INFORME FINAL DE INVESTIGACION

AIDA SEMILDE CAMARGO
CARLOS ANDRES RODRIGUEZ GONZALES

PROPUESTA DE PLAN DE CONTINUIDAD, DISPONIBILIDAD Y RECUPERACIÓN PARA EL SISTEMA DE PLANIFICACIÓN DE RECURSOS EMPRESARIALES (ERP) DE LA UNIVERSIDAD EAN

UNIVERSIDAD EAN
FACULTAD DE ESTUDIOS A DISTANCIA
ESPECIALIZACIÓN EN GESTIÓN DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN EN LA EMPRESA
BOGOTA D.C

2012

AGRADECIMIENTOS

Al Padre Creador arquitecto del universo por guiar y enviar todo el apoyo necesario para el desarrollo de este documento.

Carlos Andrés Rodríguez González agradece;

A mi esposa Karen Fonseca, por toda su paciencia, comprensión y gran apoyo.

A mis padres Emma y Carlos y mi Abuela Ana por estar tan pendientes, así como a mi hermana Ivonne, mis hermanos Johan y Hernán Prieto por su gran motivación y apoyo.

A mis tíos Jairo y Betty mis segundos padres, por sus invaluables consejos.

A nuestros familiares y amigos que de una u otra forma han sido parte de esto

Aida Camargo Agradece;

Gracias a mi amigo y compañero Carlos Andrés Rodríguez por su inmenso esfuerzo por hacer de esta idea un hecho.

A mi familia por ser siempre los grandes ángeles que guían y acompañan mi camino, a mi madre Amanda Camargo por su confianza y amor incondicional y a todos aquellas personas que hicieron parte de este proyecto en algún momento

Queremos agradecer de manera Especial:

A nuestros profesores, tutores y amigos Elizabeth Chaparro, Manuel Riveros Villalobos, Martha Aldana, por todo su tiempo, gran dedicación e invaluables aportes, al Ing, Rafael Barros, Ing. Jose Divitt Veloza, Ing Luz Marina, Ing Cesar Idrobo, Ing. John Porras, y a nuestro amigo el Ing. Henry Díaz por todos sus grandes aportes.

UNIVERSIDAD EAN

TABLA DE CONTENIDO

UNIVERSIDAD EAN

ÍNDICE DE TABLAS

UNIVERSIDAD EAN

ÍNDICE DE ILUSTRACIONES

OBJETIVOS

Objetivo General

Generar una propuesta de plan de continuidad, disponibilidad y recuperación, mediante la aplicación de medidas de seguridad y control de riesgos, para el sistema de planificación de recursos empresariales (ERP) SEVEN de la universidad EAN.

Objetivos Específicos

- Definir, modelos de análisis adecuados, que serán utilizados para establecer el nivel de riesgo y seguridad en el ERP de la Universidad EAN.

- Determinar los posibles eventos que pueden afectar la continuidad del (ERP) SEVEN de la universidad EAN.

- Proponer las medidas adecuadas que deben ser contempladas para implementar planes de continuidad, disponibilidad y recuperación del (ERP) SEVEN de la universidad EAN.

1. INTRODUCCIÓN

La continua evolución a nivel informático, ha permitido la sistematización de muchos procesos de manera más efectiva y eficiente.

En algunos casos, muchos de estos, dejaron se realizarse de manera presencial, a realizarse de manera virtual, por medio de lo que ahora se conoce como transacciones digitales.

La demanda en cuanto a la implementación de estos procesos y de la nueva generación de sistemas de información en línea, ha crecido exponencialmente en la última década, permitiendo así ofrecer servicios no solo a nivel interno de la empresa, sino a nivel externo.

Debido a lo anterior la información se ha convertido en el nuevo activo más celado y cuidado de las empresas, ya que con este se pueden tomar decisiones que van de la mano de los objetivos misionales de la empresa, permitiendo así posicionarse en niveles estratégicos en la competencia.

Por otra parte, teniendo en cuenta que para poder implementar estos sistemas es preciso contar con ciertos recursos a nivel humano y físico, es necesario analizar las posibles vulnerabilidades que se puedan presentar, convertirse en una amenaza, materializarse y generar, no solo tiempos muertos en la producción, sino perdida irrecuperable de la información o robo de la misma.

Por tal razón, y partiendo desde la afirmación de que ningún sistema es 100% seguro, es necesario contar con ciertos protocolos o lineamientos a seguir, para poder afrontar estos posibles riesgos y minimizarlos a un ítem cuantificable y manejable.

El presente Informe Final de Investigación, no solo analiza diferentes criterios a tener en cuenta para poder detectar ciertas vulnerabilidades, sino las herramientas y

metodologías que se pueden implementar para poder crear una propuesta de plan de continuidad y recuperación de un sistema ERP en la universidad EAN.

2. JUSTIFICACIÓN

En el siglo XXI con el surgimiento de la llamada era del conocimiento el uso de las tecnologías es cada vez más frecuente no solo a nivel organizacional sino también doméstico, este avance se ve promovido por las entidades gubernamentales debido a la generación de diversas políticas en las cuales se contempla en fomentar el uso masivo de las tecnologías de la información y la comunicación para cada habitante del territorio nacional. Es por esto que en la actualidad, cada vez es más frecuente ver que las organizaciones bancarias, gubernamentales, académicas entre otras implementan parte de su portafolio de servicios en la web con el objetivo de minimizar las filas, las demoras y ahorrar tiempo en el desplazamiento de los usuarios y aumentar la cobertura de los servicios.

Para poder cumplir con las expectativas de los usuarios las grandes compañías fabricantes de partes tienen el reto de elaborar piezas que permitan aumentar la capacidad de almacenamiento y obtener tiempos de respuesta cada vez más cortos, las velocidades de transmisión de igual manera son cada vez más rápidos y la cantidad de información que es enviada es aún más grande que la que era enviada hace unos años, este continuo crecimiento exige que los anchos de banda sean cada vez más grandes y se deje de lado términos de Bits o Kilobytes para hablar de megabytes, gigabytes y terabytes.

Este crecimiento que se tiene en la actualidad en términos de procesamiento y velocidad de transmisión fue determinado por el Dr. Gordon Moore en 1965 donde indico que el crecimiento del número de transistores en los procesadores aumentaría en un tiempo estimado de 18 meses duplicando su capacidad; cuando realizamos un análisis vemos que este crecimiento se ha cumplido y se espera se mantenga por unos años más , pero a pesar de que aumentan los transistores y con esto la velocidad, el tamaño de los procesadores es cada vez menor lo cual permite

que donde estaba antiguamente un solo núcleo en la actualidad se pueden colocar dos o más núcleos mejorando aún más el rendimiento de los equipos y asegurando su portabilidad.

Con el aumento del número de usuarios en los portales de internet y la escalabilidad de las redes de comunicación también crecen los riesgos, las vulnerabilidades, es por ello que las grandes organizaciones en cargadas de las normalización y estandarización generan modelos de calidad que buscan establecer los parámetros básicos sobre los cuales deben operar las diversas plataformas y los requisitos mínimos que deben tener para asegurar que la información que esta almacenada en línea no pueda ser vulnerada, consultada, modificada o eliminada afectando así la seguridad de las personas mismas.

En la actualidad el termino de seguridad informática toma mayor fuerza cada día y el estudio de esta área de la informática es cada vez más importante para poder hacer frente a los diversos eventos de agentes malintencionados que a través de las redes, que buscan acceder a plataformas a través de las vulnerabilidades o puertas traseras para extraer información que les permita obtener beneficios ya sean económicos o de otra índole.

Es por esto que para aquellos profesionales que deseen profundizar en el estudio de la seguridad informática, es claro el conocimiento que deben tener o alcanzar de cada uno de los tres actores que están involucrados en un delito informático los cuales son intruso, administrador e investigador.

Con el objetivo de comprender como es que piensa un atacantes ya sea interno o externo a la organización en el momento de determinar el sistema al cual desean acceder, analizar cómo actúan los administradores cuando configuran un sistema y las acciones que ejecutan los investigadores cuándo desea encontrar las rutas por las cuales el intruso ingreso y ejecuto sus acciones y las razones porque el administrador del sistema no evidencio la existencia de dichas rutas y tomo las acciones preventivas o correctivas necesarias que aseguraran la disponibilidad y

continuidad del servicio evitando así la perdida de información, tiempo y dinero para la organización.

3. GLOSARIO DE TERMINOS

RECURSOS DEL SISTEMA: Son aquellos activos del sistema informático de la organización a proteger.

AMENAZAS: Es considerada una amenaza, cualquier evento premeditado o accidental, que pueda ocasionar algún daño en el sistema informático y de esta manera tener pérdidas materiales, financieras o de otro tipo a la organización.

VULNERABILIDADES: Es cualquier debilidad en el sistema informático, el cual puede permitir a las amenazas materializarse, causar daños y generar pérdidas.

IMPACTO: Es la medición y valoración del daño que un incidente de seguridad puede producir a una organización.

RIESGOS: Es la probabilidad que una amenaza se materialice sobre una vulnerabilidad y esta cause un determinado impacto en la organización.

Posicionamiento: Desde donde se llevara a cabo el análisis.

Visibilidad: relacionada directamente con la información que nos puede ser brindada.

4. DEFINICIONES

Antes de dar inicio al el desarrollo de un plan de continuidad, es necesario definir y aclarar ciertos conceptos, los cuales una vez apropiados, permitirán realizar un entendimiento, del tema expuesto en este documento.

4.1. Recursos Del Sistema

Son aquellos activos del sistema informático de la organización a proteger. Básicamente se encuentran definidos en los siguientes grupos;

A nivel del sistema informático como tal;

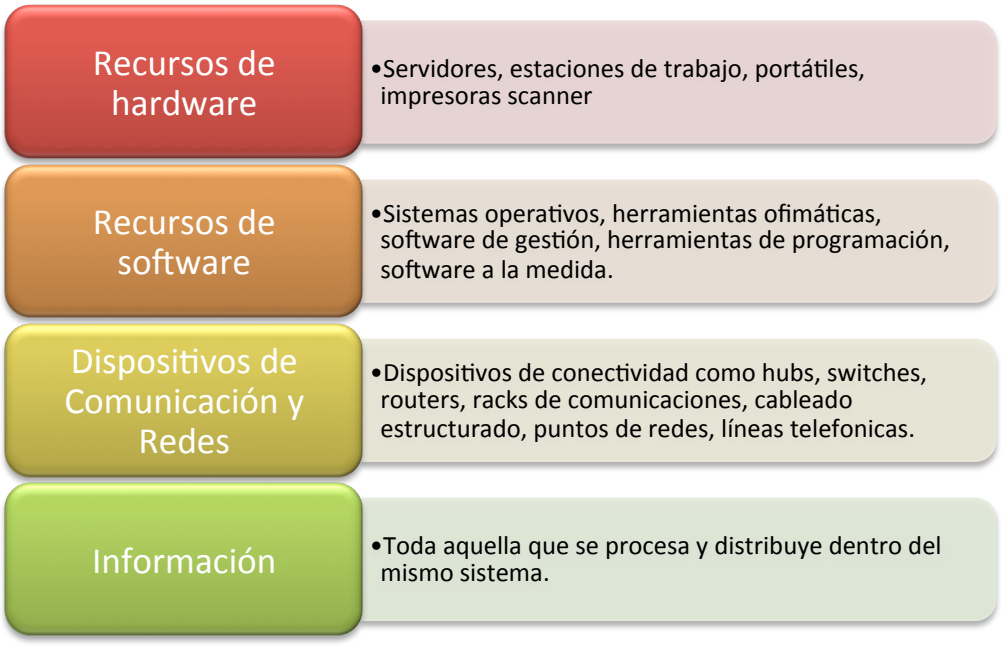


Ilustración 1 – Recursos del Sistema - Fuente Diseño Propio

A nivel estructural;

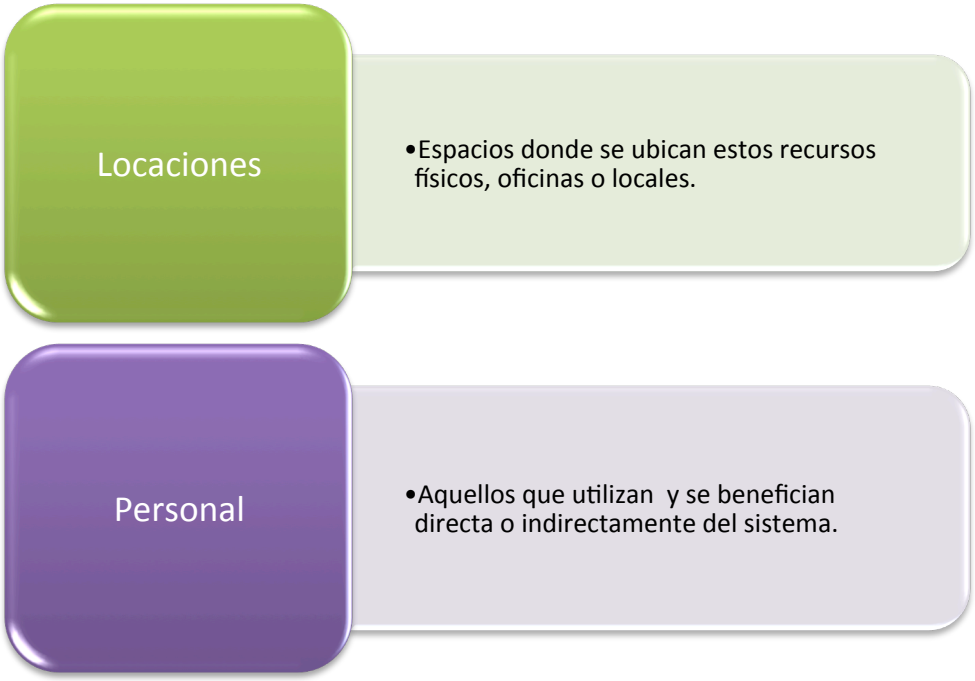


Ilustración 2 – Recursos del Sistema Estructural – Fuente Diseño Propio

4.2. Amenazas

Es considerada una amenaza, cualquier evento premeditado o accidental, que pueda ocasionar algún daño en el sistema informático [1]y de esta manera tener pérdidas materiales, financieras o de otro tipo a la organización.

Estas amenazas se pueden presentar a nivel;

- ***Interno,*** por personal de la misma compañía. Empleados descuidados o malintencionados.

[1] Activos o Recursos que requieren protección, para evitar su pérdida, modificación o el uso inadecuado de su contenido, para impedir daños para la institución. Básicamente compuestos por 3 grupos, Datos e Información Sistemas e Infraestructura y Personal.

- ***Externo***, como agresiones técnicas o naturales. Virus informáticos, ataques de una organización criminal, sabotajes cyber terroristas, intrusos en la red, robos y estafas a nivel de información.

Por otra parte existen ciertos tipos de amenazas que se pueden presentar a nivel de averías en el hardware y fallos en el software o errores de ejecución de ciertos procedimientos.

En algunos casos algunos riesgos serán difíciles de eliminar, como es el caso de los virus informáticos.

Por esta razones de vital importancia prevenirlos por medio de la implementación de medidas de protección, y de esta manera minimizar el daño.

4.3. Vulnerabilidades

Es cualquier debilidad en el sistema informático, el cual puede permitir a las amenazas materializarse, causar daños y generar pérdidas.

Las vulnerabilidades explotan los fallos en los sistemas lógicos y/o físicos, o en las ubicaciones, instalaciones y configuraciones defectuosas.

A nivel lógico podemos encontrar vulnerabilidades;

En bases de datos

- **Nombre de usuario y contraseñas:** En blanco, por defecto o débil.

- **Inyecciones SQL**: Método de infiltración de código intruso en el nivel de validación de las entradas, obteniendo acceso no autorizado.

- **Escalada de privilegios**: Procedimiento en el cual es posible escalar privilegios en una cuenta de bajo nivel hasta tener acceso a los derechos de un administrador.

- **Ataque de denegación de servicio (Denial Of Service):** El propósito es derribar un servido de DB por medio de un alto flujo de tráfico.

Programación

- **Autentificación y Manejo de Sesión Rotos**: Cuando las funciones de sesión no son implementadas adecuadamente, permite que un atacante comprometa claves de acceso tokens de sesión (llaves de control) y de esta manera, asumir identidades de las víctimas.

- **Cross Site Request Forgery (CRSF):** Fuerza al navegador "logueado", en este se envía un "request HTTP", incluyendo el cookie de sesión de la víctima y cualquier otra información de validación de la misma, a una aplicación web vulnerable. Esto permite al atacante forzar al navegador para acometer daños o estafas, que la aplicación inicia con datos ya iniciados por un usuario legítimo.

- **Fallas en restricción de acceso a URLs:** La mayoría de las aplicaciones verifican las credenciales de acceso antes de que el usuario ingrese a la aplicación por primera vez. Sin embargo, puede cometerse el error de no solicitar este tipo de verificación en todas las páginas y los atacantes podrán acceder a recursos prohibidos.

- **Fallas de Configuración de Seguridad:** Definir una adecuada configuración en torno al servidor de aplicaciones, de base de datos y plataforma. Todo lo

anterior ya que al implementar un sistema, este no se entrega con estas configuraciones.

- **Almacenamiento criptográfico inseguro:** Algunas aplicaciones no protegen ciertos datos sensibles, como números de tarjetas de crédito, números de identificación del usuario y credenciales de autentificación con los tipos de cifrado y hashing apropiados. Personal externo no autorizado pueden robar o modificar estos datos para realizar ataques de robo de identidad, fraudes de tarjetas de crédito y otros crímenes.

- **Redirecciones y re-envíos sin debida validación:** Las aplicaciones web, normalmente re direccionan o envían a los usuarios a otras páginas y sitios web usando datos que no se encuentran validados para hacerlo. Sin esta apropiada validación, intrusos externos sin autorización, pueden redirigir a las víctimas a sitios de phishing, malware, o usar los re-envíos para acceder a páginas no autorizadas.

Software

- Instalación y configuración indebida de programas.
- Sistemas operativos sin políticas de usuarios y restricciones adecuadas.

A nivel de Físico

Redes físicas

- Cableado desordenado y expuesto
- Instalaciones inadecuadas.
- Ausencia de equipos y dispositivos de seguridad o sin la configuración adecuada.

Debido a la propagación de la señal en todas direcciones, las redes wifi son susceptibles a cierto tipo de vulnerabilidades

- **Acces point spoofing "asociación maliciosa**": En el cual el atacante se hace pasar por un acces point. Y el cliente se conecta a él pensando que se está conectando a una LAN verdadera. Este ataque es común en redes descentralizadas (ad-hoc) en las cuales cada nodo está autorizado para enviar y recibir datos de los demás.

- **ARP Poisoning "envenenamiento ARP":** Ataque al protocolo ARP (Adres Resolution Protocol). Similar al ataque man in the midle, en la cual una estación de trabajo invasora se ubica en el medio del envío y recepción de paquetes entre dos estaciones de trabajo. Es decir todo lo que se envía de la estación A para la estación C tiene que pasar por B, la cual es la estación de trabajo invasora.

- **Enmascaramiento de la dirección MAC**: Ocurre cuando alguien roba una dirección MAC de alguna red, y se hace pasar por un cliente autorizado. Esto sucede ya que las placas de redes pueden cambiar su número MAC por otro.

Hardware

- Uso inadecuado o incorrecto de los recursos.
- Defectos de fabricación.
- Plazo de validez o caducidad.
- Ubicación la infraestructura en lugares inadecuados. Expuestos a humedad, calor, moho, magnetismo.

Todas las anteriores se encuentran sujetas a aspectos;

- Organizativos y procedimentales mal definidos, ausencia de políticas de seguridad.

- Factor humano, falta de formación y de estructuración al personal con accesos a ciertos recursos del sistema.
- Condiciones ambientales del sistema, medidas de seguridad deficientes, escasa protección contra incendios o mala ubicación.

- Wardriving o Warchalking: En la cual se desea encontrar puntos de acceso a redes inalámbricas, mientras se desplaza en la ciudad por medio de un automóvil.

Para definir el nivel de vulnerabilidad, se suele utilizar una escala cuantitativa (Baja, Media, Alta) y de esta manera definir el nivel de vulnerabilidad de un determinado recurso.

5. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDAD

Existe una serie de herramientas que ofrecen datos útiles para el análisis de vulnerabilidades.

Dentro de las más destacadas;

- Analizadores de configuraciones.
- Analizadores de logs.
- Herramientas de escaneo de puertos (Port Scanners)
- Sniffers.

- Network Mapping.
- Testing Tools.

6. INCIDENTE DE SEGURIDAD

Es todo evento que tenga como resultado la interrupción de un servicio que está siendo suministrado por un sistema informático o posibles pérdidas relacionadas con activos físicos o financieros.

En resumen, un incidente físico, es la materialización de una amenaza

6.1. Impacto

Es la medición y valoración del daño que un incidente de seguridad puede producir a una organización.

Para poder valorarlo, es importante tener en cuenta los daños tangibles (físicos) e intangibles (datos e información), así como una calificación cuantitativa o cualitativa y de esta manera clasificar dicho impacto en

- Bajo, recursos secundarios inhabilitados, disminución referente al rendimiento de los procesos o actividades de la organización
- Medio, recursos físicos inhabilitados o perdida de información, pero que puede ser recuperada mediante procesos de respaldo, disminución notable, referente al rendimiento de los procesos o actividades de la organización.
- Alto, recursos físicos inhabilitados o perdida de información. Interrupción en los procesos del negocio, robo de información estratégica.

6.2. RIESGOS

Es la probabilidad que una amenaza se materialice sobre una vulnerabilidad y esta cause un determinado impacto en la organización.

El nivel de este depende del previo análisis de las vulnerabilidades, amenazas y del impacto que puede causar en los procesos y funcionamiento de la organización.

Existen diferentes tipos de riesgos tales como el riesgo residual[2] y riesgo total[3].

7. MARCO TEORICO

7.1. Análisis De Riesgo

Este es el primer paso en el proceso de gestión de riesgo, cuyo propósito es la identificación, evaluación y determinación los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar el grado de riesgo y toma de decisiones para reducir este a un nivel aceptable.

El análisis de riesgo, es un procedimiento, cuyo objetivo es analizar las amenazas, que se puedan presentar y a los que puedan estar expuestos ciertos activos informáticos, a raíz de ciertas vulnerabilidades, la cuales podrían generar situaciones y consecuencias no deseadas.

[2] Es aquel riesgo remanente que queda una vez se han tomado las medidas necesarias.
[3] Es aquel el cual no se está dispuesto a sumir.

Por lo anterior, el análisis de riesgos [4]permite la detección y evaluación del mismo, con el propósito de tomar decisiones e implementar controles adecuados para aceptar, disminuir, transferir o evitar la materialización de este riesgo.

Básicamente análisis de riesgos está compuesto por 4 faces fundamentales. ***Ver gráfica***.

Estas se encuentra fundamentado en las políticas de seguridad y filosofía institucional que estructuran el marco operativo del proceso, cuyo propósito se enfoca en;

- Potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas obteniendo un resultado de reducción de riesgo.
- Orientar el funcionamiento organizativo y funcional.
- Garantizar un comportamiento equilibrado.

[4] El análisis de riesgo es un elemento que forma parte del programa de gestión de continuidad de negocio (Business Continuity Management)

- Minimizar y ajustar las conductas o prácticas que nos hacen vulnerables.

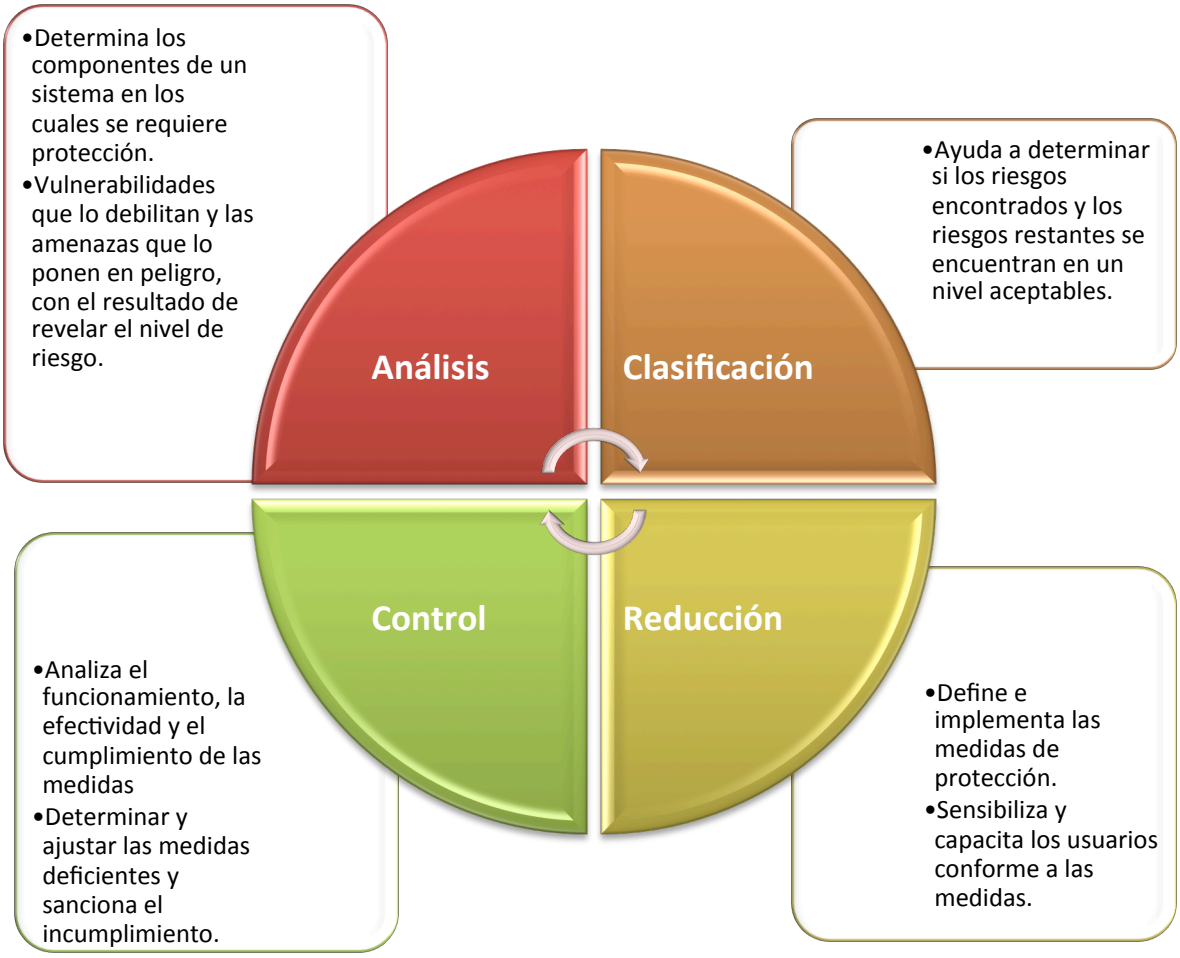


Ilustración 3 – Faces análisis Riesgo – Fuente Diseño Propio

En este proceso es necesario generar una matriz, llamada matriz de riesgo, en la cual se muestran los elementos que se han detectado, relacionándolos entre sí, para poder determinar el tratamiento y la gestión del mismo.

Una vez cuantificados, es posible determinar el riesgo total por medio de la siguiente formula y de esta manera obtener el riego residual para poder aplicar los controles necesarios.

Si estos controles existen, los riesgos se llamaran riesgos controlados. En caso de no existir se llaman riesgos no controlados.

RT (Riesgo Total) = Probabilidad x Impacto Promedio

Riesgo = Probabilidad de Amenaza x Magnitud del daño

La variable (Probabilidad de amenaza) hace referencia, al interés o atracción por parte de personal externo, el nivel de vulnerabilidad y la frecuencia en la cual ocurren los incidentes

Una vez realizado este análisis, se debe determinar las acciones a tomar con respecto a los riesgos residuales que se identificaron.

Las acciones pueden ser:

- Controlar el riesgo.- Fortalecer los controles existentes y/o agregar nuevos controles.

- Eliminar el riesgo.- Eliminar el activo relacionado y con ello se elimina el riesgo.

- Compartir el riesgo.- Mediante acuerdos contractuales parte del riesgo se traspasa a un tercero.

- Aceptar el riesgo.- Se determina que el nivel de exposición es adecuado y por lo tanto se acepta

Entre más alta sea la probabilidad de amenaza y magnitud de daño, más grande será el riesgo y el peligro del sistema.

Así será posible valorar la amenaza en criterios cuantificables;

- Baja: condiciones de ataque muy lejanas.

- Mediana: condiciones de ataque a corto plazo poco probables, pero no suficientes para evitarlo a largo plazo.

- Alto: No existen condiciones internas y/o externas que impidan dicho ataque.

7.2. Plan de Continuidad

Un plan de continuidad es un conjunto de procedimientos y metodologías, que se aplican progresiva y sistemáticamente, para poder afrontar cualquier tipo de desastre de tipo natural (terremoto, incendio, etc.) o por robos, sabotajes a nivel interno y externo.

Básicamente lo que se busca es evitar la interrupción en los procesos al asegurar la integridad y recuperación de los datos, por medio de respuestas adecuadas.

Para ello es de vital importancia determinar los objetivos y prioridades sensibles para la organización, al tener presente los recursos disponibles e infraestructura necesaria para la recuperación de la información, permitiendo así el restablecimiento de los sistemas de información y aplicaciones, las cuales se utilizan como soporte a la organización.

Para poder afrontar lo anterior, el plan de continuidad pretende implementar;

- La disponibilidad de un centro alternativo o de reserva, en el cual se pretende ubicar los principales recursos informáticos servidores, bases de datos etc.
- la
- Existencia de líneas de back-up para comunicaciones.
- Sistemas de almacenamientos RAID en los servidores
- Implantación de clúster de servidores con balanceo de carga

- Herramientas para llevar a cabo procedimientos de replicación de documentos y bases de datos.
- Definir un equipo de dirección que coordinará las actividades de recuperación ante un desastre.

7.3. Gestión de la disponibilidad O Plan de Disponibilidad

Forma parte de los procesos definidos en el libro diseño del servicio (service design o delivery service) de ITIL.

Su objetivo es definir, analizar, planificar y mejorar los servicios de IT.

Optimizar la capacidad de la infraestructura y servicios de IT así como el soporte, con el propósito de ofrecer un nivel de disponibilidad efectivo en costos al minimizar la interrupción en los servicios.

7.4. Plan de Recuperación de Desastres

Un plan de recuperación de desastres es una serie de procesos y acciones consecuentes, las cuales se deben realizar antes durante y después de un desastre.

En él se define qué es lo que hay que hacer, quien y como, al instante de presentarse una falla en algún proceso o sistema de información, asegurando de esta manera la continuidad de las operaciones.

Su objetivo fundamental es preparar al área de TIC, para afrontar adecuadamente una situación que pueda afectar la infraestructura tecnología de la organización.

Este se presenta como un documento el cual debe ser aprobado por la dirección de la empresa.

8. METODOLOGIAS

Ahora bien, teniendo claro los conceptos anteriormente descritos, nos es posible diferenciar la diferencia entre amenazas y vulnerabilidades, lo cual es vital al momento de realizar un análisis de riesgo, el cual como se enuncio en el apartado anterior es el primer paso en el proceso de gestión de riesgos.

Pero, para poder analizar estos posibles riesgos es necesario aplicar algunas metodologías, las cuales implementan ciertos pasos y procesos organizados cuyo objetivo es detectar que tan seguro es el sistema de información y que riesgos y con qué frecuencia se pueden presentar.

La aplicación de estas metodologías, nos permitirán obtener una visión más general de estado (en cuanto a seguridad y riesgos), en el cual se encuentra el sistema de información y de esta manera poder medir con datos reales las acciones a tomar.

8.1. Metodologías para la Medición de Riesgos

Dentro de las más destacadas encontramos;

8.1.1. Cramm (Ccta Risk Analysis And Management Method)

Metodología y herramienta de análisis y gestión de riesgos desarrollada por la "*Central Computer and Telecommunications Agency*" del Reino Unido y gestionada por "*Insight Consulting Limited*" (Grupo Siemens)

Permite, mediante un análisis cualitativo y cuantitativo, la situación actual de la organización

Para ello usa una matriz, donde las filas representan los diferentes "activos de información" y las columnas los riesgos que amenazan la integridad, confidencialidad y disponibilidad de estos activos, entendiendo como integridad, a la precisión de información así como su validez de acuerdo con ciertas expectativas, confidencialidad, protección de la información contra la divulgación no autorizada y disponibilidad, a la disponibilidad de la información cuando esta es requerida.

La metodología para evaluar la integridad, confidencialidad y disponibilidad de los activos de información se basa en la estructuración de unas tablas.

Como resultado final de la aplicación de la metodología de CRAMM se obtiene, una Matriz de Análisis de Riesgos y un Reporte de Análisis.

8.1.2. Metodología Margerit

Publicada en España desde 1996 por los ministerios de administraciones públicas. Actualmente está en su versión 2.

Mide la vulnerabilidad por la frecuencia histórica de la materialización de la amenaza sobre un activo, cuando es factible[5] o mediante la potencialidad de dicha materialización.

Lo anterior lleva a emplear una escala de pseudo-frecuencias', en la cual las amenazas potenciales son consideradas reales.

Por otra parte otros países han elaborado sus propias metodologías como son la MARION francesa de 1985 por la Asociación de Empresas Aseguradoras francesas y la MELISA de 1984 enfocada al entorno militar francés.

9. SEGURIDAD INFORMÁTICA

Cuando se habla de seguridad de la información, se plantean una serie de cuestionamientos que deben ser resueltos, a través de procesos e implementación de una u otra metodología.

Dentro de estos, los cuestionamientos, que comúnmente se plantean son:

- ¿Qué debe ser protegido?
- ¿Cómo debe ser protegido?
- ¿Con que debe ser protegido?
- ¿Quiénes van a ser los encargados de la custodia?
- ¿Cómo se va a evaluar la eficacia de los mecanismos de protección seleccionados?

Para lograr dar respuesta a cada uno de estos interrogantes, las organizaciones deben tener claro el tema de la gestión del riesgo así como cada una de sus etapas.

[5] Fiabilidad de un componente hardware, número de fallos de software

Para lograr una estrategia de seguridad se debe tener como foco metodológico dos tipos de estrategias de tipo ***proactivo*** y ***reactivo***.

La estrategia proactiva como primera etapa analiza el contexto organizacional y el contexto en el cual se encuentran localizados los activos que deben ser protegidos para con esto culminar en una tercera etapa en la cual se deben predecir los posibles daños , determinar las vulnerabilidades , implementar controles y respuestas a posibles problemas e incidentes.

La estrategia reactiva ya es pos evento y busca evaluar los daños presentados, determinar las causas que lo generaron, reparar los daños ocasionados , implementar los planes de respuesta generados en la etapa anterior y realizar un levantamiento de información sobre lo que sucedió, por qué sucedió y como fue solucionado.

Siempre que un evento de intrusión o afectación a la seguridad a los activos que están siendo custodiados, se debe emplear una estrategia reactiva, y además se debe regresar y generar una estrategia proactiva que evite que este tipo de incidentes se vuelvan a generar en la organización.

Para generar las estrategias anteriores se debe seleccionar una de las metodologías existentes que sirven como guía de trabajo para asegurar el éxito de la iniciativa propuesta entre las principales metodologías encontramos ITIL, King II, Cobit, ISO17799, ISF, ITPM.

Para realizar un análisis de seguridad se deben tener en cuenta 11 áreas específicas tanto a nivel proactivo y reactivo:

1. Política de seguridad
2. Organización de la seguridad de la información
3. Seguridad de los recursos humanos
4. Gestión de las comunicaciones y operaciones
5. Gestión de activos

6. Gestión de continuidad del negocio
7. Adquisición, desarrollo y mantenimiento de sistemas
8. Gestión de activos
9. Seguridad física y del entorno
10. Control de acceso
11. Cumplimiento

Estas 11 áreas están basadas en el estándar ISO/IEC 17799 2005 Guía B de la norma 27001.

Para desarrollar un análisis eficaz se recomienda que el equipo de trabajo sea un equipo multidisciplinario:

Área jurídica: Encargados de dar el soporte legal en marco nacional e internacional además de verificar el cumplimiento de los lineamientos establecidos en los estándares que se desea implementar.

Área de auditoria: Responsable por verificar el cumplimiento de las políticas y lineamientos establecidos en los procedimientos.

Área de Riesgo: responsable de la evaluación de riesgos.

Área de Recursos humanos: responsable por la contratación de personal idóneo, por liderar campañas de concientización sobre la importancia del buen manejo de la información, implementar cláusulas de responsabilidad en los contratos además de definición de perfiles y funciones claras y específicas para cada miembro de los procesos.

Oficial de seguridad: Responsable de la planificación, desarrollo, control, y gestión de la política de seguridad y procedimientos requeridos para asegurar la protección de la información en la organización.

Analistas y administrador de seguridad: Encargado de conocer estándares y normatividad vigente además de herramientas de software y software que puedan ser implementadas en la organización que apoyen los objetivos estratégicos.

En algunas organizaciones el oficial de seguridad y el analista de seguridad están en un solo perfil.

9.1. Metodologías de Análisis de Seguridad

Actualmente existen varias metodologías asociadas a este tipo de análisis, muchas de estas son de licencia abierta y están disponibles para su descarga y lectura.

Una de estas es desarrollada por la ISECOM *(Institute for Security and Open Methodologies),* llamada OSSTM (*Open Source Test Methodology*), la cual se encuentra ligada al manual OSSTMM (*Open Source Security Test Methodology Manual*).

Desarrollado por Pete Herzog y 130 profesionales, todos multidisciplinarios, entre los cuales se encontraban, security testes, hackers, abogados, legisladores, entre otros.

Esta metodología se caracteriza por enfocarse en los siguientes aspectos, con el propósito de obtener métricas confiables y de esta manera poder emitir decisiones objetivas.

- Ser cuantificable.
- Se valida en el tiempo.
- Ser consistente.
- Cumplir con regulaciones (Leyes nacionales e internacionales).

Por otra parte, en un análisis de seguridad es importante tener claro ciertos conceptos, ya que dependiendo del enfoque deseado y de selección de los anteriores, se obtendrán ciertos resultados.

- **Posicionamiento** desde donde se llevara a cabo el análisis. Este puede ser ***interno o externo***. Es importante definir el tipo de posicionamiento, ya que si no de selecciona el adecuado, se obtendrán resultados no deseados. Lo anterior ya que es diferente analizar tipos de amenazas a nivel externo y a nivel interno.

  Aunque es común tener la percepción de que los ataques de nivel externo son los más representativos referentes a un riesgo de intrusión exitoso, los ataques a nivel interno no son muy frecuentes pero su impacto es superior, ya que la resistencia implementada por los controles de seguridad no es la adecuada.

  Un análisis desde el posicionamiento interno permite que la posibilidad de concreción de intrusión exitosa, ya que hay menos barreras.

- **Visibilidad,** relacionada directamente con la información que nos puede ser brindada. Para lo anterior existen diferentes alternativas de visibilidad.

  - **Blind/BlackBox:** El security tester no cuenta con información alguna con el objetivo, pero el cliente si conoce el tipo de test y cuando se llevara a cabo.

  - **Double blind / Black Box**: El security tester no conoce información referente al objetivo y el cliente no conoce el tipo de test ni cundo se llevara a cabo.

- **Gray Box**: El security tester conoce información parcial del objetivo. Esta información será seleccionada por el cliente. El cliente conocerá que tipo de test se llevara a cabo y cuando.

- **Double Graybox:** El security tester conoce información parcial del objetivo. El cliente conoce las técnicas que se utilizaran pero no conoce cómo ni cuándo.

- **Whitebox:** El security tester tiene pleno conocimiento del objetivo. Esta información será otorgada antes de iniciar el test. El cliente tiene pleno cocimiento de las técnicas y tareas que utilizara el teste, así de cómo y cuándo.

- **Reversal:** El security tester tiene pleno conocimiento del objetivo. Esta información será otorgada antes de iniciar el test. El cliente no cuenta con información referente a las tareas y técnicas que el tester llevara a cabo ni cuándo.

- **Perfil adoptado**: Aunque es posible que se presente cierto tipo de complejidad a la hora de identificar patrones metodológicos y de conducta asociados a los diferentes perfiles del atacante, podemos identificar su posición al ubicarlos al interior o exterior de la organización, así como de aquellos cuales incidentes han sido premeditados como aquellos que se han realizado sin ninguna intención.

  Por tal razón luego de realizar el análisis y sobre la base de los resultados, tratar de asociar que perfiles se encuentran más cercanos a atacar los sistemas de información.

Logrando emular ciertos tipos de perfiles, al relacionar conocimiento relacionado al objetivo y la posición del mismo;

- Usuario sin privilegios.
- Usuario con privilegios.
- Tercero ajeno a la organización con acceso físico a la misma.
- Tercero ajeno a la organización sin acceso físico a la misma.
- Usuario con conocimiento técnico avanzado.
- Usuario con conocimiento técnico intermedio.
- Usuario con conocimiento técnico básico.

9.2. Etapas de un Análisis De Seguridad

Las siguientes son las etapas más habituales en los análisis de seguridad.

9.2.1. Etapa de Reconocimiento Pasivo:

Permitirá informarle al cliente le nivel de visibilidad de los objetivos desde el posicionamiento exterior, a los ojos de un potencial atacante.

Por otra parte, una alta visibilidad desde el exterior no implica una vulnerabilidad.

Si bien gran parte de la información referente a los objetivos, será brindada por el cliente, como valor agregado se tratara de obtener información relacionada, mediante el uso de motores de búsqueda, grupos de consulta, mediante registros DNS y todo aquello que no tenga una relación directa con el objetivo.

9.2.2. Etapa de Reconocimiento Activo Superficial

Su propositivo es identificar objetivos directamente relacionados con el objetivo al interactuar con los mismos y de esta manera identificar los que se encuentran activos, para luego practicar un análisis más profundo.

9.2.3. Etapa de Reconocimiento Activo en Profundidad

Su propósito es realizar prácticas sobre los objetivos detectados en la etapa anterior y realizar un análisis más profundo.

Estas pruebas se enfocan en identificar puertos abiertos, (a nivel TCP y UDP), identificar con mayor precisión servicios que corren en puestos abiertos identificar topologías de red en la cual se encuentran los objetivos y de esta manera analizar la adecuada implementación de dispositivos de filtrado y detección.

9.2.4. Etapa de Análisis de Vulnerabilidades

Su principal objetivo, es detectar potenciales vulnerabilidades tanto a nivel de infraestructura como a nivel de aplicaciones.

9.2.5. Etapa de Explotación o Ataque Puro:

Su objetivo recolectar toda la información posible con el propósito de desarrollar una correcta estrategia de ataque y explotar las vulnerabilidades detectadas mediante diferentes códigos

Esta etapa se enfoca tanto a nivel de infraestructura, en la cual puede comprometerse seguridad de aplicaciones.

9.2.6. Etapa de Consolidación:

Si el compromiso del objetivo fue exitoso, permitirá al tester avanzar en su intrusión, y mediante los host comprometidos cambiar información y la visibilidad que pueda tener.

9.2.7. Etapa de Borrado de Rastro:

Su objetivo es tratar de borrar todos los rastros posibles que el proceso de intrusión haya ocasionado y mostrar que pruebas se podría tener o no el cliente para que de esta manera pudiera realizar algún tipo de investigación sobre esta intrusión.

9.2.8. Etapa de Reporte:

El cliente recibirá un informa con toda la información obtenida en la realización de test, así como recomendaciones para corregir los mismos, tratando las vulnerabilidades desde su origen con el propósito de solucionarlas desde su raíz y evitar su aparición en corto plazo.

Esta información es presentada mediante un informe ejecutivo, el cual está dirigido a la alta gerencia en el cual se comunican las mayores fortalezas y debilidades, así como remediar las vulnerabilidades encontradas, y mediante un informe técnico cuyo contenido será el mismo que el del informe ejecutivo, pero con un lenguaje más técnico y detallado, el cual se encontrará orientado a los departamentos de IT y auditoria.

10. TIPOS DE ANALISIS DE SEGURIDAD

Aunque estas pueden variar según su alcance y profundidad, es posible categorizar tres tipos principales de seguridad las cuales tiene en cuenta aspectos como el posicionamiento y visibilidad.

10.1. Vulnerability Assessment:

En este tipo de análisis no se alcanza un gran grado de profundización pero, involucra menos cantidad y tiempo en recursos.

Se enfoca en el análisis y pruebas en puertos abiertos, servicios disponibles y vulnerabilidades conocidas en los sistemas de información objetivos.

Este análisis busca identificar e informar fallas en los dispositivos y procesos tecnológicos.

No pretende explotar las vulnerabilidades detectadas sino que solo trabaja sobre la correcta identificación de estas.

Las siguientes etapas pueden estar dentro de este tipo de análisis:

- Etapa de reconocimiento pasivo
- Etapa de reconocimiento activo superficial
- Etapa de reconocimiento activo en profundidad
- Etapa de análisis de vulnerabilidades
- Etapa de reporte

10.2. Penetration Test

Es tipo de análisis hace uso de tareas asociadas a la explotación y post explotación de las vulnerabilidades.

Se destaca por tener un objetivo definido que finaliza cuando es alcanzado o cuando el tiempo acordado para la detección del mismo llega a su fin.

A diferencia del anterior, no solo busca las vulnerabilidades, sino que las explota con el propósito de verificar los niveles de intrusión expuestos en el sistema de información el cual se está analizando.

Las siguientes etapas pueden estar dentro de este tipo de análisis:

- Etapa de reconocimiento pasivo.
- Etapa de reconocimiento activo superficial.
- Etapa de reconocimiento activo en profundidad.
- Etapa de análisis de vulnerabilidades.
- Etapa de explotación o ataque puro.
- Etapa de consolidación.
- Etapa de reporte.

10.3. Ethical Hacking

Aunque guarda muchas de las características anteriormente descritas, su diferencia más puntual se destaca en el objetivo.

En un Ethical Hacking todo es un objetivo posible., por lo tanto este tipo de análisis es más profundó que los anteriores ya que pretende analizar íntegramente la

seguridad de los sistemas de información, al combinar técnicas de ingeniería social al explotar las vulnerabilidades del factor humano y mediante la realización de pruebas a los controles de acceso físico.

Las siguientes etapas pueden estar dentro de este tipo de análisis:

- Etapa de reconocimiento pasivo.
- Etapa de reconocimiento activo superficial.
- Etapa de reconocimiento activo en profundidad.
- Etapa de análisis de vulnerabilidades.
- Etapa de explotación o ataque puro.
- Etapa de consolidación.
- Etapa de reporte.

10.4. Seguridad Informática Contexto Latinoamericano y Colombiano

En la mayoría de los países latinoamericanos en la actualidad la inversión que se hace en el área de seguridad informática es mínima comparada con la inversión realizada por otros países, esto se debe a que aún no se tiene una conciencia real del peligro y el riesgo que la información en la red mal administrada representa, en muchos casos algunos expertos consideran que el hecho de sentir que se tiene un menor crecimiento que los países potencia se siente que las organizaciones latinoamericanas son menos vulnerables a los ataques y más si las organizaciones están en el sector privado.

De acuerdo a los informes de seguridad de diversas empresas como Symantec, ESET, Cisco Systems, entre otras, durante el 2011, implementaron distintos modelos de encuestas los cuales fueron enfocados en los directivos de IT de diversas compañías en Latinoamérica, después de realizar la depuración y análisis de los

resultados se determinó que entre los principales temores que tienen los expertos en seguridad encontramos los siguientes:

Ilustración 4 – Mayores Preocupaciones en la SI – Fuente Informe ESET 2012

Según el grafico anterior podemos deducir que para las organizaciones latinoamericanas la visión global del tipo de incidentes a nivel informático es muy reducida solo se contemplan los ataques más comunes mas no se tiene una visión clara de las técnicas empleadas por los intrusos no solo para extraer información sino para entrar y generar o alterar procesos que actúen ya sea para beneficio económico propio o de otras organizaciones y después de ingresar permanecer por tiempo indefinido sin ser detectado.

Además de esto las empresas dedicadas al desarrollo de soluciones en seguridad informática indican que para gran parte de las organizaciones latinoamericanas la seguridad informática y la protección de los datos aun no es considerado como tema

primordial, además de lo anterior las organizaciones no disponen de los presupuestos indicados para la implementación de los mecanismos de seguridad necesarios para poder hablar de reducción de las vulnerabilidades y mitigación de los riesgos.

Para el año 2012 uno de los ataques más comunes fueron los provenientes de los movimientos hacktivistas con los denominados ataques selectivos, entre los grupos hacktivistas más sonados en el 2011 fueron Anonymus y Lulz Security.

Por otra parte la falta de estándares y protocolos de seguridad implementados, se presentan con un 60.8% como causantes de pérdidas de datos.

En Colombia no ha sido ajena a la aparición de los grupos hacktivistas y para dar un claro ejemplo podemos hablar de Anonymus Colombia quienes tuvieron su primera presentación en público en el año 2011 el 11 de Abril cuando bloquearon la página web del ministerio del Interior y justicia en queja por la ley antipiratería y el bloqueo de páginas de descarga, durante todo el mes de abril se detectaron varios ataques más a las páginas web de la entidades gubernamentales como senado, gobierno en línea, pagina presidencial, ministerio de defensa, así como las páginas de las fuerzas militares, el modo de ataque más conocido de este grupo es a través de la modalidad de negación de servicios.

Entre los programas de código malicioso que más daño hicieron y que se plantea continuara su continua evolución es el gusano denominado Conficker el cual hizo su primera aparición aproximadamente en el año 2008, se determina que este gusano durante todo este tiempo este programa malicioso ha logrado infectar a más de 11 millones de equipos en todo el mundo, según datos de la empresa Shophos.

Otro ataque común durante el 2012 se centró en el Malware y los denominados antivirus falsos los cuales dicen encontrar posibles amenazas en los equipos y le brindan la posibilidad a los usuarios de instalar versiones trial para realizar supuestos escaneos más avanzados y con solo la instalación de estos triales los

intrusos comienzan a extraer información del usuario y escanear las páginas visitadas y capturar claves y usuarios de acceso, en especial las de cuentas de correos y cuentas bancarias posterior a esto comienza él envió de mensajes indicando que se requieren un pago moderado a través de la web para descargar supuestas versiones completas para poder erradicar las amenazas encontradas con el tiempo estos programas afectan seriamente el rendimiento del equipo y además de esto terminan por dañar la configuración y dejando los equipos fuera de servicio.

Para el segundo semestre del año 2001, este ataque de antivirus falsos era uno de los métodos de hurto más frecuente, a pesar de que el FBI desmantelo una organización culpable del desfalco de un aproximado de 1 millón de personas a través de la web por la descarga de estos programas, para el segundo semestre de 2011 este ataque no fue tan común pero aún se toma como una amenaza activa que en el 2012 estará presente.

A pesar de los datos anteriores se evidencia que los resultados que se obtienen sobre el número de ataques informáticos registrados anualmente en las organizaciones, no muestra el escenario real, puesto que la gran mayoría de las organizaciones no disponen de los mecanismos o herramientas necesarias que les permitan monitorear la cantidad de accesos no autorizados que se presentan a los diversos sistemas de información y determinar cuáles son las vulnerabilidades reales que tienen los mismos.

Los expertos de seguridad toman como un riesgo latente la facilidad que tienen muchos empleados de ingresar a internet desde celulares, PDA's, computadoras sin ningún tipo de bloqueos además de esto se agrava por la falta de políticas a nivel organizacional que regulen el manejo de estos medios de comunicación.

El uso de los recursos informáticos en acceso a portales no autorizados no solo representa perdida en la productividad organizacional sino que además coloca en riesgo a la misma organización abriendo puertas de acceso a intrusos interesados en extraer, modificar o eliminar la información almacenada no solo en el equipo que da

el acceso, sino que a través de la red los intrusos pueden llegar hasta los servidores que almacenan la información más importante y confidencial de la organización.

El número de ataques sufridos por las organizaciones a través de las redes sociales actualmente no pueden ser medidos, ni se pueden dar cifras exactas pero podemos hablar de cifras en encuestas sobre políticas organizacionales que reglamenten o limiten el uso de las redes sociales para lo cual podemos ver el siguiente grafico estadístico, que nos muestra un estudio realizado sobre el número de organizaciones que tienen contemplado y limitado el uso de las redes sociales:

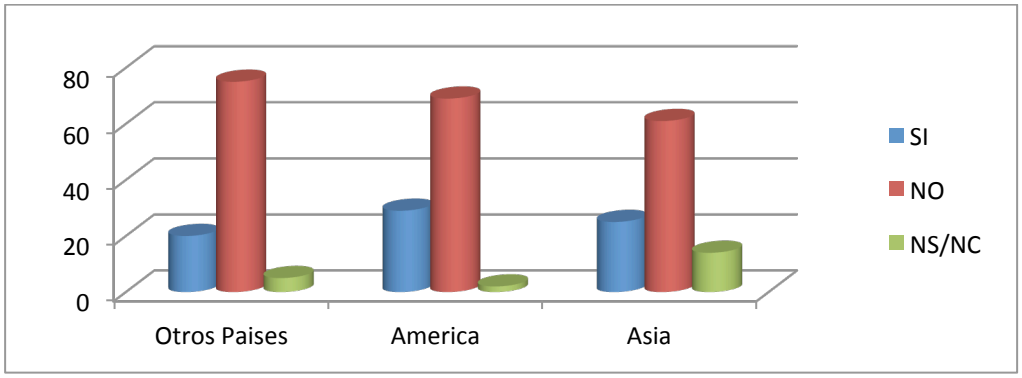


Ilustración 5 Número de Empresas con Políticas de Seguridad - Fuente Social Net Working

De acuerdo a los datos anteriores podemos ver que en América es mayor el número de organizaciones con políticas para el uso de las redes sociales frente a Asia y otros continentes, pero es claro que gran parte de esta suma la colocan empresas de Norteamérica esto debido a que para Latinoamérica la aplicación de las políticas de seguridad no es una práctica común a pesar de que las estadísticas nos muestran que día a día son más las empresas que están adoptando esta práctica.

De igual manera vale la pena resaltar que la imagen general cuando se habla de políticas para el uso de las redes sociales es que se limita o prohíbe el uso dentro de la empresa pero esto hace referencia solo a los equipos propios de la organización porque no hay forma de limitar el uso en equipos personales como PDA'S, celulares, Tablet entre otros, pero para algunas organizaciones con una visión diferente es el

poder orientar el uso de las mismas para obtener un valor agregado en cuanto a mercadeo se refiere.

En el caso colombiano diversos estudios han demostrado que Colombia en el tema de seguridad informática está por debajo del promedio regional, de acuerdo a un informe presentado por Cisco Systems en el 2008, para ese año Colombia obtuvo un puntaje de 62 de promedio siendo 64 el promedio regional

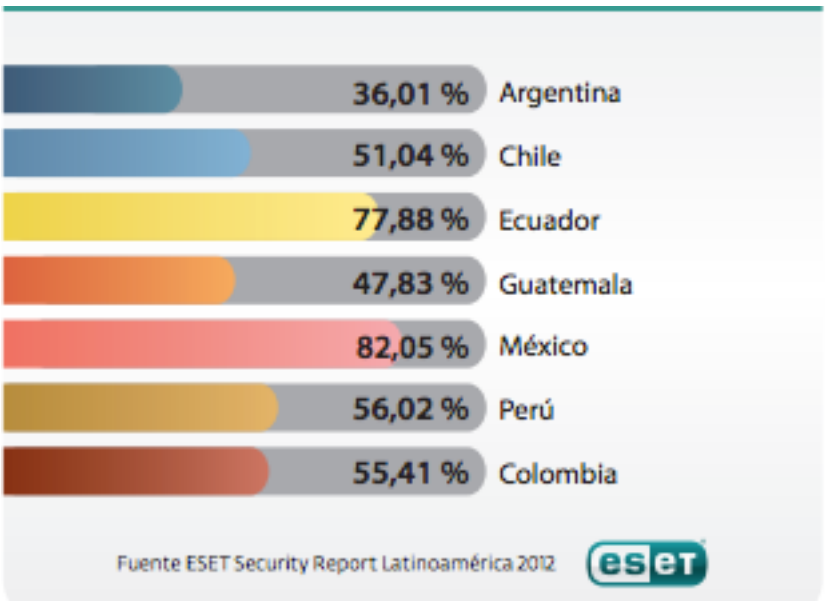


Ilustración 6: Estudio ESET 2008- Fuente: Security Report Latino América

Uno de los aspectos más relevantes en las encuestas es que queda claramente evidenciado que en el 65% de las organizaciones encuestadas las juntas directivas son reacias a la aprobación de las políticas de seguridad que son propuestas por los departamentos de sistemas, otra de las preocupaciones de mayor índice es el ataque de virus, malware y Spyware a pesar de esto Colombia es el país que presenta menor preocupación frente a los demás encuestados.

Colombia demuestra estar en los primeros puestos al presentar mayor preocupación frente a la perdida de información producto de ataques terrorista caso contrario

Colombia demostró tener la menor penetración en el ámbito de la autenticación biométrica.

En el estudio realizado por ACIS (Asociación Colombiana de Ingenieros de sistemas) en el año 2010 para analizar las tendencias en seguridad que estarían para los años 2010 -2011 se contó con la participación de 215 personas y como en otras encuestas se incluyó a personas de países como Paraguay, Argentina, Uruguay, Venezuela y México, este estudio se realizó a través de una encueta que contaba de 35 preguntas en las cuales se buscaba obtener información acerca de

- Demografía: Busca reunir todos los aspectos demográficos de las empresas encuestadas y determinar cuál es el personal de seguridad con que cuentan y las obligaciones de los mismos.

- Presupuestos: Busca determinar el porcentaje del rublo anual de operaciones que las organizaciones destinan a la seguridad de la información.

- Fallas de seguridad: Esta sección busca identificar las fallas más recurrentes que son detectadas por las organizaciones y los mecanismos que estas emplean para detectarlas y mitigarlas.

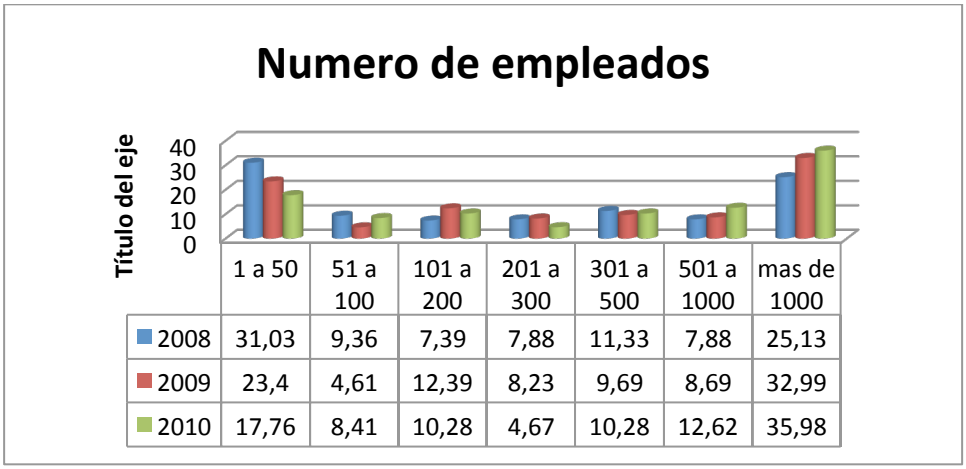
- Herramientas y prácticas de seguridad: Busca identificar las prácticas de seguridad y las herramientas que implementan las empresas para evitar la pérdida de información.

- Políticas de seguridad: Busca identificar la formalidad fe las políticas de seguridad, los procesos de implementación en las empresas entre otros.

- Capital intelectual: Busca detectar la formación y la preparación del personal del área de TI en cada una de las organizaciones, así como su experiencia en el área previa.

En el área demográfica se identificó que el área de mayor participación en la encuesta estuvo en el área de la educación con un 16%, seguida por el área de las telecomunicaciones y la de consultoría especializada con 14% las dos, después encontramos el área del gobierno y sector público con un 12%, posterior a esto encontramos los servicios financieros y de banca con un 10% en los últimos lugares encontramos las áreas de construcción e ingeniería, sector hidrocarburos, salud, alimentos, manufactura entre otras vemos que solo hubo participación de las fuerzas armadas en el año 2008 con un porcentaje de 0,93% de la muestra de ese año.

De igual manera al analizar el número de empleados podemos ver que la gran y mediana empresa tuvo una participación muy importante en la encuesta, esto debido a que en la mayoría de los casos están más sujetas al estricto cumplimiento de los diversos estándares de calidad en el área de seguridad.



	1 a 50	51 a 100	101 a 200	201 a 300	301 a 500	501 a 1000	mas de 1000
2008	31,03	9,36	7,39	7,88	11,33	7,88	25,13
2009	23,4	4,61	12,39	8,23	9,69	8,69	32,99
2010	17,76	8,41	10,28	4,67	10,28	12,62	35,98

Ilustración 7: Número de empleados Fuente – Seguridad Informática en Colombia

Otro de los resultados de esta encuesta se evidencia un aumento significativo en el número de cargos de Directores del área de seguridad informática junto al de gerentes de tecnología, pero se evidencia que estos cargos aún mantienen la generación de propuestas muy técnicas, que distan del tipo de propuestas que se espera apoyen las decisiones de los comités directivos lo cual genera que no sean tomadas como prioritarias para la organización, se determina que este tipo de propuestas deben ser contempladas en términos económicos demostrando a los líderes de los procesos el impacto que una falla de seguridad informática representa para la organización.

Tabla 5 ASIGNACIÓN DEL GASTO DE SEGURIDAD	2009	2010	2011	2012
Protección de la red	**74.40%**	**17.46%**	**17.63%**	**78.33%**
Proteger los datos críticos de la organización	57.90%	**14.34%**	**13.85%**	64.44%
Proteger la propiedad intelectual	23.10%	4.46%	4.56%	25.00%
Proteger el almacenamiento de datos de clientes	44.90%	10.19%	0.00%	41.94%
Concientización/formación del usuario final	26.70%	6.94%	6.74%	16.39%
Comercio/negocios electrónicos	16.20%	3.37%	2.89%	52.78%
Desarrollo y afinamiento de seguridad de las aplicaciones	25.10%	5.54%	12.54%	22.50%
Seguridad de la Información	53.10%	**13.12%**	**16.48%**	32.50%
Contratación de personal más calificado	15.10%	2.61%	4.82%	5.56%
Evaluaciones de seguridad internas y externas	29.20%	6.24%	7.19%	27.22%
Pólizas contra cibercrimen	6.00%	1.14%	0.78%	52.22%
Cursos especializados en seguridad informática(cursos cortos, diplomados, especializaciones, maestrías)	21.30%	5.35%	5.96%	33.33%
Cursos de formación de usuarios en seguridad informática	12.60%	3.12%	6.75%	13.06%
Monitoreo de Seguridad Informática 7 x 24	27.70%	5.28%	6.49%	18.61%

Ilustración 8 Asignación Gastos de Seguridad 2009-2012 – Fuente: XII Jornada de Seguridad

En el tema de la seguridad de acuerdo a la encuesta realizada en 2010 por ACIS se muestra que en los últimos años se ha generado una confianza algo excesiva frente al tema de la seguridad esto debido a la implementación de algunas normativas en los estados, pero esto mismo genera lo que se denomina un hueco de seguridad, pero a pesar de esto se tiene que los informes demuestran n aumento en la conciencia para el monitoreo de los incidentes de seguridad a pesar de no contar con herramientas demasiado especializadas se busca mitigar los accesos no autorizados; Entre las fallas de seguridad con mayor índice de recurrencia tenemos entre 2009 y 2010 el software no autorizado 21,50 y los caballos de Troya y virus con 32,71%, seguidos por accesos no autorizados a las web de las empresas 21,50% entre otros.

Se identifica en el informe de ACIS que entre las fuentes de detección de fallas de seguridad está el análisis de los procesos de auditoría, registros de firewall, seguido por la notificación por personal interno de la organización, de igual manera se indica que estas fallas en su gran mayoría son reportadas a las directivas de la organización, seguido de los expertos en la atención de seguridad como lo son los entes públicos especializados en atención a delitos informáticos.

En muchas organizaciones Colombianas el no reportar ante las autoridades competentes las fallas de seguridad que se detectan es un practica por decirlo de alguna manera algo común siempre y cuando estas falla solo afecten de forma superficial las operaciones internas y con esto se evita colocar en riesgo la reputación de la organización, la pérdida de clientes potenciales y hacer que la organización se vea vulnerable ante la competencia.

A pesar de lo anterior podemos decir que para el año 2010 hubo un aumento en el compromiso de las empresas encuestadas a reportar los incidentes de seguridad gracias a la creación de una legislación más efectiva en Colombia frente a los delitos informáticos, pero a pesar de esto muchas veces los procesos de investigación pueden ser más costosos y los resultados infructuosos.

Para el caso de las herramientas de seguridad que son empleadas vemos en el estudio que solo el 42,04% de las organizaciones entre el 2008 y el 2009 realizaron por lo menos una prueba anual a su sistema de seguridad seguido de un 30,32% que no realiza ninguna al compararlo con años anteriores es claro que la tendencia a evaluar y colocar a prueba los sistemas de IT en las organizaciones es cada vez menor debido a que muchos directivos consideran que con solo implementar costosas herramientas y mecanismos de seguridad se genera lo que se denomina una falsa conciencia de seguridad.

De acuerdo a lo anterior y al consultar por las herramientas de seguridad que son empleadas en las organizaciones Colombianas encontramos las siguientes:

	2008	2009	2010
Smart cards	11,3	13,9	12,62
Biometría	19,7	16	29,44
Antivirus	76,4	77,8	83,18
Contraseñas	78,3	75,8	79,44
Cifrado de datos	42,9	41,2	42,06
Filtro de paquetes	28,1	30,9	27,1
Firewalls Hardware	49,3	55,7	62,62
Firewalls Software	58,1	52,6	55,61
Firmas digitales/certificados digitales	27,6	34,5	35,98
VPN/IPSec	51,2	54,1	51,87
Proxies	54,2	44,8	48,6
Sistemas de detección intrusos	27,1	30,9	30,84
Monitoreo 7X24	22,7	19,1	23,83
Sistemas de prevención de intrusos	20,7	27,3	28,97
Sistemas de detección de anomalías ADS	4,93	7,2	4,21

Firewalls de aplicaciones web WAF	22,2	21,6	17,29
Administración de logs	26,6	26,3	26,64
Herramientas de validación de cumplimiento con regulaciones internacionales	8,8	7,2	7,01
Monitoreo de bases de datos	-	23,7	28,04
Otros, especifique: Antispyware, antispam, honeypots, inForce, monitoreo transaccionales.	-	3,1	2,34

Ilustración 9: Herramientas de Seguridad de las Organizaciones

De acuerdo a la tabla anterior se evidencia que el uso de dispositivos como Firewalls de hardware, sistema de detección y prevención de intrusos son las herramientas más empleadas además se identifica un alza importante en el uso de las firmas digitales y sistemas de biometría.

Para el año 2010 el 78,14% de las organizaciones encuestadas demostró tener una política de seguridad ya institucionalizada o en proceso de creación, pero a pesar de tener políticas instauradas es claro que el cumplimiento de las mismas aún se ve obstaculizado por la falta de integración entre los diversos procesos q integran la organización misma, esta falta de integración hace ver a la seguridad de la información como un tema nuevamente puramente técnico y sin importancia en el proceso de toma de decisiones.

Parte de esta falta de integración se debe a la falta de conocimiento del flujo real de la información, la no definición de las responsabilidades de cada uno de los actores en cada proceso del flujo de la información.

Según el informe de criminalística presentado por la policía nacional en su edición semestral muestra que durante el 2010 el número de crímenes cometidos a través

del internet tuvo un aumento considerable con relación al año inmediatamente anterior de acuerdo a la siguiente Tabla:

Delito	2009	2010
De la protección de la información y los datos	589	985
Delitos contra derechos de autor	17.623	19.927

Ilustración 10: Delitos Informáticos Colombia 2010 Fuente – Revista Seguridad Policía Nacional

De acuerdo al informe presentado por la policía el siguiente es el cuadro de los delitos que fueron reportados en cada uno de los departamentos en el primer semestre del año 2011.

Siendo el delito más reportado el de hurto por medios informáticos o semejantes con un total de 396 reportes en todo el país (Ver tabla 4), y el departamento que más delitos informáticos reporto fue Magdalena con un total de 89 seguido por Boyacá con un total de 79 delitos reportados, en esta tabla también podemos analizar que el delito más reportado durante el año 2010 fue el de Hurto por medios informáticos o semejantes con un total 251 casos, seguido por el acceso abusivo a un sistema informático con un total de 76 reportes.

De acuerdo al promedio de reportes de las principales ciudades tenemos que Bogotá tuvo el mayor número de reportes con un total de 212 seguido de Cali con una clara diferencia de 97 y Barranquilla con un total de 95 (Ver tabla 5) el principal delito reportado en las ciudades también fue el de Hurto por medios informáticos o semejantes con un total de 233 reportes y el de acceso abusivo a un sistema de información con un total de 221 reportes.

Este reporte hace referencia principalmente a la modalidad delictiva de robo de identidad, como es la clonación de tarjetas de crédito, este tipo de daños no solo afectan a los usuarios que son víctimas del hurto sino la imagen de las empresas que son sujetas a estos procesos de intrusión

DELITO	DEPARTAMENTO																					TOTAL X DELITO
	ARAUCA	BOLIVAR	BOYACA	CALDAS	CAUCA	CESAR	CUNDINAMARCA	GUAJIRA	MAGDALENA	MAGDALENA MEDIO	META	PUTUMAYO	QUINDIO	RISARALDA	SANTANDER	SUCRE	TOLIMA	HUILA	URABA	VALLE	VICHADA	
Acceso abusivo a un sistema de información	1		13	10		1	6		9		5	1	1		9		1	11		8		76
Obstaculacion ilegitima de un sistema informatico o red de telecomunicaciones			1										2									3
Interceptacion de datos informaticos	1		2			1			2									1		1		8
Daño informatico									1			1						6		2		10
Uso de software malicioso																				1		1
Violacion de datos personales	4		1			1		1	4		4		2					12		6		35
Suplantacion de sitios web para captura de datos personales						1			1											1		3
Hurto por medios informaticos y semejantes	1	2	60	33	2	16			71	7	1		1	3				23	3	25	3	251
Transferencia no consentida de activos	3		2	1									1			1				1		9
TOTAL X DEPARTAMENTO	10	2	79	44	2	20	6	1	88	7	10	2	7	3	9	1	1	53	3	45	3	

Ilustración 11: Reporte de Delitos Informáticos por Departamentos Policía Nacional – Fuente Revista policía Nacional

	DEPARTAMENTO							
	BARRANQUILLA	BOGOTA	CALI	CARTAGENA	CUCUTA	MEDELLIN	PEREIRA	TOTAL X DELITO
Acceso abusivo a un sistema de información	14	173	19	5	4	3	3	221
Obstaculacion ilegitima de un sistema informatico o red de telecomunicaciones								0
Interceptacion de datos informaticos		1	1					2
Daño informatico			2					2
Uso de software malicioso								0
Violacion de datos personales		9	7	1	8		2	27
Suplantacion de sitios web para captura de datos personales		10					7	17
Hurto por medios informaticos y semejantes	81	19	53	1	66	6	7	233
Transferencia no consentida de activos			15		1			16
TOTAL X DEPARTAMENTO	95	212	97	7	79	9	19	

Ilustración 12: Reporte de Delitos Informáticos por Principales Ciudades - Fuente Policía Nacional

11. ERP (ENTERPRISE RESOURCE PLANNING) SISTEMAS DE PLANEACIÓN DE RECURSOS EMPRESARIALES

En el presente, debido al gran auge de la tecnología, que crece a pasos agigantados todos los días en el mundo entero, la información es generada cada segundo e instantáneamente en todos los niveles y ámbitos de la Sociedad. Las organizaciones no son ajenas a este suceso, ya que las tendencias del mercado actual y futuro, obligan a éstas a ser cada vez más competitivas y a considerar la información como uno de los activos más importantes. Por ende, logran de esta manera tener una cantidad de información que debe ser manejada de la forma más efectiva posible con el objetivo de sacarle el mayor provecho, teniendo en cuenta que el manejo de ésta puede significar ganancias o pérdidas para las mismas.

Como respuesta a una manera positiva de manejar este tipo de activo importante en las organizaciones nacen los ERP: (por sus siglas en ingles ERP, *Enterprise Resource Planning*) Sistemas de Planeación de Recursos Empresariales en forma de software, que han ido evolucionando a través de los años y que tienen como objetivo permitirle a las empresas controlar y manejar la información que se genera en cada dependencia y en todos los niveles de la misma. El fin de los ERP es Integrar en un solo sistema, los sistemas de información especializados que existen para cada proceso de las organizaciones, generando una base de datos completa que trabaje con información en tiempo real, donde la obtención de datos sea instantánea y que permita la automatización de los aspectos operativos y productivos de la organización.

Los sistemas de planeación de recursos ERP son sistemas de gestión integrales que están compuestos por diferentes partes, las cuales tienen diferentes usos en una única aplicación. Aplicaciones de carácter financiero, de logística, de compras, de ventas, control de inventarios, pedidos, nominas etc. son las que componen un ERP, logrando de esta manera la unificación de los diferentes procesos, al

contrario del manejo de forma aislada e independiente de cada uno. Por medio de la aplicación se integra todo lo necesario para el funcionamiento de los procesos de negocio de una empresa, garantizando la disponibilidad de toda la información, para todos, todo el tiempo.

A través del software ERP los programas no trabajan de manera independiente y sin tener conexión entre sí, sino que trabajan de manera interconectada e integrada generando una base de datos centralizada que permita optimizar los procesos y donde la información sea manejada de manera rápida, precisa, compartida y accedida entre todos los usuarios de la organización constantemente.

Los objetivos fundamentales de un ERP son: dar apoyo a los clientes del negocio, acceso a la información por medio de la integración de los datos, la eliminación de datos y operaciones innecesarias, optimización de los procesos, la disminución de costos de operación y el empleo de esta información para la correcta toma de decisiones en las organizaciones.

11.1. Mercado de los ERP

El mercado de los ERP está dominado en su mayoría por tres grandes fabricantes los cuales tienen la mayor aceptación de sus productos, estas son: SAP, Oracle y Microsoft. La compra de JD Edwards por parte de PeopleSoft y el intento de fusión entre SAP y Microsoft son la clara muestra de lo que estos están dispuestos a hacer por tener el liderazgo. La tendencia de los proveedores, es crear grandes sistemas con multifunciones que incluyen CRM y SCM entre otros, la diferencia entre cada uno de ellos será la funcionalidad de cada sistema. Oracle por ejemplo, ha intentado mejoras sus prestaciones de bases de datos con el fin de mejorar sus prestaciones en recursos humanos donde PeopleSoft ocupaba la mejor posición.

Los ERP tienen un camino que está siendo recorrido el cual debe permitirles la competencia en igualdad de condiciones con las aplicaciones especializadas. La verdadera funcionalidad de los ERP llega de la mano con tecnologías estándar que permitan que aplicaciones diseñadas desde distintas ópticas y por distintos fabricantes puedan interactuar sin problemas.

11.2. Características de Los ERP

Un ERP posee características fundamentales que lo diferencian de cualquier tipo de software empresarial. Las 3 características fundamentales son las siguientes:

Integridad: La propiedad de integridad de los ERP permite la unión, relación y control de varios sistemas especializados en uno solo, funcionando de manera conjunta. Los diferentes procesos de la organización se relacionan entre sí, entendiendo que el resultado de un proceso desencadena el comienzo del otro. Por medio de la integración, se evitan las operaciones innecesarias y la duplicidad de información, las áreas funcionan como un todo, para todos los usuarios y se optimizan así los procedimientos. Lo anterior elimina el problema de tener varios programas que manejan áreas diferentes en la empresa, con la desventaja de que al no estar integrados crece el margen de contaminación de la información y de errores en la operación.

Modularidad: Es claro que una organización es el conjunto de diferentes áreas o procesos que están interrelacionados entre sí porque comparten la información generada en sus funciones. Los ERP entienden este concepto y por ende, su funcionalidad se encuentra dividida en módulos, los cuales se conectan a distintas bases de datos y son instalados de acuerdo a los requerimientos de la organización. Lo anterior se convierte en una ventaja tanto económica como técnica. Ejemplo de estos módulos son: ventas, finanzas, inventarios etc. Según la

necesidad de una u otras funcionalidades, estos módulos se tendrán en cuenta para el diseño del ERP.

Adaptabilidad: los ERP son diseñados para adaptarse a los requerimientos y necesidades de la organización para la cual son creados. Esta propiedad está basada en la parametrización y la configuración de los procesos de acuerdo a las salidas que deba generar cada uno de ellos, la cual es diferente para cada tipo de organización.

11.3. Estructura de un ERP

Por su finalidad y funcionalidad un ERP esta subdividido en módulos cada uno creado con el objetivo de satisfacer las necesidades propias de un cliente o área de negocio específica en la siguiente grafica se podrá observar los módulos generales que contiene un ERP y las actividades básicas a las que da apoyo.

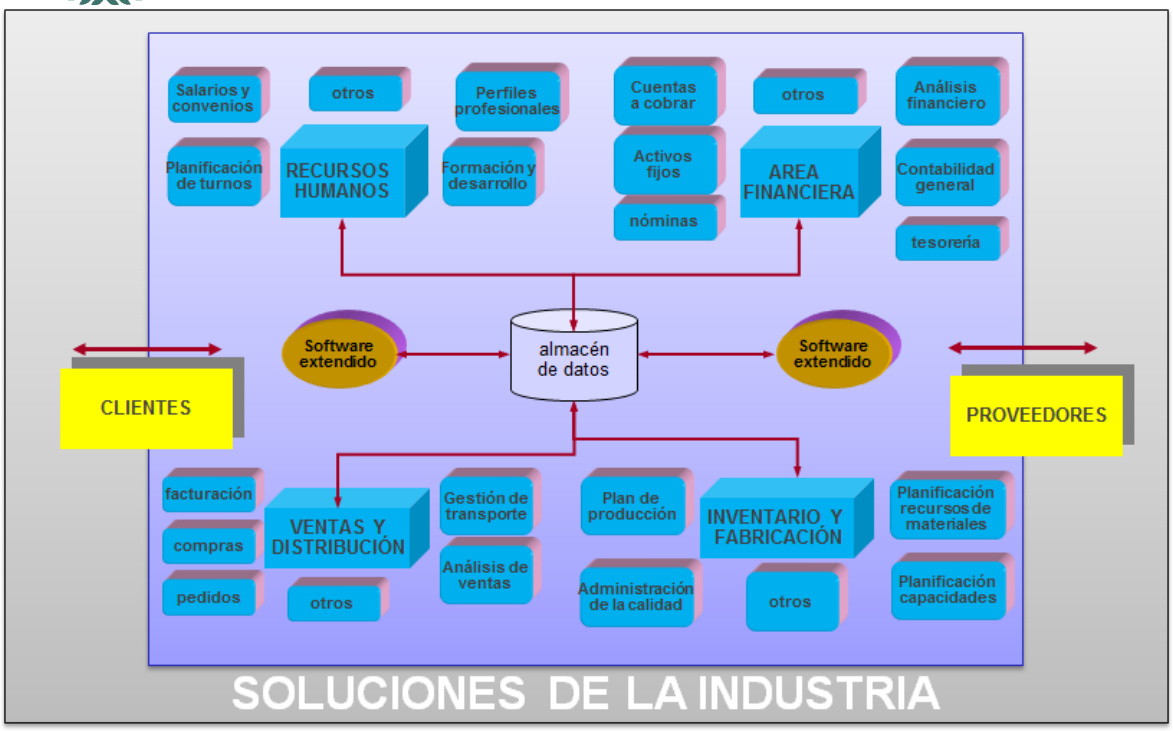


Ilustración 13: Creación propia basada en La nueva Generación de los ERP (Enterprise Resource Planning)

Según el grafico anterior podemos observar que como áreas principales de cubrimiento encontramos las siguientes:

Área Financiera: Este módulo está enfocado en dar apoyo a las actividades económico- financieras de la organización, en el encontramos: flujo de caja, nominas, contabilidad, tesorería, área de compras, cuentas por pagar, cuentas por cobrar, activos fijos, análisis financiero, entre otros.

Ventas y distribución: Este módulo es el encargado del control de las últimas etapas del ciclo de vida de un producto, la venta y posterior distribución del mismo, entre las cadenas de distribuidores y clientes

En este módulo también se contemplan los módulos propios de la posventa como lo es fidelización de clientes con módulos de atención a clientes y módulos de

servicio para tención de quejas, sugerencias o reclamaciones por procesos de garantía.

Recursos Humanos: El control de personal es una de las tareas más delicada que tiene la organización. Para ello, los ERP a través de este módulo permite la administración de personal, control de procesos de capacitación, manejo de nóminas, definición de perfiles, control de turnos además algunos ERP le brindan la posibilidad aquellas organizaciones que no cuentan con Intranets la posibilidad de generar y personalidad su propio espacio para poder compartir información de una manera más sencilla con todo el personal.

Inventario y Fabricación: Este módulo da apoyo a las actividades de generación de productos controlando gran parte de su ciclo de vida iniciando desde la etapa de diseño, aprobación, gestión de materiales controlando la relación con los proveedores, Control de calidad, procesos de mantenimiento preventivo/ correctivo, y para ejecutar las actividades anteriores el ERP permite realizar gestión de proyectos a través del control de tareas, actividades, tiempos de ejecución, personal asignado entre otros.

Análisis de Datos: Los ERP's también contemplan módulos de análisis de datos enfocados en los procedimientos propios de Bussiness Inteligence (BI), brindado especial atención en el análisis de riesgos que brinda a la alta gerencia de las organizaciones la capacidad de tomar decisiones basados en datos reales de cada uno de los niveles de la organización.

Estas herramientas le aportan a la organización la capacidad de homogeneizar la información que proviene de fuentes tanto internas como externas, manejo de información en tiempo real, fácil distribución de la información a través de la cadena de valor, modificación del modelo de datos de la información para ser ajustado a los requerimientos inmediatos, gestión de indicadores.

Existen cuatro tipos de herramientas, cada una encargada de una parte del proceso de análisis:

- Encargadas de la extracción de datos, limpieza e integración para evitar la duplicidad, datos innecesarios debido a la diversidad de fuentes de las cuales provienen tanto a nivel interno como externo.
- Herramientas que gestionan el almacenamiento y resguardo de los datos de una manera segura y confiable.
- Instrumentos de minería de datos que permiten el análisis de la información con el objetivo de identificar patrones de conducta en los mismos.
- Suites que permiten la integración entre cada una de las anteriores además de su usabilidad pues son las que se encargan de la gestión de la interface gráfica.

11.4. Tipos de Sistemas ERP

11.4.1. Sistema ERP Propietario

Se refiere a los sistemas que deben ser pagados para poder usar sus licencias. Normalmente estas licencias son pagadas de acuerdo al número de puntos operativos y pueden llegar a veces a representar la mitad de la implantación total del sistema. A veces el costo total de la implantación suele encarecerse alejando la posibilidad a las microempresas de acceder a este tipo de sistemas en las organizaciones.

La mayor cantidad de los sistemas ERP propietarios son creados por reconocidos desarrolladores de software dando como resultado un producto sólido, con mayor madurez y soporte técnico. Algunos, son creados por microempresas de software generando un producto en la mayoría de las veces, especializado en áreas o sectores concretos de la empresa.

11.4.1.1. Ventajas de un ERP Propietario

Algunas de las ventajas para una organización al implementar un ERP propietario son:

- Control de calidad. Por lo general las compañías que producen el software tienen departamentos de control de calidad donde se realizan pruebas de funcionamiento del software para dar un mejor respaldo a sus clientes.
- El personal que produce el software es altamente entrenado, calificado y con experiencia en el campo.
- Debido a que el ERP es producido por una empresa de software conocida, muchas organizaciones compran los productos y por ende, muchas personas son usuarios de los mismos por lo cual es más fácil encontrar a alguien que lo sepa usar.
- Una parte de los recursos obtenida de las ventas es destinada a la investigación sobre los usos del mismo.
- Acceso a un gran número de publicaciones que son ampliamente difundidas acerca del uso y aplicación del software. De esta manera se facilita el uso de las tecnologías que proveen las compañías de software propietario.
- Existe software propietario para aplicaciones muy específicas para sectores concretos que no existen en ninguna otra compañía productora de software.

11.4.1.2. Desventajas de un ERP Propietario

- Código fuente secreto. Las empresas productoras son las únicas que tienen acceso al código fuente del software por lo cual es imposible estudiar sus componentes o encontrar la causa de errores en su funcionamiento.
- Adaptación costosa de módulos particulares. En el caso de que se requiera una modificación o extensión de una pieza de software, se debe pagar a la

empresa una suma importante para la realización de la misma. La extensión del software de manera arbitraria es ilegal.

- Soporte técnico deficiente. En la mayoría de los casos se presenta esta desventaja que se traduce en un soporte técnico demorado en responder satisfactoriamente. Si la compañía se va a la quiebra, el soporte técnico no se podrá volver a utilizar.
- Cursos de aprendizaje costosos. Aprender a usar el software de manera eficiente requiere la asistencia a los cursos de aprendizaje que tienen un valor elevado.
- Exclusivo derecho de innovación. Solo la compañía que hace el software puede realizar cambios o innovaciones en el mismo.
- Copias sin licencia son ilegales. Hacer copias del software se considera ilegal sino se ha contratado el pago de las mismas.
- Imposibilidad de compartir. Las compañías no pueden compartir entre sí los sistemas que tienen funcionando exitosamente.
- Si una compañía fabricante de software es comprada por una más poderosa, lo más probable es que esa línea de software quede descontinuada perjudicando así a la organización compradora.
- Se crea dependencia a proveedores ya que en la mayoría de los casos el estado se hace dependiente de un solo proveedor.

Ejemplos de ERP propietarios: SAP Business One, Microsoft Dynamics NAC, Sage Línea 100, Solmicro, CCS Agresso, entre otros.

11.4.2. Sistemas ERP Opensource O De Software Libre

Los sistemas ERP Opensource o de software libre, son una excelente alternativa a los ERP propietarios. Aunque existe la tendencia a pensar que si el software es libre significa que sea gratis no siempre es de esta

manera. Las empresas desarrolladoras de este tipo de aplicaciones por lo general tienen un grupo de comunidades donde se ofrecen servicios de implantación, configuración, parametrización y capacitación para los usuarios del ERP. Facilitando de esta manera el manejo del software.

Estas aplicaciones usan código abierto asegurando así un buen servicio, ya que diferentes empresas pueden dar soporte técnico a las organizaciones que lo emplean sin tener que depender del proveedor como en el caso de las aplicaciones de software propietario.

Además de esto, los proyectos OpenSource le entregan al usuario final garantía y libertad en el software dándole vía libre para usar el programa para cualquier actividad, libertad para acceder y modificar el código fuente del software y libertad para distribuir la aplicación sin que esto incurra en actos ilegales.

11.4.2.1. Ventajas de un ERP Opensource

- Se tiene el código fuente. Esta ventaja permite al usuario modificar y adaptar el software a sus necesidades y requerimientos. Se pueden corregir errores y realizar cambios en el funcionamiento del mismo.
- Se tiene una licencia. Es preferible usar un software Opensource a recurrir a actos ilegales haciendo copias de licencias que no han sido pagadas en el caso del software propietario.

- Se puede obtener soporte técnico de desarrolladores o de cualquier empresa que haya usado la aplicación, obteniendo información basada en la experiencia de uso.

11.4.2.2. Desventajas de un ERP Opensource

- Falta de responsabilidad. El software OpenSource suele obtenerse sin garantía de ningún tipo. Para evitar los inconvenientes que pueden resultar de lo anterior, es indispensable documentarse y tener buenas referencias del software que se está implementando. Se debe también contratar un servicio de mantenimiento que permita solucionar la mayor parte de los problemas que puedan presentarse.
- Software sin terminar. Muchos proyectos de software OpenSource se caracterizan por no estar completos en el sentido de que no ofrecen todas las funcionalidades necesarias. Siempre se encuentran en proceso de realización.
- Cambio en las licencias. El modo de la licencia puede cambiar, es decir, puede convertirse en cerrada trayendo esto el posible problema de quedarnos con una aplicación obsoleta.
- Costos ocultos. Para poder entender la aplicación e implementar las soluciones de manera satisfactoria debemos acudir al conocimiento de los desarrolladores y a la formación por parte de los mismos. De esta manera resulta necesario pagar por estos servicios en lugar de la licencia del software.

Ejemplos de ERO OpenSource: Compiere, Fistera, Openbravo, FacturaLUX, TinyERP, OpenBluelab, Project Open, penXpertya, Opentaps entre otros.

11.4.3. Sistema ERP Modalidad Saas (La Nueva Tendencia)

El mercado de los ERP ha marcado una nueva tendencia de sistemas ERP, esta nueva tendencia es el software como servicio o SaaS donde el modelo de entrega de software lo hace una compañía implantadora, la cual es la encargada de proporcionar mantenimiento, operación técnica diaria y provee la ayuda al cliente para el uso de la aplicación. El cliente tiene hospedado el sistema en la compañía proveedora de IT. El modo de entrega se puede hacer desde a consumidores caseros o a grandes organizaciones. La modalidad SaaS es compatible tanto con los tipos de ERP propietarios como con los tipos de software OpenSource o de software libre anteriormente mencionados.

Para este tipo de aplicaciones las actividades son administradas en lugares centrales y no en la oficina del cliente, la distribución del software tiene un modelo en el que el producto realizado es el mismo para varios clientes y la lógica del negocio reside en la localidad central del proveedor, es decir, es software con acceso vía red.

Debido a los bajos costos de entrada que representa este tipo de software, está popularizándose en las pequeñas organizaciones. Las grandes organizaciones se están viendo interesadas en este tema principalmente para programas de recursos humanos y aplicaciones ERP y CRM. Teniendo en cuenta lo anterior, las grandes compañías desarrolladoras de software, están estudiando la posibilidad de crear su versión de software SaaS. Estados Unidos está teniendo un éxito considerable en este aspecto, mientras que Europa está comenzando a despertar en el tema.

11.4.3.1. Ventajas de un ERP Modalidad SAAS

- La empresa proveedora tiene el total de la responsabilidad de la operación de la aplicación. Es decir, la compañía de IT es la encargada de dar garantía sobre la disponibilidad de la aplicación y de su correcto funcionamiento.

- Para que el cliente siga pagando el servicio, la compañía proveedora permanentemente le brinda atención continua sin desatender sus necesidades.

- Bajan los costos y disminuye el riesgo de inversión debido a que el cliente no debe tener necesariamente, un área especializada en la organización para soportar el sistema.

- La empresa proveedora de la aplicación suministra los medios de acceso seguros a los entornos de la aplicación, para evitar la filtración de datos privados en la red pública.

11.4.3.2. Desventajas de Un ERP SAAS

- En la mayoría de los casos, el cliente o usuario no tiene acceso al programa para hacer modificaciones, a diferencia del software OpenSource, el cual en este aspecto se encuentra disponible.

- El usuario no tiene acceso directo a los contenidos de la aplicación ya que estos se encuentran custodiados en un lugar remoto. Esto podría verse reflejado en inconvenientes en la privacidad, control y seguridad de la aplicación.

- Debido a que la aplicación y el servicio dependen de la misma empresa, no se permite la migración a otro servicio usando la misma aplicación, sino que deben funcionar de la mano.

Algunos ejemplos de ERP SaaS son: Netsuite, Salesforce, Intacct, Workday, GSInnovate, entre otros.

11.5. Tabla Comparativa Entre Tipos de Software

En la siguiente tabla, se muestra la comparación de diferentes aspectos a tener en cuenta por una organización, al tomar la decisión acerca de qué tipo de software es el más conveniente.

	Software Propietario	**Software OpenSource**	**SaaS**
Coste de adquisición	Malo	Bueno	Medio
Rapidez de despliegue	Medio	Medio	Bueno
Coste de mantenimiento	Medio/Malo	Medio	Bueno
Capacidad	Medio	Bueno	Malo

Personalización			

Tabla 1 Comparativa entre Tipos de Software - Fuente Elaboración Propia

Según esta tabla podemos observar que en cuestión de precios el software propietario es el perdedor, el tiempo de despliegue es normal, la capacidad de personalización es algo limitada y el costo de mantenimiento de la aplicación va de medio a malo. El software OpenSource en cambio, se destaca por ofrecer un buen costo y libertad para personalizar la aplicación. Por su lado, el software como servicio SaaS se comporta bien en el aspecto de los costos y en la despreocupación de la organización por los aspectos técnicos del mismo. La desventaja para este tipo de software SaaS es que, la capacidad de personalización es prácticamente nula.

11.6. ERP y Cloud Computing

El Cloud Computing o computación en la nube es una nueva modalidad de computación donde la realización de esta, se hace desde un sitio remoto (en la nube) por medio de la utilización de internet. En esta modalidad, en lugar de acceder a la información y a las aplicaciones que se encuentran de forma local en un computador de escritorio estos datos son accedidos desde cualquier computador y son obtenidos a través del internet.

Este tipo de tecnologías permite al usuario evitar la preocupación que dan las instalaciones de software, servidores, bases de datos, sistemas operativos y toda la complejidad y trabajo que trae consigo la instalación de un nuevo sistema en cualquier organización.

11.6.1. Beneficios del uso de Cloud Computing

- Más Flexibilidad
- Fácil Implementación.
- Requiere de menores recursos empresariales.
- Acceso a la gestión de la organización desde cualquier lugar.
- Elimina costos de actualización y mantenimiento.

El sistema líder en estos momentos a nivel mundial por operar de manera Total en internet (todas las aplicaciones en la nube) es netSuite. Este sistema integra las más importantes funcionalidades de un Sistema empresarial como: ERP, CRM y Ecommerce. Este sistema se contrata como un servicio, es decir, no se tiene que realizar ningún tipo de instalación en la empresa, aprovechando los servicios que esta clase de sistemas ofrecen.

11.6.2. Impacto del Cloud Computing en Los Sistemas ERP- CRM

La aparición del cloud computing en los sistemas ERP cambió el enfoque en el que un solo fabricante de software era el que ofrecía de una manera integrada todos los módulos o aplicaciones necesarias en una organización. El cloud computing ofrece una integración de las mejores aplicaciones y servicios web construyendo de esta manera una solución global de gestión en la nube con el objetivo de satisfacer las necesidades de las empresas.

Por medio de las arquitecturas de Cloud Computing las diferentes categorías de sistemas, tales como: ERP, CRM, SRM, E-Commerce etc. se integran entre sí, tomando lo mejor que ofrece cada proveedor de acuerdo a las necesidades de la empresa. Los módulos clásicos del Concepto de ERP se encuentran también disponibles en esta arquitectura como servicio que se presenta como nueva. Como ventaja está la posibilidad de poder escoger entre diferentes ofertas de diferentes fabricantes debido a que la oferta es mucha más amplia para las organizaciones.

En este nuevo enfoque donde el Software es un servicio las plataformas de Desarrollo como PaaS y Force.com entre otros representan un papel fundamental ya que estas plataformas son las que permiten que el desarrollo de las aplicaciones se haga a la medida de las necesidades que tiene la empresa y permite por medio de mecanismos como Appexchange integrar todas las aplicaciones o servicios Web que pueden ser de diferentes fabricantes pero que han sido elegidos como herramienta para el logro de los objetivos de la organización.

Esta integración de aplicaciones de la empresa se realiza también por medio de los servicios de integración en la nube que son diseñados para la conexión de las bases de datos y de los sistemas ERP con nuevas aplicaciones en la nube.

11.6.3. Las Tendencias de Cloud Computing y ERP

En la última década el panorama de la computación en la Nube para ERP ha cambiado de manera dramática y sustancial. Debido a los cambios en los factores económicos resultado de las crisis financieras mundiales, las empresas de cada sector y tamaño han estado luchando para afrontar de la mejor manera los retos del mercado en lo que tiene que ver con las aplicaciones ERP y soluciones empresariales.

En esta lucha, las aplicaciones ERP Cloud Computing han ganado muchos seguidores y demanda de empresas que se enfrentan contra los retos empresariales día a día. Estos retos incluyen déficit empresarial, incertidumbre, aumento de competidores, mayor expectativas de los clientes, y los cambios en la dinámica del mercado. Debido a los presupuestos ajustados o reducidos en la gerencia de las tecnologías de información, las directivas de las organizaciones están en la búsqueda de soluciones más asequibles que ofrezcan sistemas muy potentes para la empresa y que den soluciones ERP tales como las basadas en Web o en la nube.

Los administradores de Tecnologías de Información en muchas ocasiones han encontrado aplicaciones de Cloud Computing que incluso son más fáciles de usar e implementar, reduciendo lo anterior en gran medida el costo y el tiempo de satisfacer las necesidades específicas de la organización.

En resumen podemos decir que las ventajas de usar aplicaciones Cloud Computing son la implementación de Sistemas ERP en menor tiempo, menos recursos de TI necesarios, importante reducción de costos de operación, implementación y mantenimiento del mismo además de una fácil integración e implementación. Por los anteriores motivos las personas que toman las decisiones acerca de los sistemas a emplear en las organizaciones están reconsiderando la forma en que se están haciendo negocios, no solo para ahorrar costos, sino para seguir siendo competitivos en el mercado. Las empresas que están considerando

cambiar su aplicación ERP a código abierto o aplicación Web deben estar seguros de que están configurados correctamente para poderse integrar con la aplicación Cloud Computing y poder obtener un ERP que mejor se adapte a su organización.

11.7. Evolución del Mercado Global ERP

El mercado de los ERP está en un proceso de cambio continuo, las más importantes compañías productoras de software están entrando poco a poco en pequeños mercados que eran conformados por decenas de pequeñas empresas enfocadas a sectores específicos. Por ende, estas empresas necesitan sistemas especializados que se adapten a sus características propias y a su modelo de negocio de una manera concreta. Estos, eran casi siempre provistos por pequeñas organizaciones desarrolladoras de software que vendían sus productos a pequeñas cantidades de clientes.

En los últimos años, esta realidad ha ido cambiando debido a la incursión de Microsoft Dynamics, entre otros que han venido ocupando ese espacio por medio de la incorporación de pequeños partners locales que trabajan en el desarrollo de soluciones verticales y de esta forma incursionando en pequeños nichos de mercado.

El mercado de los ERP tiende a la concentración y se prevé que en unos años, solo unas cuantas compañías tendrán la completa participación en el. Las pequeñas empresas están viendo peligrar su futuro ya que sus clientes se están decidiendo por adquirir otro tipo de soluciones que prometen ser adaptables y personalizables a sus entornos. Los empresarios se están dando cuenta de que ya no necesitan un programa hecho a su medida que además implica más tiempo, un proceso de implementación más largo y futuras necesidades de soporte más

cuestionables. Las soluciones de las grandes compañías le están proporcionando más confianza.

El dinamismo es el actor principal en el mercado de los ERP: se están realizando ciertos movimientos entre las grandes compañías como uniones y compras de acciones que han dejado cierto grado de incertidumbre entre los directores de organizaciones que hacen parte de estas empresas que están en proceso de cambio. El mensaje que se capta es de dualidad, por un lado se puede decir que el mercado de los ERP se está encaminando hacia nuevas áreas por lo que las corporaciones buscan aumentar su cuota de mercado por medio de la compra de compañías competidoras y por otro lado parece dar a entender que la cadena evolutiva de este segmento está consolidada y que realmente se está dando el enfrentamiento corporativo.

Los puntos más importantes que definen el mercado actual de los ERP son:

1. Los fabricantes globales se están orientando hacia el mercado Pyme: (Pequeñas y medianas empresas) debido a que el mercado de las grandes empresas ya está muy saturado.
2. Los pequeños fabricantes que sobreviven y que son orientados a PYME tienen una ventaja debido a su mejor conocimiento del segmento de las Pyme y de las necesidades específicas que estas tienen. Su posicionamiento de cercanía y de generación de confianza frente a sus clientes y su preocupación por el uso de las soluciones, son puntos a su favor.

3. Soluciones que van más allá de los tradicionales ERP. Los ERP tradicionales están ofreciendo ciertos componentes adicionales a las Pyme como respuesta a sus requerimientos especiales.

4. La estrategia de los fabricantes es la realización de soluciones verticales y la obtención de clientes de mayor envergadura. Luego que sus productos ya están introducidos en el mercado y ya se tiene una buena base de clientes que asegura su viabilidad económica, los fabricantes de ERP para pyme están invirtiendo de manera estratégica en el desarrollo de integración vertical para sus productos en sectores específicos de mercado. Hay un gran interés general en atraer clientes de mayor tamaño, desplazando su atención precisamente en este tipo de clientes objetivo. Esta estrategia de expansión busca una mayor capacidad de inversión y mayor número de licencias a comercializar, entre otras. Por ende, las Pyme siguen siendo el interés de los fabricantes globales y de las medianas empresas desarrolladoras que se encuentran en un mercado común.

5. El software libre como nuevo competidor. El panorama competitivo puede complicarse por la aparición de soluciones de software libre y el afianzamiento progresivo de sus soluciones. Ejemplos: TinyERP y Openbravo.
6. No se ha logrado la completa funcionalidad. Se ha detectado que a pesar de la múltiple oferta existente de soluciones en el mercado, todavía existe carencia en lo que se refiere a funcionalidades adicionales que van más allá de lo que se puede considerar habitual en un ERP estándar.

7. La usabilidad de las herramientas es un aspecto clave. Esta característica si bien es importante en cualquier solución de software donde intervenga el usuario, se convierte en especialmente crítica en el entorno de las Pyme ya que la utilización de la herramienta es bastante alta y en muchas ocasiones el usuario es de un perfil inferior. En general, se percibe que todos los fabricantes principales y pequeños desarrolladores tienen siempre este aspecto muy presente.

8. Un área funcional por explotar: Recursos Humanos y Nómina. Se prevé que en los próximos años las Pyme demandarán de forma progresiva cubrir necesidades de gestión de personas y recursos humanos como lo hacen en estos momentos las grandes empresas.

9. La atención personalizada es valorada por los clientes. Los grandes productores de software deben seguir trabajando en este aspecto ya que sus clientes los perciben pocos cercanos a ellos y a sus necesidades. La estrategia generalizada de comercialización debería tener en cuenta este aspecto.

10. La relación entre costo Vs valor percibido no es satisfactoria. La variable económica es un hecho mucho más sensible en las Pyme que en la gran empresa y puede ser un aspecto muy importante y decisivo en el momento de seleccionar una herramienta u otra. Es importante que durante el proceso de selección de la herramienta se tengan en cuenta los costos de implantación.

La elección y clasificación de un determinado software de gestión como los ERP determina que disponga de una serie de requisitos y funcionalidades que posibiliten en buena medida su diferenciación. Hoy en día es muy común encontrar cualquier suite de gestión que quiera ser vista como un ERP y tener mayor reconocimiento en el mercado. Muchas empresas emplean como estrategias nombrar este software de gestión que llevan varios años en el mercado como ERP buscando expandir su mercado y con el fin de obtener una mayor remuneración sin incrementar proporcionalmente la funcionalidad de estos.

12. NORMATIVIDAD Y SEGURIDAD

En el caso de los sistemas de información es claro que las plataformas dependiendo su rango de acción están sujetas a ciertos tipos de riesgos o poseen ciertas vulnerabilidades que en caso de ser ejecutadas pueden llegar a colocar en riesgo a las compañías de formas inimaginables.

Es por eso que en los patrones de seguridad se deben contemplar tres aspectos fundamentales los cuales son contemplados en la norma ISO17799 los cuales son integridad confidencialidad y disponibilidad como parte de los principios fundamentales para poder comenzar hablar de seguridad en un sistema de información.

Para que una organización pueda garantizar una adecuada utilización de los recursos limitando la posibilidad de pérdidas de información mediante la eliminación o disminución de los riesgos y trabajando dentro de los marcos legales establecidos, debe tener claros la capacitación de su personal, los recursos técnicos que requiere, la estructura organizacional y los parámetros legales que se deben cumplir para poder mantener una adecuada operación y gestión.

Antes de iniciar a hablar sobre el tema de normatividad que rige los aspecto de la seguridad de los sistemas de información de las organizaciones debemos hablar de la importancia que tiene la gestión de riesgos, puesto que así como es de vital importancia el velar por el adecuado uso de los recursos económicos y físicos de la organización, también es importante analizar los riesgos a los que están expuestos los recursos informáticos y más en esta era donde día a día surgen nuevas técnicas de intrusión.

Uno de los aspectos de mayor importancia está en la identificación de perfiles de usuario con el objetivo de minimizar el riesgo de intrusiones de personal no autorizado a información confidencial de la organización, es por esto que se habla

de estandarización de usuarios control de accesos, monitoreo de las acciones que ejecuta cada usuario tanto en tiempo laboral como en horarios de baja actividad.

Cuando hablamos de información como el activo más importante de una organización debemos tener claridad sobre lo que significa este término, según ISO17799 - 2005[6] *la información es un activo de la organización, el cual posee la misma importancia de otros activos tangibles por lo cual requiere ser protegido y preservado.*

Otra definición que encontramos de Información[7] *es una agregación de datos que tienen significado especifico más allá de cada uno de estos y tendrá un sentido particular según quien y como la tenga.*

Por lo cual podríamos decir que la información es un conjunto de datos que poseen un significado dependiendo del tipo de análisis que se desee dar, esto debido a que un conjunto de datos especifico no tendrá el mismo significado para un nivel operativo que para un nivel ejecutivo debido a que el análisis y la perspectiva desde la cual se observen estarán en ángulos diferentes y los resultados o decisiones que se puedan tomar serán completamente diferentes, pero en ambos casos las decisiones tomadas con base en esta información estarán enmarcadas dentro de los objetivos organizacionales que ya estén definidos

12.1. Estándares y Regulaciones de Seguridad de Información

[6] Estándar internacional ISO/IEC 17799 segunda edición 2005 Consultada 17 de Marzo de 2012

7 Glosario Básico Inglés- Español para usuarios de internet 1994. 2000
http://www.ati.es/novatica/glosario/glointv4.pdf 17 de Marzo

.

Dentro de los principales estándares de calidad encontramos que los más empleados en Colombia ISO/IEC 27001, Cobit 4.1, Guías NIST, ITIL, Common Criteria, Octave, Guías ENISA, OSSTM, ISM3.

12.2. ISO (International Organization For Standardization)

Organización internacional de estandarización, fundada en el año 1947 cuya sede está en Ginebra y actualmente está integrada por miembros de más de 153 países.

Para la generación de las normas referentes al tema de seguridad de la información ISO (International Organization for Standarization) estableció un comité técnico en unión con IEC (International Electrotechnical Commission) el cual se denomina JTC1 (Joint Technical Committee), este comité a su vez posee una subdivisión en la cual el SG27 tiene por misión el desarrollo de proyectos de seguridad

ISO/IEC JTC1 SG27 /WG1: Este proceso tiene por misión el desarrollo y actualización de la familia de norma ISO27000, la identificación de futiros requerimientos, además de tener que mantener una estrecha colaboración con los demás grupos del JTC1 para el desarrollo de los diversos estándares.

ISO/IEC JTC1 SG27/ WG2: Encargado de analizar los temas de seguridad y criptografía, este grupo tiene la responsabilidad de identificar las técnicas y mecanismos de seguridad de los sistemas de TI, definición de la terminología , definir los mecanismos de uso de las técnicas de seguridad, manejo, desarrollo y actualización de todo tipo de técnicas de seguridad que brinden confidencialidad , sistemas de control de acceso, integridad entre otros a las organizaciones que implementen los estándares propuestos .

ISO/IEC JTC1 SG27/ WG3: Este grupo es el encargado de definir los criterios de evaluación de la seguridad, además de tener que definir los criterios que deben

ser evaluados, las técnicas que deben ser empleadas y los mecanismos de evaluación que serán empleados, además de tener que trabajar en conjunto con los demás grupos de ISO responsables de definir los estándares de comprobación y gestión de la calidad para evitar malos entendidos.

ISO/IEC JTC1 SG27/ WG4: este grupo es el encargado de los servicios y controles de seguridad, encargado de definir las bases de los futuros estándares en temas como continuidad de negocio, ciberseguridad, outsourcing entre otros. Determinación de mecanismos de control de servicios establecidos en cada uno de las normas de la familia de ISO 27000.

ISO/IEC JTC1 SG27/ WG5: Este grupo es el encargado de los temas que hacen referencia a la gestión de identidad y privacidad, en este grupo se desarrollan los estándares propios de los sistemas de control de datos personales, biometría, además de definir las bases de futuros estándares en control de acceso como es control de roles RBAC (Role-based access control), Single sing-on, mecanismos de anonimato y en general tecnologías para la mejora de la privacidad o PETs (Ver glosario).

12.2.1. ISO27000

Es un conjunto de estándares que le proporcionan a las organizaciones un marco de acción para la gestión de la seguridad de la información. El origen de esta familia de estándares está en los primeros lineamientos que fueron generados por BSI (British Standards Institution) como lo son BS5750 que paso a ser ISO9001, BS7750 que dio origen a ISO14001 y BS 8800 que da origen a OHSAS 18001, acá también encontramos la norma BS7799 que fue publicado en el año de 1995 para brindar un conjunto de buenas prácticas para las organizaciones británicas, esta norma estaba compuesta por dos partes las vuales era BS77991 y BS 77992 la primera parte daba una guía de buenas prácticas y tal como se maneja en los

estándares actuales no era certificable pro BS77992 contenía los modelos aplicables y por lo cual certificables.

En el año de 1999 el estándar BS77991 fue adoptado por ISO sin realizar mayores modificaciones baso el nombre ISO17799 la cual fue finalmente publicada en el año 2000, en el año 2002 el comité de ISO verifico la segunda parte del estándar de BSI y finalmente en el año 2007 se publicó la norma ISO27001y de igual manera se verifico nuevamente la ISO17799 y se publicó nuevamente como ISO27002:2005.

Posterior a estos acontecimientos tanto ISO como BSI han continuado con la publicación de estándares dentro de la familia ISO 27000 y BS 7799 que apoyen la gestión de las organizaciones en temas de seguridad.

NORMA	FECHA PUBLICACIÓN	TEMA	CERTIFICABLE	VERSIÓN
ISO/IEC 27000	1 DE MAYO DE 2009	VISIÓN GENERAL DE LA FAMILIA DE NORMAS ISO 27000	NO	
ISO/IEC 27001	15 DE OCTUBRE DE 2005	REQUISITOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD	SI	
ISO/IEC 27002	1 DE JUNIO DE 2007	GUÍA DE BUENAS PRÁCTICAS EN SEGURIDAD	NO	2 EDICIÓN
ISO/IEC 27003	1 DE FEBRERO DE 2010	SE CENTRA EN LOS ASPECTOS CRÍTICOS PARA EL DISEÑO E IMPLEMENTACIÓN DE UN SGSI DE ACUERDO A ISO27001	NO	
ISO/IEC 27004	15 DE DICIEMBRE DE	GUÍA PARA EL DESARROLLO E IMPLEMENTACIÓN DE	NO	

	2009	MÉTRICAS APLICABLES PARA DETERMINAR LA EFICACIA DE UN SGSI		
ISO/IEC 27005	1 DE JUNIO DE 2011	DIRECTRICES PARA LA GESTIÓN DE RIESGO EN SEGURIDAD	NO	2 EDICIÓN
ISO/IEC 27006	1 DE DICIEMBRE DE 2011	REQUISITOS PARA ACREDITACIÓN DE ENTIDADES DE AUDITORIA Y CERTIFICACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD	SI	2 EDICIÓN
ISO/IEC 27007	14 DE NOVIEMBRE DE 2011	GUÍA DE AUDITORIA DE UN SGSI	NO	1 EDICIÓN
ISO/IEC 27008	15 DE OCTUBRE DE 2011	GUÍA DE AUDITORIA DE LOS CONTROLES IMPLEMENTADOS EN UN SGSI	NO	1 EDICIÓN
ISO/IEC 27010	SIN FECHA DE PUBLICACIÓN	GUÍA PARA LA GESTIÓN DE LA SEGURIDAD CUANDO SE COMPARTE ENTRE ORGANIZACIONES	N/A	N/A
ISO/IEC 27011	15 DE DICIEMBRE DE 2008	GUÍA PARA LA IMPLEMENTACIÓN DE ISO 27001 EN EMPRESAS DE TELECOMUNICACIONES	NO	1 EDICIÓN
ISO/IEC 27013	SIN FECHA DE PUBLICACIÓN	GUÍA PARA LA IMPLEMENTACIÓN DE ISO27001 E ISO20000	NO	N/A
ISO/IEC 27014	SIN FECHA DE PUBLICACIÓN	GUÍA DE GOBIERNO CORPORATIVO DE LA SEGURIDAD DE LA INFORMACIÓN	NO	N/A

ISO/IEC 27015	SIN FECHA DE PUBLICACIÓN	GUÍA DE SGSI PARA EMPRESAS DEL SECTOR FINANCIERO Y DE SEGUROS	NO	N/A
ISO/IEC 27016		GUÍA DE VALORACIÓN DE LOS ASPECTOS FINANCIEROS DE SEGURIDAD	NO	N/A
ISO/IEC 27017	SIN FECHA DE PUBLICACIÓN	GUÍA PARA LA SEGURIDAD EN CLOUD COMPUTING	NO	N/A
ISO/IEC 27031	1 DE MARZO DE 2011	GUÍA DE APOYO PARA LA ADECUACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TIC) DE UNA ORGANIZACIÓN PARA LA CONTINUIDAD DEL NEGOCIO.	NO	1 EDICIÓN
ISO/IEC 27032	SIN FECHA DE PUBLICACIÓN	GUÍA DE CIBERSEGURIDAD	NO	N/A
ISO/IEC 27033	SIN FECHA DE PUBLICACIÓN	NORMA DE SEGURIDAD EN REDES LA CUAL ESTÁ COMPUESTA DE 7 PARTES **ISO/IEC 27033-1** GUÍA DE CONCEPTOS **ISO/IEC 2033-2** DIRECTRICES DE DISEÑO E IMPLEMENTACIÓN DE SEGURIDAD EN REDES **ISO/IEC 27033-3** ESCENARIOS DE REFERENCIA **ISO/IEC 27034-4** ASEGURAMIENTO DE LAS COMUNICACIONES ENTRE	SI	N/A

		REDES A TRAVÉS DE GATEWAYS **ISO/IEC 27033-5** ASEGURAMIENTO DE LAS COMUNICACIONES A TRAVÉS DE VPNS **ISO/IEC 27033-6** CONVERGENCIA IP **ISO/IEC 27033-7** REDES INALÁMBRICAS		
ISO/IEC 27034	SIN FECHA DE PUBLICACIÓN	SEGURIDAD EN APLICACIONES INFORMÁTICAS COMPUESTA DE 5 PARTES **ISO/IEC 27034-1** CONCEPTOS GENERALES **ISO/IEC 27043-2** MARCO NORMATIVO PARA LA ORGANIZACIÓN **ISO/IEC 27034-3** PROCESO DE GESTIÓN DE SEGURIDAD EN APLICACIONES **ISO/IEC 27034-4** VALIDACIÓN DE LA SEGURIDAD EN APLICACIONES **ISO/IEC 27034-5** ESTRUCTURAS DE DATOS Y PROTOCOLOS DE SEGURIDAD EN APLICACIONES	SI	N/A
ISO/IEC 27035	17 DE AGOSTO DE 2011	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	NO	N/A

ISO/IEC 27036	SIN FECHA DE PUBLICACION	ESTÁNDAR DE SEGURIDAD EN RELACIÓN CON LOS PROVEEDORES COMPUESTA DE 4 PARTES **ISO/IEC 27036-1** VISIÓN GENERAL Y CONCEPTOS **ISO/IEC 27036-2** REQUISITOS COMUNES **ISO/IEC27036-3** SEGURIDAD EN LA CADENA DE SUMINISTRO **ISO/IEC27036-4** SEGURIDAD EN OUTSOURCING	N/A	N/A
ISO/IEC 27037	SIN FECHA DE PUBLICACIÓN	IDENTIFICACIÓN, RECOLECCIÓN Y CUSTODIA DE EVIDENCIAS DIGITALES	N/A	N/A
ISO/IEC 27038	SIN FECHA DE PUBLICACIÓN	GUÍA PARA LA REDACCIÓN DIGITAL	N/A	N/A
ISO/IEC 27039	SIN FECHA DE PUBLICACIÓN	GUÍA PARA LA SELECCIÓN, DESPLIEGUE Y OPERATIVA DE SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIÓN (IDS/IPS).	N/A	N/A
ISO/IEC 27040	SIN FECHA DE PUBLICACIÓN	GUÍA PARA LA SEGURIDAD EN MEDIOS DE ALMACENAMIENTO.	N/A	N/A
ISO/IEC 27799	12 DE JUNIO DE 2008	PROPORCIONA DIRECTRICES PARA APOYAR LA INTERPRETACIÓN Y APLICACIÓN EN EL SECTOR SANITARIO DE ISO/IEC 27002, EN CUANTO A LA SEGURIDAD DE LA INFORMACIÓN SOBRE LOS DATOS DE SALUD DE LOS PACIENTES	N/A	N/A

Tabla 2 Normas ISO 27000 - Fuente ISO 27000 - Fuente Elaboración Propia

12.2.2. ISO/IEC 27001

Este estándar de calidad fue aprobado y publicado en el año 2005 y la versión actual de ISO/IEC 17799:2002, es considerado que a corto plazo será uno de los requisitos obligatorios que las empresas grandes, mediana o pequeñas deben cumplir para poder competir en los diversos mercados, para la aplicación del primero se debe seguir cada uno de los pasos y tener conocimientos en el estándar anterior de esta amanera se puede decir que la implementación será considerada un éxito dentro de cualquier organización.

ISO/IEC27001:2005 tiene por objetivo ayudar a las organizaciones gestionar y proteger sus activos de información, esta es la única norma de seguridad que hasta el momento es auditable y fue concebida para garantizar que las organizaciones logren seleccionar los controles de seguridad más adecuados y proporcionales para la misma este estándar adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

El enfoque que propone la norma no es tecnológico si no por el contrario es un enfoque organizativo del denominado ISMS por sus siglas en Ingles (Information Security Management Systems) o (Sistema de Gestión de la seguridad de la Información) en español el cual es considerado como un factor de implementación de tipo estratégico y para cada organización es diferente de acuerdo a las necesidades, tamaño y el modelo estructural de la misma.

Los tres aspectos fundamentales que conforman esta norma podríamos indicarlos como ISMS, valoración de los riesgos y los controles que deben ser incorporados en la organización.

Esta norma además establece los parámetros para que las organizaciones puedan generen planes de continuidad, para el caso Colombiano este estándar permite

que las organizaciones cumplan con la reglamentación de protección de datos 1998.

ISO/IEC 27001 adopta un modelo de proceso PDCA por sus siglas Planear, Hacer, chequear y Actuar, este estándar busca tomar todos los requerimientos y las expectativas que tiene una organización y plantearlos a través de procedimientos, manuales y buenas prácticas que generan los resultados esperados minimizando los riesgos en la organización.

Este estándar de calidad se fue creado para alinearse con ISO 9001:2008 e ISO 14001:2004, buscando que la organización logre una integración consistente y funcional.

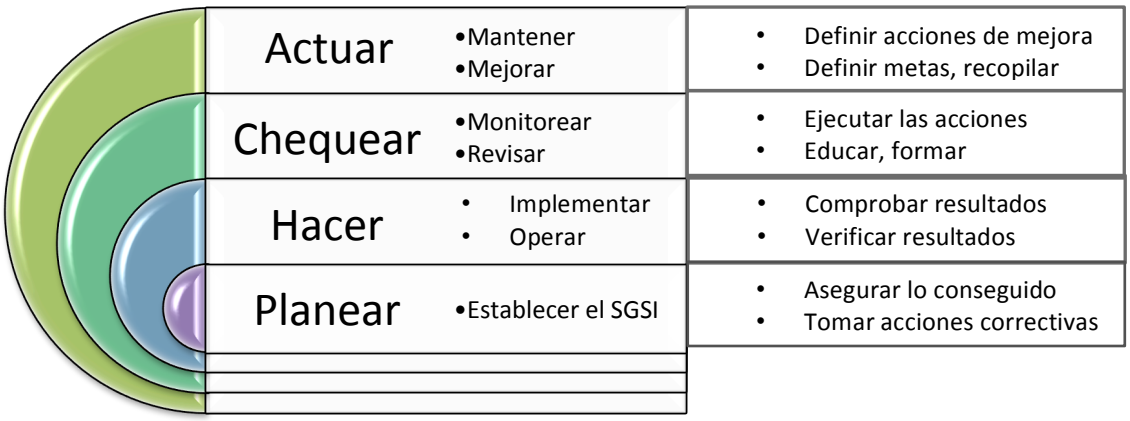


Ilustración 14: Lineamientos de la OECD para redes y sistemas de seguridad de la Información Fuente: ISO2007:2005

Los estándares establecidos en ISO/IEC 27001 se consideran de tipo genérico por lo cual son aplicables a cualquier organización pero vale la pena resaltar que para que una organización logre su certificado de conformidad en ningún caso podrá excluir los apartados de la norma 4 generación de un Sistema de Gestión de la seguridad de la Información , 5 Responsabilidad de la Administración, 6 Auditoria interna del Sistema de Gestión de la seguridad de la Información , 7

Administración de las revisiones del Sistema de Gestión de la seguridad de la Información y 8 Mejora del Sistema de Gestión de la seguridad de la Información, las clausulas anteriores pueden ser tomadas como parte del cuerpo principal de la norma.

Como en la implementación de cualquier estándar de calidad cualquier control que este especificado como necesario en caso de no ser implementado debe quedar debidamente justificada la razón y dejar claramente evidenciados las razones por las cuales la organización decide asumir los riesgos de la no implementación de he dicho control, además de esto la organización debe evidenciar que esto no afecta la responsabilidad del ente de proveedor de seguridad y no violen los factores legales vigentes.

Todos los documentos que sean generados en el proceso de implementación de la norma deben ser custodiados y protegidos los parámetros de esta protección son los mismos que exigen los demás estándares como ISO/IEC 9001:2008.

Otro de los factores prioritarios en esta norma es el compromiso que debe demostrar la organización y en esto veremos claro el concepto de política de establecida para el Sistema de Gestión de la seguridad de la Información, generar un análisis de riesgos donde quede claro al finalizar que riesgos serán asumidos, cuales mitigados y cuales tercerizados , tener un plan de auditorías establecido, además de esto otro aspecto fundamental es que la organización debe asegurar que el personal que sea seleccionado para el control del Sistema de Gestión de la seguridad de la Información tenga las competencias requeridas y la experiencia para que pueda ejecutar los procedimientos establecidos.

De igual manera ISO/IEC 27001:2005 exige que la organización tenga muy bien definido todo lo referente a la gestión de Riesgos como análisis, metodologías, alcances, evaluación, controles

12.2.3. COBIT 4.1

Cobit fue desarrollado para servir de guía a las organizaciones para poder establecer sistema de control interno junto a un marco de trabajo seguro, esta metodología busca que las metas de la organización se alineen con las metas de TI.

La metodología COBIT contiene mecanismos de control de Información y tecnología las cuales le brindan a las organizaciones un marco de trabajo por dominios o procesos los cuales son implementados a través de estructuras lógicas y manejables.

Esta metodología establece conexiones entre los modelos propuestos y los requerimientos de la organización, ayuda con la identificación de los recursos de TI necesarios que están al alcance de la organización, todo esto tiene como objetivo fundamental lograr la alineación de los objetivos estratégicos de la organización con los objetivos de TI

Ilustración 15: Áreas de Enfoque del Gobierno TI – Fuente Cobit 4.1

En el grafico anterior podemos ver los principales tópicos, en los cuales la dirección de la organización debe centrar su atención. Este moldeo se determinó después de realizar una comparación entre los esquemas propuestos por Cobit y los procesos de las organizaciones basados en los estudios realizados sobre cuáles son las áreas en la cuales los gerentes requieren central su atención por el flujo de información que se tiene y con esto lograr las metas propuestas.

Para lograr esto las organizaciones deben concientizarse de los riesgos a los cuales están sujetos y para ello, requieren implementar estrategias coherentes con su realidad y a la vez realizar inversiones objetivas con vista a futuro.

La metodología COBIT dirige la inversión en Recursos de TI los cuales son empleados en TI con el objetivo de brindar información confiable, eficiente y

precisa a la organización la cual debe dar respuesta a los requerimientos de la misma.

El modelo Cobit proporciona un modelo de procesos de referencia y un lenguaje común para todos en la organización, para eso se genera una clasificación para los riesgos y las actividades que requieren ser catalogadas y las organiza dentro de 8 dominios de responsabilidad, de plan, de construcción, ejecución y monitoreo.

Estos dominios son:

Planear y Organizar (PO): Este dominio cubre las estrategias y tácticas y busca establecer las necesidades que las TI deben satisfacer en la organización, establece estructura organizacional y tecnológica real y aplicable.

Las actividades de este proceso son:

- PO1: Definir un plan estratégico de TI
- PO2: Definir la Arquitectura de la información
- PO3: Determinar la dirección de tecnológica
- PO4: Definir los procesos, organización y relación de TI
- PO5: Administrar la inversión en TI
- PO6: Comunicar las aspiraciones y la dirección de la Gerencia
- PO7: Administrar recursos humanos de TI
- PO8: Administrar la calidad
- PO9: Evaluar y administrar los riesgos de TI
- PO10 Administrar proyectos

Adquirir e Implementar (AI): Para llevar a cabo las estrategias y tácticas propuestas en el dominio anterior se deben adquirir y/o desarrollar soluciones tecnológicas e implementarlas a nivel interno y externo según requerimientos,

pero buscando que las inversiones en TI estén alineadas con las estrategias de la organización.

Las actividades de este dominio son:

- AI 1: Identificar soluciones automatizadas
- AI 2: Adquirir y mantener software aplicativo
- AI 3: Adquirir y mantener infraestructura tecnológica
- AI 4: Facilitar la operación y el uso
- AI 5: Adquirir recursos de TI
- AI 6: Administrar cambios
- AI 7: Instalar, acreditar las soluciones y cambios.

Entregar y dar Soporte (DS): Este dominio cubre todo el proceso de entrega de las soluciones planteadas a la organización así como la capacitación, soporte y generación de planes de continuidad y seguridad.

Las actividades de este dominio son:

- DS 1: Definir y administrar los niveles de servicio
- DS 2: Administrar los servicios a terceros
- DS 3: Administrar el desempeño y la capacidad
- DS 4: Garantizar la continuidad del servicio
- DS 5: Garantizar la seguridad de los sistemas
- DS 6: Identificar y asignar costos
- DS 7: Educar y entrenar a los usuarios
- DS 8: Administrar la mesa de ayuda y los incidentes
- DS 9: Administrar la configuración
- DS 10: Administrar los problemas
- DS 11: Administrar los datos
- DS 12: Administrar el ambiente Físico

- DS 13: Administrar las operaciones

Monitorear y evaluar (ME): Todas las soluciones de TI deben ser evaluadas periódicamente para identificar su nivel de eficiencia, el cumplimiento de metas y expectativas frente a las propuestas al comienzo.

Las actividades de este dominio son:

- ME 1: Monitorear y Evaluar el desempeño de TI
- ME 2: Monitorear y Evaluar el desempeño de Control interno
- ME 3: Garantizar el cumplimiento Regulatorio
- ME 4: Proporcionar gobierno de IT

Ilustración 16: Dominios Cobit - Fuente Cobit 4.1

13. MARCO METODOLOGICO

Antes de iniciar con la propuesta de un plan de continuidad disponibilidad y recuperación de desastres, es necesario conocer, por lo menos a nivel general, como está compuesta la Gerencia de Innovación y Desarrollo de Tic.

Esto permitirá entender un poco la dinámica de sus procesos, así como lograr identificar los grupos encargados y los procedimientos para realizar ciertas actividades.

Para lo anterior y con total discreción de la información, se hará uso documentación ISO facilitada por La Gerencia de Innovación y Desarrollo de TIC.

Así mismo y cómo se trató anteriormente en el apartado de Seguridad Informática (Marco Metodológico), llevaremos a cabo un análisis desde un posicionamiento interno y algunos casos externo, con lo cual podremos identificar ya en primera instancia, ciertos aspectos necesarios para el desarrollo de este documento.

13.1. Análisis A Nivel Estructural de la Gerencia de Innovación y Desarrollo TIC

Análisis Estructural Universidad EAN

La universidad EAN es una institución educativa creada en el año 1967 inicio como una institución universitaria con el nombre de Escuela de Administración de Negocios gracias al compromiso demostrado con la formación de profesionales de alta calidad y ser una de las pioneras en la formación en emprendimiento en el año 2006 se le da el reconocimiento como Universidad EAN.

Misión

"Contribuir a la formación integral de la persona y estimular su aptitud emprendedora, de tal forma que su acción coadyuve al desarrollo económico y social de los pueblos".

Visión

"Ser líder en la formación de profesionales, reconocidos por su espíritu empresarial"

Principios

- La acción académica de la Institución está encaminada a la formación de profesionales Líderes Integradores, honestos, eficientes, probos, creativos, emprendedores y multiculturales en función de un espíritu de servicio a la sociedad.
- La Institución considera como su principal activo a sus grupos humanos: profesores, alumnos, ex alumnos y cuadros administrativos. Por consiguiente, propiciará un ambiente adecuado para su desarrollo personal, para el estudio y para el mantenimiento de un espíritu de convivencia y de fraternidad.
- En la formación de los estudiantes, la EAN hace énfasis en el desarrollo de líderes que contribuyan activamente en la solución de las necesidades sociales, buscando con ello la plena vigencia de los derechos del hombre.
- La Institución actúa dentro de los principios y las normas que rigen la Educación Superior y de los que están consagrados en la Constitución y en las Leyes de Colombia.
- La actividad de la Institución está orientada hacia el fortalecimiento de los valores cívicos y hacia el desarrollo de una actitud de superación cultural y científica, *enm*arcada dentro del propósito permanente de respeto a los valores humanos.

Actualmente la Estructura Orgánica de la universidad EAN, se encuentra compuesta diversas unidades de trabajo y cada una de ellas cuenta con un objetivo y alcance para contribuir con el cumplimiento de los postulados anteriormente mencionados, estos objetivos y alcances son:

1. ***Consejo Superior:*** Es el máximo órgano de gobierno de la Universidad y es el encargado de estipular las políticas que indican los caminos que la institución debe seguir.

2. ***Rectoría:*** En esta unidad de trabajo se encuentra el Rector quien es el representante legal de la Universidad y es el responsable de dirigir, liderar y coordinar la gestión académica, administrativa y financiera de la misma.
3. ***Vicerrectoría de Planeación:*** Es el organismo encargado de la integración de la información del entorno de cada proceso con el objetivo de proponer planes de mejoramiento, proyectos que estén alineadas con la misión y objetivos estratégicos de la Universidad.
4. ***Vicerrectoría de Investigaciones:*** Asimila, recolecta, genera y divulga el conocimiento que se requiere para cumplir con los objetivos organizacionales de igual manera con el conocimiento recolectado asesora al sector empresarial.
5. ***Vicerrectoría de Formación:*** Genera los planes académicos que le aseguren a la Universidad que sus egresados serán competentes y emprendedores para esto es el responsable de la evaluación y certifi8cacion de las competencias de sus emprendedores.
6. ***Gerencia de Desarrollo Humano:*** Encargada de la vinculación, capacitación y evaluación de cada uno de los colaboradores de la Universidad, encargada de generar una cultura de alta calidad entre cada uno de los miembros de la comunidad administrativa de la misma.
7. ***Dirección de Medio Universitario:*** Encargada de desarrollar, liderar programas y actividades diseñadas para generar un ambiente que permita el desarrollo integral de cada uno de los miembros de la Comunidad estudiantil y administrativa.
8. ***Vicerrectoría de Extensión y Proyección social:*** Gestiona el desarrollo de programas de educación no formal, consultoría, , responsabilidad social, formación empresarial entre otros dirigidos a cada uno de los diferentes grupos de interés que posee la universidad y con esto se busca fortalecer el lazo Universidad - Empresa - Gobierno
9. ***Dirección de gestión del conocimiento:*** Unidad encargada del diseño y desarrollo de herramientas interactivas que apoyen las actividades académicas y administrativas de la Universidad, brinda soporte en cada una de las etapas de la generación de conocimiento desde su creación hasta su utilización.
10. ***Gerencia de Mercadeo y servicios al estudiante:*** Desarrolla actividades de promoción, publicidad, venta y posicionamiento de la Universidad.

11. ***Vicerrectoría Financiera y de logística:*** Gestiona y controla el manejo de los recursos físicos y financieros de la organización además brinda apoyo logístico en el desarrollo de las diversas actividades que son propuestas al interior de la organización.
12. ***Gerencia de Innovación y desarrollo de Tecnologías de Información y Comunicación:*** Proceso encargado de la generación y desarrollo de soluciones innovadores en Tecnologías de Información y la comunicación para brindar apoyo a las labores y actividades propuestas por los diferentes procesos.
13. ***Dirección de la internacionalización y las relaciones Institucionales:*** Brinda apoyo en la generación de acuerdos de colaboración, convenios, afiliaciones, y alianzas brinda todo el apoyo requerido para gestionar diversos procesos de internacionalización de los miembros de la Universidad, coordina el manejo de las relaciones públicas de la Universidad además de gestionar la búsqueda de recursos de carácter no reembolsable para la gestión de proyectos en la Universidad.

Esta organización horizontal le permite a la universidad EAN obtener una mayor escalabilidad, al implementar cada uno de sus procesos vitales en ciclo corto y con un alto valor agregado, además de generar una cadena de trabajo colaborativo donde ningún proceso es independiente y siempre depende de los demás para lograr un objetivo común permitiendo la apropiación de conocimiento en grupos autónomos.

Dentro de la esta estructura, podemos encontrar La Gerencia de Innovación y Desarrollo de Tecnologías de Información y comunicación (TIC), al observar la imagen de la cadena de valor podemos observar que está clasificado como un proceso de apoyo.

A continuación, podemos observar el mapa de procesos de la Universidad EAN

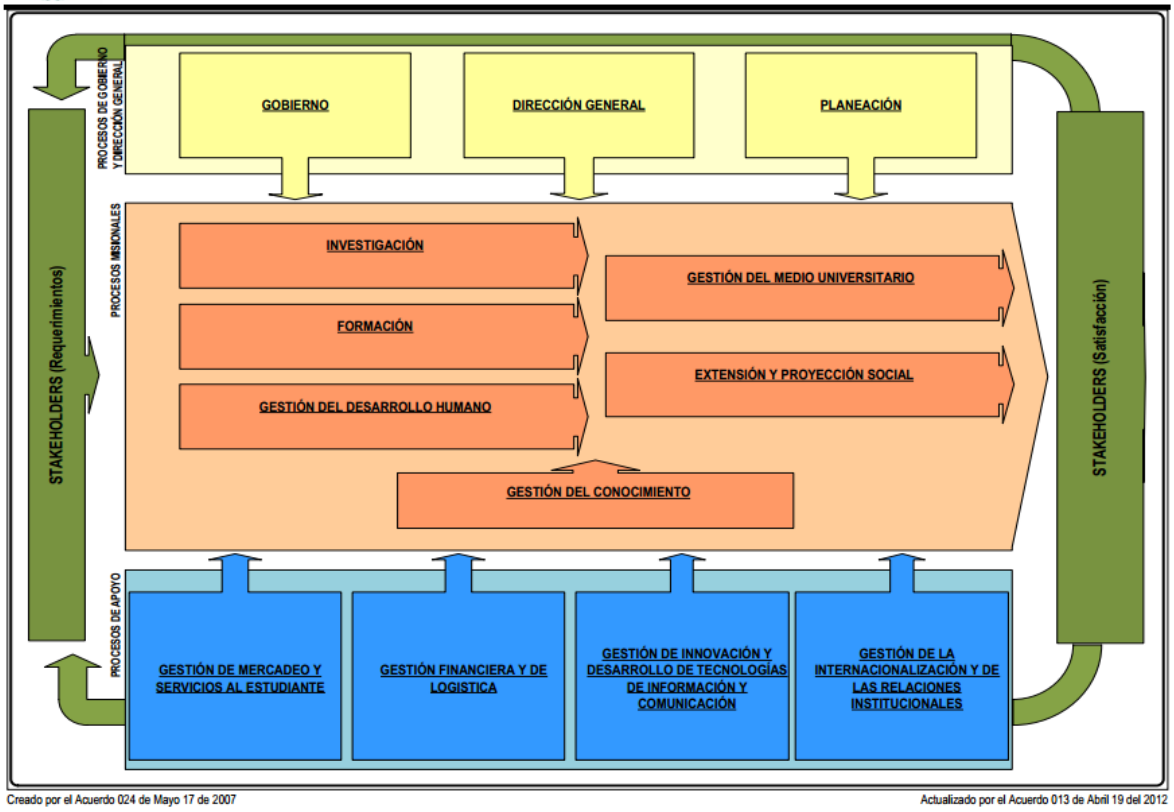


Ilustración 17 Mapa de procesos Universidad EAN – Cortesía universidad EAN

Gerencia de Innovación y desarrollo de Tecnologías de Información y Comunicación

Como lo indicamos anteriormente la Gerencia de Innovación y desarrollo de TIC tiene como objetivo brindar las soluciones tecnologías más innovadores que le permitan a los demás procesos el correcto desarrollo de cada una de sus actividades.

La misión de la Gerencia de Innovación y desarrollo de TIC es:

Incorpora, mantiene y suministra la infraestructura tecnológica y la gestión de la información, necesaria para prestar los servicios informáticos de comunicación y de acceso a la información referencial que requiere la Universidad EAN, para el cumplimiento de su misión en la formación integral, el estímulo de la aptitud emprendedora y el desarrollo económico y social de los pueblos.

Cada uno de los proyectos y actividades que son desarrolladas por el equipo que conforma este proceso siempre están alineadas con el plan de acción y cada uno de los objetivos planteados por el PEI de la Universidad

Entre los principales principios de trabajo que posee este proceso podemos resaltar los siguientes:

•Cultura del servicio con oportunidad, calidad y eficacia.

•Responsabilidad.

•Sinergia en sus acciones.

•Trabajo por procesos.

•Innovación y cambio permanente.

•Confiabilidad y estabilidad de los sistemas y tecnologías.

•La seguridad en la información como elemento indisoluble en los procesos informáticos.

•La incorporación de tecnología de punta como parte fundamental de los resultados.

•El posicionamiento del proceso de Tecnología de información y comunicación en la Universidad EAN.

•La permanente utilización de técnicas de relación costo – beneficio en el análisis e proyecto tecnológicos.

•La actualización y capacitación permanentes del grupo colaborador.

El proceso de la gerencia de Innovación y desarrollo de TIC, se encuentra conformado por unos subprocesos los cuales son:

- Gestión Proyectos de Tecnologías y Comunicación.
- Gestión de la Infraestructura de Tecnología de Comunicaciones.
- Seguridad Computacional.
- Gestión de Servicios de Información.

El primero de los subproceso se enfoca en facilitar soluciones haciendo uso de la infraestructura tecnológica, disponible.

En el segundo, su objetivo es atender las solicitudes referentes a la adquisición de nuevas tecnologías, soporte a nivel preventivo y correctivo con el propósito de asegurar una mejor disponibilidad en cuanto a esta infraestructura.

El tercer tiene como propósito, según texto de la caracterización de este proceso, preservar, respaldar y/o restaurar la información de los procesos de la universidad EAN[8].

Por último, el cuarto subproceso, se enfoca en garantizar la disponibilidad a nivel de software y hardware, así como facilitar servicios de información enfocados a procesos de enseñanza e investigación.

Cada uno de estos subprocesos está compuesto por un equipo de trabajo, el cual se encarga de actividades específicas, con el propósito de lograr un adecuado desarrollo y desempeño de cada una de las funciones asignadas.

En conclusión, con la implementación de estos subprocesos, La Gerencia de Innovación y Desarrollo de TIC busca, gestionar soluciones utilizando como apoyo las IT, buscando mantener un 100% de disponibilidad de las mismas para evitar cortes en los flujos de trabajo, para esto y contando con la ayuda del sistema de Gestión de calidad que actualmente maneja la Universidad bajo la Norma ISO9001:2008 la solución y atención a fallos se da por medio de acciones correctivas y/o preventivas, asegurando que la información procesada pueda ser respaldada, suministrando servicios de información adecuados a los diferentes procesos y/o stakeholders, al ofrecer un servicio con calidad y mejoramiento continuo.

Actualmente la Universidad EAN gracias a la gestión de cada uno de los miembros de los equipos multidisciplinarios cuenta con herramientas robustas a nivel tecnológico para el desarrollo de tareas específicas ya sean del día a día como la gestión de sistemas de información o tareas cíclicas como lo son los procedimientos de mantenimiento preventivo.

Un claro ejemplo de esto lo podemos observar en el subproceso de Seguridad Computacional, podemos ver que ya se cuenta con algunas acciones que permiten salvaguardar la información y restaurarla posteriormente.

[8] Caracterización de Procesos – Seguridad Computacional – Generación y Restauración de Copias de Respaldo. Universidad EAN

Pero a pesar de la excelente gestión que se evidencia vale la pena resaltar algunos interrogantes que requieren de un constante análisis por parte de los responsables de actividades tan precarias como lo es el Backup frente a temas como:

- ¿A qué sistemas de información se les realiza el proceso de backup?
- ¿Cuál es la periodicidad con la cual se realizan las copias de seguridad?
- ¿Cuál es la fiabilidad de estas copias de seguridad?
- ¿Se tiene algún registro de los casos en los que se ha requerido emplear las copias y de su fidelidad?
- ¿Cuáles con las falencias que posee el proceso actualmente y que se está haciendo para solucionarlas?

En cuanto a nuestro centro de interés para el desarrollo de este trabajo podemos cuestionar a los responsables

- ¿Si el ERP Seven se encuentra dentro de estos sistemas de información sujetos a Backup?
- ¿Dónde es salvaguardada esta información?
- ¿Hasta qué nivel llega el proceso de copias de respaldo de esta información?
- ¿La restauración de esta información permitiría reconstruir nuevamente el escenario que se encontraba antes de presentarse algún tipo de desastre?
- ¿Cuál es la periodicidad de la copia de respaldo?

Al verificar en la documentación propia del sistema de calidad podemos encontrar que según lo descrito en la documentación, se realiza respaldo de bases de datos corporativas y de servidores de aplicación, sistema financiero, sistema académico, portal institucional, plataformas de aulas virtuales, sistemas de autenticación, SRM, sistemas de biblioteca y sistemas de correo.

Así mismo una vez se realizan las copias de respaldo, estas son entregadas a una custodia externa.

Por otra parte es importante analizar, que tecnología se utiliza para realizar estas copias de respaldo.

Con todos estos datos, ya contamos con la información para tener una visión más global de la forma como se encuentra estructurada y como opera La Gerencia de Innovación y Desarrollo de TIC. Lo cual es de vital importancia al momento de

realizar un BIA (Business Impact Analysis) y de esta manera poder realizar un análisis más adecuado.

13.2. Procesos y Panes de Contingencia Utilizados Por La Dirección De Innovación Y Desarrollo Tic, Ante Cualquier Ataque O Desastre.

13.3. Digital Ware- Proveedor de ERP- SEVEN

Ilustración 18 DigitalWare

DigitalWare es una empresa colombiana que viene trabajando desde 1992 y que tiene como propósito proporcionar soluciones en el área informática basada en principios de calidad, eficiencia, robustez y alto rendimiento para las organizaciones tanto del Sector público como del Sector privado, a Nivel nacional e internacional por medio de alianzas estratégicas. A lo largo de estos años se ha obtenido la satisfacción de los clientes por medio de la Excelencia en el Servicio.

En el año 2005 DigitalWare fue premiada como la empresa más innovadora de Software en Colombia y en el 2007 fue la ganadora del premio Portafolio a la empresa más innovadora de Colombia en la que se incluyeron empresas de todos los sectores. En la actualidad sus productos son utilizados por más de 500 compañías en el Mundo.

DIGITAL WARE. Se especializa en Asesorías, Consultoría, Interventoría, Outsourcing, así como el Análisis, Diseño e Implementación de Software Aplicativo de acuerdo a las necesidades de las organizaciones del sector gobierno y privado tomando como base los Estándares de Calidad ISO 9001:2000. Son los creadores

de KACTUS-HR, SEVEN-ERP, SEVEN-CRM y HOSVITAL-HS, Soluciones para ambientes Cliente / servidor Multinivel e Intranet interactuando con flujos de trabajo (SEVEN- Work Flow®) totalmente parametrizable conformando la base de soluciones a la medida para la gestión Administrativa, financiera, comercial, Contratos y Licitaciones, Manufactura, Hospitalaria y Administración de Recursos Humanos y de Nómina.

13.3.1. Filosofía de Digital Ware

Con el pasar del tiempo, teniendo en cuenta el tema de la globalización en esta época de rápidos cambios tecnológicos, las organizaciones han ido descubriendo nuevos métodos que conllevan a la ejecución de mejores prácticas de negocio mediante la planeación de recursos y el manejo más eficiente de los mismos. Las exigencias del mercado constituyen la base para la integración total de las organizaciones creando alianzas estratégicas con sus proveedores y clientes, garantizando de esta manera la supervivencia de los mismos en tiempos de cambio.

Pensando en lo anterior **DIGITAL WARE** ha iniciado a proveer a sus clientes una solución tecnológica que permite la ejecución de la filosofía ERP mediante su producto SEVEN- ERP el cual fue creado para la optimización de los procesos de negocio logrando de esta manera mejores productos y servicios para los clientes de la organización.

Ilustración 19 Seven ERP

13.3.2. Seven-ERP (Universidad EAN)

El ERP que se encuentra implementado en la Universidad EAN se llama SEVEN-ERP el cual es el sistema de planificación usado para gerencia eficientemente las necesidades en las áreas administrativas, Financieras y comerciales de la Universidad EAN. SEVEN-ERP es un sistema modular desarrollado con tecnología cliente / Servidor Multinivel, Bases de datos relacionales, intranet, internet y procesamiento distribuido integrando de esta manera herramientas que automatizan procesos, procesa documentos y Administra las relaciones con Clientes.

SEVEN- ERP es una aplicación Diseñada por el Proveedor de Software Digital Ware como una reunión de las mejores prácticas mundiales para empresas que se desempeñan en diferentes sectores económicos. Con SEVEN- ERP la información en tiempo real es una realidad permitiendo esto, la toma de decisiones de una manera más fácil y rápida y la obtención de conocimiento de toda la organización. Es una aplicación multimoneda y multicompañía que se adapta fácilmente a cualquier tipo de negocio ya sea industrial, de servicios, financiero y Educativo como es nuestro Caso en la Universidad.

Algunas consideraciones a tener en cuenta para el funcionamiento del Sistema SEVEN.

- La configuración recomendada para el servidor se estima para operar con 30 usuarios concurrentes.
- No se puede saber de antemano cómo será el crecimiento de servidores y canales de comunicación ya que no se conoce el volumen de transacciones, el número de usuarios del Sistema y los tiempos de respuestas requeridos por el cliente. El grupo de Tecnología de la Información y la Comunicación de la Empresa deberá hacer las respectivas mediciones del caso para determinar este crecimiento.
- El sistema SEVEN puede operar instalando el Servidor de aplicaciones y el Servido de base de datos en un mismo computador si el motor de base de Datos soporta la plataforma de Windows 2000 o 2003 Server.
- El sistema SEVEN permite, si el cliente lo considera conveniente, distribuir los componentes del Sistema en diferentes Servidores (Uno o más servidores de aplicaciones, Servidor de bases de datos, Servidor Web y Servidor de Reportes).

13.3.3. Requerimientos de Funcionamiento Generales

- **Cliente**: Procesador Pentium o Superior. Sistemas operativos Windows XP o Superior.
- **Servidores:** Procesadores Intel / RISC/ Alpha. Sistemas Operativos: Windows, Linux, Unix, Solaris, Hpux, IX.
- **Bases de Datos:** SQL Server, Oracle, Sybase, Informix- DB2.
- **Opera en Redes:** LAN, WAN, Intranets y Extranets.
- **Modo de operar:** El 100% de sus transacciones e informes se encuentran habilitadas para trabajar en internet, permitiendo proveer servicios informáticos vía internet (ASP).

13.3.4. A nivel de Software

- **Equipo servidor de aplicaciones:** Sistema Operativo Windows 2003 Server, IIS- Internet Information Server, Crystal Reports Versión 8, Servicios FTP.
- **Equipo Servidor de Datos:** Sistema operativo Windows 2003 Server, Sistema operativo Windows 200 Server, Unix, Solaris, Linux. Motor de Base de Datos (Oracle versión 9i /Oracle versión 10G/ SQL Server 2000/ SQL Server 2005 / Sybase 11.9.2, Informix).
- **Equipo Cliente: Sistema** operativo Windows NT Work Station / Windows 2000 Professional / Windows XP Professional / Windows Vista Business, Internet Explorer 5.0, Internet Explorer 7.0.

13.3.5. A nivel de Hardware

- **Equipo servidor de Aplicaciones:** 2 Procesadores Intel Dual Core 3.0 Ghz, Memoria RAM de 8 GB, Espacio libre en Disco Duro de 80 GB, Tarjeta de Red 10/100 Mbps.
- **Equipo Servidor de Datos:** 2 Procesadores Intel Dual Core 3.0 Ghz, Memoria RAM de 8 GB, Espacio Libre en Disco Duro de 80 GB, Tarjeta de Red 10/100 Mbps.
- **Equipos Cliente:** Procesador de 1.2 Ghz, Espacio Libre en Disco Duro de 15 GB, Memoria RAM de 256 MB, Monitor color SVGA con resolución 800*600, Tarjeta de Red 10/100 Mbps.
- **Canales de Comunicación:** Red LAN: 10/100 Mbps, Red WAN: 250 Kbps, El espacio en Disco Duro, Procesadores y Memoria RAM depende del volumen de la información manejada por el cliente.

13.3.6. Beneficios de la Utilización del Sistema SEVEN- ERP

- Optimización de los procesos de la organización por medio de la reducción de los tiempos de espera en las transacciones.
- Transmisión de conocimiento e información en toda la organización.
- Integración total de toda la cadena de servicios hasta llegar a los clientes finales.
- Aumento en los ingresos de la compañía.
- Cambio cultural con el objetivo de alcanzar un nivel de competencia en el mercado.
- Manejo de altos volúmenes de procesamiento en tiempos adecuados.
- Reducción de costos y gastos en la organización.
- Reubicación y Capacitación del personal.
- Soluciones estandarizadas para la industria.
- Satisfacción del cliente interno y externo.

13.3.7. Módulos de SEVEN- ERP Usados en la Universidad EAN

En la universidad EAN tenemos implementados la mayoría de los módulos que ofrece el ERP SEVEN y los que se consideran más importantes en una organización de carácter educativo como esta.

Trabajamos con varios grupos de módulos principales que son la Parte Administrativa, Financiera, Comercial, General e Imágenes distribuidos por diferentes módulos de esta manera:

- **Administrativa :**
  - Inventarios
  - Activos Fijos

- Compras
- Contratos
- Work Flow

- **Financiera:**
  - Contabilidad
  - Proveedores
  - Tesorería
  - Presupuesto financiero

- **Comercial**
  - Facturación
  - Cartera
  - Cartera Financiera

- **General**
  - Seguridad y control de Acceso
  - Parámetros Generales
  - Utilitarios

- **Imágenes**

A continuación una breve descripción del funcionamiento de cada uno de estos módulos implementados en la Universidad EAN.

13.3.8. SEVEN E- Administrativa

Optimiza los procesos de negocios logrando de esta manera convertir lo que antes era logística integrada de la empresa ahora sea una reducción de costos y mejores productos y servicios para los clientes.

13.3.9. Módulo de Inventarios

Este módulo sirve para la toma de decisiones de la alta gerencia de la organización que están relacionadas con el manejo de los productos de consumo, devolutivos y comerciales de la Universidad, además permite llevas un control detallado de las cantidades y los costos de los productos diversos manejados en la empresa. Provee herramientas para el manejo y control de los inventarios por medio de un kardex donde se muestra la información actualizada al minuto y con la opción de filtrarla en periodos de tiempo.
El módulo de inventario permite realizar la separación de movimientos en los distintos centros de utilidad definidos en el sistema. Los costos y transacciones pueden llevarse a cabo en moneda local y en moneda alterna.

El sistema SEVEN permite también la parametrización en línea de las transacciones del módulo de inventario a la contabilidad de forma automática.

13.3.9.1. Módulo de Activos Fijos

Este módulo proporciona las herramientas apropiadas para la adecuada administración de los activos fijos de la Universidad EAN.
Permite el manejo de los activos de la empresa, llevando un registro histórico de los diferentes movimientos que pueden afectar al activo, la depreciación acumulada, los ajustes debido a la inflación y los movimientos que no afecten la parte contable y que permitan así, un control administrativo de los activos.

Este módulo funciona en línea, realizando la contabilización de manera directa de los movimientos realizados en el Sistema o como complemento a otros sistemas que se encarguen de realizar la contabilización desde el inicio de la transacción y solo requieran realizar el movimiento operativo sobre el activo. Conserva toda la parametrización definida para el producto devolutivo que se encuentra definida en el módulo de inventarios. Asocia cada uno de los activos a diferentes grupos de activos fijos que están definidos de acuerdo a la necesidad de la organización.

13.3.9.2. Módulos de Compras

Este módulo sirve como apoyo a la alta gerencia en el seguimiento y control de los diferentes procesos de compras dentro de la Universidad como las solicitudes internas y requerimientos de compras, las cotizaciones a los proveedores, registro de los mismos, generación de órdenes de compras, diferentes despachos de una orden y la recepción de la mercancía.

Esta aplicación está totalmente integrada con los módulos de presupuesto, tesorería, inventarios y activos fijos permitiendo al usuario hacer entradas al inventario por compras que se realizan.

Las solicitudes de compras se pueden definir por medio de cualquiera de las terminales de la aplicación y estas pueden ser realizadas por cualquier usuario del sistema que tenga permisos, lo que permite que cada usuario realice sus requerimientos de suministros. En el caso de la Universidad EAN las Asistentes son las encargadas de realizar estas solicitudes de compras en la aplicación SEVEN referentes a su proceso. Por medio de un módulo de Seguridad se garantiza que los usuarios de acuerdo a sus perfiles puedan consultar, aprobar y diligenciar las solicitudes realizadas.

El módulo de compras también permite el registro de proveedores de la Universidad por medio de un detalle de todas sus características y definiendo los

artículos que el proveedor suministra a la empresa. Pueden guardarse las ofertas realizadas por un proveedor con el objetivo de generar cotizaciones de manera automática en el momento en que se considere necesario. La recepción de los suministros se realiza en una bodega definida para entrada de proveedores. La orden de compra es contabilizada en base al documento relacionado en la recepción de los suministros (factura, orden de entrega, factura etc.) y una vez que el proveedor entrega la correspondiente factura el siguiente paso es originar la cuenta por pagar en el módulo de cuentas por pagar con el fin de realizar el pago desde el módulo de tesorería.

13.3.9.3. Módulos de contratos

Este módulo permite la administración y control de los procesos de contratación que se llevan a cabo en la Universidad como licitaciones, invitaciones directas y otras. Permite la selección de los proveedores, el manejo de las pólizas y garantías de los mismos, el flujo de pagos, adiciones contractuales, liquidaciones contractuales y actas. El módulo de contratos se integra con el módulo de Work Flow en el manejo de documentos a través del módulo con el mismo nombre.

13.3.9.4. Módulo de Work Flow

Realizar cambios en los procesos del negocio la mayoría de veces genera retrasos y depende en mayor parte de las personas que hacen parte de la organización. En estos cambios existen muchos participantes, procesos, proyectos y operaciones que pueden verse afectados si no existe un orden de trabajo en los procesos de compras, requerimientos, radicaciones, trámites y demás. El módulo de Work Flow permite a los usuarios del Sistema SEVEN la definición de los nuevos procesos de negocio y la modificación de los procesos existentes brindando así a la organización la oportunidad de definir el negocio en

flujos de trabajo que van escalando desde un sistema de radicación, procesos diversos de compras, presupuestos o cualquier tipo de proceso que interactúe con los sistemas administrativos, financieros, de producción y documentales de la organización en un solo sistema. Lo anterior logra un trabajo compartido y cooperativo muy importante en la Organización ya que se manejan los documentos de manera distribuida, correo electrónico, las transacciones y las operaciones facilitando el flujo de la información entre los diferentes grupos que conforman la parte Administrativa de la Universidad y disminuyendo significativamente los costos administrativos.

El sistema de Work Flow se basa en una herramienta de gestión documental que gestiona y almacena todos los documentos que pasan de un lugar a otro de usuario a usuario como imágenes, textos, archivos ofimáticos y más. Las técnicas de Gestión documental permiten a los usuarios clasificar y organizar todos los archivos electrónicos y se pueden usar técnicas de base de datos para la localización de la información que se necesita realizando la búsqueda por fechas, autores de los documentos o contenidos de los mismos.

Para acceder al archivo central de los documentos electrónicos hay un control de acceso garantizado. El usuario debe identificarse con su nombre y una palabra clave y de esta manera tiene derecho a realizar operaciones de acuerdo a los permisos para su perfil controlando de esta manera el acceso a usuarios no autorizados.

SEVEN Work Flow en resumen permite el control de quien maneja la información de la organización, que puede hacer la persona o usuario que tiene este acceso y en qué momento es necesario el acceso a la Información.

13.3.10. SEVEN E- Finanzas

13.3.10.1. Módulo de contabilidad

Este módulo tiene el objetivo de lograr la uniformidad, el procesamiento y la consolidación de la contabilidad General de la Universidad EAN controlando todas y cada una de las operaciones contables que se realizan diariamente recibiendo en línea todas las operaciones que se realizan en una operación contable.

Permite el control administrativo y de la gerencia de la información contable a nivel de centros de costos, unidades de negocio, proyectos y conceptos fiscales facilitando de esta manera la generación de reportes, balances, libros auxiliares y el control de los planes de cuenta en todos los niveles de la organización.

Características Generales

- Maneja el Plan Único de cuentas (PUC) y el Plan General de la Contabilidad Pública (PGCP)
- Manejo de las diferentes compañías asociadas con sus respectivos números de cuenta.
- Se puede definir libremente la jerarquía del plan contable de la organización.
- Se manejan y controlan 3 grupos de plan de cuentas definidas por el centro de costos, unidad de negocios y proyectos permitiendo estas estructuras la generación de balances y estados de resultados para cada uno de ellos.
- Se definen documentos contables controlando un consecutivo para estos de manera manual o automática, la impresión en línea entre otros.
- Permite la Parametrización en forma predeterminada del proceso contable.
- Controla el acceso de usuarios a los comprobantes contables y a la contabilidad de la organización.
- Permite la definición, formulación y generación de los índices financieros.
- Definición de parámetros para los informes en medios magnéticos que deben ser entregados a entes externos.
- Definición de anexos contables para la declaración de renta.

13.3.10.2. Módulo de Proveedores

Este módulo es el encargado de Administrar y Controlar las obligaciones que tiene la Universidad EAN, es decir, las cuentas por pagar.

Características Generales

- Provee auxiliares que contienen la historia del movimiento y los saldos por cada una de las cuentas por pagar que posee la Universidad. Adicionalmente mantiene los registros correspondientes a los pasivos de la empresa, en lo relacionado con proveedores y acreedores varios, por concepto de productos, contratos, servicios y suministros.
- Con este módulo se obtiene un adecuado manejo de pagos bajo un estricto seguimiento de los documentos que componen las obligaciones.
- Suministra información sobre los vencimientos y prioridades de pago dando así la posibilidad de llevar a cabo una óptima planeación de los mismos, con los beneficios financieros que esto representa.
- Efectúa las recepciones de acuerdo con la orden de compra y la factura del proveedor, genera el estado de cuenta, controla las respectivas obligaciones y realiza los pagos con emisión automática de cheques.
- Permite la definición de la Facturación incluyendo dentro de esta las características generales, los productos, las condiciones comerciales e impuestos.
- Recomienda proveedores de un producto y relaciona los productos que ofrece un proveedor.
- Suministra información de Cuentas Por Pagar por edades.
- Permite definir las diferentes listas de precios por producto y proveedor.

- Clasificación de los proveedores por tipo, permitiendo al usuario organizar sus proveedores de la manera más conveniente.
- Definición de las diferentes condiciones de pago pactadas con un proveedor.
- Registro de los proveedores con información básica como identificación, nombre, dirección, teléfono, tipo, clase, y condiciones de pago.
- Permite el control de anticipos y cruce de cuentas.

13.3.10.3. Módulo de Tesorería

El módulo de tesorería tiene como fundamento el control diario de los ingresos y egresos de la Universidad, compromisos adquiridos, presupuesto e inversiones. En este módulo se producen los estados necesarios para el correcto manejo de las operaciones basadas en estrictas normas de auditoría y control.
Administra y hace seguimiento de los ingresos que tiene la organización por medio de la parametrización de los diferentes tipos de ingresos que esta posee con sus correspondientes consignaciones a nivel nacional y local. A nivel de egresos se pueden programar los giros de las diferentes cuentas por pagar de la empresa. Permite la generación de manera automática de las conciliaciones bancarias para cada banco asociado y cada cuenta bancaria de los mismos ofreciendo de esta forma un reflejo en tiempo real del flujo de caja de la Universidad.

Características Generales

- Permite la definición de los diferentes tipos de comprobantes de Ingreso y Egreso, como el Recibo de Caja, las Consignaciones, el Comprobante de Egreso, Notas Débito y Crédito.
- Generación automática de los consecutivos para los comprobantes de ingreso y egreso.

- Libre definición jerárquica de las diferentes cajas, incluidas las cajas menores.
- Aplicación de pagos y actualización de los saldos de cuentas por pagar y por cobrar en línea.
- Calcula sobre el valor de la factura, el valor correspondiente a la Retención en la Fuente, I.V.A, e ICA y registrar los descuentos en el Comprobante de Egreso.
- Interactúa en línea con el Módulo de Presupuesto y actualiza la ejecución de los Ingresos y Gastos.
- Interactúa en línea con el Módulo de Contabilidad y actualiza las cuentas contables y presupuestales.
- Obtiene información rápida y oportuna acerca del estado de los Bancos y disponibilidad de giro.
- Reporte del resumen diario de Caja por los diferentes conceptos por los que hubo movimiento.
- Manejo dinámico de Bancos, Sucursales y Cuentas Bancarias.
- Diseño de plantillas de cheques manejados por los diferentes bancos, directamente por el usuario.
- Conciliaciones bancarias
- Control de Flujos de Caja

13.3.10.4. Módulo de presupuesto Financiero

Encargado de controlar y administrar la ejecución, contabilización y el control de los presupuestos de la organización, presupuesto de reservas y presupuesto disponible para pagar las cuentas pendientes.

Características Generales

- Manejo de presupuesto a nivel de Centros de Costos, Sucursales, Unidades de Negocios y Proyectos.
- Restricción de ejecución presupuestal.
- Codificación de los documentos de ejecución presupuestal, Requisiciones, cuentas por pagar y recibos de caja facturas de clientes.
- Codificación de los documentos soporte a la ejecución presupuestal, como son contratos, órdenes de compra, y ordenes de servicio.
- Manejo de Reservas Presupuestales
- Opción de controlar el presupuesto a nivel de cuenta contable, centro de costos por periodos.

13.3.11. SEVEN E-Comercial

SEVEN Comercial ayuda a los procesos de ventas y de recaudo a definir las reglas de negocio en cuanto a producto, proveedor y cliente por medio de la cadena de abastecimiento. Realiza el manejo de cotizaciones y pedidos controlando los requerimientos, restricciones y necesidades de las solicitudes hechas por los diferentes usuarios y clientes. Para la realización de lo anterior se presenta interacción con los módulos de cartera e inventarios.

Por medio del módulo se pueden realizar facturaciones directas con base en un pedido que afecta directamente el inventario de la organización y la contabilidad de la misma. Permite manejar cupos de crédito, formas de pago y la parametrización de las diversas condiciones comerciales al tiempo que calcula de forma automática todos los impuestos relacionados con los diferentes conceptos facturados.

Características Generales

- Controla los diferentes cupos asignados a los clientes
- Reporte por proveedor, ventas acumuladas por mes, año (movimiento por vendedores), con comparativos de presupuestos.
- Estadística de descuentos por cliente y por producto (consolidado).
- Comprobante contable de ventas del mes.
- Control de ventas cliente trimestral por producto comparado con el año anterior vs. Presupuesto.
- Manejo de la cartera, control de notas débito, créditos a clientes, abonos a facturas de clientes, rotación de cartera, incluyendo adicionalmente estadísticas de ventas o recaudos por clientes.
- Extracto de cuenta y circularización (estado de cuentas), rotación de cartera, auxiliar de cartera, liquidación de intereses por mora, Informe de vencimientos de cartera por vencer o vencida por fechas, Informe para planeación de cobros-Estadísticas de ventas o recaudos por clientes.

13.3.11.1. Módulo de Facturación

El módulo de SEVEN de Facturación y Devolución, tiene como propósito fundamental finalizar el procesamiento de pedidos a través de la facturación, administración de guías y el manejo de la logística de reversa.

Entre sus aspectos más importantes se encuentran: la generación de facturación por pedidos, rutas, clientes, ciudades, la administración de devoluciones de mercancía, la conciliación de guías de transporte, la reimpresión de facturas, la integración con el módulo de estadísticas (Inteligencia de Negocio) y el módulo de contabilidad a nivel de cuenta, centro, área, proyecto.

Como beneficios se establecen: la actualización de fechas de vencimiento de cartera a partir de las fechas reales de entrega, la conciliación de guías de transporte, la actualización de cartera según parámetros, la integración directa con

el módulo de contabilidad, la generación de indicadores de cumplimiento, generación de información confiable para la determinación del comportamiento de las ventas y el mercado y la generación de estrategias comerciales y de mercadeo.

13.3.11.2.Módulo de Cartera

Este módulo tiene fundamentalmente permite controlar notas débito y crédito a clientes, Manejos de cupos y topes de facturación; además que parametriza las condiciones comerciales para cada uno de los clientes, las formas de pago y cupos de crédito, Administra Intereses por mora, define intereses periódicos y maneja acuerdos de pago. Maneja y controla las cuentas por cobrar de los clientes que han contraído obligaciones con la organización, a partir del Módulo de Facturación a clientes.

Características Generales

- El sistema controla notas débito, crédito a clientes.
- Permite abonos a facturas de clientes.
- Manejos de cupos y topes de facturación. Adicionalmente controla las condiciones comerciales parametrizadas para cada uno de los clientes.
- Permite la parametrización de los clientes por medio de las condiciones comerciales, formas de pago y cupos de crédito.

13.3.12. SEVEN E- General

13.3.12.1.Módulo de Seguridad y Control de Acceso

Mediante este módulo el usuario que es el Administrador del sistema se encargará de definir los diferentes permisos a los diferentes perfiles de usuario creados para la organización. Se define aquí lo que puede o no realizar con la información y las transacciones cada uno de las personas que trabajan con el uso del sistema SEVEN. Se pueden también definir los programas y los módulos a usar y su ubicación en el menú.

13.3.12.2. Módulo de parámetros Generales

Aquí se diseñan y se revisan cada uno de los parámetros que son requeridos por la organización para garantizar el buen funcionamiento de todos sus procesos y operaciones en las diferentes áreas de la Universidad con el fin de lograr que los resultados finales sean los esperados con el sistema SEVEN.

13.3.12.3. SEVEN E-Imágenes

Módulo que tiene como objetivo principal la eliminación de las tediosas carpetas y grandes archivos que almacenan los documentos físicos de la organización. La aplicación permite el archivo de estos documentos en forma digital relacionados con el colaborador como su hoja de vida, estudios realizados y todos los certificados laborales relacionados con el mismo además de su contrato firmado de manera digital

Además de permitir el almacenamiento de todos estos documentos digitalizados, también permite la consulta rápida y fácil acceso de estos por medio de la aplicación. El usuario podrá consultar y verificar toda la información relacionada con el colaborador sin la necesidad de transportar la carpeta física permitiendo esto, la consulta de la misma información de varios usuarios al mismo tiempo.

13.4. APLICACIÓN DE BIA (BUSINESS IMPACT ANALYSIS) A LA DIRECCIÓN DE INNOVACIÓN Y DESARROLLO TIC.

Es el primer aspecto a evaluar para poder realizar un adecuado plan de disponibilidad, continuidad y recuperación de desastres, ya que permite identificar cuáles son las funciones vitales del negocio así como sus dependencias (otros procesos, proveedores o servicios IT), los cuales necesitan ser cuidadosamente custodiados y en caso de alguna eventualidad rápidamente recuperados teniendo claros los tiempos y la efectividad de los procesos a ejecutar.

El análisis de impacto de negocio nos ayuda a visualizar que está en riesgo cuando un fallo se presenta, además nos permitirnos medir la inversión que se requiere determinando los costos financieros en temas relacionados con tiempo de respuesta, personal requerido, infraestructura necesaria, entre otros; Por otra parte ayuda a determinar los tiempos máximos de inactividad que pueden tener los procesos más críticos de la organización, sin que estos causen pérdidas financieras, penalizaciones legales o quejas por parte de los clientes.

El desarrollo de este tipo de metodologías a nivel organización tienen una importancia vital puesto que en esta época al interior de muchas organizaciones el tema de seguridad no es tomado con la seriedad que se requiere y no se realizan las inversiones de capital tanto económico como humano que se requiere para evitar la pérdida de información valiosa para la organización y se cae el error de tomar acciones correctivas después de que se presentan los fallos que tienen una repercusión grave para la organización mas no la implementación de soluciones eficaces preventivas que mitiguen la perdida, cuando hablamos de la definición de la importancia que tienen los planes de acción para mitigar el impacto de los riesgos debemos tener claridad de que una vez estén definidos no indica que se eliminen los problemas para la organización y que los riesgos y vulnerabilidades desaparezcan se podría considerar esto como una transformación que en algunos casos lo que hace es convertir esos riesgos y vulnerabilidades en unos más pequeños y más aceptables

Para poder determinar la causa de la materialización de posibles amenazas y la consecuencia que estas puedan producir, es necesario realizar como primer paso un Análisis de Riesgos, el cual aportara valiosa información, que será utilizada posteriormente en el BIA.

13.4.1. Análisis de Riesgos

Como se trató en el apartado anterior, un Análisis de Riesgos, es una técnica o proceso que apoya la dirección de la empresa en la toma de sus decisiones, al identificar el riesgo, controlarlo y minimizar el impacto en un evento determinado.

Permite a los encargados de los activos, gestionar y tomar acciones de protección, de una manera razonable y prudente.

Así mismo, permite crear un balance entre los costos operativos y económicos en relación con las medidas de protección aplicadas, y lograr ganancias teniendo en cuenta la protección de los objetivos misionales de la empresa.

Su objetivo es reducir el riesgo a un nivel aceptable, el cual será aprobado por la dirección de la empresa.

Este proceso debe realizar un análisis costo-beneficio, en el cual se deben incorporar las características y beneficios de cada revisión del activo a evaluar. Esta revisión incluye costo del proyecto, adquisición e implementación de recursos.

Un ejemplo claro de esto es el desarrollo de la documentación, usuarios, soporte a la infraestructura y actualizaciones, costos de adecuación o migración.

Por otra parte, para ser efectivo, este proceso no debe extenderse demasiado. Debe realizarse en un tiempo prudente y efectivo.

Esta técnica se basa en el uso de matrices, en las cuales se identifican los activos que se puedan ver comprometidos, los posibles riesgos que se puedan presentar así como una valoración aproximada de la frecuencia en la que se podrían presentar estos posibles riesgos.

Una vez se logran obtener estos datos, se puede dar inicio a un análisis para poder tomar las medidas necesarias, así como los procedimientos a seguir.

Para poder aplicar esta técnica existen diferentes metodologías, guías y herramientas que ayudan a procesar la información y de esta manera obtener resultados más precisos.

Esta metodología, debe seleccionarse dependiendo de los objetivos y metas de la empresa.

Entre las herramientas con mayor reconocimiento dentro del mercado encontramos MAGERIT, Octave Cramm Iram.

Para ello se ha realizado un comparativo con diferentes metodologías en las cuales se evalúan diferentes indicadores que son de vital importancia para el análisis de riesgos a tratar en este documento.

		Metodología			
		MAGERIT	OCTAVE	CRAMM	IRAM
Alcance	Análisis de riesgos	C	N	C	C
	gestión de riesgos	C	C	C	C
Tipo de análisis	Cuantitativo	C	S	C	C
	Cualitativo	C	S	C	C
Gestión de riesgo	Intrínseco	C	N	C	C
	Efectivo	C	C	C	C
	Residual	C	P	N	S
Elementos que tiene en cuenta el modelo	Procesos	C	C	N	N
	Activos	C	C	C	C
	Recursos	C	C	N	N
	Dependencias	C	C	C	C
	Vulnerabilidades	C	C	C	C
	Amenazas	C	C	C	C
	Salvaguardas	C	C	C	C
Objetivos de seguridad	Confidencialidad	C		C	C
	Integridad	C	C	C	C
	Disponibilidad	C	N	C	C
	Autenticidad	C	N	N	N
	Trazabilidad	C	N	N	N
	Otros	N	N	N	N
Implantación	Herramientas	C	N	C	N
	Plan de proyecto	C	C	S	N
	Roles	C	C	C	N
	Comparativas	C	N	C	N

Leyenda		
	C	COMPLETO
	N	NO TIENE
	S	SATISFACTORIO
	P	POBRE

Tabla 3 Metodologías Análisis de Riesgos - Fuente Elaboración Propia

Después de realizar ese análisis, se puede observar que MAGERIT es la metodología más completa y apropiada para este análisis, debido a que permite evaluar diferentes aspectos necesarios para determinar las acciones a tomar y los planes a seguir, que se adecuen más a los objetivos de la organización.

Así mismo para poder procesar toda la información que requiere esta metodología, se utilizará la aplicación PILAR, la cual es un desarrollo en java enfocado a la metodología MAGERIT.

El uso de esta herramienta es solo como apoyo, permitiéndonos así la agilización en cuanto a la cuantificación de los resultados.

Debido a que este desarrollo es corporativo, se utilizará una licencia educativa, la cual ha sido solicitada por medio de un docente de la Universidad.

Aplicación de la Metodología

Como se trató con anterioridad, MAGERIT, está compuesto por tres libros, Métodos, Catalogo de Elementos y Guías Técnicas.

Según el primer libro, METODOS, es necesario realizar en el siguiente orden;

1. Planificación: En esta sección se realiza un pequeño estudio del estado actual de lo que se pretende analizar
2. Análisis de Riesgo: Se realiza la matriz de riesgos, valoración y catalogación de los activos, cuantificación y estudio de los datos obtenidos después de procesar la información.
3. Definición de tareas y actividades, que no son más que los controles a implementar.

Planificación

Hasta este punto, como primera medida, se ha logrado determinar que metodología es la más apropiada para el analisis de riesgos y la herramienta que se utilizará para el análisis de la información.

El siguiente paso es realizar un pequeño estudio o análisis del estado actual del ERP SEVEN en la Universidad EAN.

Par ello, según lo propone el primer libro de la metodología MAGERIT, es necesario realizar una tabla en la cual se definan actividades y tareas a seguir.

Estas se pueden observar en la siguiente tabla.

PROCESO P1 PLANIFICACIÓN
ACTIVIDAD A1 Situación actual del ERP Seven • Tarea T1.1 Infraestructura Tecnológica • Tarea T1.2 Red de datos • Tarea T1.3 ERP SEVEN • Tarea T1.4 Gestión Infraestructura • Tarea T1.5 Procesos actuales de control

Tabla 4 Proceso de Planificación - Fuente Elaboración Propia

Para ello es necesario tener en cuenta diferentes aspectos que son vital importancia para que este sistema funcione.

Estos aspectos van relacionados con la infraestructura tecnológica y la gestión de la misma.

En cuanto a la primera, Seven se encuentra alojado en un servidor físico, dentro del Data Center de la universidad.

Se cuentan con perfiles de usuarios a nivel de administración, de gestión, así como de consulta.

En lo referente a la seguridad, su acceso solo es posible mediante la red local administrativa de la institución. Así mismo es necesario contar con un usuario y contraseña para poder acceder a la aplicación.

Debido a cláusulas de privacidad de la universidad, no se profundizarán temas como tipo de red, rango de IP, o seguridad implementada a nivel de hardware y software en la misma.

En cuanto a la segunda, tanto para el Data Center, Red de Datos y Telefonía, se cuentan con ciertos procedimientos y actividades cuyo propósito es mantener la disposición de los servicios y la información.

Es posible acceder a SEVEN vía WEB mediante la página institucional, siempre y cuando el usuario se encuentre registrado y tenga los permisos adecuados según las políticas preestablecidas en los roles de usuario.

En los apartados anteriores, se profundiza más en cuanto a el ERP Seven, que es, servicios que presta, módulos que lo componen y empresa que lo desarrollo.

Ahora bien, en lo referente a la gestión, se cuenta con una matriz de riesgos, en al cual se han registrado diferentes procesos, el posible riesgo y los controles a tomar.

Por otra parte, como se comentó en el capítulo anterior, se cuenta con un proceso de generación de copias de respaldo en medios magnéticos a datos e información considerada necesaria y vital para la restauración del Sistema SEVEN.

Análisis de Riesgos

Matriz de análisis de Riesgos

Luego de determinar la metodología a utilizar, la herramienta que nos ayudará a procesar la información y de tener un panorama genérico del estado actual en cuanto al sistema SEVEN, el paso a seguir es realizar una matriz de riesgos.

El propósito del análisis de riesgo es la identificación de los activos, su descripción, las amenazas que pueda tener, los posibles riesgos, las causas por las cuales se puede presentar, la probabilidad de aparición y el impacto que pueden causar.

Para ello, como se muestra en la siguiente tabla, se llevaran a cabo las siguientes actividades.

PROCESO P2 Análisis de Riesgos
ACTIVIDAD A2 .1 Caracterización de Activos • Tarea T2.1.1 Identificación de los activos • Tarea T2.1.2 Dependencias de los Activos • Tarea T2.1.3 Valoración de los Activos ACTIVIDAD A2.2 Caracterización de las amenazas • Tarea T2.2.1 Identificación de las amenazas • Tarea T2.2.2 Valoración de las amenazas ACTIVIDAD A2.3 Estimación del Riesgo • Tarea T2.3.1 Estimación del Impacto • Tarea T2.3.2 Estimación del Riesgo ACTIVIDAD A2 .4 Caracterización de las salva guardas • Tarea T2.4.1 Identificación de las salvaguardas existentes • Tarea T2.4.2 Valoración de las salvaguardas existentes

Tabla 5 Actividades – Tareas - Fuente Elaboración Propia

Las anteriores actividades y tareas del proceso dos, se determinaron según los libros 2 y 3 de la metodología MAGERIT “Catálogos de Elementos” y “Guías y Técnicas”, los cuales proponen estrategias para poder clasificar y valorar los activos e identificar las amenazas y riesgos.

Antes de continuar es importante aclarar que en la metodología MAGERIT el concepto de vulnerabilidad eta compuesto por 2 métricas llamadas Degradación del activo y Frecuencia e materialización de la amenaza.

ACTIVIDAD A2 .1 Caracterización de Activos

El objetivo de esta actividad es listar los activos más relevantes que se encuentran directamente relacionados con el ERP Seven, para su posterior análisis.

Como se describió en la tabla anterior, esta actividad está compuesta por las siguientes tareas.

- Tarea T2.1.1 Identificación de los activos
- Tarea T2.1.2 Dependencias de los Activos
- Tarea T2.1.3 Valoración de los Activos

Cada activo identificado debe estar compuesto por una serie de atributos como son, el nombre una descripción y un código, así mismo a la seccion o capa a la cual pertenece.

Actualmente la Universidad cuenta con una matriz de riesgos en la cual se han identificado y cuantificado ciertas variables en los procesos y subprocesos correspondientes a; El Data Center, La Telefonía IP y la Red Interna.

Para esta tarea, como en las posteriores, haremos uso de la aplicación Pilar, la cual nos ayudará a sistematizar y procesar la información.

Una vez se accede a la aplicación, se puede observar que se encuentran 4 pasos a seguir para la realización del análisis de riego.

Estos pasos se encuentran clasificados en;

- D: Datos referentes al nombre, código, descripción y versión del proyecto. Definición de los dominios de seguridad[9] y faces del proyecto.
- A: Análisis de Riesgo, en el cual se realiza la identificación de los activos en cada dominio de seguridad, su clasificación y posterior valoración, identificación de las amenazas, clasificación y valoración. Identificación y valoración de las salvaguardas, así como el impacto.
- R: Informes, resultados textuales o por gráfica.
- E: Perfiles de seguridad: Observar la seguridad desde un perfil dado.

[9] Se conoce como dominio de seguridad a un grupo de activos enfocados a un objetivo común. Por ejemplo para efectos de este proyecto, se ha creado como dominio de seguridad, Equipamiento, en el cual se agrupan activos a nivel de software y hardware. Otro activo podría ser servicios internos, en el cual se encuentran activos como internet y los sistemas de información.

Tareas T2.1.1 Identificación de los Activos

Estas tareas van directamente relacionadas con el paso A de la aplicación Pilar.

Para ello, hemos identificado los siguientes seis dominios de seguridad.

- Procesos
- Servicios internos
- Equipamiento
- Servicios sub contratado
- Instalaciones
- Personal

Así mismo se ha creado en cada dominio un grupo de activos y los activos correspondientes.

Podemos observar los dominios así como el grupo de activos correspondientes, en la siguiente gráfica.

Debido a cláusulas de confidencialidad solo se mostraran algunos de los activos seleccionados.

Esta selección se realizó de acuerdo a un catálogo de selección de activos.

Ilustración 20 Selección de Activos – Fuente Elaboración Propia

Como podemos observar en la imagen anterior, podemos encontrar el código [PS] el cual representa el dominio referente a los procesos.

Así mismo encontramos un grupo de activos identificado por una carpeta de color amarillo e identificado con el código [DC] Data center.

De igual manera encontramos unos activos o subprocesos

Posteriormente se procede a clasificar cada activo, con base a una lista predeterminada. Esta clasificación la podemos observar en la siguiente gráfica.

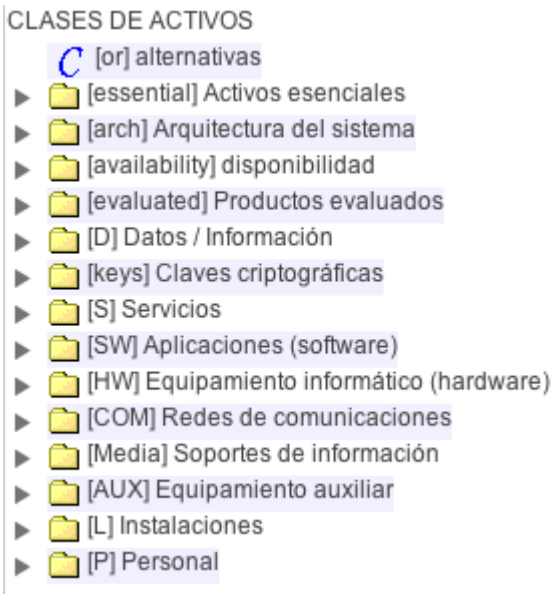


Ilustración 21 Clasificación de Activos – Fuente Elaboración Propia

De esta manera a cada uno de estos activos se le asigna una clase de activo. Para efectos de este ejemplo, observemos la siguiente imagen;

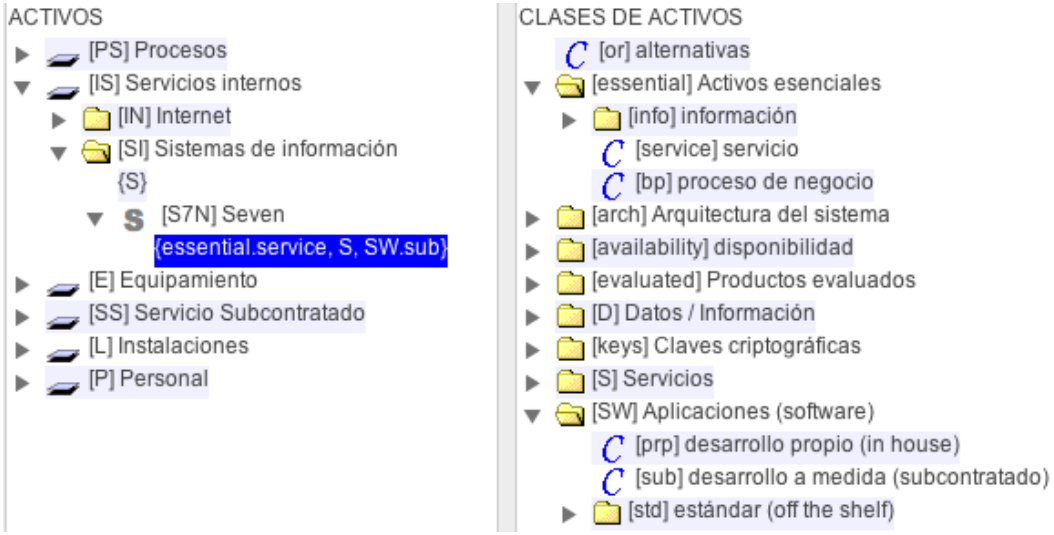


Ilustración 22 Clases de Activos - Fuente Elaboración Propia

Para el activo correspondiente a Seven, podemos observar que se trata de un activo de servicio esencial (essential service) y que es un software (SW) desarrollado por terceros (Sub).

T2.1.2 Dependencias de los Activos

Para este paso, se siguió la metodología descrita por el libro Catálogos de Elementos, de la metodología Magerit.

La jerarquía utilizada, se basa básicamente en la dependencia que tiene un activo[10] superior de un activo inferior. Teniendo en cuenta que los requerimientos de seguridad de este activo superior, se vean reflejados en los requerimientos del activo inferior.

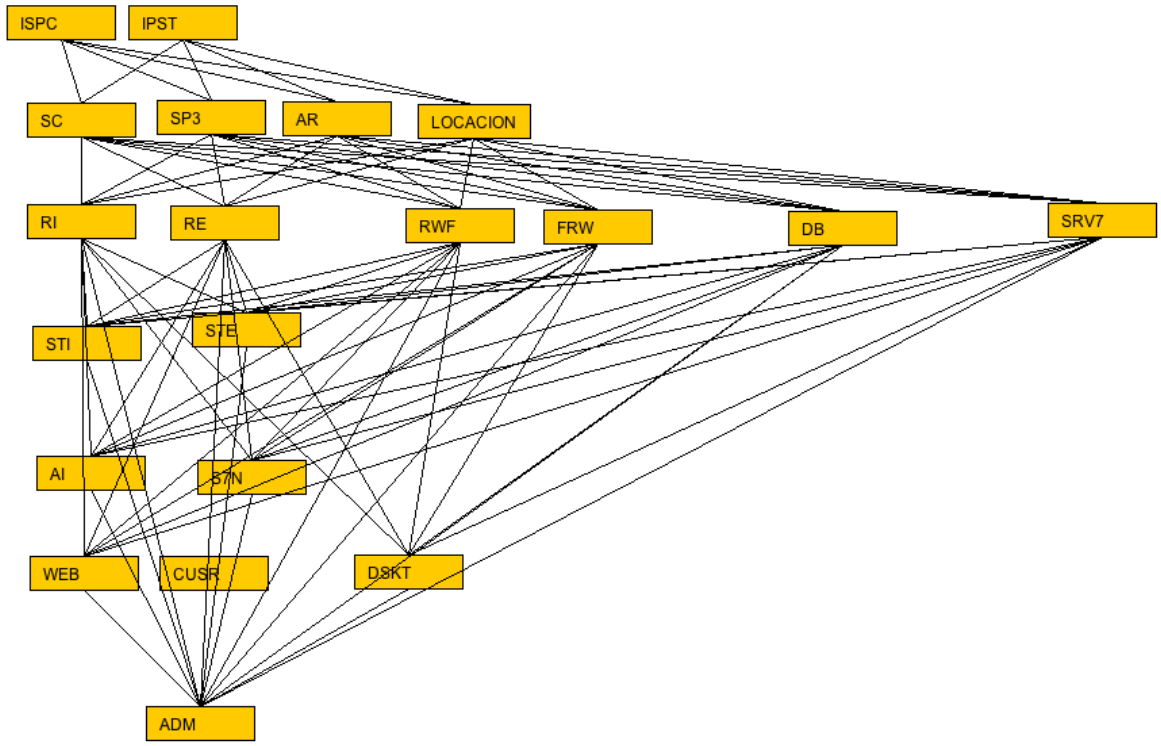


Ilustración 23 Catalogo activos superiores a activos inferiores. Fuente Elaboración Propia

[10] Dependencia de un activo es la medida en las cual un activo superior se podría encontrar afectado debido a un incidente de seguridad de un activo inferior. Definición sacada del libro 2 Catálogos de Elementos, Metodología Magerit.

La grafica anterior nos permite observar esta jerarquía. En la cual, que activo depende de otro.

Tarea T2.1.3 Valoración de los Activos

Este paso se puede realizar de dos maneras en Pilar. Colocando un valor a cada dominio de activos, por lo cual se cada activo que se encuentre en ese dominio, será valorado. La segunda, es que a cada activo de manera individual asignar un valor.

Para efectos de este proyecto, valoraremos los activos de manera individual, con base a unas dimensiones de seguridad que es necesario tener en cuenta. Según la metodología MAGERIT, estas son los siguientes;

- [D] Disponibilidad: Asegurar que este activo se encuentra disponible cuando se necesite.
- [I] Integridad de Datos: Permite comprobar que los datos no han sido alterados accidental o intencionalmente.
- [C] Confidencialidad de Datos: Asegurar que solo se pueda acceder a esta información por personal autorizado.
- [A] Autenticidad de los Usuarios y de la Información: Confirmar que el usuario que está accediendo es el correcto.
- [T] Trazabilidad de los Datos y de la Información: Permite realizar seguimiento de cada acción realizada por el usuario.

Para lo siguiente se tendrá en cuenta un catálogo de valoración de activos, por medio de una escala estándar recomendada por la metodología Magerit en su catálogo de elementos.

Así mismo, con base a este catálogo se procederá a realizar la valoración de todos los activos.

Valoración			**Descripción**
10	Muy alto	**MA**	Daño muy grave a la organización
7-9	Alto	**A**	Daño grave a la organización
4-6	Medio	**M**	Daño importante a la organización
1-3	Bajo	**B**	Daño Medio a la organización
0	Despreciable	**MB**	Daño irrelevante a la

			organización

Tabla 6 Catalogo valoración de activos - Fuente Elaboración Propia

Como se explicó con anterioridad debido a cláusulas de confidencialidad, tomaremos como ejemplo una sección de la valoración que se realizó en algunos de los activos.

El listado completo, se utilizará para los análisis posteriores y será entregado a la Gerencia de TIC.

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[PS] Procesos					
[IS] Servicios internos					
[IN] Internet					
[AI] Acceso a Internet	[10]	[8]	[3]	[9]	[9]
[SI] Sistemas de información					
[S7N] Seven	[9]	[10]	[9]	[9]	[8]

Ilustración 24 Valoración de activos Fuente Elaboración Propia

En la tabla anterior podemos observar, la valoración de los activos correspondientes al dominio de servicios (Internet y el ERP Seven).

Cada uno de estos activos fue valorado teniendo en cuenta la importancia de este activo, según los criterios anteriormente descritos.

En el caso del activo correspondiente a Seven, se puede observar que la valoración es una de las más altas.

Para ello, se realizó un pequeño análisis;

- Es necesario que el sistema cuente con una disponibilidad alta para poder realizar todos los procesos necesarios en cada uno de los módulos (financieros, gestión humana, etc.), así mismo, la capacidad para asegurar que los datos sean registrados adecuadamente en los campos que corresponde (integridad de datos), sin existir la posibilidad de generarse registros fantasmas que más adelante puedan alterar los resultados.

- Por otra parte en encontrarse diseñado para que el acceso de estos datos solo debe ser realizado por el administrador o personal autorizado (Confidencialidad de Datos y Autenticidad de los Usuarios y de la Información).

- Así mismo esta información debe encontrarse disponible para que pueda ser consultada en el momento adecuado, permitiendo así tomar decisiones adecuadas.

Como se puede observar, Seven se encuentra dentro de los activos más preciados, debido al manejo de información, la cual puede servir como apoyo a los procesos, permitiendo así la toma de ciertas decisiones.

Adicionalmente, al momento de realizar esta valoración, el sistema solicita seleccionar, unos criterios de valoración adicionales. Estos criterios de valoración van directamente relacionados con posibles causas que se puedan presentar y afectar a este activo así como el nivel de impacto que pudiera tener en la organización.

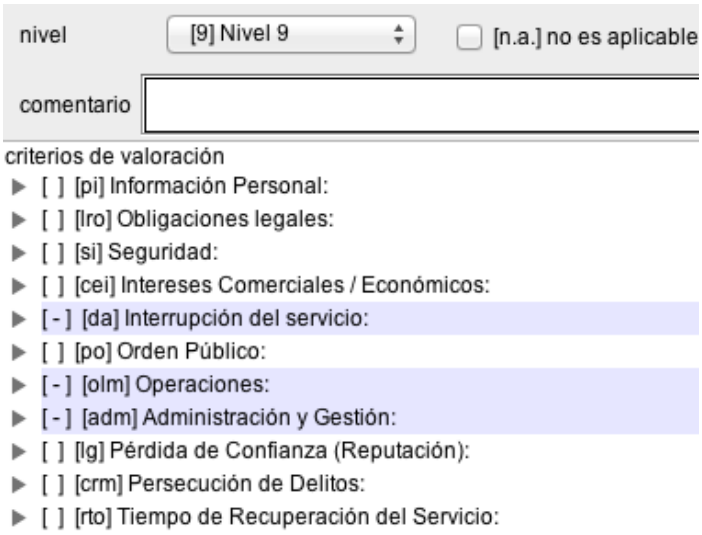


Ilustración 25 Criterios de valoración de activos - Fuente Elaboración Propia

En la imagen anterior, se puede observar la valoración que se da a Seven con respecto a la [D] Disponibilidad, que en este caso es 9, y adicionalmente los criterios de valoración que se tuvieron en cuenta, como son; Interrupciones de orden público, Interrupción en las operaciones, situaciones de administración y gestión que pudieran afectar el adecuado funcionamiento de este activo.

Tarea T2.2.1 Identificación de las amenazas

Esta identificación se realizará mediante el uso de un catálogo, en el cual se realiza una clasificación de amenazas.

Magerit básicamente clasifica 4 grupos de posibles amenazas;

- De tipo natural **[N].**
- De origen industrial **[I].**
- Errores y fallos no intencionados **[E]**.
- De ataques deliberados. **[A]**

Para la identificación de estas amenazas, haremos uso de las tablas del libro II Catalogo de Elementos de la metodología Magerit, en el cual se agrupan las amenazas de acuerdo al activo en que dimensión[11] se pueden materializar.

Esta agrupación y catalogación se realiza, teniendo en cuenta los siguientes, criterios adicionales.

- **[D]** Disponibilidad.
- **[I]** Integridad.
- **[C]** Confiabilidad.
- **[A_*]** Autenticidad de servicios y datos.
- **[T_*]** Trazabilidad de servicio y datos.
- **[N…n]** Grupo de amenazas desastres naturales.
- **[I…n]** Grupos de amenazas de origen industrial.
- **[E…n]** Grupos de amenazas de errores y fallos no intencionales.
- **[A…n]** Grupos de amenazas de ataques no intencionados.

Similar que con la valoración de los activos, la identificación de la amenazas se puede realizar asignando una amenaza a cada dominio y de esta manera el grupo de activos es identificado con un grupo de amenazas en común, o identificando una amenaza específica a cada activo.

Así mismo, Pilar puede configurarse para que realice una identificación automática de posibles amenazas a cada activo.

Para ello, Pillar obtiene los datos teniendo en cuenta unos criterios de valoración adicionales realizados en el paso anterior, en los cuales se califica a cada activo y la posible consecuencia al momento de presentarse, interrupción en el funcionamiento del servicio y su posible consecuencia en la organización.

[11] Son características o atributos que hacen valioso a un activo. Esta es de gran utilidad al momento de valorar las consecuencias de materialización de una amenaza. Es una un indicador que permite evaluar a la organización que tan perjudicial puede llegar a ser el activo si este se llega a dañar.

En la gráfica siguiente, se pueden observar un listado de posibles amenazas que se podrían presentarse y afectar al activo Seven.

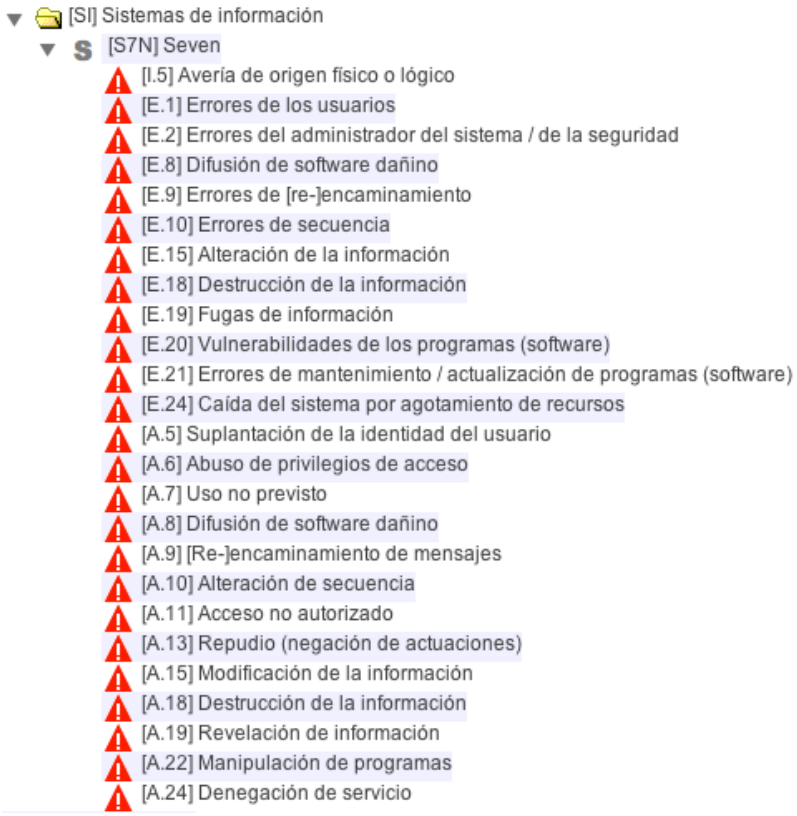


Ilustración 26 Identificación de Amenazas - Activo Seven - Fuente Elaboración Propia

Así mismo, en la siguiente tabla podemos observar la amenaza **[A.24] Denegación de servicio** para cada uno de los activos, en qué nivel se encuentra y la valoración para cada una de las dimensiones

[A.24] Denegación de servicio

activo	nivel	[D]	[I]	[C]	[A]	[T]
[DC.SC] Seguridad	A	-	-	-	-	-
[DC.SP3] Sub Proceso 3	A	-	-	-	-	-

[DC.AR] Alimentación Regulada	A	-	-	-	-	-
[RD.RI] Red Interna	A	-	-	-	-	-
[RD.RE] Red Externa	A	-	-	-	-	-
[RD.RWF] Red Inalámbrica	A	-	-	-	-	-
[RD.FRW] Firewall	A	-	-	-	-	-
[TF.STI] Servicio Telefonía Interno	A	-	-	-	-	-
[TF.STE] Servicio Telefonía Externo	A	-	-	-	-	-
[IN.AI] Acceso a Internet	A	5%	-	-	-	-
[SI.S7N] Seven	**A**	**5%**	**-**	**-**	**-**	**-**
[SW.WEB] Pagina Institucional	A	50%	-	-	-	-
[SW.DB] Bases de Datos	A	50%	-	-	-	-
[HW.SRV7] Servidor Seven	A	100%	-	-	-	-
[HW.DSKT] Equipo de Escritorio - Estación de Trabajo	M	100%	-	-	-	-
[ISP.ISPC] Proveedor de Servicios de Internet - Claro	A	5%	-	-	-	-
[ISP.IPST] Proveedor de Servicios de Internet - ETB	A	5%	-	-	-	-

Tabla 7 Amenaza Denegación de Servicio en los activos - Fuente Elaboración Propia

Un listado de los resultados completo se entregará a la Gerencia del TIC. **Anexo A**

Tarea T2.2.2 Valoración de las amenazas

En esta sección Pilar nos ayuda a agilizar un poco el trabajo, debido a que se basa en la catalogación y la valoración de los activos para asignar un valor a cada amenaza así como la frecuencia en la cual se pueda presentar.

Esta frecuencia[12] se puede visualizar en modo numérico o de acuerdo a un criterio de 4 rangos [B] Bajo, [M] Medio, [A] Alto y [MA] Muy alto.

Así mismo se estima la degradación[13] de las materializaciones de estas amenazas sobre cada uno de estos activos.

Estos criterios los podemos observar en el siguiente catalogo:

[12] Cada Cuanto se Materializa esta amenaza
[13] Que tanto se encontraría perjudicado este activo.

Nivel / Frecuencia	Dimensiones	Descripción
MA	100%	Muy alto
A	80%	Alto
M	50%	Medio
B	10%	Bajo

Tabla 8 - Catalogo Valoración de las amenazas - Fuente Elaboración Propia

Una vez se ha aplicado el ejercicio a todos los activos, se obtiene como resultado de esta tarea un informe en el cual se describen las amenazas posibles y la frecuencia en la cual se puedan presentar. Así mismo que tanto podrían degradarse dichos activos.

Con lo anterior será posible determinar los riesgos repercutidos por las amenazas según los niveles de criticidad propuestos por MAGERIT.

Ilustración 27 Niveles de Criticidad- Fuente Elaboración Propia

Un ejemplo lo podemos observar nuevamente para el activo Seven. En la siguiente imagen se describe el tipo de amenaza, la dimensión, el nivel en el que se encuentra y la valoración según los criterios adicionales, descritos en los puntos anteriores.

activo	[D]	[I]	[C]	[A]	[T]
[RI] Red Interna	{6,0}	{3,6}	{3,9}	{4,5}	
[RE] Red Externa	{5,4}	{5,4}	{3,9}	{3,3}	
[RWF] Red Inalambrica	{3,6}		{1,6}	{0,98}	
[FRW] Firewall	{5,4}	{4,2}	{3,3}	{3,9}	
[STI] Servicio Telefonia Interno	{6,4}	{4,0}	{4,4}	{6,2}	
[STE] Servicio Telefonia Externo	{6,4}	{4,0}	{4,4}	{5,7}	
[AI] Acceso a Internet	{6,4}	{6,5}	{3,2}	{6,2}	
[S7N] Seven	{5,8}	{7,7}	{6,9}	{6,2}	
[D] disponibilidad	{5,8}				
[SI.S7N] Seven	{4,8}				
[I.5] Avería de origen físico o lógico	{3,9}				
[E.1] Errores de los usuarios	{2,7}				
[E.2] Errores del administrador del sistema / de la seguridad	{3,2}				
[E.8] Difusión de software dañino	{2,7}				
[E.18] Destrucción de la información	{3,9}				
[E.24] Caída del sistema por agotamiento de recursos	{4,8}				
[A.7] Uso no previsto	{4,5}				
[A.8] Difusión de software dañino	{4,5}				
[A.18] Destrucción de la información	{3,9}				
[A.24] Denegación de servicio	{4,8}				
[ADM] Administrador	{5,8}				
[I] integridad de los datos		{7,7}			
[SI.S7N] Seven		{7,7}			
[ADM] Administrador		{6,9}			
[C] confidencialidad de los datos			{6,9}		
[SI.S7N] Seven			{6,9}		
[ADM] Administrador			{6,7}		
[A] autenticidad de los usuarios y de la información				{6,2}	
[SI.S7N] Seven				{6,2}	
[T] trazabilidad del servicio y de los datos					

Ilustración 28 Tipo de Amenaza por Dimensión, Nivel y Valoración - Fuente Elaboración Propia

Como se observó con anterioridad, cada nivel de criticidad se encuentra identificado con un color específico. Así mismo cada riesgo repercutido se encuentra en una escala de 0 a 10, siendo cero un riesgo despreciable y el rango de 7 a 10 un riesgo al cual hay que prestar atención.

Por tal razón es de vital importancia mitigar por medio de salvaguardas, aquellos activos cuya magnitud es más alta.

Según nuestra imagen, los niveles más críticos para Seven, se encuentran relacionados con la dimensión relacionada a integridad de datos, dentro de la cual encontramos; [A.13] Repudio (Negación de actualizaciones), [A.15] Modificación de información y [A.22] Manipulación de programas, como amenazas con magnitud alta.

amenaza	nivel	[D]	[I]	[C]	[A]	[T]
[I.5] Avería de origen físico o lógico	M	5%	-	-	-	-
[E.1] Errores de los usuarios	M	1%	10%	10%	-	-
[E.2] Errores del administrador del sistema / de la seguridad	M	2%	20%	20%	-	-
[E.8] Difusión de software dañino	M	1%	10%	10%	-	-
[E.9] Errores de [re-]encaminamiento	M	-	-	10%	-	-
[E.10] Errores de secuencia	M	-	10%	-	-	-
[E.15] Alteración de la información	M	-	1%	-	-	-
[E.18] Destrucción de la información	M	5%	-	-	-	-
[E.19] Fugas de información	M	-	-	10%	-	-
[E.20] Vulnerabilidades de los programas (software)	M	-	20%	20%	-	-
[E.21] Errores de mantenimiento / actualización de programas (software)	A	-	1%	-	-	-
[E.24] Caída del sistema por agotamiento de recursos	A	5%	-	-	-	-
[A.5] Suplantación de la identidad del usuario	M	-	50%	50%	100 %	-
[A.6] Abuso de privilegios de acceso	M	-	10%	10%	-	-
[A.7] Uso no previsto	M	10 %	10%	10%	-	-
[A.8] Difusión de software dañino	M	10 %	100 %	100 %	-	-
[A.9] [Re-]encaminamiento de mensajes	M	-	-	100 %	-	-
[A.10] Alteración de secuencia	M	-	50%	-	-	-
[A.11] Acceso no autorizado	M	-	10%	50%	-	-
[A.13] Repudio (negación de actuaciones)	A	-	100 %	-	-	-
[A.15] Modificación de la información	A	-	50%	-	-	-
[A.18] Destrucción de la información	M	5%	-	-	-	-
[A.19] Revelación de información	M	-	-	50%	-	-
[A.22] Manipulación de programas	A	-	100 %	100 %	-	-
[A.24] Denegación de servicio	A	5%	-	-	-	-

Tabla 9 - Valoración Amenazas / Criterios Activo Seven

Un listado de los activos completos y la valoración de sus amenazas, se utilizarán para análisis posteriores y será entregado a la Gerencia de TIC. **Anexo B**

ACTIVIDAD A2.3 Estimación del Riesgo

Tarea T2.3.1 Estimación del Impacto

Al igual que en los pasos anteriores, Magerit recomienda la elaboración de un catálogo, el cual servirá de ayuda para determinar el impacto potencial y residual que puede presentarse en un activo relacionado con Seven.

Para ello es necesaria la realización de una tabla, para evaluar el activo con base a sus dimensiones, el nivel de degradación que una amenaza puede ejercer sobre dicho activo y por consiguiente el impacto generado sobre el sistema.

Lo anterior se basa en la formula;

Impacto = valor * degradación

Ahora bien ara como se realizó en el punto **T2.1.2 Dependencias de los Activos**, es claro que cada activo superior depende de uno inferior. Debido a dicha dependencia, se pueden presentar 2 tipos de impactos;

- **Impacto Acumulado**; El cual resulta de sumar el valor calculado de las amenazas a la cual está expuesto este activo, más el resultante de los valores acumulados de los activos que dependen de él, así como la degradación.
  Una vez detectado el valor acumulado es posible determinar que salvaguardas aplicar.
- **Impacto Repercutido**; El cual es el resultado de trascender las amenazas de un impacto inferior al superior. Todo lo anterior teniendo en cuenta las consideraciones del impacto acumulado.

Para la creación de la siguiente tabla, se ha tomado el libro tres “Guías Técnicas” de la metodología MAGERIT. Y de esta manera, poder categorizar la magnitud del impacto y riesgo para los activos;

Degradación en porcentaje	Simbología	Descripción
100%	MA	Muy alto
80%	A	Alto
50%	M	Medio
10%	B	Bajo

Tabla 10 Estimación Degradación - Fuente Elaboración Propia

Una vez más, nos apoyamos en la Herramienta Pilar para obtener los resultados. Estos son los informes de impacto acumulado y residual por activo.

Allí Pilar nos mostrara una matriz en la cual podremos encontrar en columna correspondiente cada activo, la amenaza asociada, la dimensión que se encuentra asociada a este activo, el Valor de este activo, el valor acumulado según los activos que dependen de él, la degradación, (recordemos que en esta versión MAGERIT cuando se habla de vulnerabilidad, es la integración de las métricas Degradación y Frecuencia de la materialización de las amenazas), el impacto que puede causar esta amenaza en la empresa si se materializa, el nivel en el que se encuentra asociada esta degradación y la valoración del riesgo si esta amenaza se materializa.

La matriz es resultado de todos los pasos anteriores con el propósito de obtener el informe de estado de riesgo.

Es posible acceder a varas vistas;

- **Potencial**; Nos muestra el impacto potencia sin salva guarda alguna.
- **Current**; Nos muestra la situación actual.
- **Target**: Análisis de Riesgo.
- **PILAR**: Sugerencia o Recomendación
- **Resumen de impacto**. Nos muestra a cada activo con su correspondiente amenaza y el impacto asociado a cada dimensión según las vistas potencial, current, target y pilar.

Por defecto PILAR, nos muestra los impactos con la estimación de degradación más alta de primeras y progresivamente los de degradación más baja, como se puede observar en la siguiente grafica;

Ahora bien, hasta este punto ya podemos observar cuales son los activos cuya amenaza hay que prestar mucha atención ya que el nivel de degradación es muy alta.

Por ejemplo, unos de los niveles más altos lo podemos observar en los activo **Seven**, cuya amenaza ***Repudio (negación de actualizaciones)***, **Acceso a Internet**, relacionadas con la ***dimensión Integración de datos***, tiene una valoración de 10 y una catalogación A (Alto) según la tabla definida con anterioridad.

Otro ejemplo lo podemos encontrar con el activo **Bases de Datos**, cuya amenaza ***Destrucción de la información*** asociada a la dimensión ***Disponibilidad***, tiene una valoración de 10 un valor de degradación de 50% y un impacto de 10 puntos, así mismo su catalogación en el nivel de degradación es A (Alta).

A estas amenazas son a las primeras que hay que controlar con las salvaguardas adecuadas, para tratar mitigarlas o de disminuir a un nivel aceptable.

potencial | current | target | BIA | PILAR | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensión	V	VA	D
[SI.S7N] Seven	[A.13] Repudio (negación de actuaciones)	[I]	[10]	[10]	100%
[IN.AI] Acceso a Internet	[A.13] Repudio (negación de actuaciones)	[I]	[8]	[10]	100%
[HW.SRV7] Servidor Seven	[A.24] Denegación de servicio	[D]	[10]	[10]	100%
[SI.S7N] Seven	[A.22] Manipulación de programas	[I]	[10]	[10]	100%
[SI.S7N] Seven	[A.15] Modificación de la información	[I]	[10]	[10]	50%
[IN.AI] Acceso a Internet	[A.15] Modificación de la información	[I]	[8]	[10]	50%
[SW.DB] Bases de Datos	[A.18] Destrucción de la información	[D]	[10]	[10]	50%
[HW.SRV7] Servidor Seven	[E.24] Caída del sistema por agotamiento de r...	[D]	[10]	[10]	50%
[HW.DSKT] Equipo de Escritorio - Estación de...	[E.24] Caída del sistema por agotamiento de r...	[D]	[5]	[10]	50%
[SW.DB] Bases de Datos	[E.24] Caída del sistema por agotamiento de r...	[D]	[10]	[10]	50%
[SW.WEB] Pagina Institucional	[E.24] Caída del sistema por agotamiento de r...	[D]	[8]	[10]	50%
[SW.DB] Bases de Datos	[A.24] Denegación de servicio	[D]	[10]	[10]	50%
[SW.WEB] Pagina Institucional	[A.24] Denegación de servicio	[D]	[8]	[10]	50%
[HW.DSKT] Equipo de Escritorio - Estación de...	[A.24] Denegación de servicio	[D]	[5]	[10]	100%
[SW.DB] Bases de Datos	[A.5] Suplantación de la identidad del usuario	[A]	[9]	[9]	100%

Ilustración 29 Impactos Cuyo Nivel de Degradación Mas Alta - Vista Potencial (Informe Valores Acumulados por Fase) - Fuente Elaboración Propia

Por otra parte si queremos ver en más detalle el comportamiento de cada activo, solo basta con dar clic en el título correspondiente a Activo y allí la lista se organizara por activos, como se puede observar en la siguiente grafica

potencial | current | target | BIA | PILAR | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensión	V	VA	D
[SI.S7N] Seven	[A.13] Repudio (negación de actuaciones)	[I]	[10]	[10]	100%
[SI.S7N] Seven	[A.22] Manipulación de programas	[I]	[10]	[10]	100%
[SI.S7N] Seven	[A.15] Modificación de la información	[I]	[10]	[10]	50%
[SI.S7N] Seven	[A.22] Manipulación de programas	[C]	[9]	[9]	100%
[SI.S7N] Seven	[A.8] Difusión de software dañino	[I]	[10]	[10]	100%
[SI.S7N] Seven	[A.10] Alteración de secuencia	[I]	[10]	[10]	50%
[SI.S7N] Seven	[A.5] Suplantación de la identidad del usuario	[I]	[10]	[10]	50%
[SI.S7N] Seven	[A.9] [Re-]encaminamiento de mensajes	[C]	[9]	[9]	100%
[SI.S7N] Seven	[A.5] Suplantación de la identidad del usuario	[A]	[9]	[9]	100%
[SI.S7N] Seven	[A.8] Difusión de software dañino	[C]	[9]	[9]	100%
[SI.S7N] Seven	[A.11] Acceso no autorizado	[C]	[9]	[9]	50%
[SI.S7N] Seven	[A.5] Suplantación de la identidad del usuario	[C]	[9]	[9]	50%
[SI.S7N] Seven	[A.19] Revelación de información	[C]	[9]	[9]	50%
[SI.S7N] Seven	[E.20] Vulnerabilidades de los programas (soft...	[I]	[10]	[10]	20%
[SI.S7N] Seven	[E.2] Errores del administrador del sistema / d...	[I]	[10]	[10]	20%
[SI.S7N] Seven	[E.24] Caída del sistema por agotamiento de r...	[D]	[9]	[10]	5%
[SI.S7N] Seven	[A.24] Denegación de servicio	[D]	[9]	[10]	5%

Ilustración 30 Impactos Nivel de Degradación Activo Seven - Vista Potencial (Informe Valores Acumulados por Fase) - Fuente Elaboración Propia

Así mismo como se puede observar, en la parte superior se pueden visualizar las vistas correspondientes a potencial, current y target. Al alternar en estas vistas el resultado es el mismo.

La vista Pilar, nos muestra resultados que son a los que tenemos que llegar.

Ahora bien en las siguiente Tabla, podremos observar por fases o vistas (potencial, current, target y pilar) **el impacto acumulado**.

Este resultado se puede observar por dominio o por activos. Para efectos de este ejemplo lo veremos por dominios. Un informe más completo por activos, será entregado como soporte a la gerencia del TIC. **Anexo C**

	Fase Potencial					Fase Pilar		
Activos	**D**	**I**	**C**	**A**	**T**	**D**	**I**	
[PS]Procesos		[7]	[7]	[9]			[2]	
[IS]Servicios Internos	[7]	[10]	[9]	[9]		[2]	[5]	
[E]Equipo	[10]	[7]		[9]		[5]	[2]	

[SS]Servicio Subcontratado	[6]	[4]	[0]	[6]		[1]	[0]	
[L]Instalaciones	[6]					[1]		
[P]Personal	[9]	[10]	[9]			[4]	[5]	

Ilustración 31 Informe Impacto Acumulado - Fuente Elaboración Propia

Si verificamos la tabla anterior, en ella podemos observar que dominios de activos tiene un impacto acumulado con magnitud alta. Dentro de estos podemos encontrar al dominio **[PS] procesos** cuyo valor se concentra más en la dimensión ***Integridad de datos, Confidencialidad de Datos y Autenticación de Datos***.

Si queremos profundizar más, podemos desplegar en Pilar el listado de activos y verificar las amenazas asociadas. (Ver gráfica.).

- Para efectos de este ejemplo aparecerán **[DC] Data Center, [RD] Redes** y **[TF] Telefonía**. Al observar se encuentra una concentración enfocada a el grupo de activos correspondiente a Data center.
- Al dar doble clic, encontramos que el activo **[SP3] Sub Proceso 3** se encuentra con un valor de **[8]** en la dimensión **Autenticidad de los usuarios y de la información**.
- Así mismo al dar doble clic, podremos encontrar que la amenaza más alta asociada a este activo se encuentra definida como, **Suplantación de identidad de usuario. Ver Ilustración.**

activo	[D]	[I]	
ACTIVOS	[10]	[10]	
[PS] Procesos		[7]	
[DC] Data Center		[4]	
[SC] Seguridad			
[SP3] Sub Proceso 3		[4]	
[N.1] Fuego			
[N.2] Daños por agua			
[N.*] Desastres naturales			
[I.1] Fuego			
[I.2] Daños por agua			
[I.*] Desastres industriales			
[I.11] Emanaciones electromagnéticas			
[E.1] Errores de los usuarios		[1]	
[E.2] Errores del administrador del sistema / de la seguridad		[2]	
[E.9] Errores de [re-]encaminamiento			
[E.10] Errores de secuencia		[1]	
[E.15] Alteración de la información			
[E.18] Destrucción de la información			
[E.19] Fugas de información			
[E.24] Caída del sistema por agotamiento de recursos			
[A.5] Suplantación de la identidad del usuario		[3]	

Continuando con otro ejemplo y tomando a Seven nuevamente, podemos observar que la amenaza cuyo indicador más alto es **Repudio (Negación de Autenticaciones),** asociada a la dimensión **Integridad de Datos.**

Si recordamos en las páginas anteriores (***Grafica– Impactos Cuyo Nivel de Degradación Mas Alta - Vista Potencial),*** habíamos observado también este comportamiento.

Todo lo anterior hace referencia a las faces **Fase Potencial** la cual muestra el estado de los activos sin tener en cuenta ningún tipo de salvaguarda. Esto con el propósito de cómo será el comportamiento y el impacto de este activo en la organización, si no se cuentan con los salvaguardas adecuados o si estos no se aplican debidamente.

Continuando con el análisis de nuestra ***Tabla– Informe Impacto Acumulado***, al observar el bloque relacionado con la fase Pilar (bloque de color naranja), podemos observar como disminuyen los indicadores al aplicar las salvaguardas adecuadas. Esta fase es la ideal. Recordemos que el propósito de las salvaguardas es mitigar si no es en su totalidad, por lo menos a un nivel aceptable la amenaza.

Ahora bien, en las siguiente Tabla, podremos observar por fases o vistas (potencial, current, target y pilar) el **impacto repercutido**.

Este resultado se puede observar por activos. Un informe más completo por activos, será entregado como soporte a la gerencia del TIC. **Anexo C**

	Fase Potencial					Fase Pil		
Activos	**D**	**I**	**C**	**A**	**T**	**D**	**I**	
[SC]Seguridad	[4]					[0]		
[SP3] Sub Proceso 3	[6]	[7]	[7]	[8]		[1]	[2]	
[AR]Alimentación Regulada	[10]					[5]		
[RI]Red Interna	[8]	[3]	[4]	[6]		[3]	[0]	
[RE]Red Externa	[7]	[6]	[4]	[4]		[2]	[1]	
[RWF]Red Inalámbrica	[4]		[0]	[0]		[0]		

[FRW]Firewall	[7]	[4]	[3]	[5]		[2]	[0]	
[STI]Telefonía Interna	[9]	[5]	[5]	[9]		[4]	[0]	
[STE]Telefonía Externa	[9]	[5]	[5]	[8]		[4]	[0]	
[AI]Acceso a Internet	[9]	[8]	[3]	[9]		[4]	[3]	
[S7N]Seven	[8]	[10]	[9]	[9]		[3]	[5]	
[WEB]Pag Institucional	[8]	[3]	[5]	[6]		[3]	[0]	
[DB]Base de Datos	[10]	[10]	[7]	[9]		[5]	[5]	
[SRV7]Serv Seven	[10]	[9]	[8]	[9]		[5]	[4]	
[DSKT]Desktop	[5]	[5]	[3]			[0]	[0]	
[ISP]Proveedor de Servicios Internet Claro	[9]	[4]	[3]	[6]		[4]	[0]	
[SC]Proveedor ETB	[9]	[4]	[3]	[6]		[4]	[0]	
[Locación]Sitio de Cobertura	[9]					[4]		
[ADM]Administrador	[8]	[1]	[5]			[3]	[0]	

Ilustración 33 Impacto Repercutido - Fuente Elaboración Propia

Similar que el análisis con la ***Tabla– Informe Impacto Acumulado***, podemos encontrar concentraciones con valor alto en ciertos indicadores.

Pero si observamos con detenimiento, podemos ver que esta tabla nos muestra los activos como tal. Y en que dimensión se encuentra la concentración más alta. Así mismo que activo repercute en otro superior.

Así mismo si queremos profundizar y averiguar que amenaza se encuentra asociada a dicho activo, realizaremos los pasos que se llevaron a cabo anteriores.

Ahora bien, para la estimación del impacto, es necesario analizar el valor de los impactos potencial y acumulado en las fases del proyecto. Lo anterior con el propósito de obtener un informe de impacto potencial y/o residual por activo.

Para ello nuevamente nos apoyaremos nuevamente con Pilar para sacar una gráfica por área y de esta manera observar como es el comportamiento de la mitigación del impacto al aplicar las salvaguardas adecuadas. Ver grafica Comportamiento Impacto.

Con la gráfica esta gráfica, podemos observar de una manera más clara el comportamiento del impacto.

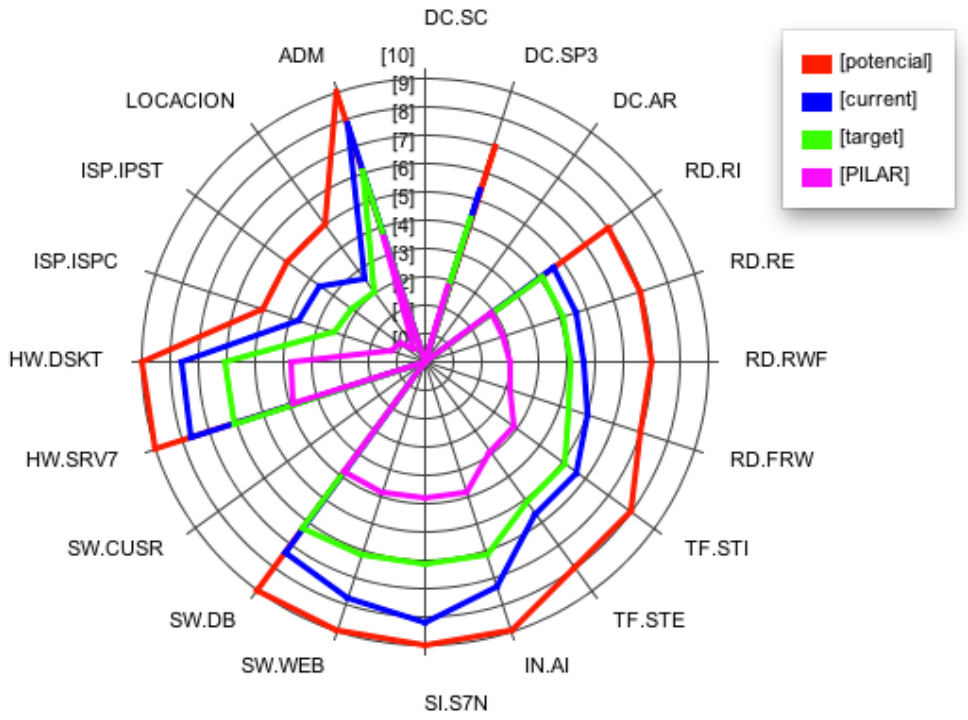


Ilustración 34 Comportamiento Impacto - Fuente Elaboración Propia

El impacto potencial (representado por el color verde, fase Target, la cual corresponde al análisis de riesgo), se encuentra en una escala 0 a 10.

Un ejemplo; el servicio [SI] S7N (Seven), nos muestra que el impacto se encuentra con un valor de 10.

Al implementar las salvaguardas el impacto, representado por el color violeta, el impacto acumulado disminuye progresivamente hasta lograr tener un nivel aceptable o en los mejores casos eliminarlo por completo.

Continuando con Seven, podemos ver que el indicador de impacto disminuir a un valor de 6 en la fase Target (color verde), la cual es la fase que se pretende lograr a corto plazo con el análisis de riesgos.

Por otra parte si seguimos verificando podemos observar que Seven podría disminuir a un valor de 4 en la fase Pilar (color violeta), la cual es una fase sugerida, más no obligatoria.

Ahora bien, teniendo en cuenta todos los pasos anteriores, hemos logrado obtener los datos necesarios para poder interpretar y establecer relaciones entre los activos y determinar cuáles necesitan ser atendidos con prioridad.

Según MAGERIT el resultado de esta tarea es el informe priorizado de activos según su nivel de magnitud de impacto.

Estas técnicas de análisis entre tablas se encuentran definidas en el libro 3 Guías y Técnicas de la metodología MAGERIT, pero Pilar como siempre ha sido de gran ayuda y nos ha permitido agilizar trabajo.

Tarea T2.3.2 Estimación del Riesgo

Continuando con la metodología, MAGERIT recomienda la elaboración de un catálogo, que permitiría determinar el riesgo potencial y acumulado en cada activo de la institución.

El propósito de esta tarea es obtener el informe de riesgo potencias y residual por activo.

Según MAGERIT, el riesgo en un activo, se estima teniendo en cuenta la pérdida de valor de este activo, al materializarse una amenaza. Esto se conoce como Degradación.

Es por ello que el riesgo depende de la frecuencia en la que un incidente pueda presentarse. Este aumenta con la presencia del impacto y la frecuencia.

Teniendo en cuenta el término de dependencia, en el cual un activo depende de otro superior, se presenta un riesgo **repercutido**. En este se toma en cuenta el

valor de un activo y la degradación causada por la amenaza y la frecuencia en la que se pueda presentar.

A continuación se puede observar en al siguiente tabla la catalogación de la frecuencia en al que un riesgo de puede presentar. Esta está dada en días meses y años.

La guía para la realización de esta tabla se encuentra en el libro tres Elaboración de Guías Técnicas de la metodología MAGERIT.

Frecuencia en valor	Simbología	Descripción
100	MA	A diario – muy frecuente
10	A	Mensualmente - frecuente
1	M	Una vez al año - normal
1/10	B	Cada dos años – poco frecuente

Tabla 11 Estimación de la Frecuencia - Fuente Elaboración Propia

Similar como se realizó en la estimación del impacto, para el riesgo, se analizarán los valores correspondientes riego potencial y residual en cada fase del proyecto y de esta manera obtener un informe de riesgos potencial y/o residual en cada activo.

Nuevamente apoyados en Pilar, obtenemos las siguientes tablas correspondientes a los riesgos acumulados y repercutidos.

activo	[D]	[I]	[C]	[A]
ACTIVOS	{7,7}	{7,7}	{6,9}	{7,1}
[PS] Procesos		{5,9}	{6,3}	{6,5}
[IS] Servicios internos	{5,4}	{7,7}	{6,9}	{6,2}
[E] Equipamiento	{7,7}	{5,9}		{7,1}
[SS] Servicio Subcontratado	{5,1}	{4,2}	{0,88}	{4,5}
[L] Instalaciones	{4,5}			
[P] Personal	{6,4}	{6,9}	{6,7}	

Ilustración 35 Riesgo Acumulado - Fuente Elaboración Propia

activo	[D]	[I]	[C]	[A]
ACTIVOS	{7,7}	{7,7}	{6,9}	{7,1}
[SC] Seguridad	{4,2}			
[SP3] Sub Proceso 3	{5,4}	{5,9}	{6,3}	{6,5}
[AR] Alimentacion Regulada	{7,7}			
[RI] Red Interna	{6,0}	{3,6}	{3,9}	{4,5}
[RE] Red Externa	{5,4}	{5,4}	{3,9}	{3,3}
[RWF] Red Inalambrica	{3,6}		{1,6}	{0,98}
[FRW] Firewall	{5,4}	{4,2}	{3,3}	{3,9}
[STI] Servicio Telefonia Interno	{6,4}	{4,0}	{4,4}	{6,2}
[STE] Servicio Telefonia Externo	{6,4}	{4,0}	{4,4}	{5,7}
[AI] Acceso a Internet	{6,4}	{6,5}	{3,2}	{6,2}
[S7N] Seven	{5,8}	{7,7}	{6,9}	{6,2}
[WEB] Pagina Institucional	{6,0}	{2,8}	{4,4}	{4,5}
[DB] Bases de Datos	{7,2}	{7,7}	{5,7}	{7,1}
[SRV7] Servidor Seven	{7,7}	{7,1}	{6,3}	{6,2}
[DSKT] Equipo de Escritorio - Estación de Trabajo	{4,2}	{4,0}	{3,2}	
[ISPC] Proveedor de Servicios de Internet - Claro	{7,1}	{4,2}	{3,9}	{5,4}
[IPST] Proveedor de Servicios de Internet - ETB	{7,1}	{4,2}	{3,9}	{5,4}
[LOCACION] Sitio de Cobertura	{7,1}			
[ADM] Administrador	{5,8}	{1,6}	{4,4}	

Ilustración 36 Riesgo Repercutido - Fuente Elaboración Propia

En la primera tabla, se puede observar el riesgo acumulado por Dominios de activos y su valor correspondiente en cada dimensión. La valoración en cada dimensión, corresponde al tomar el valor de degradación de cada amenaza de un activo y sumarle los valores de degradación y amenaza de los activos que lo preceden.

Por otra parte, en la segunda tabla podemos observar el riesgo repercutido por activos. Esta valoración se muestra como cada activo repercute al activo superior. Ver Ilustración Riesgo Nivel de Degradación Activos - (Informe Valores Repercutidos por Fase).

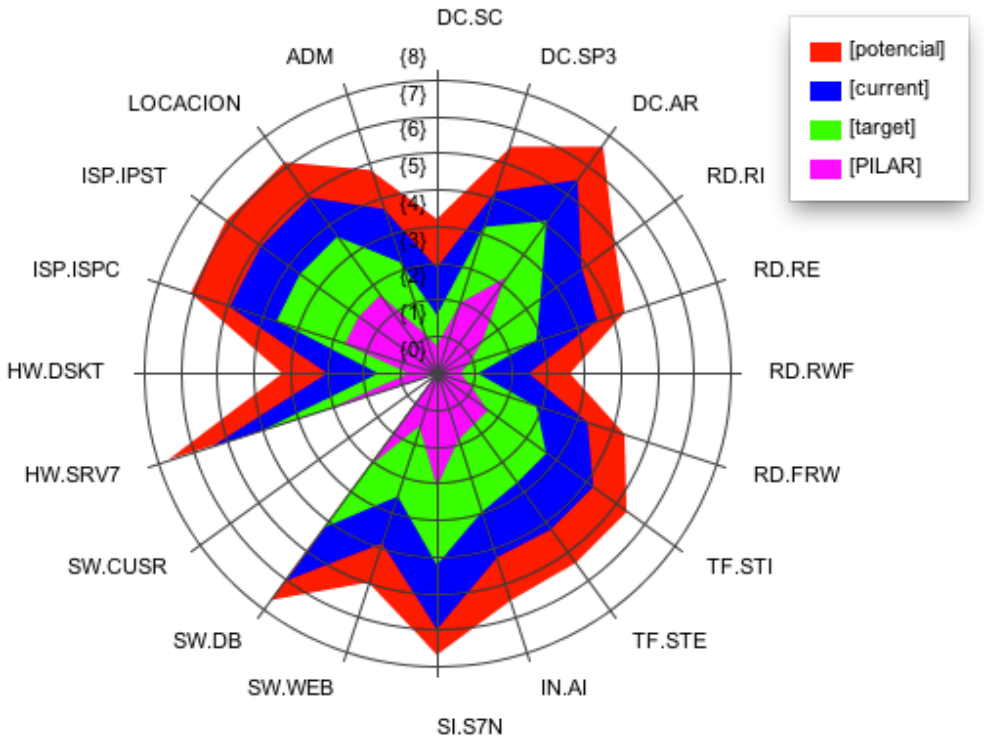
potencial | current | target | BIA | PILAR | resumen (impacto) | resumen (riesgo)

padre	D	hijo	D	amenaza	V	D	I	N	R
[DC.AR] Alimentacion Regulada	[D]	[HW.SRV7] Servidor Seven	[D]	[A.24] Denegación de servicio	[10]	100%	[10]	A	{7,7}
[SI.S7N] Seven	[I]	[SI.S7N] Seven	[I]	[A.13] Repudio (negación de actuaciones)	[10]	100%	[10]	A	{7,7}
[SW.DB] Bases de Datos	[I]	[IN.AI] Acceso a Internet	[I]	[A.13] Repudio (negación de actuaciones)	[10]	100%	[10]	A	{7,7}
[SW.DB] Bases de Datos	[I]	[SI.S7N] Seven	[I]	[A.13] Repudio (negación de actuaciones)	[10]	100%	[10]	A	{7,7}
[HW.SRV7] Servidor Seven	[D]	[HW.SRV7] Servidor Seven	[D]	[A.24] Denegación de servicio	[10]	100%	[10]	A	{7,7}
[SI.S7N] Seven	[I]	[SI.S7N] Seven	[I]	[A.22] Manipulación de programas	[10]	100%	[10]	A	{7,4}
[SW.DB] Bases de Datos	[I]	[SI.S7N] Seven	[I]	[A.22] Manipulación de programas	[10]	100%	[10]	A	{7,4}
[DC.AR] Alimentacion Regulada	[D]	[HW.SRV7] Servidor Seven	[D]	[E.24] Caída del sistema por agotamiento…	[10]	50%	[9]	A	{7,2}
[DC.AR] Alimentacion Regulada	[D]	[SW.DB] Bases de Datos	[D]	[E.24] Caída del sistema por agotamiento…	[10]	50%	[9]	A	{7,2}
[DC.AR] Alimentacion Regulada	[D]	[SW.WEB] Pagina Institucional	[D]	[A.24] Denegación de servicio	[10]	50%	[9]	A	{7,2}
[DC.AR] Alimentacion Regulada	[D]	[SW.DB] Bases de Datos	[D]	[A.18] Destrucción de la información	[10]	50%	[9]	A	{7,2}
[DC.AR] Alimentacion Regulada	[D]	[SW.DB] Bases de Datos	[D]	[A.24] Denegación de servicio	[10]	50%	[9]	A	{7,2}
[DC.AR] Alimentacion Regulada	[D]	[HW.DSKT] Equipo de Escritorio - Estació…	[D]	[E.24] Caída del sistema por agotamiento…	[10]	50%	[9]	A	{7,2}
[DC.AR] Alimentacion Regulada	[D]	[SW.WEB] Pagina Institucional	[D]	[E.24] Caída del sistema por agotamiento…	[10]	50%	[9]	A	{7,2}
[SI.S7N] Seven	[I]	[SI.S7N] Seven	[I]	[A.15] Modificación de la información	[10]	50%	[9]	A	{7,2}
[SW.DB] Bases de Datos	[D]	[SW.DB] Bases de Datos	[D]	[E.24] Caída del sistema por agotamiento…	[10]	50%	[9]	A	{7,2}
[SW.DB] Bases de Datos	[D]	[SW.WEB] Pagina Institucional	[D]	[A.24] Denegación de servicio	[10]	50%	[9]	A	{7,2}
[SW.DB] Bases de Datos	[D]	[SW.DB] Bases de Datos	[D]	[A.18] Destrucción de la información	[10]	50%	[9]	A	{7,2}
[SW.DB] Bases de Datos	[D]	[SW.DB] Bases de Datos	[D]	[A.24] Denegación de servicio	[10]	50%	[9]	A	{7,2}
[SW.DB] Bases de Datos	[D]	[HW.DSKT] Equipo de Escritorio - Estació…	[D]	[E.24] Caída del sistema por agotamiento…	[10]	50%	[9]	A	{7,2}
[SW.DB] Bases de Datos	[D]	[SW.WEB] Pagina Institucional	[D]	[E.24] Caída del sistema por agotamiento…	[10]	50%	[9]	A	{7,2}
[SW.DB] Bases de Datos	[I]	[IN.AI] Acceso a Internet	[I]	[A.15] Modificación de la información	[10]	50%	[9]	A	{7,2}
[SW.DB] Bases de Datos	[I]	[SI.S7N] Seven	[I]	[A.15] Modificación de la información	[10]	50%	[9]	A	{7,2}
[HW.SRV7] Servidor Seven	[D]	[HW.SRV7] Servidor Seven	[D]	[E.24] Caída del sistema por agotamiento…	[10]	50%	[9]	A	{7,2}
[HW.SRV7] Servidor Seven	[D]	[SW.WEB] Pagina Institucional	[D]	[A.24] Denegación de servicio	[10]	50%	[9]	A	{7,2}
[HW.SRV7] Servidor Seven	[D]	[HW.DSKT] Equipo de Escritorio - Estació…	[D]	[E.24] Caída del sistema por agotamiento…	[10]	50%	[9]	A	{7,2}
[HW.SRV7] Servidor Seven	[D]	[SW.WEB] Pagina Institucional	[D]	[E.24] Caída del sistema por agotamiento…	[10]	50%	[9]	A	{7,2}
[DC.AR] Alimentacion Regulada	[D]	[HW.DSKT] Equipo de Escritorio - Estació…	[D]	[A.24] Denegación de servicio	[10]	100%	[10]	M	{7,1}
[SW.DB] Bases de Datos	[D]	[HW.DSKT] Equipo de Escritorio - Estació…	[D]	[A.24] Denegación de servicio	[10]	100%	[10]	M	{7,1}
[HW.SRV7] Servidor Seven	[D]	[HW.DSKT] Equipo de Escritorio - Estació…	[D]	[A.24] Denegación de servicio	[10]	100%	[10]	M	{7,1}
[SW.DB] Bases de Datos	[A]	[SW.DB] Bases de Datos	[A]	[A.5] Suplantación de la identidad del us…	[9]	100%	[9]	A	{7,1}
[HW.SRV7] Servidor Seven	[I]	[IN.AI] Acceso a Internet	[I]	[A.13] Repudio (negación de actuaciones)	[9]	100%	[9]	A	{7,1}
[HW.SRV7] Servidor Seven	[I]	[SI.S7N] Seven	[I]	[A.13] Repudio (negación de actuaciones)	[9]	100%	[9]	A	{7,1}
[ISP.ISPC] Proveedor de Servicios de Int…	[D]	[HW.SRV7] Servidor Seven	[D]	[A.24] Denegación de servicio	[9]	100%	[9]	A	{7,1}
[ISP.IPST] Proveedor de Servicios de Inte…	[D]	[HW.SRV7] Servidor Seven	[D]	[A.24] Denegación de servicio	[9]	100%	[9]	A	{7,1}
[LOCACION] Sitio de Cobertura	[D]	[HW.SRV7] Servidor Seven	[D]	[A.24] Denegación de servicio	[9]	100%	[9]	A	{7,1}

Ilustración 37 Riesgo Degradación de Activos – Informe Valores Repercutidos por Fase - Fuente Elaboración Propia

Ahora bien, para poder observar mejor el comportamiento del riesgo, nos apoyaremos en Pilar y crearemos un informe grafico de tipo radial.

En esta grafica podemos observar las diferentes fases antes de implementar las salvaguardas (fases Potencial y Current) y después de implementarlos (fase Target y Pilar). Ver Gráfica – Comportamiento Riesgo.



Grafica –

Ilustración 38 Comportamiento Riesgo

Observando la gráfica anterior, podemos observar que el riesgo potencial se encuentra en una escalada 0 a 8, pero disminuye con la implementación de las salvaguardas en la fase Target o en la fase Pilar.

Estas salvaguardas permitirán reducir el riesgo residual o lograr que este indicador tenga un valor de cero.

Para ello, similar al análisis de impacto, las salvaguardas deberían revisarse periódicamente y de esta manera asegurar su efectividad.

Como se indicó anteriormente, el proceso de la estimación de riesgo, nos permite obtener un informe en el cual se puede observar por activo y dominios de activos, los riesgos repercutidos y acumulados que se presentan en las fases del proyecto.

A continuación podemos observar una fracción de este informe. Un informe completo será entregado a la Gerencia del TIC. **Anexo D.**

Los datos corresponden al grupo de activos Servicios Internos, donde se encuentran; Internet y Seven como sistema de información. **Ver Tablas.**

[IS] Servicios internos - Fase Potencial

activo	[D]	[I]	[C]	[A]	[T]
[IN] Internet	{5,4}	{7,7}	{5,7}	{6,2}	-
[IN.AI] Acceso a Internet	{5,4}	{7,7}	{5,7}	{6,2}	-
[SI] Sistemas de información	{5,4}	{7,7}	{6,9}	{6,2}	-
[SI.S7N] Seven	{5,4}	{7,7}	{6,9}	{6,2}	-

Tabla 12 Informe Estado del Riesgo Servicios internos – Fase potencial - Fuente Elaboración Propia

[IS] Servicios internos - Current (Actual)

activo	[D]	[I]	[C]	[A]	[T]
[IN] Internet	{4,0}	{6,2}	{3,7}	{4,7}	-
[IN.AI] Acceso a Internet	{4,0}	{6,2}	{3,7}	{4,7}	-
[SI] Sistemas de información	{4,6}	{7,0}	{6,1}	{5,5}	-
[SI.S7N] Seven	{4,6}	{7,0}	{6,1}	{5,5}	-

Tabla 13 Informe Estado del Riesgo Servicios internos – Fase Actual - Fuente Elaboración Propia

[IS] Servicios internos - Fase Target (Análisis de Riesgos)

activo	[D]	[I]	[C]	[A]	[T]
[IN] Internet	{2,9}	{5,2}	{2,6}	{3,7}	-
[IN.AI] Acceso a Internet	{2,9}	{5,2}	{2,6}	{3,7}	-
[SI] Sistemas de información	{3,0}	{5,2}	{4,3}	{3,7}	-
[SI.S7N] Seven	{3,0}	{5,2}	{4,3}	{3,7}	-

Tabla 14 - Informe Estado del Riesgo Servicios internos – Fase Análisis de Riesgos - Fuente Elaboración Propia

Similar que las gráficas de riesgo anteriores, en esta tabla se puede observar como disminuye el riesgo a medida que se implementan las salvaguardas.

Ahora bien, analizando un poco las tablas, Pilar nos muestra en la fase;

- **Potencial** el comportamiento del riesgo en un activo cuya amenaza se ha materializado y no se cuenta con salvaguarda alguna.
- **Current (actual),** Nos muestra el comportamiento del riesgo en cada activo, teniendo en cuenta las salvaguardas implementadas actualmente.
- El riesgo que se puede presentar si una amenaza se llega a materializar en dicho activo, Este es el escenario actual.
- **Target (Análisis de Riesgos)**, nos muestra el estado ideal. A lo que se aspira llegar teniendo en cuenta la fase Potencial y Actual. En esta fase se trata de llegar a un nivel en el cual los riesgos acumulados y repercutidos de disminuye a un indicador aceptable o se eliminan totalmente.

Todo esto teniendo en cuenta el estado actual del proyecto**.**

Existe una fase llamada Pilar. Esta fase es una fase sugerida por el aplicativo, en al cual se tratan de llevar a su minina expresión los indicadores de riesgo. Esta fase es sugerida mas no obligatoria.

El determinante de tomar presente la fase Target o Pillar, depende de los recursos actuales de la empresa y de las inversiones que esté dispuesta a hacer.

La fase Target, nos permite estimar el comportamiento del sistema a un nivel adecuadamente aceptable y en el cual ciertos riesgos que nos e han logrado eliminar, se encuentren bajo control.

ACTIVIDAD A2 .4 Caracterización de las salva guardas

Hasta este momento en los pasos anteriores hemos hablado de las salvaguardas, [14]pero no hemos tenido en cuenta la identificación de estas o su correspondiente valoración, debido a que deseamos estimar saber cómo sería el impacto o riesgo potencial si no se cuenta con acción alguna o si por el contrario se retira alguna salvaguarda.

Magerit en su libro dos en la sección "Catálogos de Salva Guardas", habla sobre 2 tipos de salvaguardas; Las que limitan el daño causado [15]o preventivas[16].

El éxito de una salvaguarda, se logra si es adecuadamente implementada. Es decir si se tiene claro cuál va a ser su función en el momento de una incidencia y si cuenta con controles que alerten a tiempo un fallo posible. Y por último si se le realizan los monitores adecuados.

Estas salvaguardas se agrupan en varios tipos de protecciones en los que podemos encontrar;

- Protección General.
- Protección de los servicios.
- Protección de la información.
- Protección de las aplicaciones informáticas (SW).
- Protección de los equipos Informatices (HW).
- Protección de las comunicaciones.
- Protección de los soportes de información.
- Elementos Auxiliares.

[14] Procesos o mecanismos tecnológicos, cuyo propósito es contribuir a la reducción de riesgos. Son todo tipo de acciones implementadas para prevenir la materialización de la

[15] Este tipo de salvaguardas se centran en identificar el ataque y limitar la degradación del activo.

[16] Este tipo de salvaguardas se enfocan en evitar la materialización por completo de la amenaza, lo cual reduce su frecuencia.

- Protección de las Instalaciones.
- Gestión del personal.
- Relaciones Externas.

Tarea T2.4.1 Identificación de las salvaguardas existentes

Pilar tiene en cuentan todas las anteriores al aplicar las salvaguardas en todos los activos.

Igual que en los puntos anteriores es necesaria la creación de unos catálogos que nos ayudaran a clasificar ciertos aspectos correspondientes a las salvaguardas y de esta manera realizar su valoración.

Para ellos es necesario tener en cuenta;

Aspectos de seguridad:

Estos aspectos ayudan a orientar hacia qué tipo de salva guarda será necesario aplicar. Así mismo estos tienen que verse reflejados en las diferentes fases del proyecto.

[G]	Gestión de la Seguridad
[P]	Normatividad Personal.
[T]	Soluciones técnicas a nivel de software hardware y comunicaciones.
[F]	Seguridad Física.

Tabla 15 - Aspectos de Seguridad - Fuente Elaboración Propia

Estrategias para reducir el riesgo:

Como se ha tratado en algunos apartados anteriores en la sección de Análisis de Riesgo, en los casos en los cuales no es posible evitar el riesgo, la meta es reducir la probabilidad de que este ocurra y de esta manera limitar la degradación hacia el activo, bien sea antes de que ocurra o estando preparado antes de que se conviertan en desastres.

Para ello se clasifican las siguientes estrategias;

[M]	Mixta.
[RF]	Reducción de frecuencia (prevenir).
[RI]	Reducción de impacto.
[D]	Detección

Tabla 16 Estrategias para Reducir Riesgo - Fuente Elaboración Propia

Estas estrategias deben contemplarse en las salvaguardas implementadas durante y después que la amenaza se materialice.

Tipos de Protección

Debido al tipo de amenaza sobre el activo, es posible clasificar los siguientes tipos de protección;

[AD]	Administrativa.
[DT]	Detección.
[PRI]	Prevención.
[CR]	Corrección.
[EL]	Eliminación
[IM]	De Minimización del impacto.
[DRI]	Disuasión
[CRC]	Recuperación
[MN]	Monitorización
[AW]	Concientización

Tabla 17 Tipo de protección - Fuente Elaboración Propia

Los anteriores deben formar parte de las salvaguardas aplicadas en las diferentes fases del proyecto. La implementación y efectividad de la protección deberá representarse en porcentaje teniendo en cuenta el tiempo estimado en cada fase.

Tarea T2.4.2 Valoración de las salvaguardas existentes

Niveles de madurez de la salvaguardas.

Para poder evaluar la eficacia de las salvaguardas, es necesario realizarlo teniendo en cuanta diferentes niveles de madurez, los cuales se encuentran propuestos en el CMM (Capability Matuiry Model – Modelo de Madurez de Capacidades), el cual permite calificar la madurez de los procesos basándose en el estándar ISO/IEC 21827:2002.

Eficacia	Nivel	Madurez	Significado

0%	L0	Inexistente	No existe
10%	L1	Inicial / ad hoc	Iniciado
50%	L2	Reproducible, pero intuitivo	Parcialmente realizado
90%	L3	Proceso definido	En funcionamiento
95%	L4	Gestionado y medible	Monitorizado
100%	L5	Optimizado	Mejora continua

Tabla 18 - Niveles de Madurez de Salvaguardas – Fuente Manual Pilar - Fuente Elaboración Propia

Pilar interpreta estos niveles como el estado actual en el que se encuentra la implementación de la salvaguarda, según la fase.

Al calificar estos niveles en las salvaguardas en la fase inicial del Análisis de Riesgo, se puede observar realmente que activos cuentan con salvaguardas y en qué nivel se encuentran. Así mismo que activo corre más riesgo y cuál debe ser atendido de manera inmediata.

Es importante tener claridad con respecto a cada uno de los niveles de madurez para poder realizar la calificación correspondiente;

[L0] Inexistente; en este nivel no se ha implementado o no existe ninguna salvaguarda.

[L1] Inicial; Aunque en este nivel la salvaguarda exista, no se realiza una adecuada gestión. Es posible que las organizaciones sobrepasen los tiempos de respuesta estipulado y no cumplan con los tiempos de respuesta acordados. Para este nivel es necesario contar con personal calificado. Por otra parte su éxito dependerá de suerte para ser efectivo.

[L2] Reproducible pero intuitivo: Similar que el nivel anterior la buena suerte y la buena voluntad son factor decisivos para que una salvaguardas sea eficaz y efectiva. Así mismo aunque el éxito es más frecuente que en el L1, todavía se sigue excediendo en cuanto a costes de inversión y tiempos de respuesta.

[L3] Proceso definido; Las salvaguardas existentes son gestionadas según normas preestablecidas que permiten reaccionar al personal ante un evento determinado. Su nivel de éxito s más alto, pero se pueden presentar imprevistos.

[**L4] Gestionable y Medible**: A diferencia de los niveles L1, L2 y L3 en los cuales la confianza se mide de manera cualitativa, en este nivel la dirección de la organización puede controlar de manera empírica el éxito de la salvaguarda.

Debido a que el funcionamiento de los procesos está bajo control mediante estadísticas. En esta fase es posible fijar metas cuantitativas de calidad.

[**L5] Optimizado:** Nivel ideal, Se concentra en la mejora continua de las salvaguardas y los procesos. Lo anterior al implementar mejoras tecnológicas e innovadoras. Permitiendo así, cumplir con los objetivos establecidos.

Por otra parte se realizan revisiones periódicas para observar el comportamiento en los objetivos y utilizarla como indicadores de gestión par a la mejora de los procesos.

Ahora bien, con lo anterior tenemos las herramientas necesarias para realizar la calificación adecuada en qué tipo de salva guarda aplicar, el tipo de protección y el nivel de madurez en el que se encuentra actualmente y en qué nivel se debería encontrar en cada fase del proyecto.

Nuevamente PILAR nos ayudará con las actividades referentes al proceso de esta información para obtener una calificación adecuada.

Para ello, adicional a los catálogos anteriormente descritos en las tablas, PILAR utiliza unos códigos y una clasificación en colores (semáforo) para evaluar y representar el nivel de madures en las salvaguardas aplicadas;

Eficacia	Códigos	Significado
0%	(espacio en blanco)	No se sabe, pero no se puede dejar así
0%	¿…?	No se sabe, pero es necesario conocer.
-----	N.A.	No aplica

Tabla 19 - Códigos Valoración Niveles de Madurez de Salvaguardas - Fuente Elaboración Propia

Blanco	Pilar deja esta casilla en blanco, si no posee la información suficiente para realizar una recomendación.
Gris	Pilar coloca este color si la salvaguardas no se aplica
Negro	Si la madures de la salvaguarda cuenta con el símbolo ¿…?
Rojo	La madurez es muy muy pobre y el riesgo de materializarse una

	amenaza es muy alto. Se debe prestar atención urgentemente.
Amarillo	Aunque la madurez no se encuentra en un nivel tan crítico, debe ser mejorada
Verde	Al nivel de madurez es suficiente (estado ideal).

Tabla 20 Clasificación de Colore (Semáforo) Niveles de Madurez de Salvaguardas - Fuente Elaboración Propia

Ahora bien, como los pasos anteriores, PILAR, puede realizar una calificación y valoración automática teniendo en cuenta todos los criterios de los catálogos de las tablas anteriores.

La valoración puede hacerse por dominio de activo o a cada activo de manera individual.

En algunos casos dependiendo como se encuentre configurada PILAR, al llegar a este paso se podrán encontrar ya unos valores propuesto por PILAR en las diferentes fases del proyecto.

Tomaremos como ejemplo el dominio de activos correspondiente a **[IS] Servicios Internos**. Lo anterior ya que Seven pertenece a este dominio.

En las siguientes imágenes podemos observar la identificación de salvaguardas para el dominio **[IS] Servicios Internos**. Ver tabla identificación de las salvaguardas existentes.

Así mismo podemos observar la valoración en cuanto a niveles de madurez de las salvaguardas en el dominio de activos **[IS] Servicios Internos.** Ver tabla valoración de las salvaguardas.

aspecto	tdp	salvaguarda	dudas	fuente	come…	recom…	on / off	aplica…
		SALVAGUARDAS						
G	PR	[H] Protecciones Generales						n.a.
G	PR	[D] Protección de la Información						n.a.
G	EL	[K] Gestión de claves criptográficas						n.a.
G	PR	[S] Protección de los Servicios						n.a.
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)						n.a.
G	PR	[HW] Protección de los Equipos Informáticos (HW)						n.a.
G	PR	[COM] Protección de las Comunicaciones						n.a.
G	PR	[IP] Puntos de interconexión: conexiones entre zonas de confianza						n.a.
G	PR	[MP] Protección de los Soportes de Información						n.a.
G	PR	[AUX] Elementos Auxiliares						n.a.
F	PR	[L] Protección de las Instalaciones						n.a.
P	PR	[PS] Gestión del Personal						n.a.
G	AD	[G] Organización						n.a.
G	RC	[BC] {or} Continuidad del negocio						n.a.
G	AD	[E] Relaciones Externas						n.a.
G	AD	[NEW] Adquisición / desarrollo						n.a.

Ilustración 39 Identificación de las Salvaguardas Existentes - Fuente Elaboración Propia

aspe…	tdp	salvaguarda	dudas	fuente	come…	reco…		current	target	BIA	PILAR
		SALVAGUARDAS									
G	PR	[H] Protecciones Generales				8		L0-L2	L2	L2	L2-L5
G	PR	[S] Protección de los Servicios				7		L1	L2	L2	L2-L4
G	std	[S.1] Se dispone de normativa relativa al uso de los servicios				3		L1	L2		L3
G	AD	[S.2] Se dispone de un inventario de servicios				2		L1	L2	L2	L2
G	IM	[S.A] Aseguramiento de la disponibilidad				4		L1	L2	L2	L2-L3
G	PR	[S.start] Aceptación y puesta en operación				4		L1	L2	L2	L2-L3
T	EL	[S.SC] Se aplican perfiles de seguridad				7		L1	L2	L2	L3-L4
G	EL	[S.op] Explotación				5		L1	L2	L2	L3
G	EL	[S.CM] Gestión de cambios (mejoras y sustituciones)				3		L1	L2	L2	L2-L3
G	EL	[S.end] Terminación				5		L1	L2	L2	L2-L3
G	EL	[S.b] Seguridad del comercio electrónico				4		L1	L2	L2	L2-L3
G	EL	[S.TW] Teletrabajo				5		L1	L2	L2	L2-L3
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7		L1-L2	L2	L2	L2-L4
G	PR	[COM] Protección de las Comunicaciones				9		L2	L2	L2	L2-L5
G	PR	[AUX] Elementos Auxiliares				6		L0	L2	L2	L3-L4
G	AD	[G] Organización				6		_-L1	L2	L2	L2-L4
G	RC	[BC] {or} Continuidad del negocio				5		L1	L2	L2	L3
G	AD	[E] Relaciones Externas				6		L1	L2	L2	L2-L4
G	AD	[NEW] Adquisición / desarrollo				5		L1	L2	L2	L2-L3

Ilustración 40 Valoración de las salvaguardas - Fuente Elaboración Propia

Como resultado se obtiene un informe donde se identifican las salvaguardas y el nivel de madurez.

Dominio de seguridad: [IS] Servicios Internos

salvaguarda	A	R	[current]	[target]	[PILAR]
[H.IA] Identificación y autenticación	G	7	L1	L2	L3-L4
[H.IA.1] Se dispone de normativa de identificación y autenticación	G	4	L1	L2	L3
[H.IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación	G	4	L1	L2	L3
[H.IA.3] Identificación de los usuarios	G	5	L1	L2	L3
[H.IA.3.1] Cada usuario recibe un identificador exclusivo (no compartido)	G	5	L1	L2	L3
[H.IA.3.2] La identificación del usuario no indica ni su función ni su nivel de privilegios	G	3	L1	L2	L3
[H.IA.3.3] Las cuentas de invitados están sometidas a un control estricto	T	3	L1	L2	L3
[H.IA.4] Cuentas especiales (administración)	G	7	L1	L2	L3-L4
[H.IA.4.1] Hay cuentas específicas para administradores del sistema	G	5	L1	L2	L3
[H.IA.4.2] Hay cuentas específicas para administradores de seguridad	G	7	L1	L2	L4
[H.IA.4.3] Hay cuentas específicas para actividades de auditoría	G	4	L1	L2	L3
[H.IA.4.4] Las cuentas especiales están sujetas a procesos específicos de gestión	G	3	L1	L2	L3
[H.IA.5] Gestión de la identificación y autenticación de usuario	G	7	L1	L2	L3-L4
[H.IA.5.1] Se mantiene un registro de todos los usuarios con su identificador	G	4	L1	L2	L3
[H.IA.5.2] Alta, activación, modificación y baja de las cuentas de usuario	G	7	L1	L2	L3-L4

Tabla 21 - Informe Salvaguardas Dominio de Activos Servicios Internos - Fuente Elaboración Propia

La tabla anterior, corresponde la identificación de salvaguardas y el nivel de madurez para los servicios internos, donde se encuentra catalogado Seven. Un informe completo será entregado a la Gerencia del TIC.

Es posible observar que en la fase actual (Current), existen salvaguardas, pero con niveles de madurez muy bajos.

Hay que tener en cuenta que pilar en esta fase realiza una calificación tomando el peor de los escenarios para poder evaluar el nivel de criticidad si se llega a presentar.

Así mismo podemos observar como los niveles de madurez van aumentando en cada fase con la implementación y gestión de las salvaguardas.

Pilar se apoya en diferentes técnicas propuestas por la metodología MAGERIT, para poder obtener estos resultados.

Estas se pueden clasificar en 2 categorías;

- Específicas:
  - Análisis mediante tablas.
  - Análisis Algorítmico.
  - Arboles de ataque.
- Generales;
  - Análisis Cotos beneficio.
  - Diagrama de flujos de datos.
  - Diagrama de Procesos.
  - Planificación de proyectos.
  - Valoración Delphi.

13.4.2. Análisis de Resultados y BIA

Retomando todos los pasos anteriores, podemos resumir que para poder realizar un análisis de riesgos, debemos tener en cuenta;

- El activo a evaluar
- Su dinámica con lo demás activos. Es decir si este activo depende de otros y viceversa.
- Aunque todos los activos de la empresa son bienes muy valiosos para la empresa, valorar dichos activos no ayudara a catalogar cuales tienen más peso en la empresa para ciertos procesos.
- Detectar ciertas amenazas en dichos activos y valorarlas, nos ayudara a analizar que activos son más propensos a un riesgo y cuáles deben ser atendidos de manera inmediata debido a su importancia en el proceso de la organización.
- La aplicación de salvaguardas en las diferentes fases del proyecto nos ayudaran a evaluar, con que contamos, si realmente existen acciones reales para afrontar estos riesgos y en el caso de no existir que tato es

posible mitigar ese riesgo para que no cause un impacto tan dramático en la organización.

Como se puede observar todo funciona como una cadena de engranajes en los cuales al anterior es vital para que el siguiente funcione.

Con estos resultados poseemos ya una visión más aterrizada y concreta del estado actual en la organización.

Por ejemplo, podemos observar que aunque el nivel de madurez en la fase actual en las mayoría de salvaguardas se encuentra enfocado en L1. Lo cual es un punto a favor ya que aunque se encuentren muy jóvenes por lo menos ya se han iniciado procesos para determinar que hacer.

Así mismo si observamos, la gráfica de Impacto, que activos como el servidor Seven, el ERP Seven, la Base de Datos así como la Administración de los mismos, generarían un gran impacto en la organización ya que se encuentran en escalas de 0 a 10.

De igual manera si observamos la gráfica de Riesgo, podemos observar que la frecuencias de la amenaza para convertirse en un riesgo en dichos activos se encuentra en una escala de 0 a 8, lo cual es un valor alto.

Así mismo el riesgo acumulado de algunos de los activos anteriores se encuentra en niveles de 0 a 7. Lo cual representa un riesgo alto.

Teniendo en cuenta esto, lo primero que es necesario hacer es poner mucha atención a estos indicadores altos que PILAR coloca en color rojo y trabajar en un **Plan de Mitigación** el cual tiene como objetivo primario estructurar en un lapso de tiempo las acciones y procedimientos de seguridad para aquellos activos críticos teniendo en cuenta los recursos actuales de la organización.

Este plan se basa en 4 aspectos fundamentales que tiene que ser aceptados por la dirección de la organización; evitación para lograr las condiciones que ayudan a que el riesgo este presente, aceptación reconocer la existencia de estos activos, mitigación para reducir al mínimo la probabilidad de un riesgo o impacto y desviación para trasferir este riesgo a un tercero (organización especializada), cuando se requiera.

Ahora bien, cuando hablamos de estructurar lapsos de tiempo para tomar acciones, debemos tener en cuenta que procesos o activos son críticos o esenciales en cuanto a su recuperación y que tiempo tolerables de inactividad pueden aceptarse en cada uno de ellos sin ver comprometida la operación de

la organización.

Lo anterior debido a dependiendo de la organización hay procesos o activos más exigentes que otros en sus tiempos de respuesta o ejecución. En concreto es necesario saber por cuánto tiempo puede dejar de funcionar un proceso o un activo sin que esto represente pérdidas financieras, quejas en clientes internos y externos o penalizaciones a nivel de contratos o legales.

Hasta que nivel básico la organización se encontrara operativa, para poder responder a todas sus obligaciones y ser funcional, mientras otros procesos, activos o recursos tecnológicos se encuentran inactivos.

Básicamente, es detectar que activos o procesos permiten sobrevivir a la organización. Esto implicara clasificar a todos aquellos activos que según su prioridad de recuperación.

Estos tiempos de recuperación se deben medirse teniendo en cuenta que las consecuencias que hay por no poder ejecutarlos.

En concreto ***lo que busca el BIA son tiempos de recuperación***, ya que toma tiempo restablecer las funciones o activos críticos de la organización para que estén operativos nuevamente.

- **RPO (Punto Objetivo de Recuperación):** Este parámetro nos ayuda a identificar qué cantidad de datos o información la organización puede perder en un rango de tiempo determinado y que protección se requiere para evitarlo.

  Por ejemplo, su uso ayuda a evaluar si los proceso de copias de respaldo se realizan en horas adecuadas y de esta manera si se presenta un colapso del sistema tratar de recuperar hasta el último bit actualizado.

- **RTO (Recovery Time Objetive**); Es el tiempo objetivo de recuperación o tiempo máximo de inactividad. Permite determinar cuento puede la organización permanecer sin ejecutar una activo.

  Su uso ayuda a determinar cada cuanto se deben hacer procesos de copias de respaldo o backups o en ciertos casos que infraestructura es necesaria para reiniciar operaciones.

- **MTD (maximun Tolerable Downtime);** Es el tiempo máximo de inactividad que una empresa puede tolerar si un activo, función o

proceso se encuentra ausente o no disponible. Se encuentra representado por la siguiente formula; ***MTD = RTO + WRT***

- **WRT (Work Recovery Time) Tiempo de Trabajo de Recuperación**, comprende el rango de tiempo o segmento antes del tiempo máximo de actividad o MTD. Es decir si se tiene un MTD de 3 días, el RTO sería el día 1 y el WRT serían los días 2 y 3.

En conclusión los pasos a seguir para poder obtener estos tiempos se podrían resumir en los siguientes;

1. Paso RPO La máxima cantidad de información que se puede perder de acuerdo al cronograma de realización de copias de respaldo y/o necesidades de información que se presenten.
2. Paso RTO Tiempo requerido para que los sistemas críticos de la Organización estén operando nuevamente.
3. Paso WRT Tiempo requerido para recuperar la información perdida (Basado en el RPO), así como de ingresar al sistema todos los datos que se generaron durante la caída del sistema.
4. Paso MTD La duración del RTO mas el WRT

El resultado de los pasos anteriores, será una tabla en la cual se establecen los tiempos máximos tolerables de inactividad para los activos y de esta manera determinar hasta qué punto es posible restaurar el sistema, por medio de los Planes de Continuidad, Recuperación y Disponibilidad.

Tanto el RPO como el RTO son tiempos que se determinan teniendo en cuenta los resultados obtenidos en el Análisis de Riesgo.

Este proceso de valoración se realiza de manera manual. Es por ello que fue importante reunirse con la Dirección de TIC y de esta manera determinar dichos tiempos.

Lo anterior, debido a que este aspecto va muy relacionado con procedimientos y aspectos políticos de la organización.

RPO

Para poder determinar el **RPO (Punto Objetivo de Recuperación),** es necesario analizar el proceso de creación y restauración de copias de respaldo.

De esta manera se podrá tener un panorama y tratar de identificar, que cantidad

de datos o información la organización puede perder en un rango de tiempo determinado.

A continuación se describe brevemente como es el proceso de restauración de copias de respaldo realizado por la Gerencia del TIC.

Esta información se obtuvo después de realizar dos reuniones con personal de la Gerencia del TIC

Una vez se ha identificado la información a la cual se debe realizar una copia de respaldo, un agente de back up en cada servidor se encarga de tomar estos registros y enviarlos a una librería virtual en el disco duro del servidor de aplicaciones. Este agente de back ups se llama Data Protector.

Este proceso se hace todos los días. Se cuentan con 4 servidores. En cada uno de estos servidores se guarda información de un sistema específico.

Las copias se realizan de acuerdo al volumen de información a respaldar.

El primer servidor inicia las copias de respaldo a las 9 P.M y el ultimo servidor a las 5 A.M.

Existen dos tipos de proceso de back up;

- El primer proceso se conoce como incremental. Este se realiza todas las noches entre semana. En este proceso se detectan que archivos han cambiado y se actualizan en el disco donde el data protector guarda el back up.
- El segundo proceso conocido como full back up, se realiza solo los fines de semana. A diferencia del incremental, se realiza copia total de los datos.

Toda esta programación se gestiona desde un servidor central donde se encuentra el Data protector.

Al día siguiente se hace una copia de todos estos archivos de respaldo en medios magnéticos.

Posteriormente, se llena una serie de formatos, para enviar estos medios magnéticos a una empresa externa responsable de velar por estas copias magnéticas. El nombre de esta empresa es SETECSA.

Esta empresa envía las copias de respaldo a unas instalaciones donde se categoriza según ciertos parámetros.

Una vez se requieran ciertas copias de respaldo, se solicita a SETECSA, quien posteriormente hará llegar a las instalaciones de la universidad la copia de backup solicitada.

El tiempo estimado de llegada de una copia, depende del nivel de urgencia. Si es muy urgente, la copia solicitada deberá llegar en 2 horas. Si no es muy urgente la copia llegara a las instalaciones en 4 horas.

La discriminación en cuanto Urgente y Medio Urgente , en cuanto a la solicitud de las copias de respaldo depende de le temporada Alta o Medio Baja, por la cual la organización está pasando.

Básicamente se cataloga de la siguiente manera;

Temporada Alta: Cada semestre en el cual los estudiantes realizan los pagos de las matriculas, pagos de nómina, pagos a proveedores.

Temporada Media Baja: Cada Ciclo académico (3 meses) ,en los cuales estudiantes de postgrados o maestrías realizan pagos o se realizan procesos de compra de papelería.

Bien hasta este punto ya podemos contar con ciertas variables de tiempo en la cuales las copias de respaldo deben llegar;

- Urgente 2 horas
- Medio Urgente 4 horas

Ahora hablemos de los datos, cada noche se hacen copias de respaldo;

- Copia de Respaldo Incremental, donde se actualizan archivos. Es un proceso de Backup Parcial.
- Copia de Respaldo Full Back up donde se hace una copia de respaldo completa de los datos.

Finalmente logramos detectar tiempo o momentos críticos en los cuales el tráfico de información es más alto (registro y consultas de datos).

Con estos datos y con la ayuda de una tabla, trataremos de determinar nuestro RPO.

Temporada	Llegada de Backups / Horas	% Mínimo de datos recuperados para que Seven funcione adecuadamente según los procesos	% Actual de datos que se pueden recuperar teniendo en cuenta procesos de Backup	% de datos perdidos RPO
A	2	90	55	35
MB	4	80	50	30

Tabla 22 RPO - Fuente Elaboración Propia

Para poder determinar estos porcentajes, se tomaron en consideración criterios como la temporada y el nivel de flujo de información en dicho tiempo.

Adicional a ellos se tomaron en cuenta aspectos a nivel, jurídico, consecuencias de no pagos a clientes, entre otros.

Así mismo se evaluó, tomando en consideración el peor de los escenarios, en el cual es posible la perdida, prácticamente en su totalidad, de los datos registrados dúrate el día.

Con la tabla anterior podemos observar que los porcentajes de datos perdidos en Seven, se encuentran entre 30% y 35%. Porcentajes que aún pueden generar gran impacto en la empresa.

RTO

Para poder determinar el RTO (**Recovery Time Objetive**) , es necesario tener en consideración el tiempo (horas o días) de inactividad de un activo. En este caso los activos de los cuales depende Seven y los que dependen de este.

Para ello, primero es necesario evaluar un rango de escalones de interrupción en días, en los cuales se pueda presentar resta interrupción.

Posteriormente ser necesario valorar a cada activo según criterios de impacto que

pueda generar su inactividad.

El resultado será una tabla en la cual el nivel de impacto por la inactividad en un rango de tiempo.

Para ello utilizaremos PILAR para el apoyo de procesamiento de datos.Ver grafica

Ilustración 41 - Escalones de Interrupción - Fuente Elaboración Propia

Se ha seleccionado un rango de escalones de interrupción máximo de 10 días.

Este escalón de interrupción se definió tomando en consideración aspectos como la infraestructura tecnología, recurso humano y experiencias anteriores.

Ahora bien, para sacar el RTO, debemos valorar nuestros activos, según la escala de interrupciones que hemos seleccionado.

A diferencia del Análisis de Riesgos, relazaremos valoración teniendo en cuenta los escalones de interrupción.

Nuestra valoración la podemos realizar por dominio la cual nos permite valorar un grupo de activos todos con un mismo valor o realizar una valoración por activo.

Para efectos de este proyecto realizaremos la valoración por dominio. Ver gráfica,

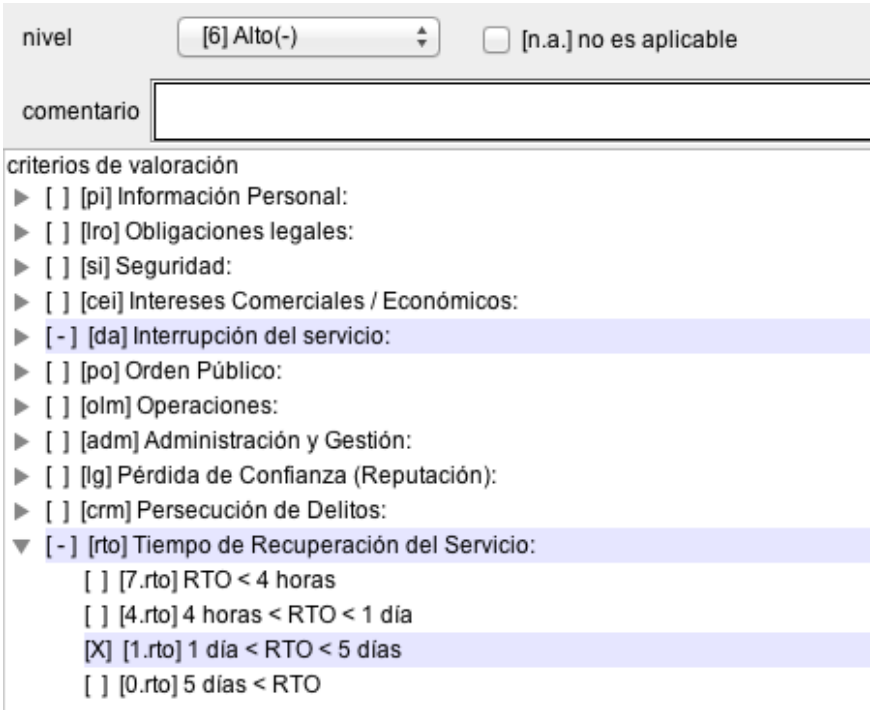


Ilustración 42 - Valoración RTO Activo Seven

Como podemos observar en la gráfica anterior, en el día 1 (1d), seleccionamos como RTO un rango no menor de 1dias ni mayor a 5 días en inactividad para el ERP Seven, con un nivel de criticidad para ese día de 6 Alto.

El RTO en cada activo se ha tomado en consideración información obtenida por la Gerencia del TIC.

La misma organización o proceso en este caso, es el que ayuda a determinar tiempos máximos de inactividad en los escalones máximos de interrupción.

Una vez realizada la valoración correspondiente, se obtiene el siguiente informe. Ver imagen.

activo / dominio de seguridad	[1d]	[2d]	[3d]	[4d]	[5d]	[6d]	[7d]	[8d]	[9d]	[10d]
[01] seven										
[essential] Activos esenciales	[6]	[7]	[8]	[9]						[9]
[DC] Data Center										
[SC] Seguridad	[3]	[4]	[5]	[6]						
[SP3] Sub Proceso 3	[4]	[5]	[6]	[7]						[9]
[RD] Redes										
[TF] Telefonia										
[AI] Acceso a Internet	[5]	[6]	[7]	[8]						[9]
[S7N] Seven	[6]	[7]	[8]	[9]						
[DB] Bases de Datos	[6]	[7]	[8]	[9]						
[SRV7] Servidor Seven	[6]	[7]	[8]	[9]						
[ISP] Proveedor de Servicio										
Dominios de seguridad										
[base] Base										
[PS] Procesos	[4]	[5]	[6]	[7]						[9]
[IS] Servicios Internos	[6]	[7]	[8]	[9]						[9]
[E] Equipamiento	[6]	[7]	[8]	[9]						

Ilustración 43 Valoración por Dominios de Activo - Fuente Elaboración Propia

WRT

Para obtener el **WRT (Tiempo de Trabajo de Recuperación),** tomaremos en cuanta aspectos como la temporada el tiempo de llegada de las copias de respaldo y el porcentaje necesario para que el sistema, en este caso Seven, se encuentra funcional, así como el tiempo necesario para lograr ese escenario y no genere un impacto dramático en los demás procesos.

Por otra parte teniendo en cuenta el estado actual de los procesos y la infraestructura, cuanto porcentaje de la información es posible recuperar y cuantos días se toman para lograr el escenario ideal.

Para ello crearemos la siguiente tabla.

Temporada	Llegada de Backups / Horas	% Mínimo de datos recuperados para que Seven funcione adecuadamente según los procesos	Días necesarios para lograr este nivel Escenario ideal WRT	% Actual de datos que se pueden recuperar teniendo en cuenta procesos de Backup	Días necesarios para lograr este nivel Escenario actual WRT
A	2	90	1 - 2	55	10
MB	4	80	2 -3	50	8

Tabla 23 WRT - Fuente Elaboración Propia

13.5. ENTREGABLES

Ahora bien, es momento de tomar todos estos datos y unirlos para poder realizar un análisis que nos permita tomar acciones.

13.5.1. PLAN DE CONTINUIDAD Y RECUPERACIÓN DE DESASTRES

El Plan de Continuidad y Recuperación de Desastres son el conjunto de estrategias y procedimientos para restaurar la normalidad del flujo de trabajo del negocio.

Para poder definir un plan de Continuidad y Recuperación de desastres, es necesario como primera medida, realizar los siguientes pasos iniciales;

- Análisis de Riesgo.
- Realizar un BIA

Los anteriores ya fueron realizados en los apartados anteriores.

Como segunda medida, establecer con los recursos actuales y con las metas deseadas definir;

- Un comité de miembros que supervise y tome acciones en el momento indicado.
- Con base a los tiempos tolerables, definir niveles de recuperación del activo. En este caso Seven.
- Establecer los Recursos necesarios para ello.
- Determinar políticas de monitoreo y seguimiento

El resultado es un informe de gerencia para la dirección de la organización.

Para ello realizaremos una plantilla de entrega.

Universidad EAN	Plan de Disponibilidad y Recuperación de Desastres	Versión	1.0
		Activo	ERP Seven

Proceso:	**Responsable:**
Gerencia de Tecnologías de la Comunicación e Información	Gerente TIC Proveedor de Servicios
Objetivo:	
Definir estrategias y procedimientos para restaurar la normalidad del flujo de trabajo del negocio.	

1. **Alcance:**

   En el presente documento se pretende identificar los aspectos críticos, que implican un riesgo para la continuidad de los procesos, así mismo determinar estrategias y procedimientos que disminuyan dicho riesgo y permitan restaurar a un nivel aceptable el ERP Seven, de manera que no genere un impacto dramático en los demás procesos.

2. **Estado actual:**

2.1. Datos de Entrada

Una vez realizada la captura de datos y entrevistas necesarias, se realizaron los siguientes análisis y estudios;

- **Análisis de Riesgos**: En el cual se valora el activo en este caso Seven, así como los otros activos de los cuales él depende el y de los activos que dependen de él.

  Lo anterior con el propósito de definir el estado actual de los activos. Cuál de estos es más importante y cual está más propenso a un riesgo debido a una posible amenaza.

  Definir qué tipos de salvaguarda implementar en cada fase para tratar de minimizar el riesgo y el impacto.

- **BIA:** Con el cual de logra definir qué días y que porcentaje de información es necesario para poder restaurar a un nivel aceptable el ERP Seven sin que se vean afectados los demás procesos. Que tanto porcentaje de información se puede perder en un tiempo determinado.

2.2. Análisis de los Resultados

Una vez procesados y cuantificados los datos, se logró determinar;

- Que el ERP Seven se encuentra con un nivel de calificación 7, en cuanto a el riesgo de materialización de una posible amenaza de tipo;
    - Humano: Acceso de personal autorizado con propósitos malintencionados.
    - El sistema no cuenta con una parametrización adecuada que permita que sus tiempos de respuesta sean más eficientes. Lo cual genere retrasos en los tiempos de respuesta.

- Existe un riesgo potencial alto debido a los activos de los cuales depende Seven. Dentro de estos encontramos, el Servidor Seven, la Base de Datos y el Data center

- El nivel de impacto en la organización es muy alto, al momento de verse afectado este activo, debido a la materialización de una amenaza.
- Los procesos de creación de copias de respaldo, no permiten el 100% de la restauración de los datos, al momento de presentar se un incidente que implique pérdida total de los mismos.

- Los tiempos actuales de recuperación de información que se necesitan para restaurar el sistema ERP Seven a un nivel aceptable para no generar una interrupción grave en el servicio son de 90% pero se encuentran en 55% en temporada alta y 80% pero se encuentran en 50%

- Los tiempos actuales tolerables (3 y 4 días) de inactividad del activo Seven, sobrepasan los ideales 5 a 10 días, en el peor de los casos.

- Por otro lado actualmente se cuentan implementadas ciertas salvaguardas, que ayudan a la disminución de un riesgo por una posible amenaza. Pero se encuentran en una fase de madurez media o baja.

- No se cuenta con un comité estructurado de personal, que permita una reacción inmediata para coordinar y realizar las acciones necesarias al momento de presentarse un incidente que implique la interrupción prolongada o recuperación de datos del ERP Seven.

3. Datos de Salida

3.1. Recomendaciones

Aunque el objetivo ideal en todos los casos siempre lograr el 100% de la recuperación del sistema y lograr el total de la funcionalidad, es importante tener en cuenta que esto implica en algunos casos la adquisición de nuevos recursos.

Tomando en cuenta los recursos actuales (a nivel tecnológico, Humano y protocolos establecidos) con los cuales cuenta la Universidad EAN, es posible establecer ciertos parámetros que ayuden a mejorar los niveles de riesgo, tiempos de respuesta y porcentajes de recuperación del sistema ERP Seven.

3.2. Parámetros Recomendados

- Definir un comité que se encuentre conformado por; el administrador del Servidor, de seguridad IT, administrador de Redes y un Gerente de Proyecto.

  Lo anterior con el propósito de contar con un grupo interdisciplinario que permita responder en el menor tiempo posible, bajo una coordinación logística.

- Definir protocolos de monitorización en cuanto a los accesos del ERP Seven, con el propósito de evitar o minimizar los riesgos de manipulación mal intencionada por parte del personal autorizado.

- Verificar con los desarrolladores de la aplicación, en este caso Digital Ware, los ajustes a la medida del sistema necesarios para un adecuado desempeño del mismo, evitando así información truncada o demora en la transacción de la información.

- Evaluar la posibilidad de implementar servidores virtuales dedicados, para realizar copias de respaldo parciales en las temporadas altas de transacción de información.

  Lo anterior con el propósito poder contar con registros actualizados de información en el menor tiempo posible. Esto evitaría realizar cambios en los protocolos de generación de copias de respaldo y envió de estas a terceros.

  Así mismo ayudaría a reducir ;

- El tiempo necesario para la llegada de las copias de respaldo y su proceso de restauración.

- Los tiempos actuales de inactividad del activo Seven.

- Reducir a un nivel aceptable la escala de interrupción de días necesarios para restablecer el sistema en los peores casos, de 5 a 10 días a 5 días.

- Incrementar los niveles de datos recuperados para lograr una adecuado funcionamiento del ERP Seven de 35% hasta un 65% 70%.

- Implementación de un servidor dedicado que sirva como Mirror espejo, que sea activado en el menor tiempo posible cuando el servidor de producción se encuentre inactivo. Lo anterior ayudaría a disminuir los tiempos de inactividad del ERP Seven, y reduciría el nivel de impacto en lo demás procesos de la organización.

- Realizar seguimiento de las salvaguardas existentes, para realizar los ajustes necesarios y de esta manera lograr disminuir los riesgos y el impacto en cada fase propuesta.

4. Tiempo de implementación

El tiempo de implementación del plan, está ligado a los recursos y aspectos recomendados que se deseen implementar.

Para lograr un escenario ideal con tomando en cuenta las recomendaciones propuestas;

- 3 meses para realizar documentación de los procesos a realizar.
- 2 meses, para implementar un programa de socialización y concientización en la organización.
- 4 y medio meses para implementar, progresivamente teniendo en cuanta los recursos que esto implique.
- 3 meses para ajustes.

Reviso:
Aprobó:

13.5.2. PLAN DE DISPONIBILIDAD

Universidad EAN	Plan de Continuidad	Versión	1.0
		Activo	ERP Seven

Proceso:	**Responsable:**
Gerencia de Tecnologías de la Comunicación e Información	**Responsable:** Gerente de TIC Proveedor de Servicios
Objetivo:	
Definir técnicas y procedimientos para cumplir y asegurar que todos los servicios de TIC estén dentro de los tiempos y niveles acordados de disponibilidad, manteniendo los objetivos según el Plan Estratégico Institucional.	

1. Alcance

El presente documento pretende determinar componentes de fallas en el ERP Seven, resultante de la materialización de posibles amenazas.

Así mismo, los aspectos necesarios que permitan asegurar la disponibilidad de las infraestructura de TI que respalda al ERP Seven, así como la mejora de los servicios de la Gerencia de TIC.

2. Datos de Entrada

Antes de realizar cualquier indicación escrita en el presente documento, es importante aclarar que este, debe ir acompañado de una serie de evaluaciones como son; el Análisis de Riesgo y el BIA o ir acompañado de un Plan de Continuidad y Recuperación de desastres, debido a que es necesario conocer cierta información vital para poder definir una estrategia de Disponibilidad en la Organización.

2.1. Estado actual:

Una vez realizada la captura, cuantificación de datos y entrevistas, se

logaron identificar ciertos aspectos e indicadores;

- RTO, para el ERP Seven es muy alto, se encuentra catalogado en una escala de interrupción de hasta 5 a 10 días, en el peor de los casos.

- Frecuencia de falla, según el análisis de riesgos para Seven, la posibilidad de materialización de una amenaza se encuentra en un nivel medio alto con una calificación que oscila de 5 a 7.

- Impacto acumulado falla para el activo Seven, se encuentra en un nivel muy alto con una calificación de 10.

- Tiempo medio de vida entre fallas MTBF (Mean Time Between Failures), al analizar los resultados obtenidos en el BIA, podemos determinar que existe un frecuencia constante de riesgo, y no se cuentan con mecanismos automatizados que permitan que el sistema se estabilice en el menor tiempo posible

- Tiempo medio entre incidentes del sistema (MTBSI), la medida de tiempo en la que puede fallar otro sistema o proceso debido a la falla de Seven es muy corta, pero puede variar dependiendo de la temporada de transacción de datos.

3. Datos de Salida

3.1. Recomendaciones

- Definir un comité que se encuentre conformado por; el administrador del Servidor, de seguridad IT, administrador de Redes y un Gerente de Proyecto.

  Lo anterior con el propósito de contar con un grupo interdisciplinario que permita responder en el menor tiempo posible, bajo una coordinación logística.

- La implementación de un servidor dedicado que sirva como Mirror espejo, que sea activado en el menor tiempo posible cuando el servidor de producción se encuentre inactivo.

  Lo anterior ayudaría a disminuir los tiempos RTO de inactividad del ERP Seven, y reduciría el nivel de impacto en lo demás procesos de la organización.

- La monitorización y actualización progresiva de las salvaguardas

que se encuentran en un nivel de madurez bajo, ayudaran a reducir el riesgo de la materialización de una amenaza.

- Contar con un esquema de servidores virtual izados dedicados solo a Seven con actualizaciones progresivas, ayudara mantener un porcentaje de datos de respaldo actualizado, que ayudaran a disminuir el indicador de impacto en la organización.

- Determinar un esquema de balanceo en el cual cuando el sistema Seven falle, el otro de respaldo entre en funcionamiento en el menor tiempo posible, con el propósito de disminuir el Tiempo medio de vida entre fallas MTBF.

  Así mismo ayudaría a incrementar el Tiempo medio entre incidentes del sistema (MTBSI)

4. Tiempo de implementación

El tiempo de implementación del plan, está ligado a los recursos y aspectos recomendados que se deseen implementar.

También dependen de los aspectos contemplados en el Plan de Continuidad y Recuperación de Desastres, ya que muchas de estas implementaciones contribuyen a la disminución de algunos de los aspectos e indicadores anteriormente analizados.

Reviso:
Aprobó:

14. CONCLUSIONES

Aunque actualmente existen varios modelos para el análisis de riesgos, se puede observar que MAGERIT es la metodología más completa y apropiada para este proyecto, debido a que tiene en cuenta ciertos criterios, como son; realizar Análisis de Riesgos de manera cualitativa y cuantitativa, Gestión de Riesgo intrínseco, efectivo y residual. Toma en cuenta diferentes elementos a analizar(procesos, Activos, Recursos, Vulnerabilidades, Amenazas, Salvaguardas).

Por otra parte, en cuanto a objetivos de seguridad maneja aspectos de confidencialidad, integridad, disponibilidad, trazabilidad entre otros, que es necesario identificar en la organización.

Una vez realizado el Análisis de Riesgo y BIA se encontró que Seven se presenta como un activo que puede generar gran impacto en la organización al momento de materializarse una amenaza que implique un gran riesgo. Esto se puede verificar en los indicadores de valoración en activos y en la catalogación de posibles amenazas. Dentro de estas podemos destacar, Avería de origen físico o lógico, ataque de denegación de servicios, manipulación de programas, de sistema, errores y alteración de secuencia y aunque en menor medida pero posible, errores de los usuarios, errores de administración Suplantación de usuario.

Así mismo aunque se evidencian en algunos casos existen ciertas salvaguardas orientadas a la detección protección, se encuentran en un nivel de madurez muy bajo.

Por otra parte, aspectos a nivel procedimental referentes a protocolos y logística, podrían causar un gran impacto tanto en el activo como en la organización. Uno de estos se encuentra relacionado con los protocolos de generación y restauración de copias de respaldo. Debido a que este proceso se realiza todas las noches, al momento de presentarse una eventualidad que implique perdida de datos durante el día, no sería posible restaurar hasta el último bit de información ingresado, debido a que las copias de respaldo no se encontrarían actualizadas.

Esto se puede observar en el indicador correspondiente a RPO (Punto Objetivo de Recuperación), el cual muestra el porcentaje de datos que se pueden perder en determinado tiempo. Este se encuentra en un 35% el cual es un

porcentaje muy alto en temporada alta.

Por otra parte no se ha determinado el nivel o porcentaje de restauración mínimo que necesita Seven, para mantener continuidad y no afectar los demás procesos que dependen de él.

Así mismo se determino que el rango escalar de interrupción previsto para restaurar el sistema a su 100% contempla tiempos de 3 y 4 días, los cuales son tiempos muy extensos en temporadas altas, (inscripción de estudiantes, pagos de sueldo y pago a proveedores).

De igual manera el indicador correspondiente a RTO (Recovery Time Objetive – Tiempo Objetivo de Recuperación) , el cual representa el tiempo en el que un servido o activo debe ser restaurado, encuentra estimado en más de 1 día, lo cual es un rango de tiempo extenso en temporada alta.

Se logra evidenciar un comportamiento similar con el WRT (Tiempo de Trabajo de Recuperación), nos muestra tiempos de restauración para Seven superiores a 6 días, lo cual es un tiempo muy exceso en temporada alta.

Ahora bien, aunque se lograron evidenciar ciertos aspectos a nivel de procedimientos, protocolos que se encuentran aun en un nivel de madurez muy bajo así como tiempos un poco largos de respuesta y recuperación ante un incidente, ya se cuenta con un gran paso y es contar con una documentación y curva de aprendizaje. Lo anterior es una gran ventaja ya que no es necesario invertir en tiempo y recursos para planear e implementar desde cero dichos procedimientos, ubicando en una posición estratégica a la organización, ya que solo debe preocuparse por afinar cada vez mas sus salvaguardas.

15. RECOMENDACIONES

Revisar nuevamente los planes actuales de contingencia aplicados tanto a Seven como a los activos o procesos de los cuales el depende, con el propósito de reducir los niveles del impacto acumulado y repercutido. De igual manera, teniendo en cuenta los reportes de análisis (Impacto y Riesgo) resultantes, implementar nuevos planes de contingencia y/o Salvaguardas si no existen.

Para ello es importante evaluar, con base a la fase actual (**Current**) el procedimiento para aplicar de manera progresiva las fases; **Target**, la cual se

acerca más a una implementación de salvaguardas teniendo en cuenta los recursos actuales de la organización, y/o la implementación de la fase **Pila**r, la cual es una fase posterior recomendada (mas no obligatoria) pero que, requiere la implementación de más recursos, pero permite una disminución mayor en la frecuencia del incidente de un riesgo o en la eliminación completa de una amenaza.

Por otra parte, aunque se cuenta con un protocolo de realización y restauración de copias de respaldo, para determinar un porcentaje aceptable de perdida de información, es necesario evaluar el **RPO (Punto Objetivo de Recuperación)** actual y depurar que datos de este porcentaje de información son vitales para la restauración del ERP Seven a un nivel equilibrado, que no afecte la productividad de los demás procesos. Por otra parte, este proceso de depuración ayudaría a incrementar los porcentajes de recuperación de datos **RTO** (**Tiempo Objetivo de Recuperación**), en tiempos aceptables, así como el **WRT (Tiempo de Trabajo de Recuperación**) y los **tiempos escalares de inactividad** en indicadores más bajos.

Este porcentaje aceptable de perdida de información debe ser determinado en conjunto con la gerencia del TIC y la dirección de la organización, para determinar perdidas y tiempos de recuperación aceptables de acuerdo con los objetivos estratégicos de la organización.

De igual manera se recomienda, evaluar la posibilidad de determinar un rango de tiempo adicional durante el transcurso del día, en el cual se realicen copias incrementales de la información más vital del Seven, sobre todo en temporada de alta transacción de datos. Esto ayudaría a asegurar un mayor porcentaje de información a recuperar en el sistema de información.

Para poder llevar a cabo todo lo anterior, es necesario designar un equipo de trabajo, compuesto por un líder de proyecto, el cual puede ser el mismo Gerente del TIC o un colaborador asignado a estas funciones, un administrador de servidor, administrador del ERP Seven y un colaborador encargado de la red y de la seguridad de la misma. La función de este equipo es determinar y aplicar los protocolos (Planes de Continuidad y Recuperación de Desastres) en un instante determinado. Así mismo implementar la infraestructura que servirá como apoyo a estos planes (Plan de Disponibilidad).

Por otra parte, aunque siempre se desea apuntar el mejor de los escenarios, en el cual el sistema se recupera al 100% en el menor tiempo, hay que ser muy realistas y cuidadosos en plantear los objetivos ya que para lograr dichos escenarios es necesario contar con sistemas automatizados, los cuales en algunos momentos implican una gran inversión por sus altos costos. Dentro de

las posibles opciones podemos encontrar;

- La implementación de una réplica exacta o parte del datacenter, la cual se encontraría en constante actualización y entraría en funcionamiento, una vez el datacenter o algún sistema entrara en colapso. Esto ayudaría a reaccionar en el menor tiempo posible y no generaría un impacto en la organización, manteniendo la continuidad en los procesos. Desafortunadamente la implementación de esta replica, implica la adquisición de nuevos recursos a un alto costo, así como al definición de nuevas locaciones.

- La virtualización de servidores se presenta como una solución que no implica grandes inversiones y de bajo costo en cuanto a mantenimiento y capacitación. La implementación de estos Servidores puede ser corporativo y/o libre, (Liux o Microsoft). Por medio de un sistema de gestión de sistemas virtualizados, el cual gestionaría que servidores y sistema, podrían entrar en funcionamiento al momento de presentarse un incidente.

Tomar como base los entregables de los planes propuestos, servirá como punto de partida para definir protocolos más precisos y adecuados en cuanto a tiempos de implementación.

Finalmente, realizar campañas de socialización en los procesos, ayudaría a generar más conciencia en los mismos, disminuyendo así la posibilidad de incidentes internos y apoyo en la monitorización de las salvaguardas implementadas.

16. BIBLIOGRAFÍA

Gómez Vieites Álvaro. Bogotá. **SEGURIDAD INFORMATICA BÁSICO** Ed Ecoe Ediciones.

Salliz Ezequie, Caracciolo Claudio. Rodríguez Marcelo. **ETHICAL HACKING**, Buenos Aires, Ed, Alfa Omega.

Gerencia De Innovación y Desarrollo De TIC Universidad EAN Documentación ISO, Caracterización de Procesos.

CALVO, Rafael Fernández. **Glosario Básico Inglés- Español para usuarios de internet** 1994. 2000

BS ISO / IEC 27001:2005

[www.iso27000.es]

Análisis y gestión de riesgos de la seguridad de los sistemas de la información

[http://www.cii-murcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.pdf]

Jornada Nacional de Seguridad Informatica 2012

[http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XII_JornadaSeguridad/PresentacionJeimyCano-IVELSI.pdf]

Informe de Estados Segudidad Latino America 2012 ESET

[http://www.eset-la.com/centro-amenazas/reporte/ESET%20Security%20Report%20Latinoamerica%202012/2797]

[http://www.ati.es/novatica/glosario/glointv4.pdf 17 de Marzo]

Gestión de Riesgos y Análisis de Cuantificación

[http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/4AnalisisycuantificaciondelRiesgo(AR)_es.pdf]

Manual en línea Pilar

[http://www.pilar-tools.com/es/tools/pilar/v52/help_es/index.html