **respaldos de información**. En ese sentido, resulta de vital importancia en el contexto de la continuidad del negocio, que busca restaurar las actividades críticas en un tiempo prudente y regresar a la normalidad de las operaciones de manera progresiva.

Pero, ¿qué lineamientos existen para ponerlo en práctica? Para continuar con el tema, en esta ocasión conoceremos diferentes **marcos de referencia** que recomiendan la aplicación de procedimientos de respaldo, resaltando las características de los diferentes frameworks, junto con sus principales diferencias.

- **COBIT y el respaldo de la información**

En el documento para la seguridad de la información considerado en la versión 5 de los Objetivos de control para la información y tecnologías relacionadas **(COBIT)**, se definen un conjunto de procesos y prácticas de gobierno y gestión para las Tecnologías de Información.

Uno de estos procesos se denomina **Gestión de la Continuidad** (con identificador DSS04), perteneciente al dominio de entrega, servicio y soporte (DSS por las siglas de Deliver, Service and Support). A diferencia de otros marcos de control, en COBIT se detallan más aspectos de las medidas de seguridad, por ejemplo, se incluyen objetivos, métricas, prácticas, actividades, entradas y salidas que retroalimentan otros procesos, con los cuales se tiene interacción.

Una de estas prácticas se relaciona con la **Gestión de acuerdos de respaldo** (DSS04.07), que tiene como propósito mantener la disponibilidad de la información crítica para el negocio. El identificador indica que se trata del cuarto proceso del dominio DSS y que a su vez, se trata de la séptima actividad definida en dicho proceso. Por lo tanto, en COBIT se considera **qué** debe realizarse en términos de procesos, lo que permite contar con mayor contexto de las prácticas y actividades de seguridad.

- **Respaldo de información en ISO/IEC 27001**

Por su parte, el estándar ISO 27001 define el dominio **Seguridad de las operaciones** (A.12) a través de distintos objetivos de control, uno de los cuales es el de Respaldo de información (A.12.3), que tiene como propósito proteger a las organizaciones contra la pérdida de información.

A su vez, el control considerado en esta sección es el **Respaldo de información** (A.12.3.1), que establece la creación y prueba regular de copias de seguridad que involucren a la información, software e imágenes de sistemas, todo en concordancia con una política de respaldo.

Mientras que ISO 27001 indica un control de aplicación general y las actividades para su implementación quedan completamente abiertas conforme a lo que convenga a las empresas, COBIT señala lo que debe realizarse con un mayor detalle, al agregar más elementos para la implementación, como los objetivos, métricas, actividades específicas y las prácticas de gobierno o gestión, todo ello englobado en procesos organizacionales.

- **NIST y los controles de respaldo**

En el caso del Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) también se consideran distintos controles de seguridad en su publicación especial 800-43, una Guía para planes de contingencia enfocada en sistemas de información gubernamental, pero que bien puede ser adoptada por otras organizaciones.

De manera específica, para el dominio de Planes de Contingencia (CP) se han definido 13 controles, entre los cuales el noveno está relacionado con el **Respaldo de los sistemas de información** (CP-9). Estos mismos controles son retomados en la publicación especial 800-53, Controles de seguridad y privacidad para organizaciones y sistemas de información federal (revisión 4). En el apéndice F se detalla la información con mejoras aplicadas al control, guías suplementarias y la relación a otros controles de seguridad.

Por ejemplo, incluyen actividades relacionadas con el control (mejoras), como la prueba de **confiabilidad e integridad** de los respaldos, pruebas de restauración utilizando muestreos, almacenamiento separado para respaldos de información crítica, protección contra modificaciones no autorizadas, transferencia a un sitio de almacenamiento alternativo, sistemas redundantes de respaldo o la aplicación de doble autenticación para la eliminación de respaldos.

- **Respaldo de información para la gestión de servicios**

Por otro lado, en Information Technology Infrastructure Library (ITIL) también se consideran las prácticas de respaldo, específicamente en la fase de operación, que tiene como propósito la entrega efectiva de los servicios de TI.

Las actividades comunes de la **operación del servicio** (consideradas en el punto 5.2.3.1) incluyen conocer la información organizacional que debe ser protegida (es decir, la clasificada como crítica e incluye las copias de seguridad), así como el almacenamiento en ubicaciones remotas que permita su protección y uso en caso de que deba ser restaurada, debido a la pérdida, modificación no autorizada o por la aplicación de planes de continuidad, desde la perspectiva de los servicios de TI.

Define actividades concretas como la identificación de la información que deba ser respaldada y la frecuencia de esta práctica, el número de respaldos que deben ser retenidos (en función del tipo de información o del tipo de archivo). Considera el tipo de respaldo a realizar (total, parcial o incremental), ubicaciones utilizadas para el almacenamiento, métodos de transportación de respaldos, así como las pruebas y revisiones a realizar, como pueden ser pruebas de integridad o restauración.

Consideraciones generales sobre los respaldos

En general, hemos revisado que distintos frameworks enfocados en Tecnologías de Información, y otros de manera concreta en la seguridad de la información, consideran la aplicación de la práctica de respaldos como una medida para mantener, por un lado, la **disponibilidad** de la información, mientras que por otro lado, se permita la **continuidad** de las operaciones en una organización.

Desde las diferentes perspectivas, es posible observar que se tiene un objetivo común, por lo que las actividades de una empresa con relación a las prácticas de respaldo pueden ser consideradas y complementadas por lo que propone cada marco de referencia.

Pero como toda implementación, es importante resaltar que más allá de que se trata de una actividad relevante, el personal de la organización deberá definir **cómo** llevar a cabo esta práctica. Por lo tanto, además de adoptar los controles, prácticas o actividades, éstas deben adaptarse a las características, necesidades y recursos de cada organización, siempre considerando que si el costo de las medidas de protección sobrepasa el valor de activo, tal vez no sea tan conveniente aplicarlas.

Legislación y Delitos Informáticos - La Información y el Delito (VALDEZ, 2006)

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún." *(1)*

En 1983, la Organización e Cooperación y Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin e luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones

respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas". *(2)*

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define **Delito Informático** como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos." *(3)*

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma". *(4)*

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos.

1. En esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.
2. La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

En este punto debe hacerse un punto y notar lo siguiente:

- No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.
- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.
- La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.
- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.
- La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

Julio Téllez Valdez clasifica a los delitos informáticos en base a dos criterios:

1. Como instrumento o medio: se tienen a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

Ejemplos:

- Falsificación de documentos vía computarizada: tarjetas de créditos, cheques, etc.
- Variación de la situación contable.
- Planeamiento y simulación de delitos convencionales como robo, homicidio y fraude.

- Alteración el funcionamiento normal de un sistema mediante la introducción de código extraño al mismo: virus, bombas lógicas, etc.
- Intervención de líneas de comunicación de datos o teleprocesos.

2. Como fin u objetivo: se enmarcan las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

Ejemplos:

- Instrucciones que producen un bloqueo parcial o total del sistema.
- Destrucción de programas por cualquier método.
- Atentado físico contra la computadora, sus accesorios o sus medios de comunicación.
- Secuestro de soportes magnéticos con información valiosa, para ser utilizada con fines delictivos.

Este mismo autor sostiene que las acciones delictivas informáticas presentan las siguientes características:

1. Sólo una determinada cantidad de personas (con conocimientos técnicos por encima de lo normal) pueden llegar a cometerlos.
2. Son conductas criminales del tipo "cuello blanco": no de acuerdo al interés protegido (como en los delitos convencionales) sino de acuerdo al sujeto que los comete. Generalmente este sujeto tiene cierto status socioeconómico y la comisión del delito no puede explicarse por pobreza, carencia de recursos, baja educación, poca inteligencia, ni por inestabilidad emocional.
3. Son acciones ocupacionales, ya que generalmente se realizan cuando el sujeto atacado se encuentra trabajando.
4. Son acciones de oportunidad, ya que se aprovecha una ocasión creada por el atacante.
5. Provocan pérdidas económicas.
6. Ofrecen posibilidades de tiempo y espacio.

7. Son muchos los casos y pocas las denuncias, y todo ello por la falta de regulación y por miedo al descrédito de la organización atacada.
8. Presentan grandes dificultades para su comprobación, por su carácter técnico.
9. Tienden a proliferar, por lo se requiere su urgente regulación legal.

María Luz Lima, por su parte, presenta la siguiente clasificación de "delitos electrónicos" *(5)*:

1. Como Método: conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
2. Como Medio: conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.
3. Como Fin: conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

(1) TÉLLES VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México. 1996 Pág. 103-104

(2) MOLINER, María. Diccionario de María Moliner Edición Digital. Copyright© 1996 Novel Inc.; Copyright © 1996 María Moliner.

(3) Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en Mayo de 1993.

(4) CARRION, Hugo Daniel. Tesis "Presupuestos para la Punibilidad del Hacking". Julio 2001. http://www.delitosinformaticos.com/tesis.htm

(5) LIMA de la LUZ, María. Criminalia N° 1-6 Año L. Delitos Electrónicos. Ediciones Porrua. México. Enero-Julio 1984.

1.6. FORMULACIÓN DE HIPÓTESIS Y VARIABLES

1.6.1. HIPÓTESIS GENERAL

La salvaguardia de la información correcta mejorará en consideración los estándares de indica las normas internacionales lograrán un proceso correcto.

1.6.2. HIPÓTESIS PARTICULAR

1. Si se determinar las herramientas que se emplearán entonces se lograra el objetivo específico de la presente tesis (Salvaguardar la información).
2. Identificar los procesos que se deben de se lograr el correcto resguardo de información.
3. Si se tiene los conocimientos por el personal tecnológico para realizar el proceso entonces no se podrá asegurar el éxito del objetivo específico.
4. Si se tiene el desconocimiento de las nuevas herramientas tecnológicas que salen al mercado tecnológico para ejecutar las acciones de salvaguardia de información.

1.6.3. VARIABLES DE OPERACIONALIDAD

1.6.3.1. VARIABLES INDEPENDIENTES

La pérdida de información debido a eventos no controlados en la organización.

1.6.3.2. VARIABLES DEPENDIENTES

La pérdida de información es de suprema relevancia y deberá poder minimizar y evitar las posibilidades de que no ocurran los diferentes eventos

1.6.4. OPERACIÓN DE LAS VARIABLES

Tabla 1 Operación de las variables

Variables	**Definición conceptual**	**Dimensiones**	**indicadores**	**Ítems**
Robo de equipos informáticos.	Proceso que determina el éxito o	Métodos Aplicabilidad y recursos	• Éxitos • Fracaso • Consultas en	¿Las herramientas FREE para

Perdida de integridad de la información. Pérdida de credibilidad de la información	fracaso al momento de realizar pruebas en el entorno en ambiente de prueba	que necesita la prueba	foros tecnológicos	el desarrollo del laboratorio son idóneas?
No Salva de información. Eventos de delincuentes comunes o especializados en informacion	Riesgos de eventos que conlleven a la perdida de información que comprometan a la empresa	Eventos suscitados Perdidas de información actuales No disponibilidad de información	• Perdidas económicas • Procesos retrasados • Información delicada insegura	¿Está de acuerdo que se debe de resguardas la información? ¿Está de acuerdo con tener la información disponible siempre?

Elaborado: 1 Autor de Tesis.

1.7. ASPECTOS METODOLÓGICOS DE LA INVESTIGACIÓN

1.7.1. CUANTITATIVO

El enfoque cuantitativo (que representa, como un conjunto de procesos) es secuencial y probatorio. Cada etapa precede a la siguiente y no podemos "brincar" o eludir pasos. El orden es riguroso, aunque desde luego, podemos redefinir alguna fase. Parte de una idea que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o una perspectiva teórica. De las preguntas se establecen hipótesis y determinan variables; se traza un plan para probarlas (diseño); se miden las variables en un determinado contexto; se analizan las mediciones obtenidas utilizando métodos estadísticos, y se extrae una serie de conclusiones. (Roberto Hernandez Sampieri, 2014)

1.7.2. TIPOS DE ESTUDIO

Cuando se aplica una metodología ya establecida por normas internacionales y las buenas prácticas, soportadas por manuales de procedimientos y políticas de uso la ejecución de las mismas se pueden tomar como un inicio a desarrollar más métricas y mejorar de los procesos.

EXPLORATORIO.- Se realiza un laboratorio o exploratorio en el que se logra determinar el éxito o fracaso de las pruebas realizadas en un ambiente de prueba.

EXPLICATIVOS.- La socialización de la procesos que se debe de seguir para lograr el éxito de lo esperado se deben de documentar para que quede plasmado como evidencia explicativa de los eventos fallidos.

1.7.3. FUENTES Y TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para el presente propuesta de realizo una investigación por medio del método de encuestas cerrada.

POBLACIÓN Y MUESTRA

“Una población es un conjunto de elementos acotados en un tiempo y en un espacio determinado, con alguna característica común observable o medible”. (Di Rienzo, y otros, 2008, pág. 2).

EL UNIVERSO O POBLACIÓN

La población y muestra fue determinada específicamente en personas que laboran en organizaciones que se encuentran en el sector comercial de la urbe guayaquileña.

CARACTERÍSTICAS DE LA POBLACIÓN

Para la toma de las muestras fueron seleccionados 100 personas que cuenten con actividad laboral activa y la premisa más importante es que su vestimenta denoten que laboran en una institución formal.

Aplicaremos la siguiente fórmula para determinar la muestra:

$$n = \frac{N\,(Z2.\ p.\ q)}{e2\,(N-1) + Z2\ p.\ q}$$

N = tamaño de la población.

Z = Desviación estándar (para un intervalo de confianza de 95% es 1,96)

p = Hipótesis de la proporción de la población que posee la característica o rasgo distintivo del universo (cuando se desconoce esa proporción se plantea la hipótesis de p= 0.05)

q = 1 – p (probabilidad de fracaso)

e = Margen de error que está dispuesto a aceptar, precisión (Error máximo admisible en términos de proporción)

Tomando como base un nivel de varianza máxima (p = 0.95; q = 0,05); con un nivel de confianza del 95% y un error máximo del 5%.

Reemplazando las variables indicadas por sus respectivos valores tenemos:

n = 94.54

TÉCNICAS DE INVESTIGACIÓN

La captación de las muestras fue realizada en base de preguntas subjetivas específicas las cuales requerían respuestas con e opciones o semi cerradas.

1.8. RESULTADOS E IMPACTOS ESPERADOS

La presente propuesta pretende establecer lineamientos completos diseñados para el respaldo de información, se deja documentación que servirá establecer políticas y procedimientos para poder mitigar el problema específico de la tesis.

Pretende minimizar el riesgo de pérdida de información como ya ha sucedido en eventos delictivos, se podrá recuperar la información inmediatamente.

Se deja políticas de deberán ser auditadas por el departamento correspondiente para poder tener una métrica y darle seguimiento, se deja abierta la opción de mejorar los procesos una vez implementados, se debe de dejar evidencias del procesos realizados como cumplimiento de las políticas.

CAPITULO II

2. ANÁLISIS, PRESENTACIÓN DE RESULTADOS DIAGNÓSTICOS

2.1. ANÁLISIS SITUACIONAL

Para poder realizar un análisis situacional de la empresa Lutexsa Ind. Com. Cia. Ltda. Es necesario indicar que su nombre comercial al nivel internacional es Terpel, y otros dependiendo el país donde se encuentre la inversión, pero como nombre comercial en Ecuador es Terpel S.A.

La Organización Terpel S.A en cumplimiento de lo establecido en el Código de Comercio ha declarado su situación de control respecto de sus subordinadas, en la Cámara de Comercio de su domicilio y en su calidad de matriz, define el rol a desarrollar en cada una de las empresas que conforman el grupo empresarial, por lo cual velará porque en cada una de las empresas que lo conforman se adopten medidas específicas respecto de su gobierno, su conducta y su información, con base en los lineamientos establecidos en el presente Código de Buen Gobierno Corporativo y para el efecto y en ejercicio de la unidad de propósito y dirección que lleva implícito el Grupo Empresarial, procurará, en cuanto sea posible y compatible con la normatividad de cada uno de los países, que se adopten las mejores prácticas de buen gobierno que se observan en el grupo.

2.1.1. MISIÓN

Movilizamos el transporte y la industria con propuestas diferenciadoras que agregan valor

2.1.2. VISIÓN

En el 2017, con un equipo altamente efectivo, seremos líderes en participación de mercado, con el mejor posicionamiento de marca, reconocidos como la número uno en servicio y por nuestro compromiso con el país.

2.1.3. VALORES

Sustentamos todos nuestros mecanismos de autorregulación, cumplimiento y gobierno corporativo en una cultura basada en valores que garantizan una gestión ética y transparente a nuestros accionistas y demás grupos de interés.

2.1.4. COMPROMETIDOS

Estamos comprometidos con el respeto de los Derechos Humanos a lo largo de nuestra cadena de valor y promovemos su respeto en otros actores de la sociedad.

2.1.5. DERECHOS HUMANOS

Transferimos a clientes y proveedores nuestras mejores prácticas en Derechos Humanos.

2.1.6. BUEN GOBIERNO

Nuestro modelo de Buen Gobierno está fundamentado en procesos que aseguran una adecuada gobernabilidad y en un compromiso de autorregulación ética. Lo aplicamos rigurosamente en Colombia, Ecuador, México, Panamá y Perú, y a partir del 2012 en República Dominicana.

2.1.7. DIRECCIONAMIENTO

Nuestros órganos y mecanismos de gobierno aseguran un adecuado direccionamiento y una alta capacidad de gobernabilidad. En cada país tenemos una Asamblea General de Accionistas como máximo órgano de gobierno y una Junta Directiva como principal ente administrador.

2.1.8. EQUIDAD

Fortalecemos los mecanismos de autorregulación en todos los países donde operamos, reflejados en el aumento del uso responsable y de la efectividad de la Línea Ética.

2.2. BUENAS PRÁCTICAS

Incorporamos dentro de nuestras buenas prácticas planes de acción de equidad de género.

2.2.1. AUTORREGULACIÓN

Tenemos mecanismos de autorregulación para una gestión ética y transparente: Código de Buen Gobierno Corporativo y Código de conducta.

2.2.2. PRINCIPIOS

El Código de Buen Gobierno Corporativo contiene los principios que enmarcan la administración y el buen gobierno de Terpel. Fue creado para fortalecer la trasparencia de la gestión y la adecuada garantía de los derechos de los accionistas.

2.2.3. CÓDIGO DE CONDUCTA

Es una declaración de políticas y procedimientos, que nos permiten conducir nuestra acción dentro de la organización, con cada uno de nuestros públicos, en forma legal y ética.

2.2.4. ANÁLISIS FODA

Para el realizar un estudio situacional se desarrolló un análisis FODA que se lo muestra a continuación.

Tabla 2 Análisis FODA

FORTALEZA	OPORTUNIDADES
• Tener una infraestructura tecnológica solida • Personal motivado • Presupuesto para inversión	• Aparición de necesidades de respaldo. • Utilización de nuevas tecnologías • Actualización de conocimientos.
DEBILIDADES	**AMENAZAS**
• No contar con políticas • No contar con procedimientos • No se cuenta con manuales a seguir de los procesos	• Riesgo latente de evento delictivos • Variaciones eléctricas • Delincuencia informática

Elaborado: 2 Autor de Tesis

El análisis FODA denota como fortaleza que se cuenta con una infraestructura tecnológica sólida, de la misma manera la organización cuenta con personal altamente motivado para probar cambio que permitan mejorar los procesos

Entre las debilidades encontradas se logra determinar que no cuentan con políticas establecidas que mitiguen los procesos y maneras que tengan una base documental oficial, por ende nada se encuentra socializado.

Las oportunidades que cuenta este análisis situacional es que tiene la oportunidad de poder aplicar nuevas tecnologías que están saliendo al mercado empresarial para lograr minimizar el problema específico.

2.2.5. ANÁLISIS FOFA DODA

Tabla 3 Análisis FOFA DODA

	FORTALEZAS	DEBILIDADES
	• Contar con una infraestructura tecnológica robusta. • Crear las políticas aterrizadas a nuestra necesidad como País. • Económica para poder invertir en minimizar el riesgo • Personal motivado a nuevos retos.	• No contar con Políticas que minimicen el riesgo. • No contar con Procedimientos que minimicen el riesgo. • No contar con Manuales a seguir. • Situación Económica País
OPORTUNIDADES	**1 F-O**	**D-O 2**
• Aparición de necesidades de respaldo. • Utilización de nuevas tecnologías.	El poder contar con solida infraestructura nos permite innovar metodologías de respaldo utilizando nuevas tecnologías las mismas que podrán ser documentadas según la situación real del negocio en el Ecuador	Logrando una buena documentación de los procesos y sabiendo seleccionar las nuevas técnicas y procedimientos que conlleven al resguardo de data de la empresa.
AMENAZAS	**3 F-A**	**D-A 4**
• Riesgo latente de eventos delictivos • Variación eléctricas • Delincuencia Informática	Gracias a la infraestructura y crear políticas se lograra poder minimizar a su máximo expresión el riesgo de pérdida de información sin importar el eventos que puedan suceder.	La estrategia es la documentación de los procesos, políticas, manuales minimizan los amenazas de perdida de información por algún tipo de evento sea cual fuera.

Elaborado: 3 Autor de Tesis

Se debe de tener muy en cuenta la continua latencia de la amenaza de que se dé un evento no esperado que pueda culminar en una pérdida de información este peligro es eminente mientras no se ejecute un plan de remediación.

Realizando un análisis actual tomando consideración la facturación realizada por la empresa según sus clientes y costumbres de compra se podría determinar en el siguiente cuadro la perdida el valor real si se deja de producir tomando en consideración diferentes eventos.

.

2.2.6. ANÁLISIS DE VENTA

A continuación de la tabla se realiza un diagnostico basado en datos reales compartidos por la empresa.

Tabla 4 Ventas 31 Diciembre Lutexsa

VENTAS 31 DE DICIEMBRE	
Suma de GALONES	
CLIENTE	**VALOR**
EDS ARUAL; ARUAL S.A.	$ 31.933,00
EDS BAHIA NORTE; GASOP COMPANY S A	$ 10.349,00
EDS BALLENITA; GALDICET S.A.	$ 24.147,00
EDS BAÑOS; JORGE ESCUDERO E HIJOS CIA. LTDA.	$ 11.958,00
EDS BRITO; BRITO ZUNIGA ANTONIO BENIGNO	$ 18.338,00
EDS CARVAJAL; MACARVA C. LTDA.	$ 4.950,00
EDS CASANOVA; GASOLINERA CASANOVA CIA. LTDA.	$ 19.721,00
EDS CORHOL 3; DISTRIBUIDORA DE HIDROCARBUROS	$ 8.910,00
EDS CORONEL; CORONEL PINA JONAS EGBERTO	$ 3.990,00
EDS COSTA NORTE; CRESPO PANDO TOMAS	$ 6.929,00
EDS DAULE; RUIZ VEGA TITO RENE	$ 6.409,00
EDS DOMINGO COMIN; CANCEL S.A.	$ 986,00
EDS EL JARDIN; ERAZO DIAGO CARLOS ALBERTO	$ 3.944,00
EDS GAPAL; COMERCIAL PALACIOS REYES CIA. LTDA.	$ 1.980,00
EDS GARITA CHIMBORAZO; ESCOBAR MENDOZA JUAN	$ 1.990,00
EDS GASOMAR; GASOLINERA MARITIMA GASOMAR S.A.	$ 5.980,00
EDS GUAYACANES; GUAYACANES	$ 9.967,00
EDS GYR; BELLASI S.A.	$ 2.955,00
EDS KENIFER; CARRERA CHACON LUIS FERNANDO	$ 16.925,00
EDS LA GARZOTA; CASANOVA REYNOSO IVAN	$ 1.980,00
EDS LAS AMERICAS; DICOMTRIZ S.A.	$ 5.939,00
EDS MA. AUXILIADORA	$ 19.796,00
EDS MACHALA DOS (TEXACO DOS); KALKOSERV S.A.	$ 5.939,00
EDS MACHALA UNO; CONSTRUSUR DEL ECUADOR S A	$ 19.310,00
EDS MAIOLI; MAIOLI S.A.	$ 12.912,00
EDS MELISSA; BLUECORP S.A.	$ 8.885,00
EDS MILCHICHIG; MARIA ANGELA FLORES	$ 4.000,00
EDS PERIMETRAL; GRANDWORK S.A.	$ 3.971,00
EDS PISONI; PISONI S.A.	$ 3.942,00
EDS PRESTOSERVICIO DEL VALLE; ERAZO DIAGO	$ 7.885,00
EDS QUATTRO (SALINAS); GALDICET S.A. (BELLASI)	$ 17.841,00
EDS SAN FRANCISCO; COOP. DE TRANSPORTE URBANO	$ 7.478,00
EDS SENSACIÓN (ANTES AUTOMODELO); TINAJERO	$ 4.941,00
EDS TRUCK STOP; EMPROSERVIS CIA.LTDA.	$ 3.942,00
EDS ZURITA; COOPERATIVA DE TRANSPORTE URBANO	$ 7.913,00
FreddyShrimps Cía. Ltda.	$ 2.000,00

HOLCIM ECUADOR S.A.-PLANTA GUAYAQUIL	$ 2.000,00
LAVANDERIAS ECUATORIANAS C.A.	$ 2.000,00
PESQUERA MARYCIELO	$ 2.000,00
TAY FULL SERVICES	$ 4.985,00
TEXACO UNIVERSIDAD DE BABAHOYO TEXUN	$ 4.437,00
TINAJERO MONTALVO MARIO RUBEN-EDS FLAMINGO 1	$ 23.408,00
TINAJERO MONTALVO MARIO RUBEN-EDS FLAMINGO 2	$ 7.919,00
TOCASA S.A.	$ 8.414,00
TORAL AGUILAR ALFREDO RODRIGO - Eds El Fortín	$ 9.898,00
TORREGASI S.A.	$ 10.939,00
TRUST GAS	$ 8.000,00
TOTAL FACTURADO DICIEMBRE 2014	$ 415.035,00

Elaborado: 4 Autor de Tesis

En base a las ventas facturadas en un día se podría estimar más aterrizada mente lo que perdería la empresa si no cuenta con un buen sistema de continuidad de operación.

La oficina matriz se encuentra ubicada en un décimo segundo piso de un edificio del norte de la ciudad, esto aumentaría el riesgo de operaciones pero como todo riesgo no puede ser eliminado el 100%, se lo puede minimizar el que el impacto del mismo no sea tan fuerte al momento de suceder el evento.

En base a los valores presentados se puede sacar una proyección de costo por hora sin vender en la empresa considerando que el evento afecta a los sistemas informáticos o de comunicación con Petrocomercial o peor aún si los sistemas del proveedor tengan eventos que impidan la operación normal de las empresas, industrial y comercio en general que dependa del consumo de derivados del petróleo.

Tabla 5 Ventas diaria / Hora

VENTAS POR DÍA Y HORA	
DIARIO	$ 415.035,00
1 HORA LABORABLE	$ 51.879,38

Elaborado: 5 Autor de Tesis

Si surge un evento con la información en las sedes remotas se podría afectar de menor manera pero no menos importante el cuadro a continuación podrá mostrar las diferentes localidades y sus clientes que dependen directamente de las localidades remotas para su operación.

2.1. ANÁLISIS COMPARATIVO, EVOLUCIÓN, TENDENCIAS Y PERSPECTIVAS.

Cuadro comparativo con respecto a otras empresas del medio en donde se puede realizar un análisis de los resultados obtenidos

Tabla 6 Cuadro Comparativo

CARACTERÍSTICAS	LUTEXSA	P&S	PRIMAX	PETROCOMERCIAL
Solidez tecnológica				
Cuentan con respaldos	✓	✓	✓	✓
Tiene definido procesos	X	✓	✓	✓
Tienen estándares de Calidad				
Llevan estándares ISO	✓	✓	✓	✓
Llevan estándares ITIL	✓	✓	✓	✓
Aplican métricas informáticas	X	✓	✓	X
Plan de continuidad				
Cuentan con un BCP		X	✓	✓
Hacen pruebas de éxito/ error	X	✓	✓	X
Personal IT				
Capacitación constante IT	X	X	X	X
Certifican a su personal	X	X	✓	X
Realizan pruebas de laboratorio	✓	X	✓	X
Tienen incentivos profesionales	X	X	X	X

Elaborado: 6 Autor de Tesis

Se debe de analizar lo positivo de las empresas del medio con el fin de poder replicar y con mejoras en la organización, adoptando las necesidades y aterrizando las prioridades del negocio

Los usuarios tiene la necesidad de tener su información a la mano y tener la seguridad de que está siendo resguardad con el departamento de sistemas de la organización.

La pérdida de información por virus informáticos, los delincuentes cibernéticos que no esperan la oportunidad de poder ingresar a los equipos y robar información que afectan al empleado, perjudicando así a la organización.

2.1.1. EVOLUCIÓN Y TENDENCIA.

La tendencia de las empresas están guiadas a mitigar los factores que más atentan contra la seguridad de la información son los robos de equipos informáticos ya que en ellos se encuentran la información más importante de la empresa.

La delincuencia en el mundo tecnológico o delincuencia tecnológica está creciendo de una manera desmedida, aprovechando el poco o nulo interés de los usuarios por respaldar la información que contienen sus equipos tecnológicos como equipos portátiles, celulares inteligentes, Tablet entre otros.

2.1.2. PERSPECTIVA.

Los procesos informáticos que generen información que requiera ser guardad en los centro de datos deben cumplir con todas las seguridades necesarias que aseguren que esa información es veraz, útil para la organización.

Se debe de dejar claro a los usuarios de equipos tecnológicos que deben de usar dichos equipos para ejercer las funciones como empleados de la organización y no como almacenamiento de información que no sea de interés de la misma, esto asegura en buen uso de los recursos entregados para poder desempeñar sus funciones encomendadas.

2.2. PRESENTACIÓN DE RESULTADOS Y DIAGNOSTICO

Actualmente existen numerosas herramientas para la salva automática de la información y cada una cuenta con variadas características que las hacen diferenciarse entre ellas pero también tienen puntos en común. A continuación se llevará a cabo el análisis de tres herramientas utilizadas para la realización de salvas en centro de cómputo, teniendo en cuenta los siguientes aspectos:

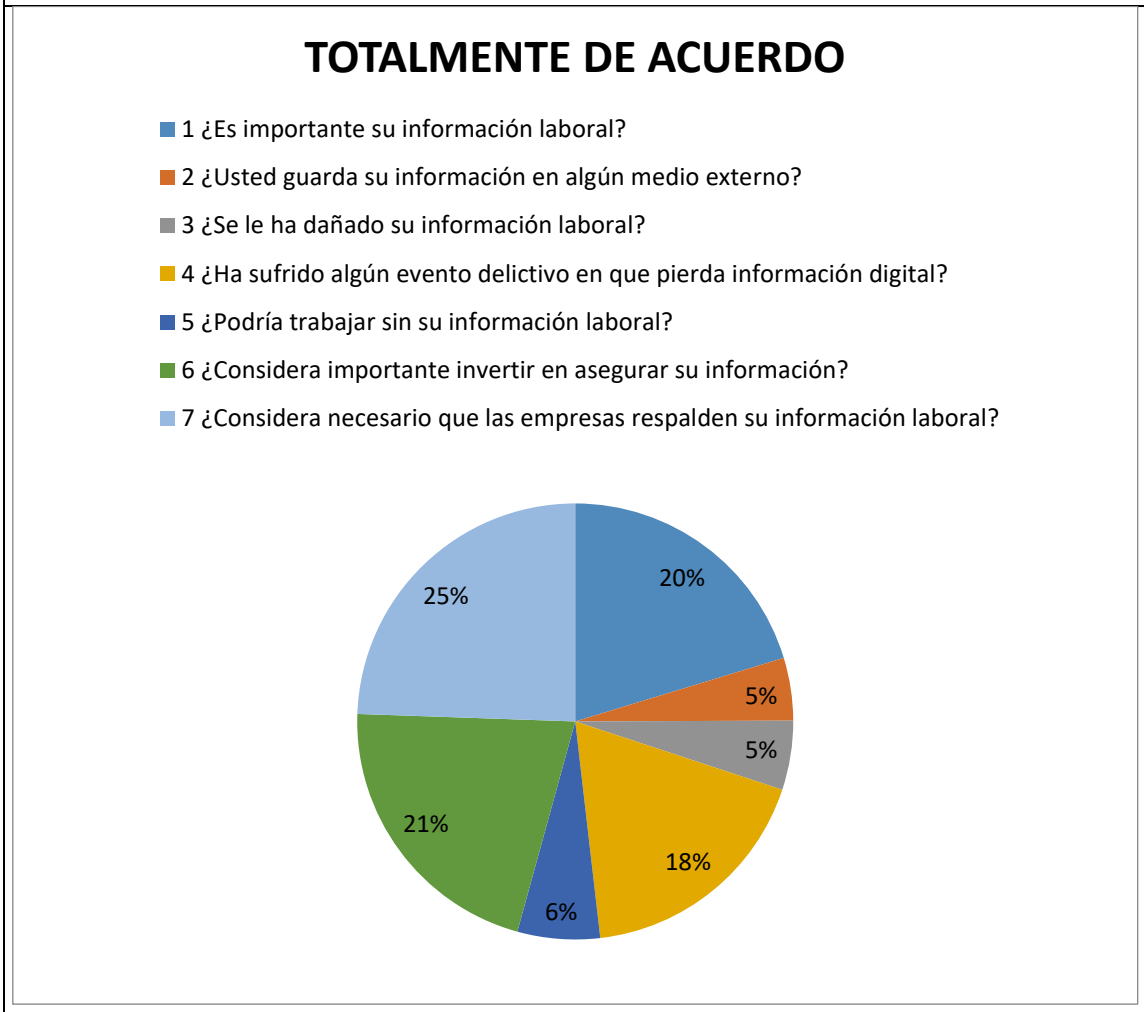
Tabla 7 Resultado de encuestas.

D= Desacuerdo, TD= Total mente de acuerdo M=Medianamente de acuerdo		TD	MD	D	TOTAL
1	¿Es importante su información laboral?	83	7	10	100
2	¿Usted guarda su información en algún medio externo?	19	30	51	100
3	¿Se le ha dañado su información laboral?	21	64	15	100
4	¿Ha sufrido algún evento delictivo en que pierda información digital?	74	21	5	100
5	¿Podría trabajar sin su información laboral?	25	44	31	100
6	¿Considera importante invertir en asegurar su información?	87	10	3	100
7	¿Considera necesario que las empresas respalden su información laboral?	100	0	0	100
8	¿Piensa que su empresa podria continuar su actividad sin su centro de datos?	80	15	5	100
9	¿Está de acuerdo con tener la información disponible siempre?	100	0	0	100
10	¿Está de acuerdo que se debe de resguardas la información?	100	0	0	100
11	¿Su empresa invierte el equipos te respaldo?	49	23	28	100
12	¿Esta su personal informático en capacitación constante?	5	35	60	100
13	¿Sabe cuánto vale la información de su empresa?	16	15	69	100
14	¿Sabe usted si puede recuperar su información en caso de pérdida?	54	26	20	100

Elaborado: 7 Autor de Tesis

El estrategia que fue aplicada para recopilación de información devuelve unos

valores que son graficados en el imagen siguiente:



Para un correcto análisis las encuestas realizadas y tomando como dato las 7 primeras preguntas que fueron elaboradas con la técnica de encuestas de intensidad podremos observar que solo el 5% de las personas guardan su información en medios externos.

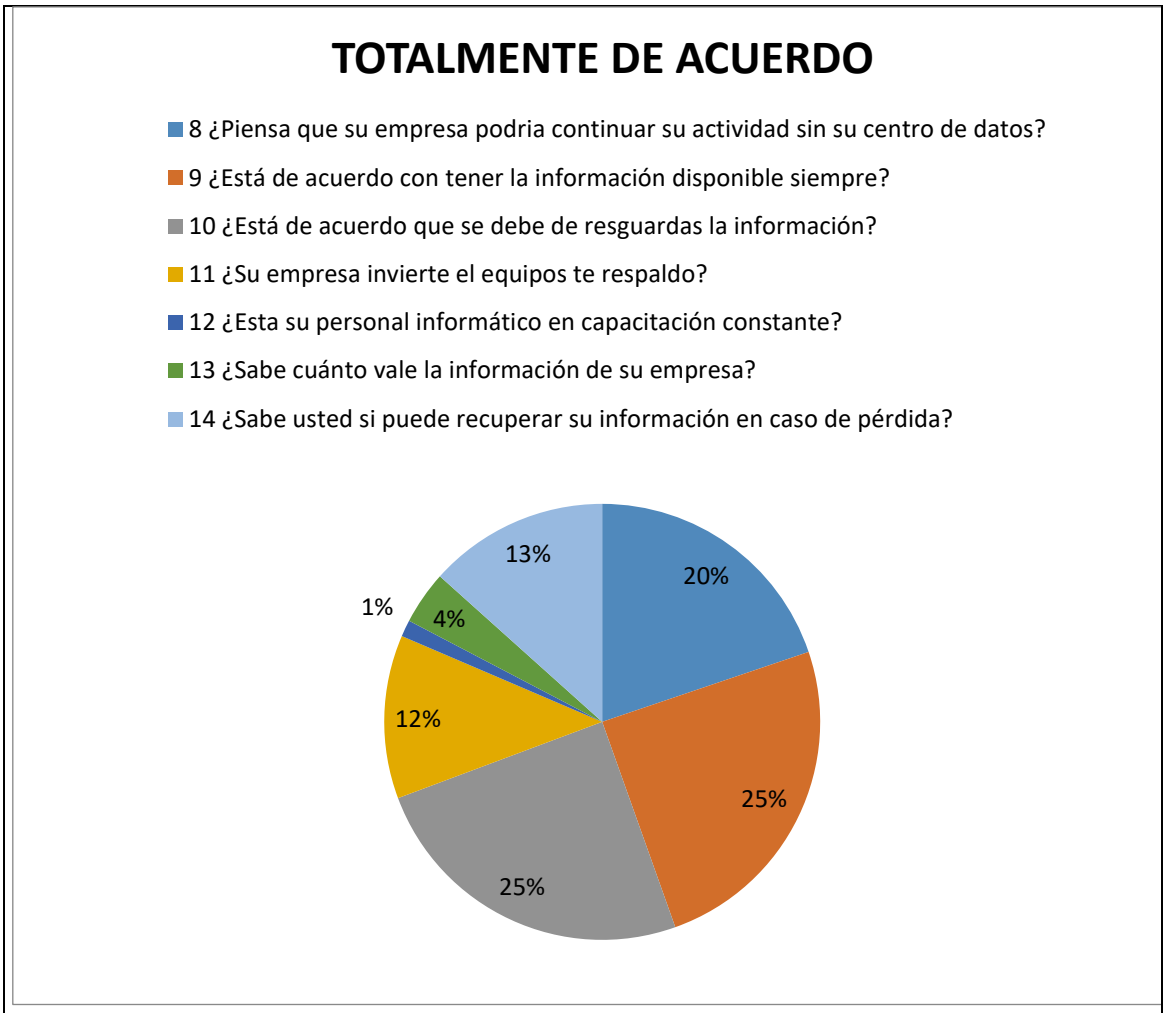
Un 5% de la persona encuestas les ha ocurrido algún evento que conlleva a pérdida de la información.

El 18% de las personas encuestadas ha sido víctima en donde se ve involucrada la información personal

El 21% de las personas encuestadas consideran que vale para pena invertir en asegurar la información.

EL 6% de indica que si podría realizar sus laborares diarias sin que le afecte la perdida de información.

Análisis de la pregunta 8 a la 14 a continuación:



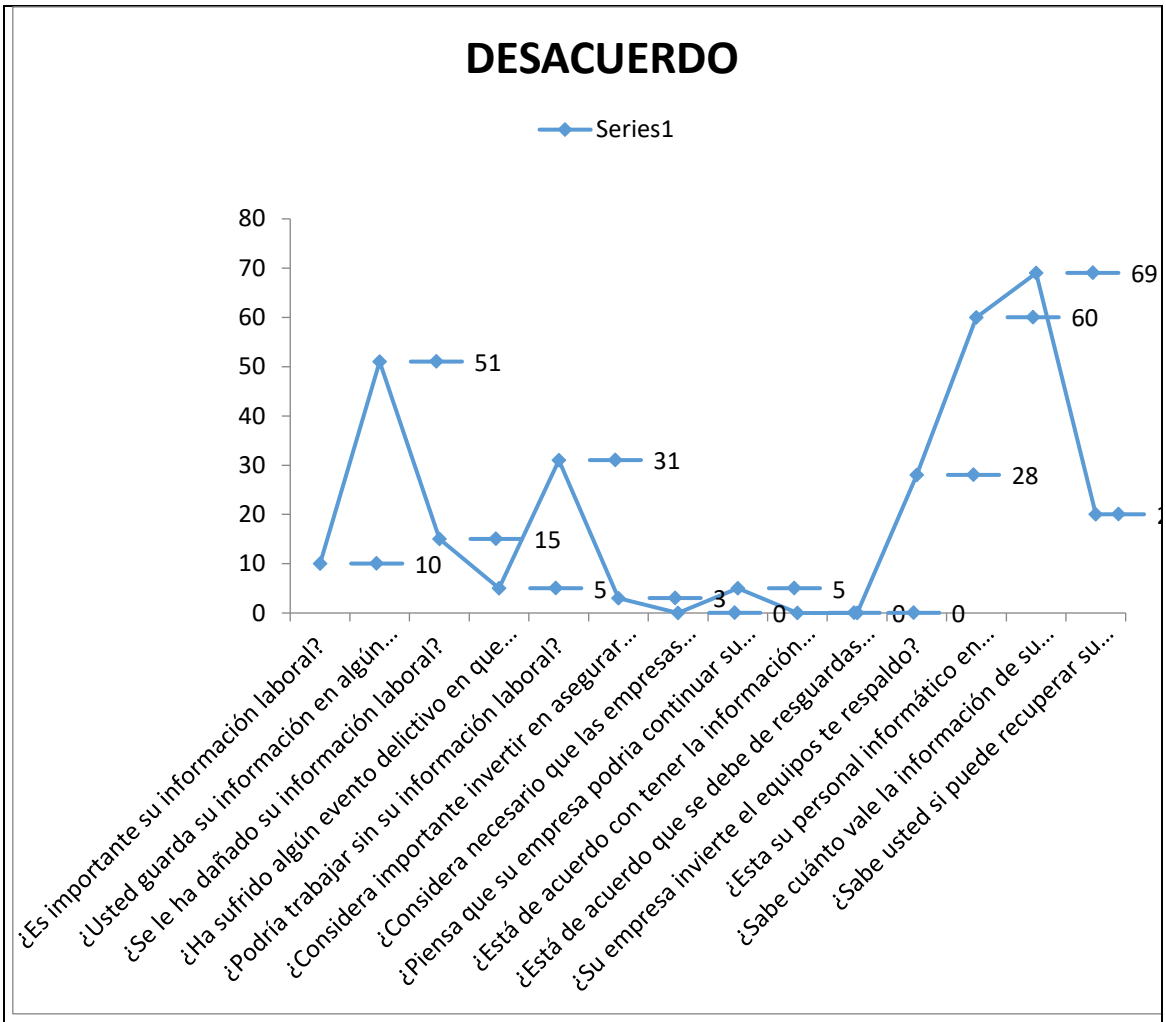
En la pregunta 8 podremos evidenciar que la personas encuestadas indican que el 20% de la empresas podría continuar operando sin su centro de datos.

Pregunta 9, indica que si está de acuerdo que la información debe estar disponible, recordando que es una característica de la información, indican el 25% que debe estar siempre disponible.

En la pregunta 10 el 25% de las personas encuestadas indican que están totalmente de acuerdo que la información debe estar debidamente resguardada.

En la encuesta numero 11 indican los encuestados que las empresas invierten poco en resguardar la información con un 12%.

La respuesta a la pregunta indica que las empresas no invierten en la capacitación informática en las empresas con apenas un 1%.



En el presente estudio tomaremos los picos estadísticos para realizar el análisis, en la pregunta 2 los encuestados responden que no hacer respaldos de su información en lo absoluto que es un 51% del total de encuestados.

En la pregunta 5 refleja que la personas piensan que la empresa no puede continuar operando sin su información digital.

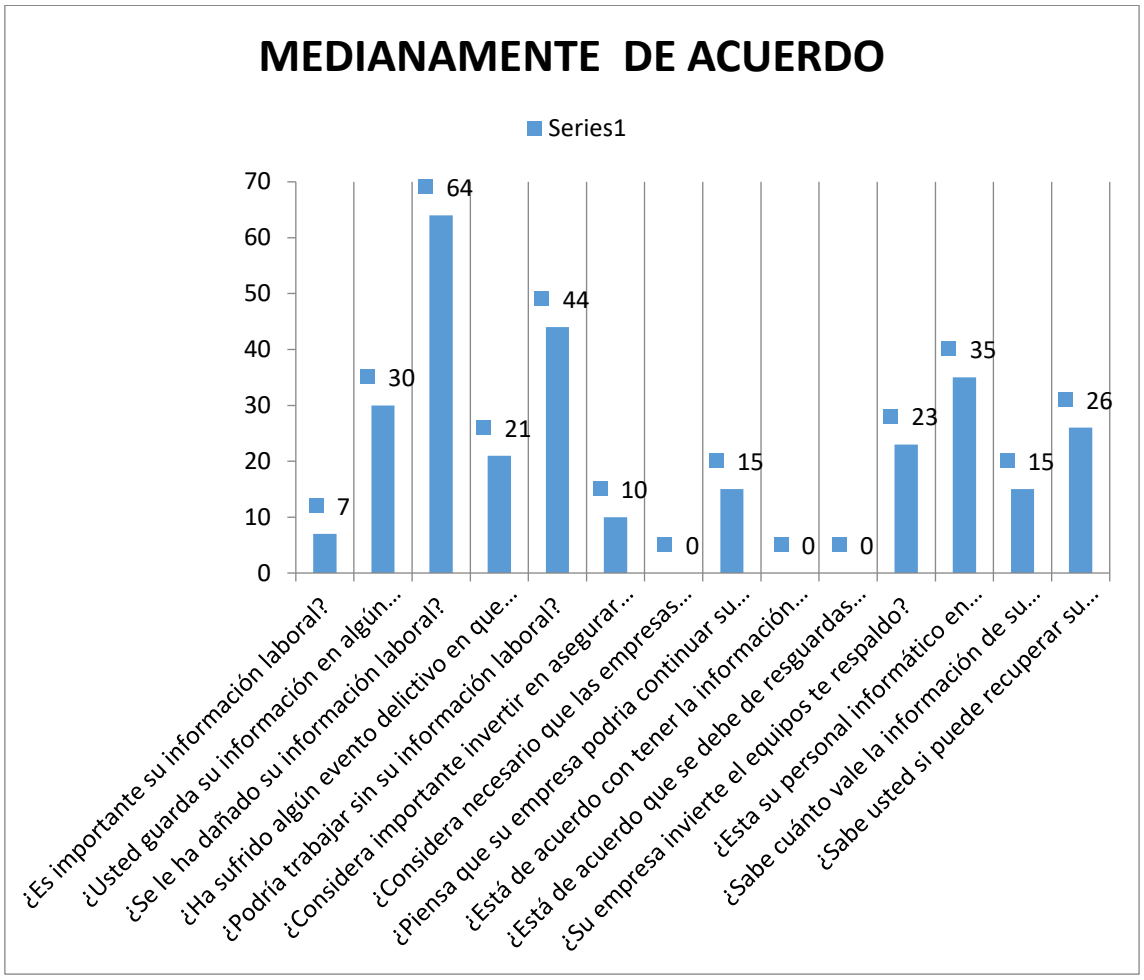
Tenemos una puntuación de 60 en la pregunta en donde indican que las empresas no invierten en capacitación de su personal informático.

En la pregunta 13 refleja el desconocimiento del valor económico que representa para la empresa la información que genera la operación económica en la que muchas empresas por la naturaleza del negocio se podría decir que es el activo más importante que debe de ser protegido celosamente sin embargo la vieja tendencia practicadas dan como gastos el aprovisionamiento de equipos especiales para el resguardo de la información.

En el siguiente cuadro se podrá revisar la muestra tomada quedando como evidencia que la mayoría de las personas encuestadas consideran que la información tal es considerada de medianamente importante para obtener los logros deseados en una organización.

Así mismo evidencia que se debe de tener una propuesta de cómo realizar dicho aseguramiento.

Ilustración 1Diagrama Pareto



Elaborado: 8 Autor de Tesis

Con este análisis de proyecto realizado se logra evidenciar las maneras correctas de llegar a tener una correcta custodia de la información en la empresa y el entorno en la que se desenvuelve.

Después del análisis realizado tomando en consideración las variables a intervenir se deberá llegar a una investigación de diferentes tipos de

herramientas tecnológicas que tendrán que tener guías y mejores prácticas de IT para luego poder realizar pruebas de laboratorio fuera de producción.

- Se dejan documentos establecidos en la organización.
- Se elevan documentos al árbol de políticas.
- Se elevan documentos al árbol de procedimientos tecnológicos para la salvaguardia de información.

2.3. VERIFICAR LA HIPÓTESIS

Tabla 8 Verificación de Hipótesis

HIPÓTESIS GENERAL	**VERIFICACIÓN DE HIPÓTESIS**
La salvaguardia de la información correcta tomando en consideración los estándares de indica las normas internacionales para lograr un proceso correcto.	¿Cree usted necesario el llevar a cabo las buenas prácticas de resguardo de información? ¿Considera necesario crear políticas y procedimientos que regularicen el proceso?
HIPÓTESIS PARTICULAR	**VERIFICACIÓN DE HIPÓTESIS**
1. Determinar las herramientas que se emplearan para el lograr el objetivo específico de la presente tesis (Salvaguardar la información). 2. Determinar los procesos que se deben de seguir para lograr el correcto resguardo de información. 3. La falta de conocimientos por el personal tecnológico para realizar el proceso. 4. El desconocimiento de las nuevas herramientas tecnológicas que salen al mercado tecnológico para ejecutar las acciones de salvaguardia de información.	Cree usted: Necesario realizar el análisis de herramientas para una salva de información dado la situación de la delincuencia. Según su razonamiento: considera necesario crear reglas para el uso de la información. Cree que es necesaria la capacitación del personal tecnológico para poder ejercer mejor sus actividades.

Elaborado: 9 Autor de Tesis

CAPÍTULO III

3. LA PROPUESTA

3.1. ANTECEDENTES

Debido a los eventos suscitados en la organización, la pérdida de información, robos de equipos tecnológicos, robo a funcionarios de la empresa se debería tener interés de poder mitigar esta falencia de seguridad que ya nos ha impactado de manera importante con el hecho de no tener historial de nuestro negocio en las sedes remotas de la empresa,

3.2. JUSTIFICACIÓN

El fin de esta tesis es poder dejar establecido las políticas, manuales de procedimientos y manuales de guía que servirán para el logro de la salvaguardia de la información.

Mitigar y reducir al máximo analizando los lineamientos indicados en la presente tesis en mismo que conlleva al éxito de la ejecución del proceso

3.3. OBJETIVOS

3.3.1. OBJETIVOS GENERALES

La elaboración de un programa documentado y socializado con las personas que interviene en el proceso expuesto, tomando siempre como objetivo general el resguardo de la información de la organización

3.3.2. OBJETIVOS ESPECÍFICOS

- Contar con un documento debidamente oficializado el cual de las directrices a seguir en el ámbito de políticas del buen proceso.
- Dejar documentado los debidos procedimientos para la ejecución del objetivo de salvaguardia de la información.
- Establecer procedimientos documentados para el uso del personal responsable y su debido control así mismo tenerlo disponible para la auditoria en el caso que lo ameriten.
- Llevar el debido control de los procesos realizados

3.4. FACTIBILIDAD

El presente trabajo es viable para mitigar la perdida de información, se lo confirma con los laboratorios realizados y documentados entre los anexos del presente documento que evidencias su operatividad y factibilidad en el entorno del negocio, cubriendo la premisa de esta documento.

3.4.1. FACTIBILIDAD HUMANA

Es necesario tener al personal consiente de los procesos de deben de seguir y para ello deben de tener documentado el departamento de talento humano la gestión y responsabilidades del personal tecnológico de la organización.

3.4.2. FACTIBILIDAD TECNOLÓGICA.-

La organización cuenta con todos los medios necesarios para hacer de este análisis un éxito, cumpliendo con los estándares de calidad y normas tecnológicas en este utilizadas.

3.5. VALORES FUNDAMENTALES

El valor fundamental del presente trabajo está en lograr identificar las mejores prácticas de como salvaguardar la información de un centro de datos y data de usuarios en equipos locales.

3.6. POLÍTICA DE LA PROPUESTA

Las políticas de la propuesta se encuentran en el anexo, el mismo que fue desarrollado bajo plantillas institucionales, se obvio información como logos institucionales, se hace hincapié en los cargos o roles de la empresa y no al recurso humano como tal, esto quiere decir que es aplicable a cualquier persona que tenga entre sus roles la responsabilidad de salva de la información.

Se anexa al presente la política desarrollada denominada:

POLÍTICAS PARA EL USO Y MANEJO DE LOS RESPALDOS INFORMÁTICOS DE **“LUTEXSA IND. COM. CIA. LTDA.”** EN CINTAS.

3.7. BENEFICIARIOS

El resultado obtenido del presente análisis deja en claro el beneficio para la organización y su talento humano, podrán tener la información de la organización disponible cumpliendo las premisas de la información.

3.8. DESARROLLO DE LA PROPUESTA

- ✓ Anexo 1.- Políticas para el uso de manejo de los respaldos informáticos de LUTEXSA IND. COM. CIA. LTDA.

En este documento de políticas se podrá evidenciar de manera clara la descripción de las funciones y los cargos a las que aplica.

3.8.1. PROCEDIMIENTO PARA RESPALDOS INFORMÁTICOS DE "LUTEXSA IND. COM. CIA. LTDA." EN CINTAS.

CONTENIDO

0. HOJA DE MODIFICACIONES

Documento en el cual se debe de tomar apuntes respecto a las modificaciones realizadas del presente documento consideradas para su mejor aplicabilidad y/o procedimiento deben ser registradas en el momento de su respectivo cambio y aprobación para su futura socialización, en dicha hoja de debe de especificar el cambio realizado, la fecha de modificación, el responsable del cambio y sus firmas aprobadoras de dicho cambio al procedimiento afectado.

1. OBJETO

Es el objeto de este documento definir el procedimiento que debe de realizar el responsable con respecto al los respaldos informáticos en la empresa **"LUTEXSA IND. COM. CIA. LTDA"** Se entiende por uso responsable el seguimiento de políticas y procedimientos que están debidamente registrados y socializados.

2. ALCANCE

Los procedimientos indicados en el presente se tendrán que aplicar a todos los empleados de la empresa **"LUTEXSA IND. COM. CIA. LTDA"** que se

encuentren entre sus responsabilidades predefinidas y socializadas el ejecutar respaldos en las unidades de cinta, los autorizados para el manejo de la información será responsabilidad exclusiva de los ingenieros de datos, coordinadores de datos, jefaturas de IT y su Gerencia, siendo ellos los responsables de hacer acatar el presente documento, cada uno de estos empleados se les deberá entregar una copia del presente y deberá ser firmada como constancia de su entrega y compromiso.

3. REFERENCIAS

Se especifica los documentos necesarios para la elaboración correcta y entendible de este documento, se deberá solicitar al departamento de Gestión Humana los respectivos roles y funciones de los siguientes cargos:

a) Ingenieros de datos
b) Coordinadores de datos
c) Jefaturas de IT
d) Gerencia de IT

La información a continuación se debe de solicitar a quien corresponda.

e) Licencias y fechas de expiración de cada software utilizado (Si fuera necesario su control)
f) Llaves de casillero Bancario
g) Unidades de tape IBM 1,5 TB
h) Entrega de Bitácora de almacenamiento en Banco.

4. RESPONSABILIDAD

En este ítem se debe detallar las personas involucradas y responsables. Este documento se lo considera como NO PUBLICO y solo deberá ser divulgado con los involucrados, incluyendo a Gerencia de Auditoría Interna, Gerencia General, y demás mandos altos.

5. IDENTIFICACIÓN

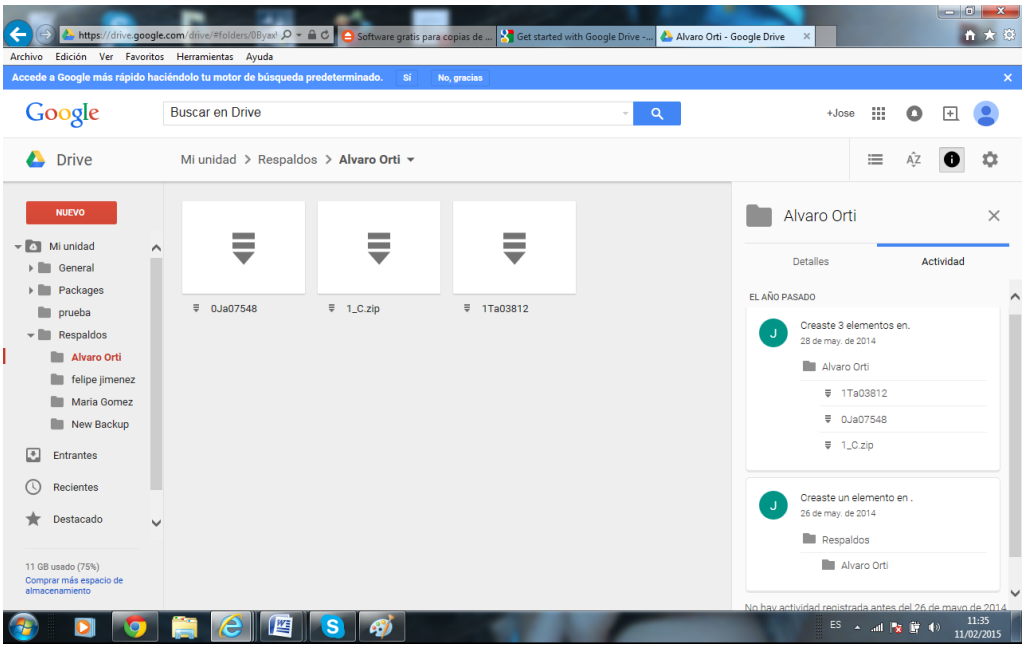
   Este documento se identifica como MANUAL DE PROCEDIMIENTO PARA LOS RESPALDOS INFORMÁTICOS DE **"LUTEXSA IND. COM. CIA. LTDA"** EN CINTAS. Con su respectivo Código: PRC.TIC.001.

1. **HOJA DE MODIFICACIONES**.- En la tabla a continuación indicada se debe de registrar los cambios realizados al presente documento y que estén aprobados para su ejecución.

# REVISIÓN	TIPO DE MODIFICACIÓN	REVISADO	APROBADO	FECHA

2. PROCEDIMIENTO PARA RESPALDAR A TAPE LA INFORMACIÓN RESPALDADA EN LA NUBE, CABE ACLARAR QUE EL PROCEDIMIENTO PREVIO ESTA DETALLADO PASO A PASO EN EL DOCUMENTO "CONFIGURACIÓN DE CLIENTES PARA RESPALDO EN LA NUBE".

El ingeniero encargado debe iniciar sesión en el servidor principal con el usuario que tiene privilegios necesarios para ejecutar la operación. En donde previamente se configuro google drive se debe de tener visible los diferentes directorios que fueron respaldados desde su origen.



a. El ingeniero encargado debe revisar las últimas fechas de actualizaciones de la información de las sedes remotas a respaldar, así como muestra la imagen siguiente ().

b. El Ingeniero encargado deberá encender el robot IBM Storage y su respectiva cinta de respaldo.

c. Deberá de ejecutar la herramienta de respaldo instalada en el servidor IBM, se referencia una guía paso a paso en Microsoft a continuación: (Microsoft, 2015)

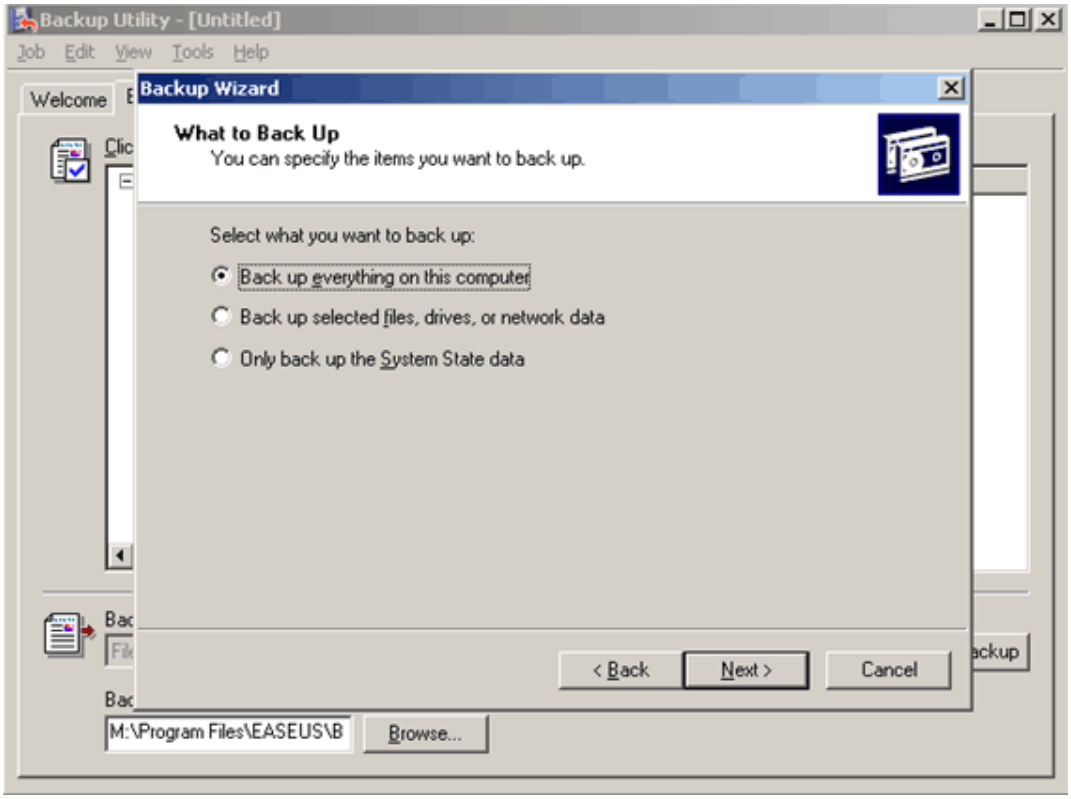
Cómo programar una copia de seguridad diaria en Windows Server 2003

NOTA: Es necesario que el servicio Programador de tareas se esté ejecutando para poder programar una copia de seguridad. Si el servicio Programador de tareas aún no se está ejecutando, inícielo. Para ello, haga clic en **Inicio**, **Ejecutar**, escriba **cmd** en el cuadro **Abrir** y, a continuación, haga clic en **Aceptar**. En el símbolo del sistema, escriba **net start schedule** y presione ENTRAR.

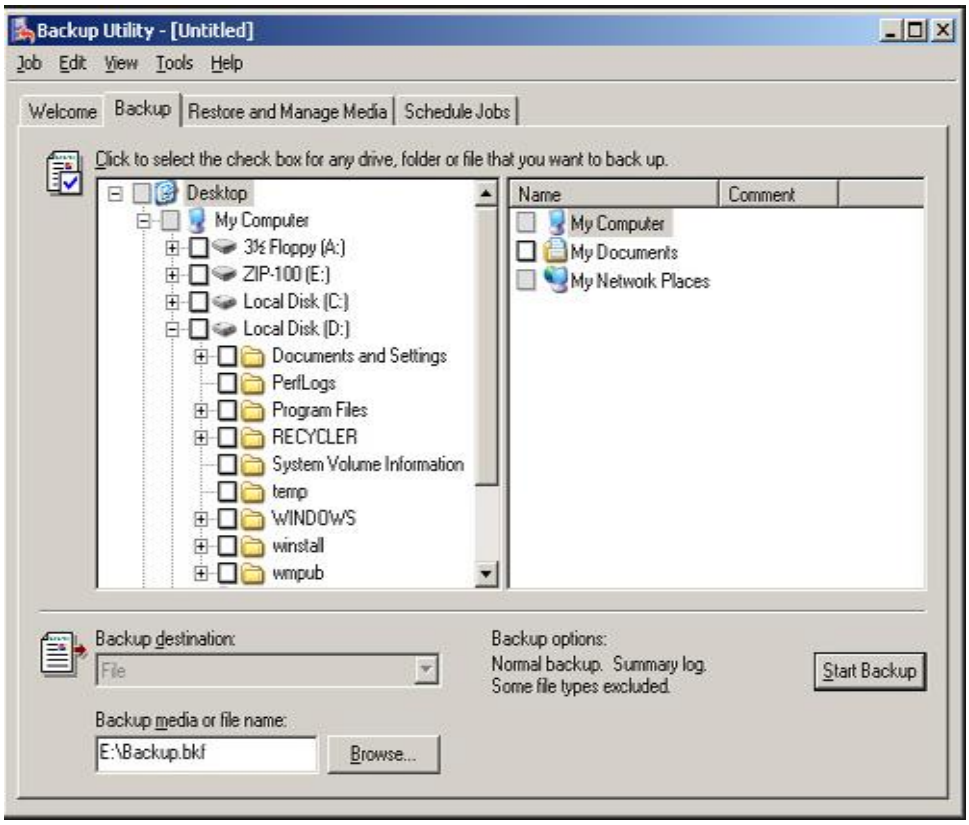
Para programar una copia de seguridad diaria en Windows Server 2003:

3. Inicie sesión como administrador o como miembro del grupo Administradores.

4. Haga clic en **Inicio**, seleccione **Todos los programas**, **Accesorios**, **Herramientas del sistema** y, a continuación, haga clic en **Copia de seguridad**. Se iniciará el Asistente para copia de seguridad o restauración.



5. Haga clic en **Modo avanzado**.
6. En la ficha **Bienvenido**, haga clic en **Asistente para copia de seguridad (avanzado)** para iniciar el Asistente para copia de seguridad y, a continuación, haga clic en **Siguiente**.
7. Haga clic en **Hacer copia de archivos y carpetas seleccionadas,** en esta sección debe direccionar la carpeta contenedora de los respaldos, El ingeniero responsable debe de direccionar el respaldo a la carpeta google drive que es la contenedora de todos los respaldos realizados automáticamente guardados de todas las sedes a la nube.



8. Si desea comprobar los datos de los que se ha creado la copia de seguridad una vez finalizada la operación, active la casilla de verificación **Comprobar datos después de la copia de seguridad**. Haga clic en cualquier otra opción que desee en la página "Cómo hacer la copia de seguridad" y, a continuación, haga clic en **Siguiente**.

9. Haga clic en **Reemplazar las copias de seguridad existentes** y, después, en **Siguiente**.

10. Haga clic en **Más adelante**. Escriba un nombre para el trabajo de copia de seguridad programada en el cuadro **Nombre del trabajo** y, a continuación, haga clic en **Establecer programación**.

11. Haga clic en la ficha Programación. En el cuadro Programar tarea, haga clic en Diariamente, especifique una hora en el cuadro Hora de inicio y, a continuación, haga clic en Aceptar.

12. En el cuadro de diálogo Establecer información de cuenta, compruebe que NombreEquipo\XXXXX aparece en el cuadro Ejecutar como, escriba la contraseña en los cuadros Contraseña y Confirmar contraseña y, a continuación, haga clic en Aceptar. Haga clic en Siguiente.

13. Se muestran las opciones que seleccionó en la página "Finalización del Asistente para copia de seguridad". Asegúrese de que estas opciones son correctas, y, a continuación, haga clic en Finalizar.

14. El trabajo de copia de seguridad que programó se muestra en el calendario en la ficha Programar trabajos. El trabajo de copia de seguridad programado se iniciará automáticamente a la hora que especificó.

15. Cierre la ventana Copia de seguridad.

    El Ingeniero responsable deberá de llenar la hoja de bitácora de respaldos realizados y entregarlo a la persona encargada de llevar los mismos al casillero del banco para su respaldo final, en el banco se le entregara una cartilla de control de acceso al casillero el que deberá de ser diligenciado en su totalidad como indica la imagen a continuación.

16. Cartilla de registro de entrega de tape a caja de seguridad bancaria.

    Una vez realizado el respaldo de la información de las sedes remotas, se deben de enviar los tapes al casillero del banco asignado para su resguardo, el proceso de respaldo tiene su propio proceso que esta normado como un proceso de IT, se contara con sus políticas y procedimientos debidamente analizados, luego se harán públicos los documentos su divulgación a los responsables del proceso y dueños del proceso re respaldo.

3.8.2. POLÍTICAS PARA USO Y MANEJO DE RESPALDOS INFORMÁTICOS DE "LUTEXSA IND. COM. CIA. LTDA" EN CINTAS.

CONTENIDO

0. HOJA DE MODIFICACIONES

   Documento en el cual se debe de tomar apuntes respecto a las modificaciones realizadas del presente documento consideradas para su mejor aplicabilidad y deben ser registradas en el momento de su respectivo cambio y aprobación para su futura socialización, en dicha hoja de debe de especificar el cambio realizado, la fecha de modificación, el responsable del cambio y sus firmas aprobadoras de dicho cambio.

1. OBJETO

   Es el objeto de este documento definir la política institucional con respecto al manejo responsable de los respaldos informáticos en la empresa **"LUTEXSA IND. COM. CIA. LTDA"** Se entiende por uso responsable el seguimiento de normas, políticas y buenas prácticas que salvaguarden la seguridad de la información, sistemas de información y los recursos tecnológicos institucionales

2. ALCANCE

   Las políticas o normas indicadas en el presente se tendrán que aplicar a todos los empleados de la empresa **"LUTEXSA IND. COM. CIA. LTDA"** que se encuentren entre sus responsabilidades predefinidas y socializadas el manejo de unidades de cinta de respaldo, los autorizados para el manejo de la información será responsabilidad exclusiva de los ingenieros de datos, coordinadores de datos, jefaturas de IT y su Gerencia, siendo ellos los responsables de acatar el presente documento, cada uno de estos empleados se les deberá entregar una

copia del presente y deberá ser firmada como constancia de su entrega y compromiso.

3. REFERENCIAS

Se especifica los documentos necesarios para la elaboración correcta y entendible de este documento, se deberá solicitar al departamento de Gestión Humana los respectivos roles y funciones de los siguientes cargos:

i) Ingenieros de datos
j) Coordinadores de datos
k) Jefaturas de IT
l) Gerencia de IT
m) Gerente de Control Interno y Auditoria

La información a continuación se debe de solicitar a quien corresponda.

n) Manual de proceso de respaldos y configuraciones.
o) Licencias y fechas de expiración de cada software utilizado (Si fuera necesario su control)
p) Llaves de casillero Bancario
q) Unidades de tape IBM 1,5 TB

4. RESPONSABILIDAD Y AUTORIDAD

En este ítem se debe detallar el cargo de las personas involucradas en la misma, debe constar los responsables de la elaboración del documento, así mismo la persona que elabora y responsable de la Política aplicada, las personas que aprueban la legalización del documento presente y su respectiva socialización.

5. Este documento se lo considera como NO PUBLICO y solo deberá ser divulgado con los involucrados, incluyendo a Gerencia de Auditoría Interna, Gerencia General, y demás mandos altos que aprueban el uso y aplicación del mismo para los fines consiguientes.

6. IDENTIFICACIÓN

   Este documento se identifica como POLÍTICAS PARA EL USO Y MANEJO DE LOS RESPALDOS INFORMÁTICOS DE **"LUTEXSA IND. COM. CIA. LTDA"** EN CINTAS con su respectivo Código: PL.TIC.001

7. HOJA DE MODIFICACIONES

# REVISIÓN	**TIPO DE MODIFICACIÓN**	**REVISADO**	**APROBADO**	**FECHA**

8. SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE

Para el acceso a los sitios y áreas restringidas se debe notificar a al responsable del centro de datos para la autorización correspondiente, y así proteger la información y los bienes informáticos.

Debe de justificar su ingreso, deberá estar acompañado de un delegado del departamento con una bitácora registrando con fecha y hora de ingreso y salida de la misma manera debe ser estar firmada la bitácora por el visitante en donde registre sus datos personales, en caso de ser externo debe de presentar identificación y el motivo del ingreso.

9. Protección de la Información y de los Bienes Informáticos

9.1 Reportar de forma inmediata:

El usuario o funcionario deberán reportar de forma inmediata a la **Oficina Nuevas Tecnologías** cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

9.2 Obligación de proteger

El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

9.3 Responsabilidad del Usuario o Funcionario

Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

9.4 Controles de acceso físico

9.4.1 Ingreso a las instalaciones de LUTEXSA IND. COM. CIA. LTDA

Cualquier persona que tenga acceso a las instalaciones deberá registrar al momento de su entrada el equipo tecnológico (computador, Tablet, filmadora, cámara fotográfica), equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción o portería, el cual podrán retirar el mismo día.

En caso contrario deberá tramitar la autorización de salida correspondiente.
Se prohíbe el uso de los aparatos tecnológicos dentro del data center que permitan realizar algún tipo de toma fotográfica o filmación de ningún tipo.

9.4.2 Equipos Personales y Portátiles

Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá ser retirado de las instalaciones de empresa, únicamente con la autorización de salida del área de Inventarios, anexando el comunicado de autorización del equipo debidamente firmado por el Secretario General o por el Jefe de la **Oficina Nuevas Tecnologías"**.

9.5 SANCIONES

El incumplimiento de normas y/o disposiciones de este reglamento estará sujeto a investigación administrativa y a la imposición de medidas disciplinarias correspondiente.

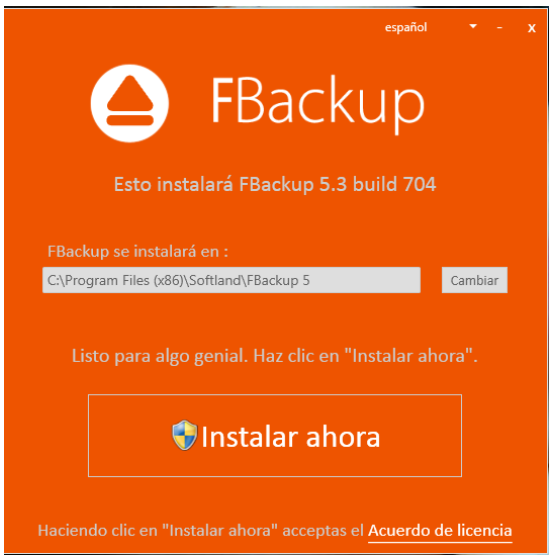
Se deberá realizar un informe en el cual especifique la infracción realizada, el mismo documento tendrá que ser firmado por la persona o personas implicadas y su conocimiento.

Deberá ser notificado a la gerencia de sistemas para que notifique al departamento de talento humano con el fin de tomar acción previa análisis de evento sucedido, de la misma manera tendrá que ser reportado a gerencia general para su notificación.

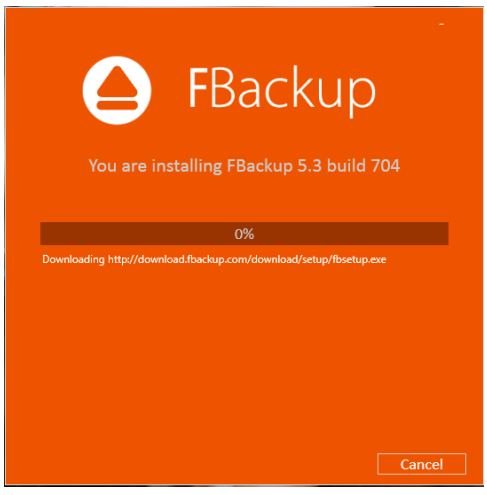
3.8.3. MANUAL DE INSTALACIÓN EN CLIENTES PARA RESPALDOS INFORMÁTICOS DE “LUTEXSA IND. COM. CIA. LTDA.”

INSTALACIÓN DE SISTEMA DE RESPALDO DE INFORMACIÓN

En la imagen siguiente muestra la pantalla inicial al momento de iniciar la instalación del programa de respaldo de información en su versión 5.3 en donde te indica en directorio en donde se instalara, puede ser cambiada la dirección por defecto a otra que el profesional IT requiera. Al presionar la opción Instalar ahora está aceptando el acuerdo de licencia del fabricante.

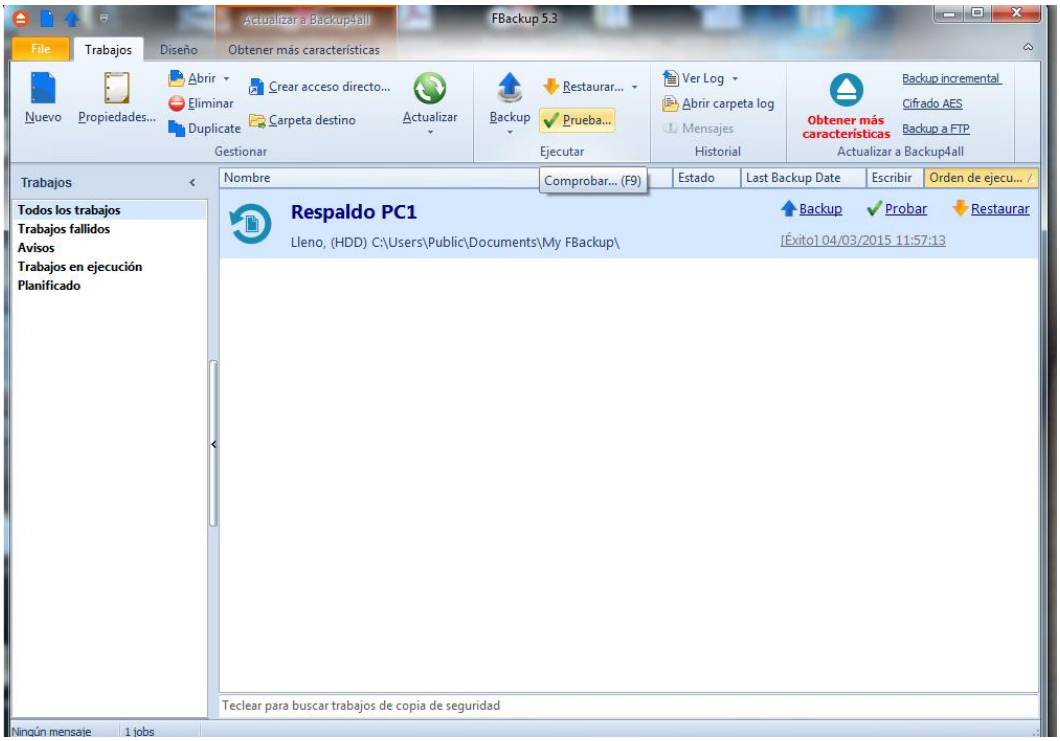


En la imagen () a continuación muestra el proceso de la instalación, se debe tomar en consideración que no muestre ningún mensaje de error al momento de su ejecución.



En la imagen a continuación observar ver la pantalla inicial por defecto al momento de iniciarlo presionando doble clic en el icono que se encuentra en el escritorio “Respaldo de información 5”.

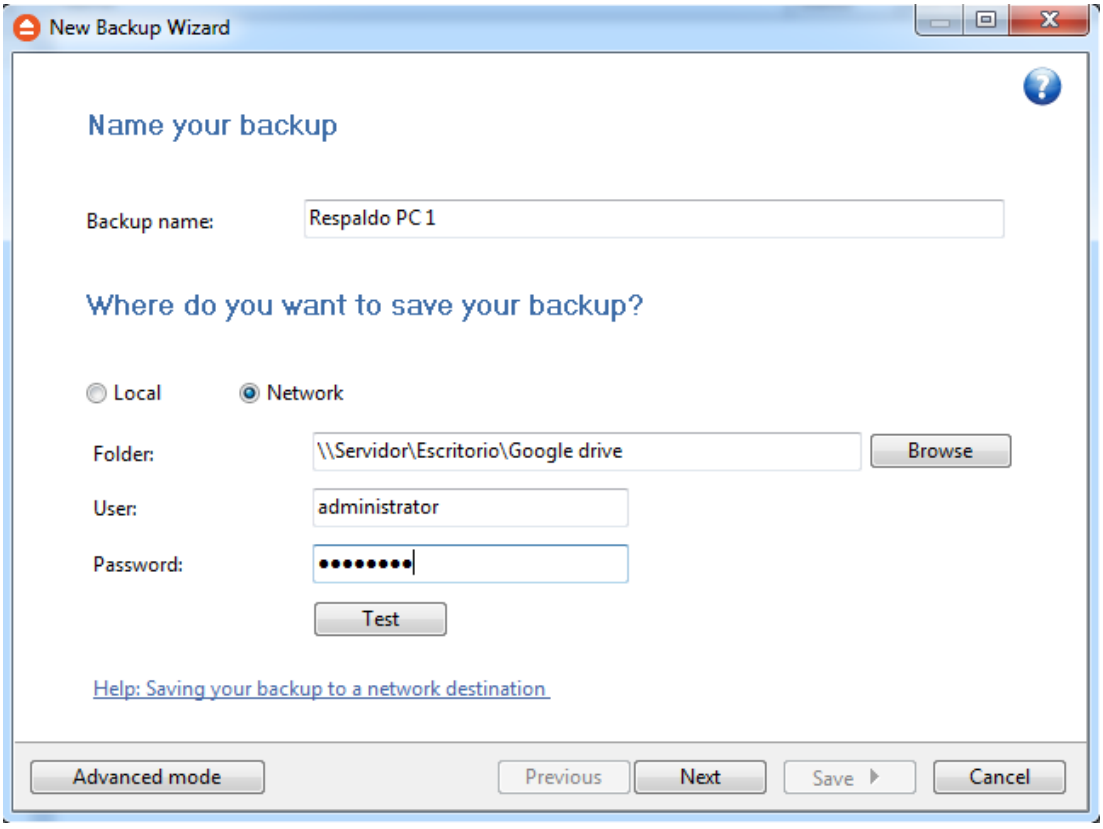
Esta pantalla cuenta con 4 menús y es la pantalla principal para iniciar la configuración de los escenarios a respaldar, cabe aclarar que los escenarios pueden ser variados dependiendo el funcionario al que se desea respaldar la información.



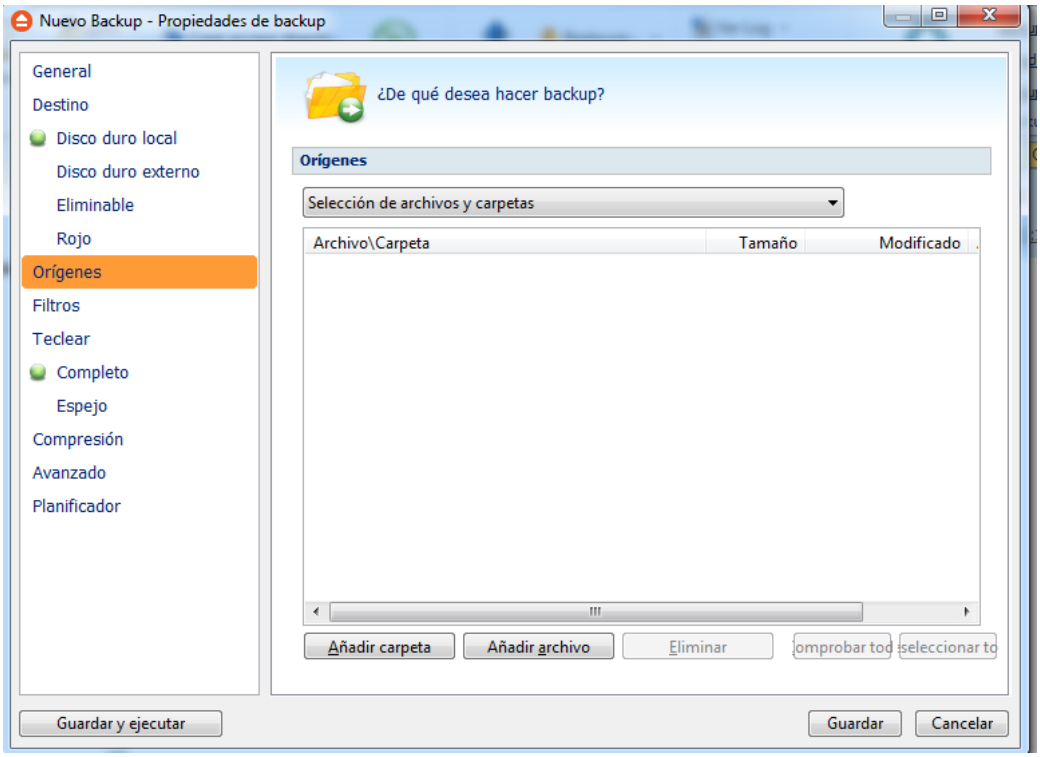
En la imagen muestra la manera de cómo empezar la configuración inicial de los respaldos en donde pide ingresar por teclado el nombre del respaldo, el nombre podría estar relacionado a un usuario por ejemplo “Gerentes” en donde se debe de respaldar la mayor información posible ya que se consideran maquinas críticas, o se podría darle el nombre de un usuario es especial si es un usuario que no es relevante respaldar sus archivos de correos pero si los archivos digitales que se encuentran en un directorio en especial. Se debe de analizar la naturaleza de su cargo junto con sus obligaciones y responsabilidades encomendadas.

Los respaldos se pueden realzar de 2 maneras, de manera local que lo que realiza es realizar el respaldo en el mismo equipo del usuario o dejarlos en la red de la empresa, en el escenario de Lutexsa Ind. Com. Cia. Ltda., se debe de seleccionar el servidor que se a configurado previamente como repositorio de los archivos de los usuarios y su respectivo directorio asignado, adicionalmente se debe de indicar un usuario con privilegios de administrador y su respectiva clave para que al momento de realizar el respaldo puedan autenticar o identificar que es un usuario valido para el ingreso al servidor y colocar sus respaldo.

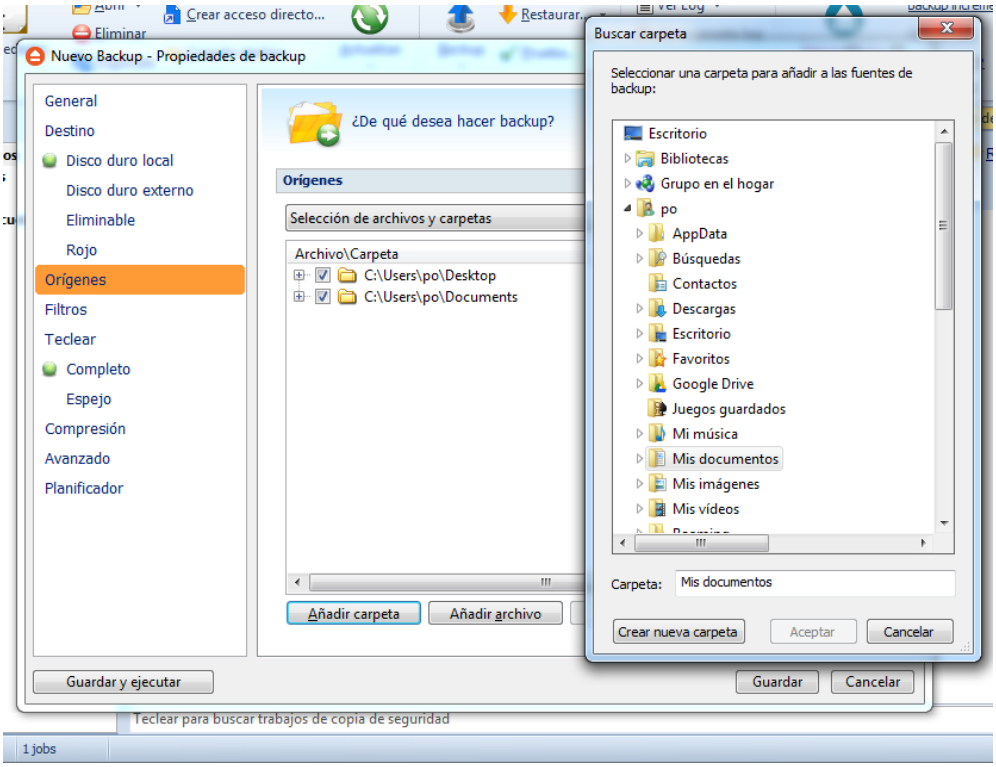
Para realizar pruebas del usuario ingresado de recomienda seleccionar “Test”, validara el usuario y clave antes ingresado.



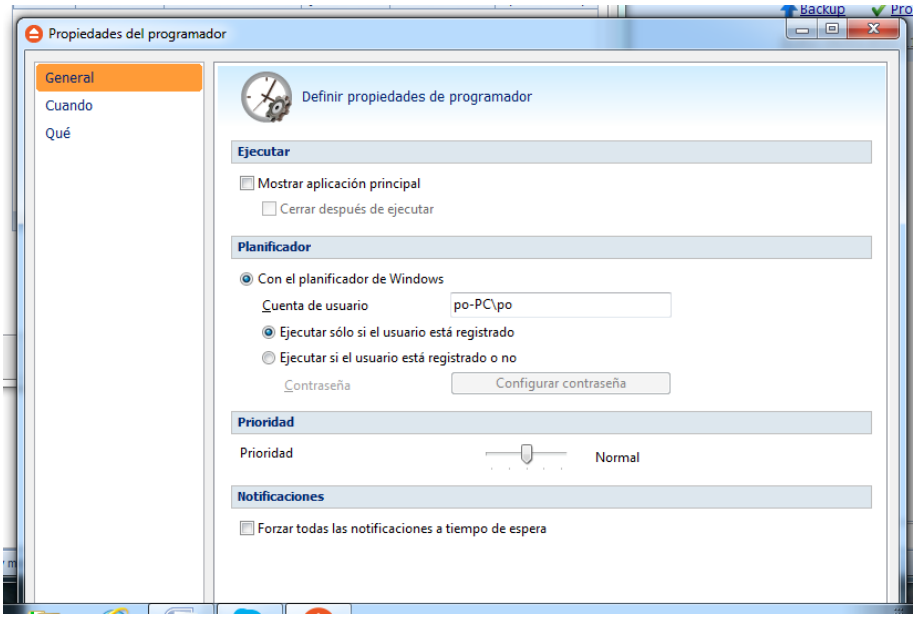
En la imagen () a continuación que se muestra al presionar “Modo Avanzado” es una manera de cómo iniciar a agregar carpetas o directorios manualmente o automáticamente seleccionando en Orígenes y desplegar la lista.



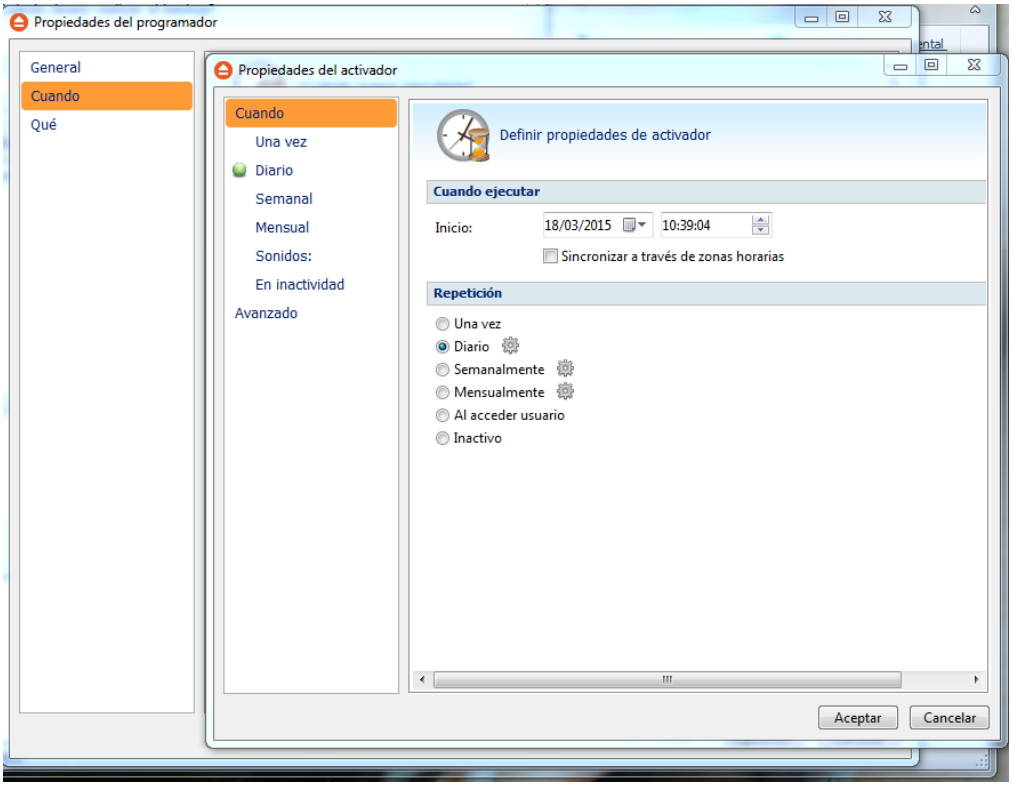
En la imagen () a continuación se procede a seleccionar los directorios que se desea respaldar se tiene que una de las políticas en las sedes remotas de Lutexsa Ind. Com. Cia. Ltda., que se deben de guardar toda la información en el “Escritorio” y “Mis Documentos” de sus equipos esta configuración se realiza solo para los usuarios de las oficinas remotas con la que cuenta la empresa y poder tener una configuración estandarizada.



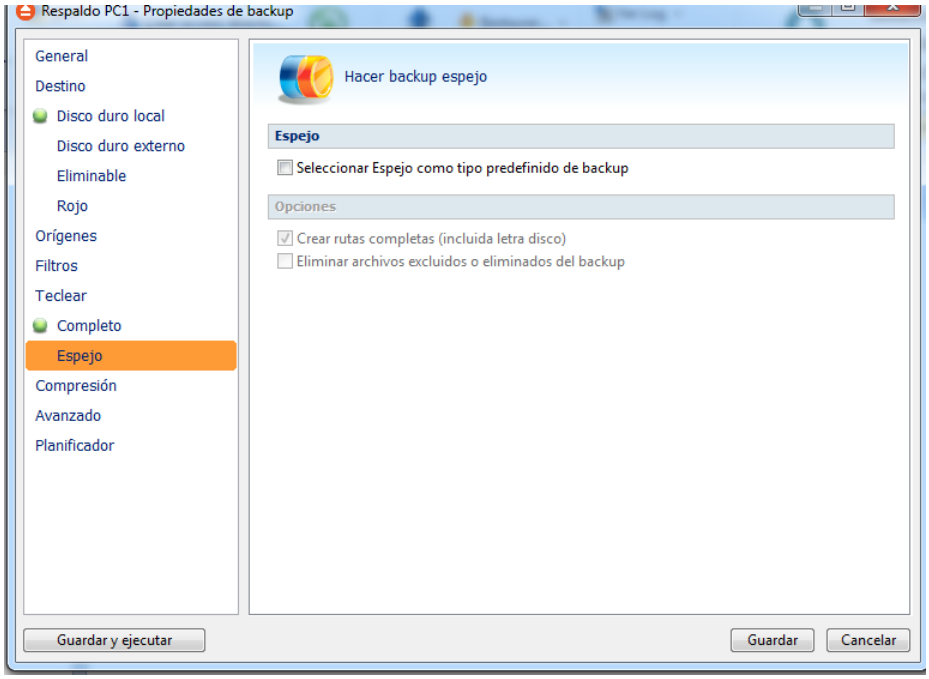
Es la figura () a continuación se podrá realizar la configuración, podrá indicar cuándo desea realizar el respaldo de la información, al presionar Añadir podrá indicar si el planificador se ejecutara cuando el usuario del equipo esté usando el equipo o no, de la misma manera ponerle prioridad de ejecución del programa.



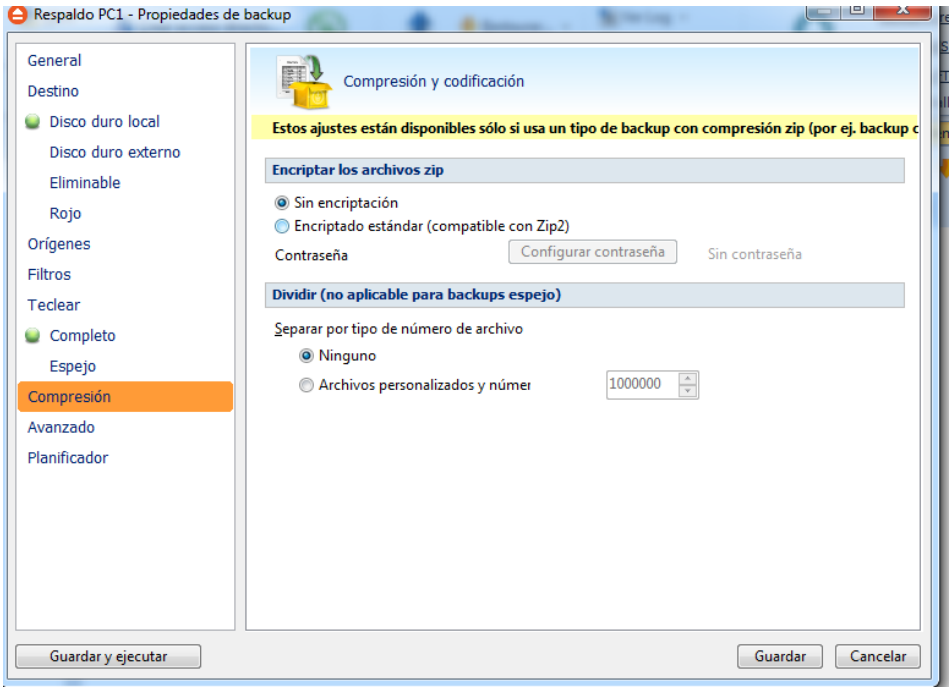
En la imagen () a continuación se debe de configurar el periodo o con qué frecuencia realizar el respaldo automático, se analizó la frecuencia de la estadía en oficina de los empleados en cada sede remota de Lutexsa Ind. Com. Cia. Ltda y se seleccionada la opción “Semanalmente” esto quiere decir que se ejecutara cuando el usuario acceda al computador los días pre configurados en este caso serán todos los lunes y viernes que por políticas deberán de estar en oficina nos equipos para su respaldo de información.



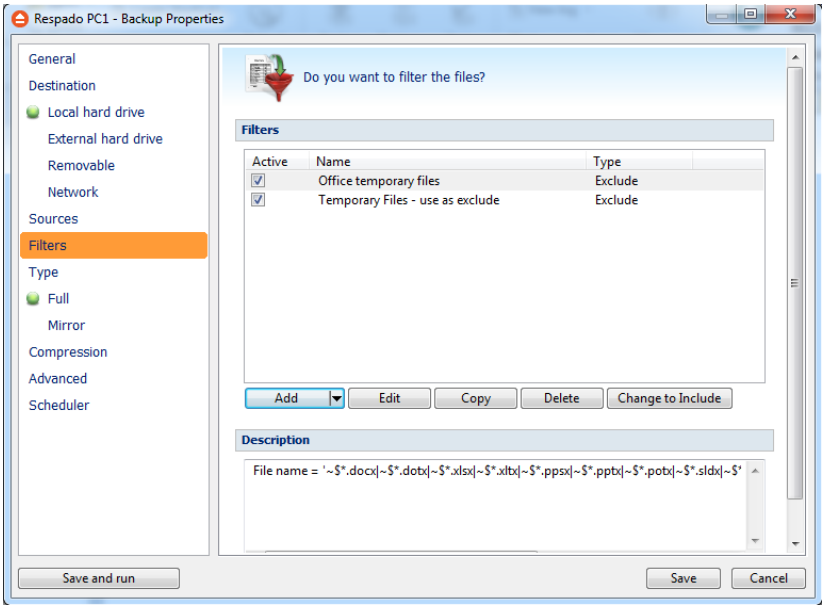
En la imagen () a continuación se podrá realizar respaldos completos o tipo espejo que es usado para equipos críticos específicos, lo que realiza es hacer una imagen total del disco y evitar perdida de alguna información este respaldo se aplica al Gerente Comercial de la sede que se considera un equipo critico para la compañía.

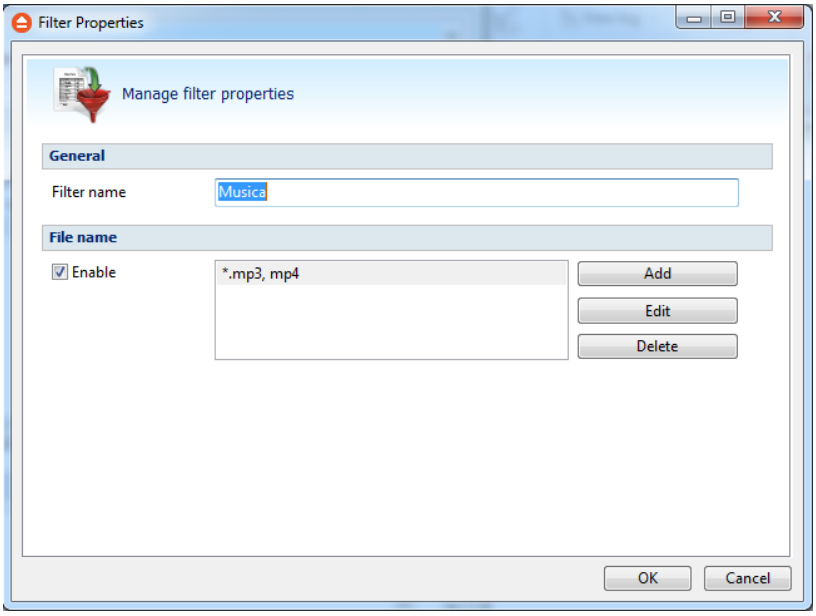


En la imagen () a continuación se puede indicar, por seguridad si lo respaldado este encriptado o sin encriptar y se le puede asignar una contraseña en el momento de realizar una restauración de archivos le pedirá la clave que autoriza a realizar la acción solicitada, la configuración antes descrita aplica a todo los trabajos realizados. Por seguridad, integridad, fidelidad de la información se dejara configurado de manera predeterminada que se ejecute el respaldo con clave de descompresión para todos los trabajos realizados.



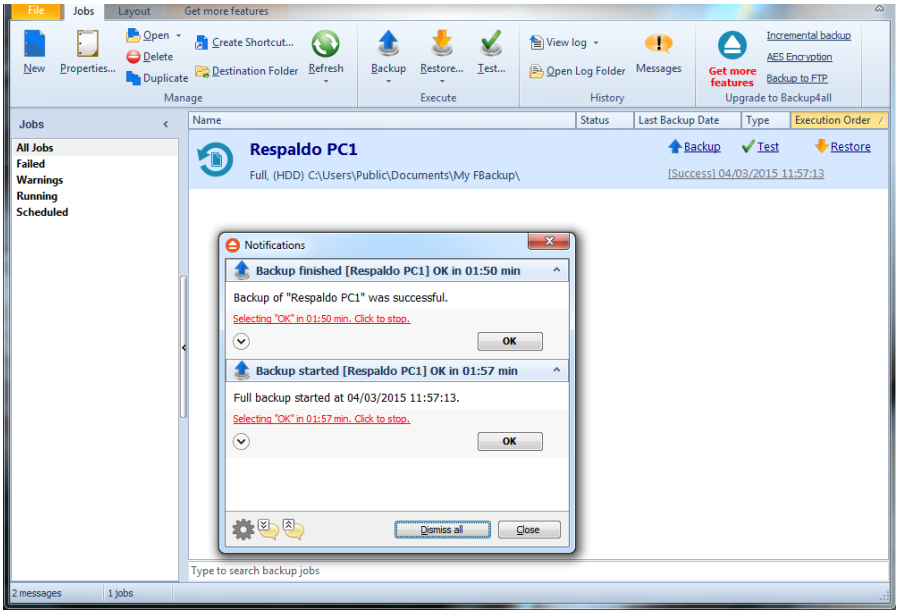
En las imágenes () a continuación es en donde se podrá crear reglas de respaldo, estas reglas sirven para excluir algún tipo de archivos a los respaldos esto se realiza previo análisis independiente de cada rol del empleado en el caso de tesis no aplica que se respalde ningún tipo de archivo multimedia esto quiere decir que se excluirán archivos con extensiones de formato musicales como .MP3, WMA, WMP, entre otros, videos como MP4, AVI, MPEG, MOV por omisión vienen configurados archivos temporales que no se respaldaran en esta ventana se adicionara todo los formatos de archivos que no se consideren críticos.





En la imagen a continuación se puede visualizar que ya se realizó un respaldo o un trabajo programado y se puede ver en la pantalla de notificación alguna novedad de cómo finalizo el mismo como indica que culmino satisfactoriamente y la hora en que termino, esto quedara como registros de los realizado.

Se deber de evidenciar el trabajo programado para dejar constancia de la ejecución y fiel cumplimiento de las políticas establecidas.



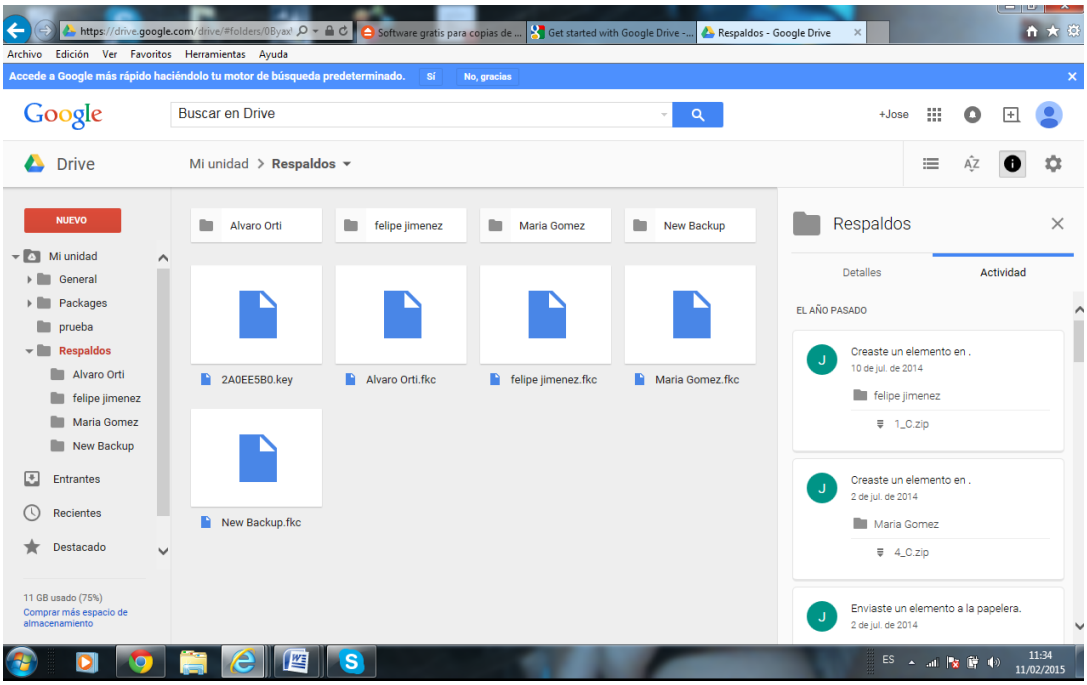
CONTROLES ISO 27002 -27005

Prueba de laboratorio de implementación para sistema de respaldo automático de información.

Para la prueba de laboratorio se cuenta con los siguientes hardware y software:

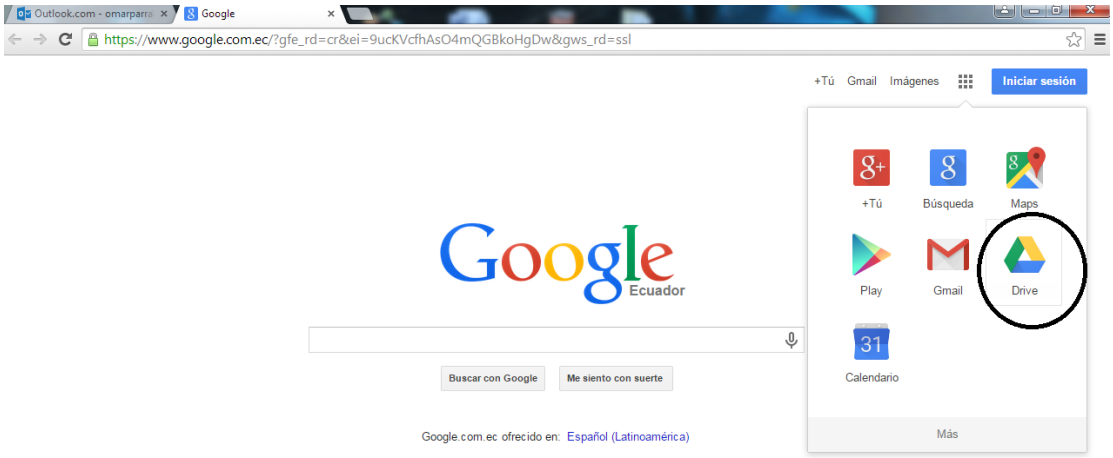
1. 2 servidor de la marca IBM,
2. 3 Clientes Windows 7 Profesional,
3. Licencia gratuitas de respaldo de información,
4. Enlace de internet de 1 mega dedicado con proveedor de última milla como telconet

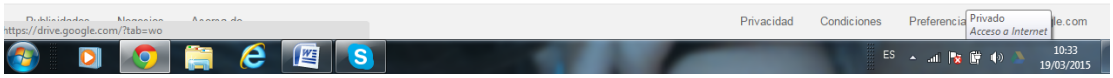
5. Una licencia free de google drive con capacidad de 15 gb.
6. Un robot de cinta Ultrium LTO 5 Capacidad 1,5TB,
7. Un servidor para respaldos
8. Un casillero de seguridad del Banco Internacional para enviar los tapes respaldados, cronológicamente previo análisis. Cartilla



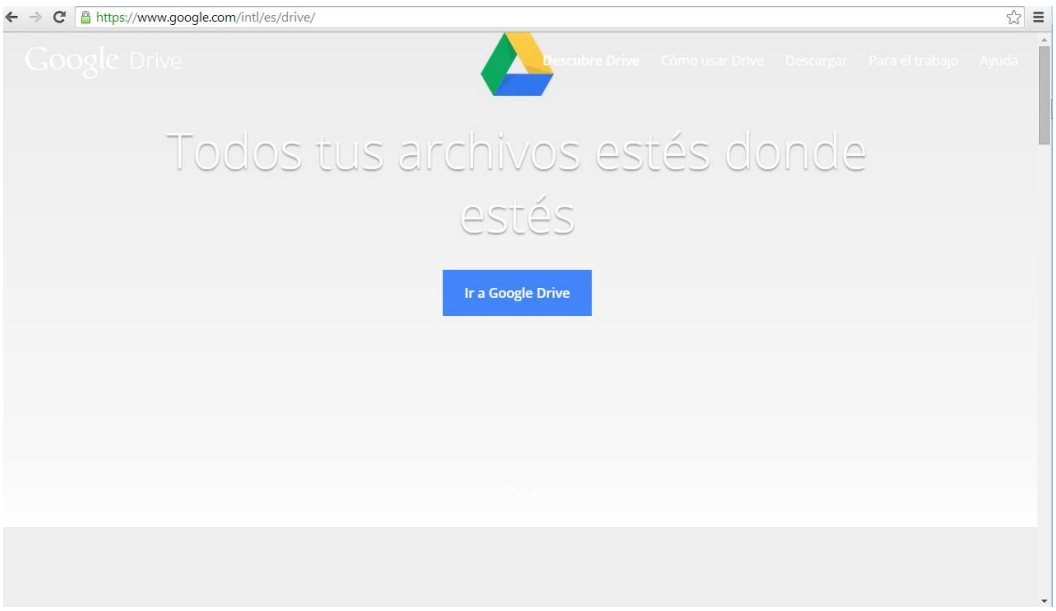
CUENTA GOOGLE DRIVE

Al ingresar a buscador e ingresar y digitamos www.google.com se podrá ver la imagen () a continuación en donde podrán observar en la parte media derecha el signo de Drive, seleccionamos esa opción y nos presenta la ventana en donde podemos iniciar la descarga del software.



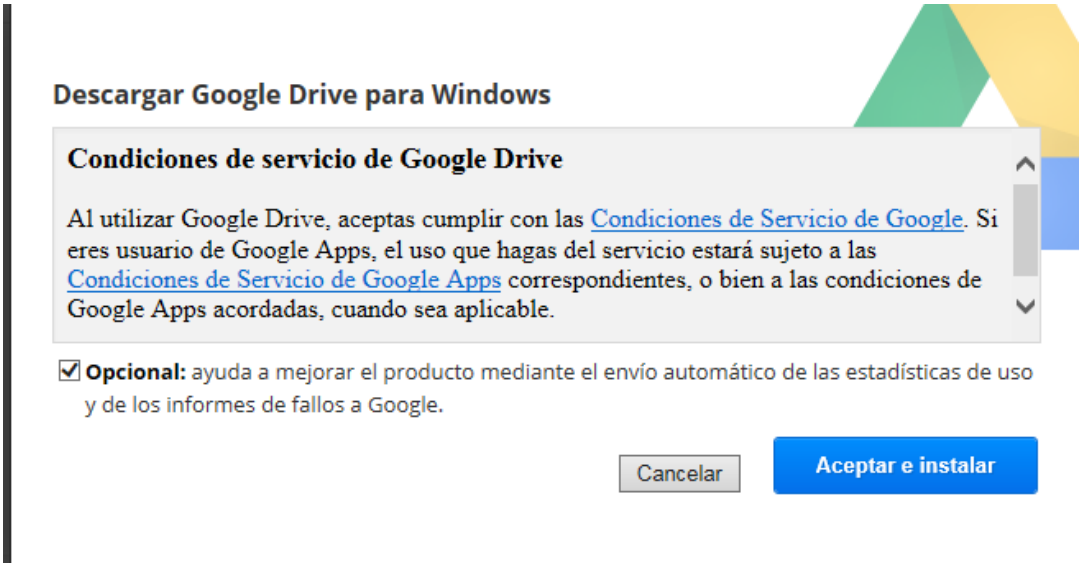


Adicionalmente de tener un respaldo en la nube de toda la información de la sede remota se cuenta con la posibilidad de tener la información en forma de copia espejo en el equipo que usted necesite.

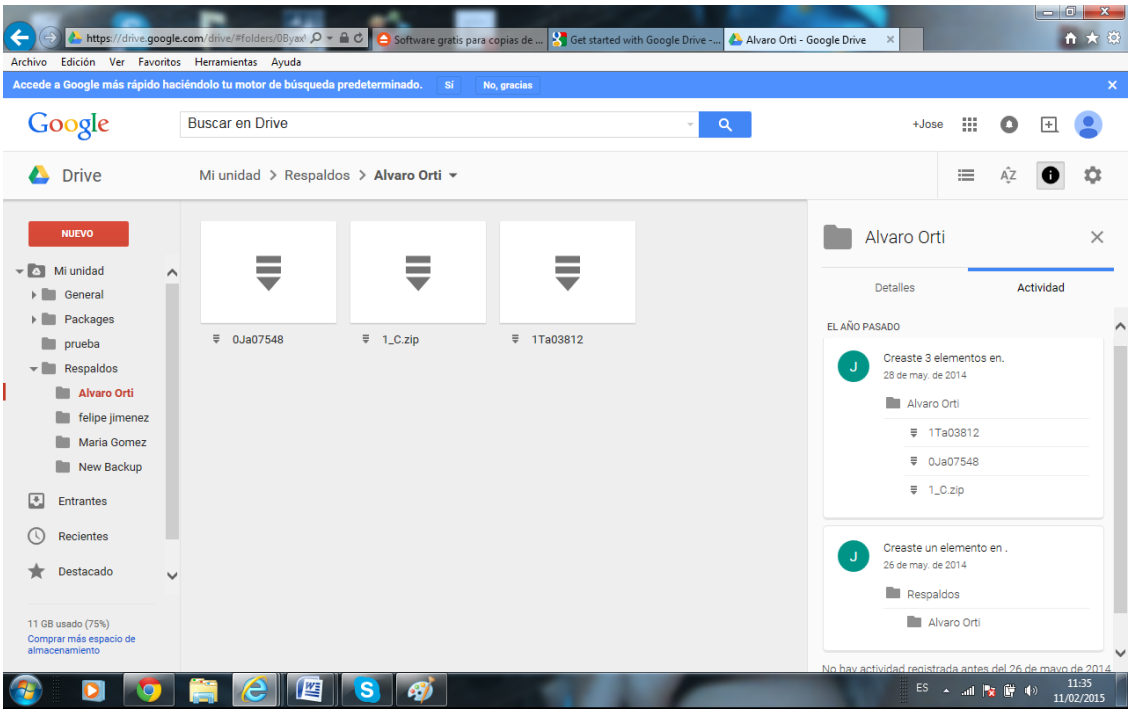


Al instalar esta aplicación también nos permite compartir información con mas personas que tengan instalado y permisos necesarios en sus equipos, esto quiere decir que si un funcionario de la empresa Lutexsa Ind. Com. Cia. Ltda se encuentra en el exterior y tiene acceso a internet el podrá subir archivos a la

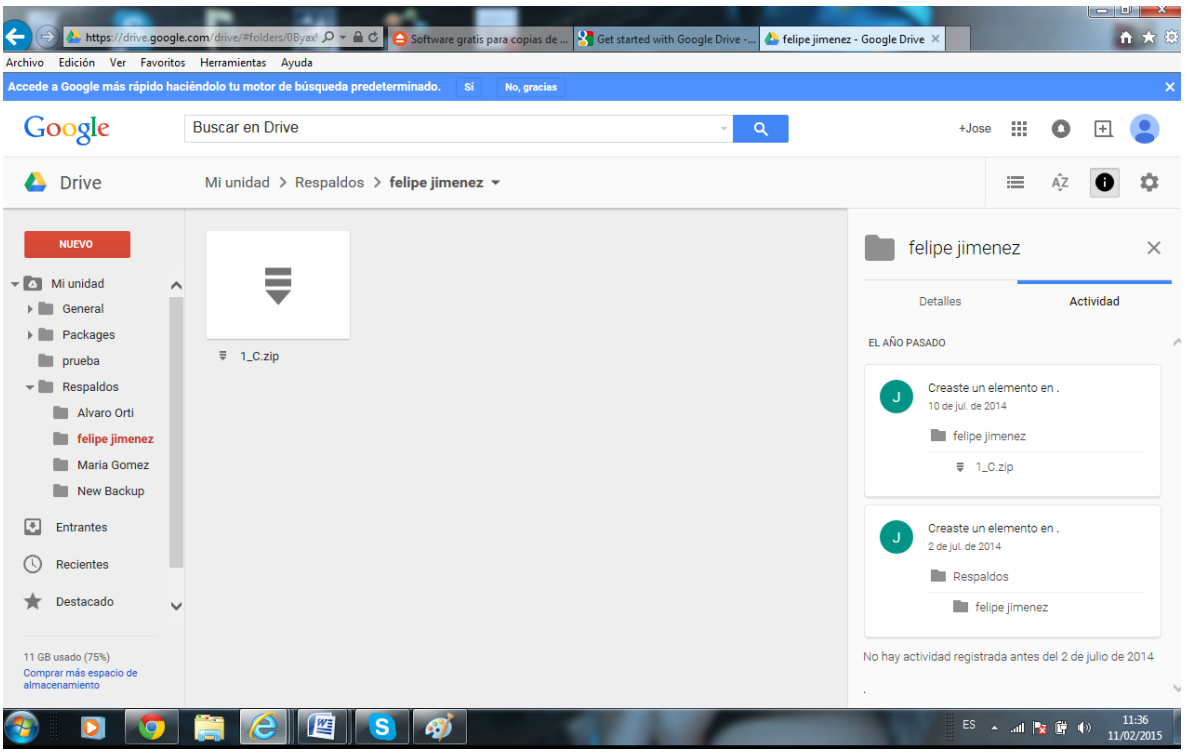
nube y se reflejara en sede remota y los usuarios de esa sede podrán acceder a esta información.



Cabe aclarar que esta instalación de debe de realizar en el servidor principal que almacenara los respaldo ejecutados con la herramienta para respaldar información, en el caso específico de Lutexsa Ind. Com. Cía. Ltda. Se aprovechara la infraestructura que se está armando se procederá a utilizar este mismo servidor como un repositorio de archivos compartidos o File Server.

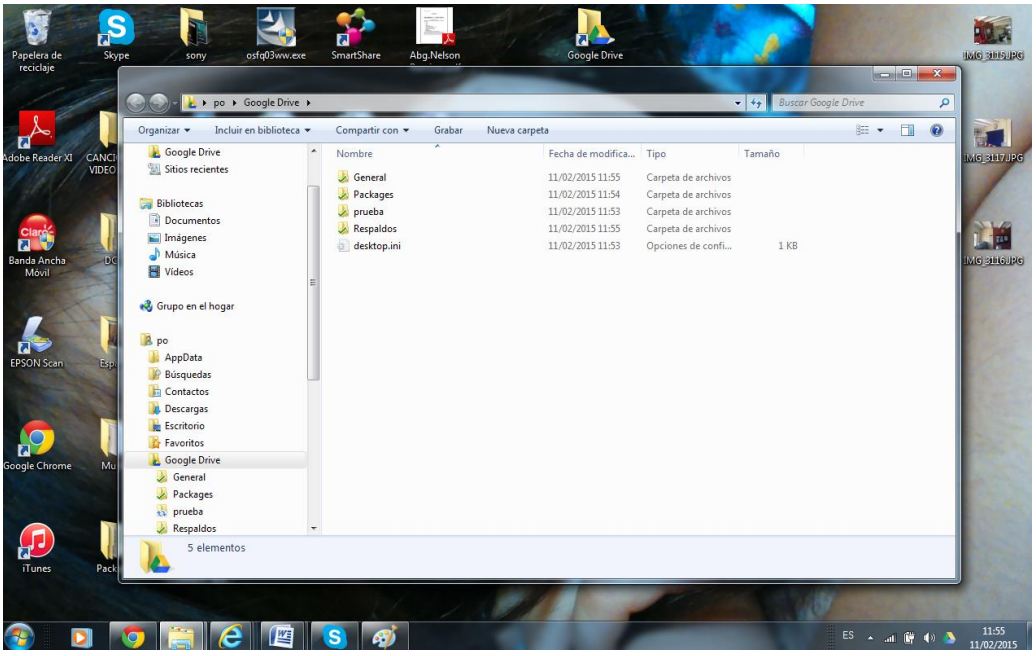


Una vez instalada la aplicación como lo muestra en la imagen anterior en el servidor que se cuenta en la oficina central de Guayaquil se puede visualizar el directorio y archivos que contiene el servidor de la sede remota de Quito Norte.



Una vez se cuenta con el acceso otorgado mediante la instalación, usuarios y claves configurados se podrá administrar completamente el directorio Google drive, que se presenta de manera de un icono en el escritorio. Al momento de instalar el directorio en las sedes remotas de todo el Ecuador de la compañía todas podrán tener acceso y estarán en red unidos por la **nube** o repositorio en internet.

Una vez culminada la instalacion del google drive en el servidor de la oficina principal se visualizara como muestra la imagen a continuacion. Se cuenta con un servidor IBM M2100 el mismo que tiene instalado un sistema operativo Windows Server 2008 STD, se cuenta con un robot de respaldo en cinta LTO 5 de marca IBM, este equipo se usara para poder sacar los respaldos de todas las sedes remotas que cuenten con las configuraciones e instalaciones indicadas..



3.9. IMPACTO DE LA PROPUESTA

Con la implementación de los manuales, políticas y procedimientos se lograra tener una confianza financiera, sabiendo que su información está totalmente resguardada y cumpliendo los procedimientos establecidos.

De la misma manera los servidores de aplicativos con los herramientas de recuperación de servidores virtuales.

3.10. TALENTO HUMANO.

Para la ejecución de la presente propuesta se debe de capacitar al analista de datos que es la persona encargada en el proceso y quien hara uso de la guía que se plantea.

3.11. RECURSOS TECNOLÓGICOS,

Para iniciar el proyecto de respaldo de información debemos de indicar los recursos informáticos a requerir con sus valores.

Tabla 9 Tabla de presupuesto

RECURSO FINANCIERO A REQUERIR		
#	**Descripción**	**Valores**
1	Tape Respaldo de información LTO 5	$ 1.638,57
1	Servidor Dell Power edge T11Q II	$ 2.636,00
1	Enlace Internet 1 MB	$ 1.800,00
1	Windows Server 2012 R2 SNGL OLP NL 2 Proc	$ 1.049,53
1	Switch 25 Ptos gigabit	$ 310,00
1	NAS Sponlogy DiskStation 3TB	$ 1.265,00
	Total	$ 8.699,10
	IVA	$ 1.043,89
	Sub- total	$ 9.742,99

Elaborado: 10 Autor de Tesis

3.12. BALANCE GENERAL

Tabla 10 Balance General

Balance de General Lutexsa Ind. Com. Cia. Ltda Al 31 de diciembre 2014		
ACTIVOS ACTIVOS CORRIENTES		
Efectivo	$	1.721.982,25
Inversiones temporales	$	105.199,19
Inv temp disponible vta	$	5.769.050,92
Deudoras	$	8.460.729,89
inventario	$	6.439.564,94
Gasto pagado anticipado	$	122.854,89
Total activo corriente	$	22.619.382,08
ACTIVOS NO CORRIENTES		
Inversiones permanentes	$	1.463.422,80
Deudores	$	25.639,41
Propiedades, planta y equipos	$	2.284.607,81
Intangibles	$	2.221.921,36
Cargos diferidos	$	1.221.269,76
Otros activos	$ 930,24	
Valorizaciones de activos	$	982.236,65
Total pasivo corriente	$	8.200.028,03
Pasivos y Patrimonio de los Accionistas Pasivo corrientes		
Obligaciones financieras	$	1.642.905,11
Proveedores	$	1.219.278,57
Cuentas por pagar	$	335.155,04
Impuestos, gravámenes y tasas	$	344.097,71
Obligaciones laborales	$	24.185,22
Pasivos estimados y provisiones	$	169.122,89
Otros pasivos	$	206.941,61
Total de los pasivos corrientes	$	3.941.686,16
Pasivos no corrientes		
Obligaciones financieras	$	3.016.990,00
Impuestos, gravámenes y tasas	$	72.710,96
Pensiones de Jubilación	$	608,30
pasivos diferidos	$	420.886,63
Patrimonio de accionistas	**$**	**749.669,61**

Capital suscrito y pagado	**$**	**2.595.839,63**
Superávit por método de participación	$	103.997,75
Reserva	$	712.348,58
Revalorización del patrimonio	$	49.072,18
Utilidad neta del año	$	503.510,65
Utilidad acumulada no apropiadas	$	705.316,44
Superávit por valorizaciones	$	982.236,65
Total patrimonio de los accionistas	$	25.607.966,00
Total del pasivo y del patr. de los accionistas	$	9.913.187,39
Cuenta de orden	$	35.800,00

Fuente: 1 Lutexsa Ind. Com. Cia. Ltda

Se realiza cuadro de depreciación como equipos computacionales según normas contables Ecuatorianas.

3.13. DEPRECIACIÓN DE EQUIPOS COMPUTACIONALES 4 PERIODOS

Tabla 11 Depreciación equipos tecnológicos

DEPRECIACIÓN DE ACTIVO	
MÉTODO:	**LÍNEA RECTA**

DATOS:		
VALOR ACTIVO	$	9.742,99
VALOR RESIDUAL	$	800,00
VIDA ÚTIL EN AÑOS		4

CUADRO DE DEPRECIACIÓN			
PERIODO	**CUOTAS DE DEPRECIACIÓN**	**DEPRECIACIÓN ACUMULADA**	**VALOR NETO EN LIBROS**
1	$ 2.235,75	$ 2.235,75	$ 7.507,24
2	$ 2.235,75	$ 4.471,50	$ 5.271,50
3	$ 2.235,75	$ 6.707,24	$ 3.035,75
4	$ 2.235,75	$ 8.942,99	$ 800,00

Elaborado: 11 Autor de Tesis

3.14. IMPLEMENTACIÓN

3.1.1. CRONOGRAMA DE ACTIVIDADES.

Se muestra un cronograma de ejecución de la actividad en el anexo #1

3.1.2. LINEAMIENTOS DE EVALUACIÓN DE LA PROPUESTA

El desarrollo de documentos para conseguir la salva de información en la empresa Lutexsa. Ind. Com. Cía. Ltda.

- Recuperabilidad de la información.
- Plan de continuidad de negocio.
- Bajo impacto en caso de eventos.

CONCLUSIÓN

El presente trabajo de tesis presenta y describe un procedimiento para llevar a cabo los procesos de almacenamiento y salva en centros de datos teniendo en cuenta las posibles condiciones tecnológicas que se puedan presentar. Se llevan a cabo una serie de actividades que conforman un ciclo de acciones para cada proceso y se complementan con la utilización de las herramientas seleccionadas.

La utilización de los debidos procesos especificados en el presente como ANEXOS los cuales detallan las acciones a seguir.

Garantiza los procesos de almacenamiento y salva en los CPD con la utilización de las herramientas seleccionadas, en él se describe el personal encargado de la ejecución de las tareas que serán llevadas a cabo en las diferentes etapas por las cuales se encuentra compuesto. Es capaz de adaptarse a las condiciones tecnológicas con que cuente el centro de datos donde se decida utilizar, siempre y cuando se cumpla con los requerimientos mínimos que se establecen a lo largo de su descripción, brindándole las soluciones que se ajusten con su equipamiento.

Durante el ciclo de vida del procedimiento se necesita de un personal especializado cuya función sea llevar a cabo cada una de las actividades que tributan a la obtención de adecuados proceso de almacenamiento y salva. Teniendo en cuenta lo antes planteado se han definido como roles que intervienen el especialista de almacenamiento y el especialista de copia de seguridad**,** responsables del proceso de almacenamiento y salva respectivamente

RECOMENDACIONES

A partir de las conclusiones abordadas se listan las recomendaciones en vistas de posibles mejoras:

- TECNOLOGÍA
    - Contar con equipamiento que asegure el éxito del proceso.
    - Contar con las garantías y plan de trabajo en el área de tecnología
    - Contar con proveedores estratégicos que garanticen los canales con una calidad de servicio debidamente certificada.

- TALENTO HUMANO
    - Difundir y controlar las estrategias que se definen y control de su realización.
    - Capacitación constante a todo el personal que interviene en la presente propuesta.
    - Plan de carrera que les permita desarrollar sus habilidades para el bien de la empresa
    - Control de conocimientos en el personal con el fin de poder determinar los niveles de conocimientos.

- ACTUALIZACIÓN DE DOCUMENTOS
    - Ampliar el alcance de la presente propuesta con la inclusión del proceso de replicación de la información en Centros de Procesamiento de Datos.
    - Realizar actualizaciones de políticas y procedimientos cada 6 meses con el fin de mejorar los procesos, deben de estar debidamente documentados.
    - Realizar pruebas de recuperabilidad cada 6 meses y mejorar acciones a realizar tomando en consideración el medio y los cambios tecnológicos.

Bibliografía

CSI, C. S. (2002). *Computer Crime and Security Survey*. Obtenido de https://www.fishnetsecurity.com: https://www.fishnetsecurity.com/6labs/blog/csi-computer-crime-security-survey-2011

Dhillon, G. y. (2000). Information System Security Management in the New Millenium.

Di Rienzo, J., Casanoves, F., Gonzalez, L., *Tablada, E., Díaz, M., Robledo, C., & Balzarini, M. (2008). Estadisticas para las Ciencias Agropecuarias.* Córdoba: Editorial Brujas .

Ecuador, C. P. (Registro Oficial. Suplemento 557 de 17 de Abril del 2002.). Tipos de Delitos Informáticos existentes en la legislacion Ecuatoriana. En *Ley de Comercio Electrónicos.* Ecuador.

El comercio. (2 de Julio de 2010). *El ciberdelito ataca al sector público*. Recuperado el Noviembre de 2015, de http://www.elcomercio.com/actualidad/seguridad/ciberdelito-ataca-al-sector-publico.html

El universo. (30 de junio de 2015). *Ecuador y Brasil firman memorando para luchar contra el crimen organizado*. Obtenido de http://www.eluniverso.com/noticias/2015/07/30/nota/5045827/ecuador-brasil-firman-memorando-luchar-contra-crimen-organizado.

Eloff, J. y. (2003). Information Security Management. En A. N. Paradigm.

En linea. (s.f.). Obtenido de http://izc.com.co/modulosIZC/modGarantias/copiasFacturas/terramaster.pdf

Freire, J. (1 de julio de 2013). *Doctor Tecno*. Obtenido de http://www.doctortecno.com/noticia/crecimiento-del-cibercrimen-ecuador-es-130

(2003). En R. y. Garigue, Information Security Governance Reporting. (págs. 36-40).

Geffert, B. (2004). Incorporating Security Requirements into an Enterprise Security Program.

Gestion empresarial. (07 de 01 de 2013). *renatamarciniak.wordpress.com*. Recuperado el noviembre de 2015, de www.renatamarciniak.wordpress.com/2013/01/07que-es-un-plan-estrategico/

Grundvig, J. (8 de Enero de 2014). La Gran ëpoca. Recuperado el Noviembre de 2015, de http://www.lagranepoca.com/archivo/30567-verdadero-costo-ciberataques-para-empresas.html

Isaac Forés, C. m. (s.f.). Red Seguridad. Obtenido de El impacto económico de los ataques de seguridad: http://www.redseguridad.com/opinion/articulos/el-impacto-economico-de-los-ataques-de-seguridad

Masacci, F. P. (2005). Using a security requirements engineering methodology in practice:.

Mendoza, M. Á. (9 de Abril de 2015). Welivesecurity. Recuperado el Noviembre de 2015, de Backup en empresas: enfoque normativo de los respaldos de información: http://www.welivesecurity.com/la-es/2015/04/09/backup-empresas-enfoque-normativo/

Microsoft. (2015). *https://support.microsoft.com*. Obtenido de https://support.microsoft.com/es-es/kb/325863/es

moraldo networks. (s.f.). Obtenido de http://www.moraldonetworks.com.ar/services/backup.htm

Openfiler. (s.f.). Obtenido de http://www.openfiler.com/products

Peltier, T. (2003). Preparing for ISO 17799. En *Security Management Practices* (págs. 21-28).

Pino, D. S. (2009). *Perfil de los delitos informáticos en el Ecuador.* Quito - Ecuador: Fiscalia General Del Estado.

Roberto Hernandez Sampieri. (2014). Metodologia de la Investigacion. México D.F.: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Siegel, C. S. (2002). Cyber-Risk Management. En *Technical and Insurance Controls for Enterprise-Level Security. Security Management Practices* (págs. 33-49).

SYMANTEC. (2012). *symantec*. Recuperado el 11 de 2015, de http://symantec.com/es/mx/about/page.jsp?id=infosurvey

Symantec Corporation. (2012). *REPORTE SOBRE EL COSTO Y MANEJO DE INFORMACIÓN EMPRESARIAL*. Obtenido de http://www.symantec.com: http://www.symantec.com/es/mx/about/page.jsp?id=infosurvey

Tsujii, S. (2004). En *Paradigm of Information Security as Interdisciplinary Comprehensive Science. Proc.* (págs. 1-12).

Veeam. (s.f.). Obtenido de http://www.veeam.com/es/vmware-esx-backup.html.

Von Solms, B. (2005). Information Security governance. En *COBIT or ISO 17799, Computers & Security* (págs. 24,99-104).

Von Solms, B. y. (2001). En *Incremental Information Security Certification. Computers & Security* (págs. 20, 308-310).

Walton, J. (2002). Developing an Enterprise Information Security Policy.