ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN

Y TRANSFERENCIA DE TECNOLOGÍA

UNIDAD DE GESTIÓN DE POSTGRADOS

TESIS DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE: MAGISTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

II PROMOCIÓN

TEMA: EVALUACIÓN DE RIESGOS TECNOLÓGICOS DEL CENTRO DE DATOS DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO USANDO LOS PROCESOS DE TI BASADOS EN COBIT Y MAGERIT

AUTOR: ING. CRISTIAN FABRICIO VITERI SILVA

DIRECTOR: ING. EDGAR HERMOSA , MGT.

CODIRECTOR: ING. LUIS ESCOBAR , MGT.

SANGOLQUI

2015

CERTIFICACIÓN

Certificamos que el presente trabajo titulado: EVALUACIÓN DE RIESGOS TECNOLÓGICOS DEL CENTRO DE DATOS DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO USANDO LOS PROCESOS DE TI BASADOS EN COBIT Y MAGERIT, fue realizado en su totalidad por el ingeniero Cristian Fabricio Viteri Silva , bajo nuestra supervisión, y cumple con las normas estatutarias establecidas por la ESPE en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas.

Sangolquí, Abril de 2015

Ing. Edgar Hermosa Mgt.
DIRECTOR

Ing. Luis Escobar Mgt.
OPONENTE

AUTORÍA DE RESPONSABILIDAD

La Tesis de Grado Titulada: EVALUACIÓN DE RIESGOS TECNOLÓGICOS DEL CENTRO DE DATOS DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO USANDO LOS PROCESOS DE TI BASADOS EN COBIT Y MAGERIT, ha sido desarrollada en base a una investigación, respetando derechos intelectuales de terceros, cuyas fuentes son citadas

En virtud de esta declaración me responsabilizo del contenido, veracidad y alcance científico de esta tesis.

Sangolquí, Abril 2015

.....

Ing. Cristian Fabricio Viteri Silva

CI: 060301132-1

AUTORIZACIÓN

Yo, Cristian Fabricio Viteri Silva, autorizo a la Universidad de las Fuerzas Armadas. ESPE, la publicación en la biblioteca virtual de la institución del trabajo de la tesis "EVALUACIÓN DE RIESGOS TECNOLÓGICOS DEL CENTRO DE DATOS DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO USANDO LOS PROCESOS DE TI BASADOS EN COBIT Y MAGERIT", cuyo contenido es de mi responsabilidad.

Sangolquí, Abril 2015

.....

Ing. Cristian Fabricio Viteri Silva

CI: 0603011321

DEDICATORIA

La realización de esta tesis la dedico con amor a mi amada esposa Verónica y mis dos bendiciones Anahely e Ian, a mis padres, a mis herman@s, que con su apoyo incondicional y sacrificio han permitido que culmine con este objetivo.

Cristian Fabricio Viteri Silva

AGRADECIMIENTO

Agradezco a Dios y a la Virgen Dolorosa por guiarme día a día y permitirme cristalizar este objetivo, a la Universidad de las Fuerzas Armadas ESPE, a sus autoridades y docentes en especial a mi tutor Ing. Edgar Hermosa, al Ing. Jorge Delgado Director de Tecnología de la Universidad Nacional de Chimborazo quien me brindo todas las facilidades para el desarrollo y culminación de la misma, a mis padres, herman@s a mi amada esposa Verónica y mis dos bendiciones Anahely e Ian.

Cristian Fabricio Viteri Silva

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

Una gran diversidad de sistemas tanto lógicos como físicos componen un Centro de Datos, cuyo principal objetivo es permitir administrar y salvaguardar la información que se encuentra alojada para lograr el funcionamiento adecuado de una Institución. Por lo tanto para garantizar su operatividad, su fiabilidad, seguridad y alcanzar su perfecto desenvolvimiento es imprescindible realizar evaluaciones que permitan conocer con veracidad el estado real de la infraestructura de los Centro de Datos. En la Universidad Nacional de Chimborazo UNACH varias aplicaciones que poseen información crítica para la Institución no están cumpliendo con las mejoras prácticas por lo que están expuestas a varios riesgos. Para minimizar este inconveniente se realizó una evaluación en la misma utilizando la metodología de análisis de riesgos denominada MAGERIT, la cual permitió identificar los riesgos en cada una de las dimensiones de seguridad y el impacto que podrían sufrir los activos del Centro de Datos en el caso de que una amenaza se materialice. Dentro de los 4 dominios y los 34 procesos de COBIT se seleccionó los procesos Planear y Organizar 9(PO9), Monitoreo y Evaluación 4 (ME4) para poder determinar el nivel de madurez que tenían estos procesos en el Centro de Datos de la UNACH. Luego de haber realizado la evaluación de riesgos se pudo determinar el nivel de madurez en el que se encuentran los procesos mencionados anteriormente, obteniéndose que el nivel de madurez en el proceso PO9 es Inicial /Ad Hoc (1) y un nivel de madurez en el proceso ME4 es Repetible pero Intuitivo (2). Las evaluaciones de riesgos realizadas a los Centros de Datos de una manera frecuente ayudan a que la gerencia a la toma de decisiones para que se implementen las mejores prácticas, políticas, planes para minimizar o eliminar los riesgos a los que están expuesta la información que se encuentran alojada en los mismos.

PALABRAS CLAVE:

- **CENTRO DE DATOS UNACH**
- **COBIT UNACH**
- **MAGERIT UNACH**
- **DIMENSIONES DE SEGURIDAD MAGERIT.**

ABSTRACT

A wide variety of both logical and physical systems make up a Data Center, whose main objective is to allow manage and safeguard the information that is hosted to ensure proper functioning of an institution. Therefore to ensure their operability, reliability, security and achieve their perfect development is essential assessments that reveal truthfully the actual state of the infrastructure of the data center. The Universidad Nacional de Chimborazo UNACH various applications that have critical information to the institution are not meeting best practices so they are exposed to various risks. To minimize this evaluation was conducted using the same methodology called MAGERIT risk analysis, which identified the risks in each of the security dimensions and the impact it could suffer assets Data Center in the case that a threat materializes. Within 4 domains and 34 processes the Plan and Organise COBIT 9 (PO9), Monitoring and Evaluation 4 processes (ME4) was selected to determine the level of maturity that had these processes in the Data Center UNACH. After completing the risk assessment could determine the level of maturity in which are the processes mentioned above, obtaining the level of maturity in PO9 process is Initial / Ad Hoc (1) and a level of maturity in the ME4 process is Repeatable but Intuitive (2). Risk assessments made data centers a frequently help the management to decision making to best practices, policies, plans to minimize or eliminate risks to which they are exposed information that are implemented are housed therein.

KEYWORDS:

- **DATA CENTER UNACH**
- **COBIT UNACH**
- **MAGERIT UNACH**
- **MAGERIT PROCESS SECURITY DIMENSIONS.**

CAPÍTULO I
INTRODUCCIÓN

Un Centro de Datos lo componen una gran diversidad de sistemas, tanto lógicos como físicos, cuyo objetivo principal es administrar y salvaguardar la información que allí se encuentra alojada. Es una parte estratégica de la actividad de una Institución y, por tanto, su seguridad y disponibilidad son esenciales .Para garantizar su operatividad, su fiabilidad, seguridad y alcanzar su perfecto funcionamiento es imprescindible realizar evaluaciones que permitan conocer con veracidad el estado real de la infraestructura del Centro de Datos, que identifiquen los posibles riesgos, las debilidades, así como los problemas de capacidad.

Con las evaluaciones es probable prevenir incidentes posteriores no esperados, determinar las eventuales líneas de actuación y eliminar o disminuir los riesgos de caídas de los sistemas. (C/Albasanz)

1.1 Justificación e Importancia

La evolución de los sistemas de información y comunicación en el mundo y en nuestro país, ha originado la necesidad de implementar la gestión de sistemas en la mayoría de las instituciones sean estas privadas o públicas; para obtener seguridad, confiabilidad y escalabilidad en todos los ámbitos, todo esto a hecho que las instituciones requieran cada vez mayor control sobre sus datos y los sistemas que estas utilizan, impulsando con esto a que el procesamiento de la información y la seguridad con la que se realiza se vuelva de vital importancia, ya que en la actualidad los sistemas de información, son vulnerables a una variedad de amenazas por parte de personas internas como externas de la institución, desastres naturales, denegación de servicios, entre otros peligros latentes.

No tomar en cuenta las amenazas y riesgos que acechan a las unidades de información y comunicación, es como jugar con la fortuna, se puede ser afortunado durante algún tiempo, pero tarde o temprano esa fortuna terminará.

Desafortunadamente, la mayoría de las amenazas son invisibles hasta que es demasiado tarde, mucho más si se hace referencia a los sistemas de información, los mismos que manejan activos tan intangibles como los datos y la información que se obtiene de estos.

Analizar los Riesgos y adoptar medidas relacionadas a sus causas es un elemento muy importante, ya que los mismos son un factor crítico para el éxito de la institución, el presente trabajo se enfocará al Centro de Datos de la Universidad Nacional de Chimborazo, donde surge la necesidad de realizar una Evaluación basada en Riesgos, emitiendo recomendaciones basadas en las mejores prácticas para evitar que estos se plasmen.

La Evaluación basada en riesgos permite a una institución considerar la dimensión con que los eventos potenciales influyan en la obtención de los objetivos, evaluándolos desde la perspectiva de la probabilidad y el impacto, es por ello que marcos de referencia como COBIT y la metodología MAGERIT, permiten determinar los riesgos al que está sometido un Centro de Datos.

1.2 Planteamiento del problema

Se han identificado algunos problemas relacionados con los procesos, los riesgos informáticos físicos y lógicos, a los que el Centro de Datos está expuesto por su propia naturaleza, ya que no existe una adecuada documentación de las actividades, riegos, creando inconvenientes al momento de gestionarlos problemas e incidentes que se presentan, los cuales frecuentemente son resueltos de manera reactiva.

El Centro de Datos de la Universidad Nacional de Chimborazo cuenta con varios funcionarios los cuales realizan las actividades de supervisión y soporte en los diferentes campos de operación con que cuenta la institución.

La Universidad Nacional de Chimborazo, como la mayor parte de las instituciones se ha vuelto cada vez más dependiente de la tecnología para manejar sus procesos de

manera ágil y correcta, por lo que la disponibilidad del Centro de Datos es un aspecto crucial al momento de generar valor para la institución.

Estas son las razones por las que se hace necesario realizar una evaluación al Centro de Datos Institucional, con el fin de determinar los riesgos a los cuales está expuesto el mismo y establecer directrices para que en el futuro se puedan implementar mejores prácticas para disminuir o eliminar los riesgos e incrementar la productividad y efectividad del Centro de Datos.

1.3 Formulación del problema

¿Tiene identificado la dirección de tecnología de la Universidad Nacional De Chimborazo los riesgos a los cuales está expuesto el Centro de Datos de la Institución?

¿Cuándo se estructuro el Centro de Datos de la Universidad Nacional De Chimborazo se tomó en cuenta un marco de referencia para la evaluación periódica de la gestión de las TICS?

¿Se ha realizado alguna evaluación del Centro de Datos de la Universidad Nacional De Chimborazo?

1.4 Objetivo General

Evaluar la situación actual de los riesgos a los que está expuesto del Centro de Datos de Universidad Nacional De Chimborazo aplicando COBIT y MAGERIT como marco de referencia y metodología respectivamente.

1.5 Objetivos Específicos

- Analizar los procedimientos para desarrollar una evaluación de riesgos informáticos utilizando el marco de referencia COBIT y la metodología MAGERIT.

- Elaborar un Plan de Auditoría para el Centro Datos.
- Ejecutar la Auditoria
- Procesar los datos obtenidos en la Auditoria.
- Elaborar una matriz de riesgos informáticos del Centro de Datos.
- Elaborar informes, conclusiones y recomendaciones en base a la auditoria

CAPITULO II

FUNDAMENTACIÓN TEÓRICA

2.1 Riesgos

Un Data Center es un espacio físico donde convergen las TIC, por lo tanto, es el entorno donde existe mayor concentración de valor a proteger. (Según el Sistema de Gestión de la Seguridad de la Información SGSI) por lo tanto es donde existe mayor riesgo.

Conceptos

A continuación se definen tres conceptos de Riesgos:

- Según Fernando Izquierdo Duarte: “El Riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos”. (Duarte, 2003)

- Según Alberto Cancelado González: “El riesgo es una condición del mundo real en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de pérdidas”. (González, 2005)

- Según Martín Vilches Troncoso: “El riesgo es cualquier variable importante de incertidumbre que interfiera con el logro de los objetivos y estrategias del negocio. Es decir es la posibilidad de la ocurrencia de un hecho o suceso no deseado o la no-ocurrencia de uno deseado”. (Troncoso, 1993)

Clasificación de Riesgos

Los riesgos que se va a analizar se los detalla a continuación:

- Riesgos del negocio
- Riesgo Inherente.
- Riesgo de Auditoría
- Riesgo de Control

- Riesgo Estratégico
- Riesgo Operativo
- Riesgo Financiero
- Riesgo de Cumplimiento
- Riesgo de Tecnología
- Riesgo Profesional

- **Riesgo de Negocios.**

Es el riesgo de los negocios trascendentales de la empresa y de sus procesos claves, es decir, es un riesgo crítico de la empresa.

- **Riesgo Inherente.**

Este riesgo tiene ver exclusivamente con la actividad económica de la empresa, independientemente de los sistemas de control interno que allí se estén aplicando.

- **Riesgo de Auditoría.**

Existe al aplicar los programas de auditoría, cuyos procedimientos no son suficientes para descubrir errores o irregularidades significativas.

- **Riesgo de Control.**

Está asociado con la posibilidad de que los procedimientos de control interno, incluyendo a la unidad de auditoría interna, no puedan prevenir o detectar los errores e irregularidades significativas de manera oportuna.

- **Riesgo Estratégico.**

Se asocia con la forma en que se administra la Entidad. El manejo del riesgo

estratégico se enfoca a asuntos globales relacionados con el cumplimiento de la misión de la Entidad, la cual busca la vigilancia de la conducta de los servidores públicos, defender el orden jurídico y los derechos fundamentales.

- **Riesgo Operativo.**

Comprende tanto el riesgo en sistemas como operativo provenientes de deficiencias en los sistemas de información, procesos, estructura, que conducen a ineficiencias, oportunidad de corrupción o incumplimiento de los objetivos fundamentales.

- **Riesgo Financiero.**

Se relaciona con las exposiciones financieras de la empresa. El manejo del riesgo financiero toca actividades de tesorería, presupuesto, contabilidad y reportes financieros, entre otros.

- **Riesgo de Cumplimiento.**

Se asocia con la capacidad de la empresa para cumplir con los requisitos regulativos, legales, contractuales, de ética pública, democracia y participación, servicio a la comunidad, interacción con el ciudadano, respeto a los derechos, a la individualidad, la equidad y la igualdad.

- **Riesgo de Tecnología.**

El riesgo tecnológico tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. Esto se debe a que la tecnología está siendo fin y medio de ataques debido a vulnerabilidades existentes.

El riesgo tecnológico puede verse desde tres aspectos, primero a nivel de la

infraestructura tecnológica (hardware o nivel físico), en segundo lugar a nivel lógico (riesgos asociados a software, sistemas de información e información) y por último los riesgos derivados del mal uso de los anteriores factores, que corresponde al factor humano como un tercer nivel.

Una falla sobre la tecnología de la organización puede implicar riesgos en otros ámbitos, como pérdidas financieras, multas, acciones legales, afectación sobre la imagen de la organización, causar problemas operativos o afectar las estrategias de la organización.

- **Riesgo Profesional.**

Conjunto de organizaciones públicas y privadas, normas y procedimientos, destinados a prevenir, proteger y atender a los trabajadores de los efectos, de las enfermedades y los accidentes que puedan ocurrirles como consecuencia del trabajo que están realizando.

Causas de Riesgos de TI

Las causas de riesgo más comunes se dividen en:

- Externas
- Internas

Las causas de riesgo externas pueden ser de dos clases:

- Naturales
- Motivadas por el Hombre.

Las causas de riesgo naturales son regularmente las siguientes:

- Inundaciones
- Temblores
- Tornados
- Tormentas Eléctricas
- Huracanes
- Erupciones Volcánicas

Las causas de riesgo originadas por el hombre, son entre otras, las siguientes:

- Incendios
- Explosiones
- Accidentes laborales
- Destrucción intencional
- Sabotaje
- Robo
- Fraude
- Contaminación Ambiental

Las causas internas de riesgo, se producen a partir de las mismas organizaciones, por lo que son más frecuentes que las causas externas.

Entre las causas internas de riesgo tenemos:

- Robo: de materiales, de dinero y de información
- Sabotaje
- Insuficiencia de Dinero
- Destrucción: de datos y de recursos
- Personal No capacitado
- Huelgas
- Fraudes
- Ausencia de seguridades físicas tanto de la empresa como dela información.

2.1.1 Riesgos de Tecnología de Información

Las definiciones que vienen a continuación son tratadas de manera general de tal forma que nos permitan tener un enfoque rápido de los temas a tratarse los mismos que más adelante se detallaran sus procedimientos.

Definición

“El concepto de riesgo de TI puede definirse como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Surge así, entonces la necesidad del control que actúe sobre la causa del riesgo para minimizar sus efectos. Cuando se dice que los controles minimizan los riesgos, lo que

en verdad hacen es actuar sobre las causas de los riesgos, para minimizar sus efectos" (Cevallos, 2005).

Valoración del Riesgo

La valoración del riesgo comprende tres etapas: La identificación, el análisis y la determinación del nivel del riesgo. Para cada una de ellas es imprescindible tener en cuenta la mayor cantidad de datos disponibles y contar con la colaboración de las personas que ejecutan los procesos y procedimientos para conseguir que las acciones establecidas logren los niveles de efectividad esperados.

Identificación del Riesgo

La identificación del riesgo debe ser permanente, incluido al proceso de planeación y responder a las preguntas qué, cómo y por qué se pueden producir hechos que contribuyen en la consecución de resultados.

Según la práctica internacional la identificación del riesgo se realiza por medio de la realización de un Mapa de Riesgos, el cual como herramienta metodológica faculta elaborar un inventario de los mismos ordenada y sistemáticamente, detallando en primera instancia los riesgos, después mostrando una descripción de cada uno de ellos y las posibles consecuencias.

Tabla 1: Mapa de Riesgos

RIESGO	DESCRIPCIÓN	POSIBLES CONSECUENCIAS
Posibilidad de ocurrencia de aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.	Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado	Corresponde a los posibles efectos ocasionados por el riesgo, los cuales se pueden traducir en daños de tipo económico, social, administrativo, entre otros

Fuente:(UNAL, 2012)

Análisis del Riesgo

Definición

"El análisis del riesgo es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado" (Comercio, 2013)

Objetivo General del Análisis de Riesgo

Su objetivo es establecer una estimación y priorización de los riesgos basados en la información proporcionada por los mapas de riesgos, con el objetivo de clasificar los riesgos y suministrar información para establecer el nivel de riesgo y las acciones que se van a implementar.

Se han establecido dos aspectos para elaborar el análisis de los riesgos:

Probabilidad

La posibilidad de ocurrencia del riesgo, la cual puede ser medida con criterios de frecuencia o tomando en cuenta la manifestación de factores internos y externos que puedan predisponer el riesgo, aunque éste no se haya presentado nunca.

Para el análisis cualitativo se establece una escala de medida cualitativa en donde se establecen las categorías que se van a utilizar con su respectiva descripción, por ejemplo:

ALTA: Es muy factible que el hecho se presente

MEDIA: Es factible que el hecho se presente

BAJA: Es poco factible que el hecho se presente

Impacto

Consecuencias que puede ocasionar a la organización la materialización del riesgo. Ese diseño puede adoptarse para la escala de medida cualitativa de IMPACTO, estableciendo las categorías y la descripción, por ejemplo:

ALTO: Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la Entidad.

MEDIO: Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad.

BAJO: Si el hecho llegara a presentar se tendría bajo impacto o efecto en la entidad.

Objetivos Específicos del Análisis de Riesgo

- Analizar el tiempo, esfuerzo y recursos disponibles y necesarios para atacar los problemas
- Definir cuáles son los recursos existentes.
- Llevar a cabo un minucioso análisis de los riesgos y debilidades.
- Identificar, definir y revisar todos los controles de seguridad ya existentes.
- Determinar si es necesario incrementar las medidas de seguridad, los costos del riesgo y los beneficios esperados.

Determinación del nivel del Riesgo

La determinación del nivel de riesgo es el resultado de comparar el impacto y la probabilidad con los controles existentes al interior de los diferentes procesos y procedimientos que se realizan. En esta etapa se deben tener muy claros los puntos de control existentes en los diferentes procesos, los cuales permiten conseguir información para la toma de decisiones, estos niveles de riesgo pueden ser:

ALTO: Cuando el riesgo hace altamente vulnerable a la entidad o dependencia. (Impacto y probabilidad alta versus controles existentes)

MEDIO: Cuando el riesgo muestra una vulnerabilidad media. (Impacto alto - probabilidad baja o Impacto bajo - probabilidad alta versus controles existentes).

BAJO: Cuando el riesgo presenta vulnerabilidad baja.(Impacto y probabilidad baja versus controles existentes).

Lo anterior significa que a pesar que la probabilidad y el impacto son altos confrontado con los controles se puede decir a manera de ejemplo que el nivel de riesgo

es medio y por lo que las acciones que se implementen entraran a reforzar los controles existentes y a valorar la efectividad de los mismos.

Matriz de priorización de los Riesgos

Luego del el análisis de los riesgos tomando como referencia los aspectos de probabilidad e impacto, se recomienda utilizar una matriz de priorización que permite establecer cuales riesgos requieren de un tratamiento inmediato.

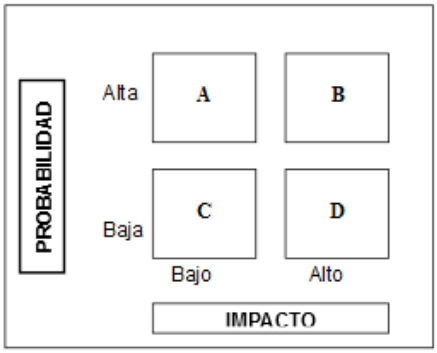


Gráfico 1: Matriz de priorización de Riesgos

Fuente: *(Auditoriapublica, 2012)*

Cuando se sitúan los riesgos en la matriz se define cuáles requieren acciones inmediatas, que en este caso son los del cuadrante B, es decir los de alto impacto y alta probabilidad, en relación a los riesgos que se sitúen en el cuadrante A y D, se debe seleccionar conforme a la naturaleza del riesgo, ya que estos pueden ser peligrosos para el alcance de los objetivos institucionales por las consecuencias que presentan los situados en el cuadrante D o por la constante presencia en el caso del cuadrante A

Manejo del Riesgo

Cualquier esfuerzo que promuevan las organizaciones en relación a la valoración del riesgo llega a ser infructuosa, si tienen un apropiado manejo y control de los mismos precisando acciones factibles y efectivas, tales como la implantación de políticas, estándares, procedimientos y cambios físicos entre otros, que formen parte de un plan de manejo.

Para el manejo del riesgo se pueden tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, relacionadas o en conjunto.

- Evitar el riesgo
- Reducir el riesgo
- Dispersar y atomizar el riesgo
- Transferir el riesgo
- Asumir el riesgo

Evitar el riesgo: Es evidentemente la primera alternativa a considerar. Se consigue cuando al interior de los procesos se producen cambios importantes por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones promovidas. Un ejemplo de esto puede ser el control de calidad, administración de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

Reducir el riesgo: Si el riesgo no se puede evitar porque crea problemas operacionales, el siguiente camino es reducirlo al más bajo nivel posible. La reducción del riesgo es posiblemente el método más sencillo y económico para superar las debilidades antes de emplear medidas más costosas y complejas. Se alcanza mediante la optimización de los procedimientos y la implementación de controles.

Dispersar y atomizar el riesgo: Se consigue mediante la distribución o localización del riesgo en diversos sectores. Por ejemplo, la información de mayor importancia se puede duplicar y almacenar en un sitio distante y de ubicación segura, en vez de dejarla centralizada en un solo lugar.

Transferir el riesgo: Se refiere a buscar respaldo y compartir con otro una fracción del riesgo como por ejemplo tomar pólizas de seguros; con esto se traslada el riesgo a otra parte o físicamente se traslada a otro lugar.

Asumir el riesgo: Inmediatamente que el riesgo ha sido reducido o transferido puede existir un riesgo residual que se mantiene. En este caso, el administrador del proceso solamente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Una vez establecidos cual o cuales de los manejos del riesgo se van a establecer, deben evaluarse con correspondencia al beneficio-costo para definir, cuáles son

apropiados de ser aplicados y proceder a elaborar el plan de manejo de riesgo, teniendo en cuenta, el análisis elaborado para cada uno de los riesgos de acuerdo con su impacto, probabilidad y nivel de riesgo.

Posteriormente se especifican los responsables de tomar las acciones definiendo el nivel de participación de las dependencias en el desarrollo de cada una de ellas. Es importante elaborar indicadores, como los elementos que permiten prescribir de forma práctica el comportamiento de las variables de riesgo, que van a permitir medir el impacto.

Plan de manejo de Riesgos

Para construir un plan de manejo de riesgos es preciso tener en cuenta si las acciones propuestas reducen la materialización del riesgo y realizar una evaluación jurídica, técnica, institucional, financiera y económica, es decir considerar la posibilidad de su adopción. La elección de las acciones más beneficiosas para la organización se puede realizar con base en los siguientes factores:

- El nivel del riesgo
- El balance entre el costo de la implementación de cada acción contra el beneficio de la misma.

Una vez efectuada la elección de las acciones más convenientes se debe proceder a la elaboración e implantación del plan, identificando responsabilidades, programas, resultados esperados, medidas para verificar el cumplimiento y las características del monitoreo. El éxito de la implementación y/o ejecución del plan demanda de un sistema gerencial efectivo el cual tenga claro el método que se va a aplicar.

2.1.2 Administración de Riesgos

Las organizaciones necesitan tomar riesgos para mantenerse, la mayoría requieren incrementar el nivel de riesgos que toman para ser exitosas a largo plazo. Para hacer realidad este cambio, los líderes a nivel mundial están fortaleciendo principalmente sus prácticas de administración de riesgos para asegurar que si las iniciativas o el funcionamiento de las unidades de negocio se desalineen, se identifique rápidamente para poder actuar y corregir la situación.

Definición

"Es un proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales". (Manslla, 2013)

Es adaptable a cualquier situación donde un efecto no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades de mejora.

Beneficios para la Organización:

- Facilita el logro de los objetivos de la organización.
- Hace a la organización más segura y consciente de sus riesgos.
- Mejoramiento contínuo del Sistema de Control Interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades de negocio.
- Fortalece la cultura de autocontrol.
- Mayor estabilidad ante cambios del entorno.

Beneficios para el Departamento de Auditoria

- Soporta el logro de los objetivos de la auditoria.
- Estandarización en el método de trabajo.
- Integración del concepto de control en las políticas organizacionales.
- Mayor efectividad en la planeación general de Auditoria.
- Evaluaciones enfocadas en riesgos.
- Mayor cobertura de la administración de riesgos.
- Auditorias más efectivas y con mayor valor agregado.

Factores a considerar en la administración de riesgos

Los principales factores que se deben considerar en la Administración de Riesgos de TI son:

- Seguridades
- Controles: Preventivos, Detectivos y Correctivos
- Objetivos

- Manuales de usuarios
- Políticas

Si no existe una adecuada atención de los factores descritos previamente y si los controles y seguridades fueran errados, los planes organizacionales, financieros, administrativos y de tecnología se verían gravemente afectados, ya que no sólo el área de tecnología será el afectado.

2.1.3 Administración de Riesgos de TI

Definición

"La Administración de Riesgos de TI es el proceso continuo basado en el conocimiento, evaluación, manejo de los riesgos y sus impactos que mejora la toma de decisiones organizacionales, frente a los riesgos de TI". (Duarte, 2003)

Por lo tanto la administración de riesgos es el conjunto de pasos secuenciales, lógicos y sistemáticos que debe seguir el analista de riesgos para identificar, valorar y manejar los riesgos asociados a los procesos de TI de la organización, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados minimizando las pérdidas o maximizando las oportunidades de mejora.

Beneficios

Se pueden mencionar los siguientes beneficios:

- **A nivel organizacional**
  - Alcance o logro de los objetivos organizacionales.
  - Énfasis en prioridades de negocio: permite a los directivos encaminar sus recursos en los objetivos primordiales. Tomar acciones para prevenir y reducir pérdidas, antes que corregir después de los hechos.
  - Fortalecimiento del proceso de planeación.
  - Apoyo en la identificación de oportunidades.
  - Fortalecimiento de la cultura de autocontrol.
- **Al proceso de administración**
  - Cambio cultural que soporta conversaciones abiertas sobre riesgos e información potencialmente peligrosa. La nueva cultura tolera

equivocaciones pero no tolera errores escondidos haciendo énfasis en el aprendizaje de los errores.

- Mejor administración financiera y operacional al garantizar que los riesgos sean adecuadamente considerados en el proceso de toma de decisiones. Una mejor administración operacional generará servicios más efectivos y eficientes.
- Mayor responsabilidad de los administradores en el corto plazo. A largo plazo, se mejorarán todas las capacidades de los directivos.

Características Generales de la Administración de Riesgos de TI

La Administración de Riesgos debe estar apoyada por la Alta Gerencia de la Organización.

La Administración de Riesgos debe ser parte integral del proceso administrativo utilizado por la Dirección de la Organización.

La Administración de Riesgos es un proceso multifacético y participativo, el cual es frecuentemente mejor llevado a cabo por un equipo multidisciplinario.

Proceso de Administración de Riesgos de TI

A continuación se describen las principales etapas definidas para el Proceso de Administración de Riesgos de TI.

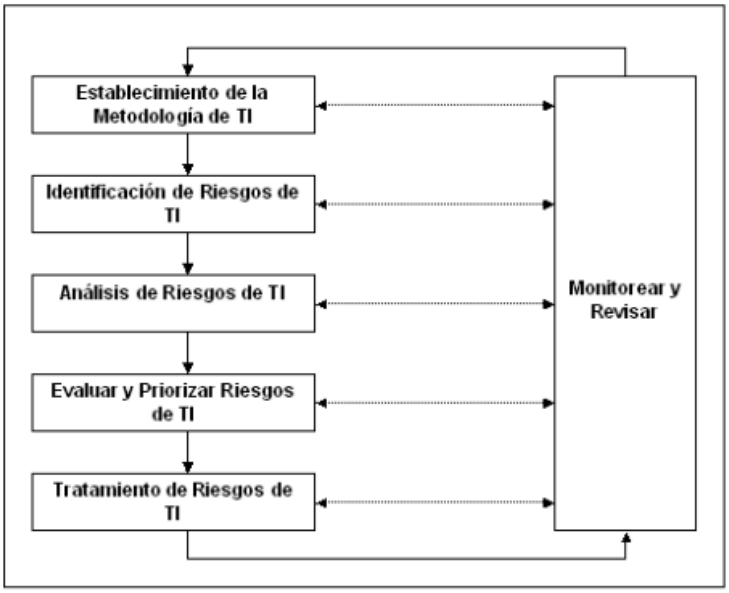


Gráfico 2: Proceso de administración de riesgo de TI

Fuente: (Cevallos M. , 2005)

- **Establecimiento de la Metodología de TI**

Consiente, a través de la comprensión del entorno y de la organización, establecer criterios generales que serán utilizados para implementar la visión de Administración de Riesgos de TI de la Organización.
En esta etapa se debe establecer la metodología que será utilizada para la Administración de Riesgos de TI de la organización.

Consiste en examinar los riesgos existentes y de acuerdo a este análisis, precisar cuál o cuáles son las metodologías que van a ser la mejor opción para la elaboración de la evaluación.

2.1.4 Metodologías de Administración de Riesgos de TI

Introducción a las Metodologías

Método es el "modo de decir o hacer con orden una cosa" (Ortega). Así mismo define el diccionario la palabra Metodología como "conjunto de métodos que se siguen en una investigación científica" (Landeau, 2007).

La Informática ha sido tradicionalmente una materia compleja, por lo que se hace obligatoria la utilización de metodologías, desde su diseño de ingeniería hasta la auditoria de los sistemas de información.

Una metodología es necesaria para que un grupo de profesionales obtenga un resultado homogéneo tal como si lo hiciera uno solo, por lo que es frecuente el uso de metodologías en las empresas auditoras / consultoras profesionales, desarrolladas por los más expertos, para conseguir resultados homogéneos en equipos de trabajo heterogéneos.

El incremento de metodologías en el mundo de la auditoria y el control informático aparecen en la década de los ochenta, paralelamente al nacimiento y comercialización de denominadas herramientas metodológicas. Una de ellas es la seguridad de los sistemas de información.

Si se define a la “Seguridad delos Sistemas de Información” como la doctrina que trata de los riesgos informáticos o creados por la informática, entonces la auditoría es una de los aspectos involucrados en este proceso de protección y preservación de la información.

Por lo que el nivel de seguridad informática en una organización es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia de un conjunto de acciones destinadas a proteger y preservar la información de la organización y sus medios de proceso.

Los Procedimientos de Control

Son los procedimientos operativos de las diferentes áreas de la organización, conseguidos con una metodología apropiada, para la obtención de uno o varios objetivos de control, los cuales deben estar documentados y aprobados por la dirección. La tendencia tradicional de los informáticos es la de dar más peso a la herramienta que al “control o contramedida”, pero no se debe olvidar que “una herramienta nunca es una solución sino una ayuda para conseguir un control mejor”. (Ensayos, 2013)

En la Tecnología de Seguridad están todos los elementos ya sean hardware o software, que coadyuvan a controlar un riesgo informático. Dentro de estos mecanismos están los cifradores, autentificadores, equipos “tolerantes al fallo”, las herramientas de control, etc.

- **Cifrado**

Consiste en transformar un texto en claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos. Se pueden dividir en dos categorías: cifradores de bloque, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y cifradores en flujo, que trabajan

sobre flujos continuos de bits.

- **Autenticadores**

Permiten el acceso remoto seguro, así como otras aplicaciones avanzadas, incluyendo la firma digital, administración de contraseñas, inicio de sesión en la red y acceso combinado físico y lógico en un dispositivo único.

- **Equipos tolerantes al fallo**

Los sistemas tolerantes a fallos pueden ser tan sencillos como usar duplicidad de elementos hardware, y tan complejos como redes enteras completamente replicadas en tiempo real entre dos ubicaciones físicamente distintas.

Es por ello que la tolerancia a fallos tienen cada vez más importancia; esto se debe a la proliferación de los sistemas de cómputo y el uso de éstos cada vez en más ámbitos. Algunas de las aplicaciones de los computadores resultan lo suficientemente críticas como para protegerlas contra potenciales fallos. En esos entornos, un funcionamiento incorrecto del sistema resultaría catastrófico y podría causar importantes perjuicios.

Ejemplos de aplicaciones de este tipo son las centrales nucleares controladas por computador, y por extensión, cualquier otro proceso industrial delicado controlado de esa forma. Otros ejemplos son los computadores que gobiernan aviones, satélites artificiales y naves espaciales.

- **Las herramientas de control**

Son elementos software que facultan definir uno o varios procedimientos de control para una normativa y un objetivo de control.

Todos estos factores están relacionados entre sí, ya que cuando se evalúa el nivel de Seguridad de Sistemas en una institución, se están evaluando todos estos factores y se plantea un Plan de Seguridad nuevo que optimice todos los factores. Al culminar el plan se habrá obtenido un nuevo escenario en el que el nivel de control sea superior al anterior.

Se denominará Plan de Seguridad a una estrategia planificada de actividades y

productos que lleven a un sistema de información y sus centros de proceso de una situación inicial a una situación mejorada.

Metodologías de Evaluación de Sistemas

Definiciones

En el ámbito de la seguridad de sistemas se emplean todas las metodologías necesarias para realizar un plan de seguridad además de las de auditoría informática.

Las metodologías de evaluación de sistemas por excelencia son las de Análisis de Riesgos y las de Auditoría Informática, con dos enfoques distintos. La auditoría informática identifica el nivel de "exposición" por la falta de controles, mientras el análisis de riesgos facilita la "evaluación" de los riesgos y recomienda acciones en base al costo-beneficio de las mismas.

Para entender de mejor manera las metodologías se definirán algunos términos como:

- **Amenaza**: Una(s) persona(s) o cosa(s) vista(s) como posible fuente de peligro o catástrofe. Ejemplo: inundación, incendio, robo de datos, sabotaje, aplicaciones mal diseñadas, etc.

- **Vulnerabilidad**: La situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera suceder y así afectar el entorno informático. Ejemplos: falta de control de acceso lógico, inexistencia de un control de soportes magnéticos, falta de cifrado en las telecomunicaciones, etc.

- **Riesgo**: La probabilidad de que una amenaza llegue a suceder por una vulnerabilidad.

- **Exposición o Impacto:** La evaluación del efecto del riesgo. Ejemplo: impacto en términos económicos, aunque no siempre lo es, como vidas humanas, imagen de la empresa, honor, defensa nacional, etc.
- **Riesgos que se pueden:**

Evitarlos no construir un centro de datos donde hay peligro constante de inundaciones.

Transferirlos uso de un centro de datos controlado.

Reducirlos con un sistema de detección y extinción de incendios por ejemplo.

Asumirlos. Es lo que se hace si no se controla el riesgo en absoluto.

Tipos de Metodologías

Las metodologías existentes y utilizadas en la auditoría y el control informático, se pueden agrupar en dos grandes familias. Éstas son:

- **Cuantitativas**. Basadas en un modelo matemático numérico que ayuda a la realización del trabajo.
- **Cualitativas**. Basadas en el criterio y razonamiento humano capaz de definir un proceso de trabajo, para seleccionar en base a la experiencia acumulada.

Metodologías Cuantitativas

Estas metodologías han sido diseñadas para elaborar una lista de riesgos que pueden ser comparables entre sí, para poder asignarles valores numéricos. Estos valores en el caso de metodologías de análisis de riesgos, son datos de probabilidad de ocurrencia de un evento que se debe obtener de un registro de incidencias donde el número de incidencias sea suficientemente grande.

Esto no se aplica con exactitud en la práctica, pero dado que el cálculo se hace para ayudar a seleccionar el método entre varias contramedidas podría ser aceptado.

Hay varios coeficientes que conviene definir:

A.L.E. (Annualized Loss Expectancy): multiplicar la pérdida máxima posible de cada bien /recurso por la amenaza con probabilidad más alta.

Retorno de la Inversión (R.O.I.): A.L.E. original menos A.L.E. reducido (como resultado de la medida), dividido por el coste anualizado de la medida.

Reducción del A.L.E. (Annualized Loss Expectancy): Es el cociente entre el coste anualizado de la instalación y el mantenimiento de la medida contra el valor total del

bien /recurso que se está protegiendo, en tanto por ciento.

Estos coeficientes y algunos otros son utilizados para la simulación que permite elegir entre varias contramedidas en el análisis de riesgos.

Metodologías Cualitativas

Requieren de la participación de un profesional con experiencia. Basadas en métodos estadísticos y lógica humana, la cual utiliza menos recursos humanos / tiempo que las metodologías cuantitativas.

Metodologías más Comunes

Entre las metodologías más habituales de evaluación de sistemas se puede mencionar a las de plan de contingencias, las de auditoría de controles generales, las de análisis de riesgos o de diagnósticos de seguridad.

Plan de contingencia

Un plan de contingencia es una estrategia planificada por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos enfocados a conseguir una restauración progresiva y rápida de los servicios de negocios afectados por una paralización total o parcial de la capacidad operativa de la empresa.

Parámetros de un Plan de Contingencia

- Sigue el prestigioso ciclo de vida iterativo (planificar-hacer-comprobar-actuar)
- Nace de un análisis de riesgo donde, entre otras amenazas, se identifican aquellas que afectan a la continuidad del negocio.
- Debe ser revisado periódicamente. Generalmente, la revisión será consecuencia de un nuevo análisis de riesgo.
- Se modifica el plan de contingencias de acuerdo a las revisiones aprobadas y, de nuevo, se inicia el ciclo de vida del plan.

El plan de contingencias comprende tres subplanes. Cada plan determina las contramedidas necesarias en cada momento del tiempo relacionada a la materialización de cualquier amenaza:

Plan de respaldo. Contempla las contramedidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.

Plan de emergencia. Contempla las contramedidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad es disminuir los efectos adversos de la amenaza.

Plan de recuperación. Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

Controles Generales

Se usan para obtener una opinión sobre la fiabilidad de los datos, basadas en cuestionarios estándares que dan como resultados informes muy generales. Por otro lado la Metodología de auditor interno también cumple la misma función pero son diseñadas por el propio auditor.

Metodologías de Análisis de Riesgo

Están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contra medidas. El esquema básico de una metodología de análisis de riesgos es, en esencia, el representado a continuación:

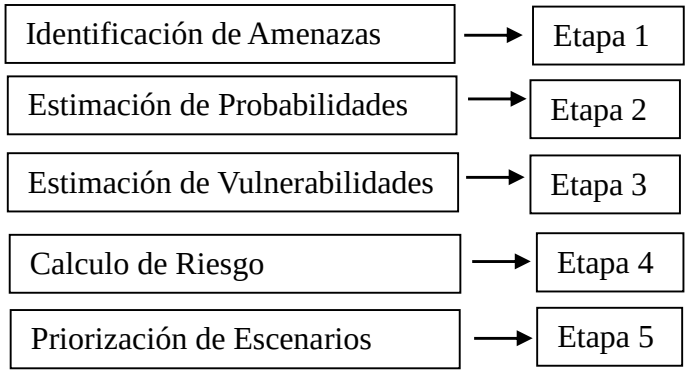


Gráfico 3: Esquema básico de metodología de Análisis de Riesgos
Fuente: (FOPAE, 2012)

- **Identificación de Amenazas** Identificación de actividades o amenazas que impliquen riesgos durante las fases de construcción, operación / mantenimiento y cierre / abandono de la Organización.

- **Estimación de Probabilidades** Una vez identificadas las amenazas o posibles aspectos iniciadores de eventos, se debe realizar la estimación de su probabilidad de ocurrencia del incidente o evento, en función a las características específicas.

- **Estimación de Vulnerabilidades** Estimación de la severidad de las consecuencias sobre los denominaos factores de vulnerabilidad que podrían resultar afectados (personas, medio ambiente, sistemas, procesos, servicios, bienes o recursos, e imagen empresarial)

- **Calculo de Riesgo** Se debe realizar el cálculo o asignación del nivel del riesgo. El riesgo está definido en función de la amenaza y la vulnerabilidad como el producto entre Probabilidad y Severidad del escenario.

- **Priorización de Escenarios** Los resultados del análisis de riesgos permiten determinar los escenarios en los que se debe priorizar la intervención.

- **Medidas de Intervención** Establecer la necesidad de la adopción de

medidas de planificación para el control u reducción de riesgos. Determinar el nivel de planificación requerido para su inclusión en los diferentes planes de acción

Existe varias metodologías como MEHARI (Security Stake Analysis and Classification Guide), MAGERIT, desarrollada por la administración española, entre otras, OCATVE (Opertionally Critical Threats, Assets and Vulnerability Evaluation) Como marco de referencia se puede mencionar a COBIT.

2.2 Metodología MEHARI

Mehari es un método para el análisis y gestión del riesgo. Esto significa que sus bases de conocimiento han sido diseñadas para un análisis de riesgos preciso, sin imponer el análisis de riesgo como una política de gestión prioritaria. La gestión de la seguridad es una actividad que evoluciona con el tiempo dependiendo de los esfuerzos realizados por una organización. (MEHARI, 2010)

Al momento de implementar seguridad siempre es necesario conocer el estado de las medidas y políticas de seguridad existentes en la organización, y de compararlas con las mejores prácticas para establecer el camino a seguir.

Luego de tomar la decisión de implementar la seguridad en la organización, deben decidirse las acciones concretas que sean necesarias llevar a cabo. Estas decisiones, que habitualmente se agruparán en forma de planes, normas corporativas, políticas o marcos de referencia de seguridad, deben llevarse a cabo utilizando una metodología estructurada. Esta metodología puede basarse en un análisis de riesgos, o incluir el concepto de riesgo, aunque no es imprescindible.

La coherencia de las herramientas es el principio fundamental de MEHARI, cada resultado obtenido en una etapa puede reutilizarse en siguientes etapas.

Las diferentes herramientas y módulos de la metodología MEHARI, están diseñadas para realizar el análisis de riesgos, pueden ser empleadas de forma

independiente en cualquier etapa del desarrollo de la seguridad, utilizando diferentes modos de gestión, y garantizando la coherencia de las decisiones resultantes.

Todas estas herramientas y módulos abarcan los instrumentos necesarios para la evaluación del estado de la seguridad, un módulo para analizar los intereses implicados por la seguridad, y un método de análisis de riesgos con herramientas de apoyo.

2.2.1 Los diagnósticos de seguridad

MEHARI plantea dos módulos para los diagnósticos de la seguridad:

- Módulo rápido
- Módulo detallado

En cada uno de los dos casos, el objetivo es evaluar el nivel de seguridad, es decir, evaluará la calidad de los servicios de seguridad. Los resultados dependerán directamente de la profundidad de la evaluación; si se realiza con el módulo rápido, se tendrá menos precisión y si se utiliza el detallado, será más confiable.

El **módulo rápido** se emplea para una primera evaluación debilidades más trascendentales. Los servicios de seguridad revisados son los mismos que los que se verifican con la evaluación detallada, pero las preguntas no son suficientes para evaluar todas las debilidades.

El **módulo detallado** investiga, cuidadosamente, las potenciales debilidades de cada uno de los servicios de seguridad. Esto constituye una base especializada, que podrá utilizada posteriormente para el análisis de riesgos.

La relación entre estos dos módulos permite empezar con el módulo rápido, cuyos diagnósticos pueden ahondar posteriormente con el módulo detallado.

- **El diagnóstico de seguridad, un elemento del análisis de riesgos**

MEHARI suministra un método de análisis de riesgos estructurado, la modelización del riesgo define "factores de reducción del riesgo", cuya evaluación depende de la calidad de los servicios de seguridad.
Un diagnostico detallado de los servicios de seguridad será la base principal para asegurar la reducción de los riesgos.

- **Planes de seguridad basados en diagnósticos de vulnerabilidad**

Una manera de gestión de la seguridad radica en la definición de planes de acción como consecuencia directa de la evaluación del estado de los servicios de seguridad.
El proceso de gestión de la seguridad es sencillo, consiste en efectuar una evaluación y perfeccionar todos los servicios que no tienen un nivel de calidad.

- **Soporte proporcionado por la base de conocimiento en la creación de un marco de referencia de seguridad**

El módulo de evaluación detallado utiliza la base de conocimiento de servicios de seguridad. Esto describe cada servicio: para qué sirve, contra que es usado, los mecanismos y soluciones que soportan el servicio, y los elementos que deberían ser considerados cuando se evalúa la calidad del servicio.

Esta base de conocimiento puede ser usada directamente para crear un marco de referencia de seguridad que incluirá las reglas seguridad e instrucciones que la organización deberá seguir.

- **Dominios cubiertos por el módulo de diagnóstico**

Para identificar todos los escenarios de riesgo y cubrir todos los riesgos no aceptables, MEHARI no se restringe únicamente al dominio informático.
El módulo de diagnóstico cubre la totalidad de la organización, la protección del sitio en general, el entorno de trabajo y aspectos legales y reglamentarios.

- **Síntesis sobre los módulos de diagnóstico**

Los módulos de diagnóstico brindan una visión extensa y coherente de la seguridad, pueden utilizarse de diferentes maneras, con diversos condiciones de progresividad según la madurez sobre la seguridad de la organización.

2.2.2 Análisis de los intereses implicados por la seguridad

Existe un principio con el que todos los responsables de los Centros de Datos están de acuerdo Independientemente de las políticas de seguridad: debe haber un justo equilibrio entre las inversiones en seguridad y el nivel de los intereses implicados por la seguridad.

Esto significa que el análisis de estos intereses merece un estudio prioritario y un método preciso y estructurado de evaluación, que debe contestar la siguiente doble pregunta:

"¿Qué puede suceder, y si sucede, puede ser grave?"

En el área de seguridad, los intereses son observados como las consecuencias de eventos que interrumpan las operaciones habituales de la organización.

MEHARI suministra un módulo denominado "análisis de los intereses implicados por la seguridad y clasificación", del cual se extraen dos resultados:

- Una escala de valoración de disfunciones.
- Una clasificación de la información y de los activos informativos

- **La escala de valoración de disfunciones**

  Establecer los acontecimientos o disfunciones que se pueden sospechar, es un procedimiento que se apoya en las actividades de la organización, la cual proporcionará:

  - Una descripción de los probables tipos de disfunciones.
  - Una explicación de los parámetros que intervienen en la gravedad de cada una de las disfunciones.
  - Una evaluación de los límites críticos de los parámetros que modifican el nivel de gravedad de las disfunciones.

  La escala de valoración de las disfunciones, está conformado por estos resultados

- **Clasificación de la información y de los activos**

  En la seguridad informática es frecuente hablar de la clasificación de la información y de la clasificación los activos.

Esta clasificación consiste en valorar, para cada tipo de información y para cada uno de los activos informáticos, la gravedad de la pérdida de cada característica como: Disponibilidad, Integridad, y Confidencialidad, de esta información o activo.

En los sistemas de información, la clasificación de la información y de los activos, es la escala de valoración de disfunciones, traducida en indicadores de sensibilidad asociados con los activos informáticos.

2.2.3 Análisis de riesgos

MEHARI tomando en cuenta que el análisis de riesgos es la fuerza motriz de la seguridad, ha suministrado una metodología estructurada para la evaluación del riesgo, basado en unos principios básicos.

Un escenario de riesgo está caracterizado por diferentes factores:

- Factores estructurales que no dependen de medidas de seguridad, pero si de la actividad principal de la organización, su entorno, y su contexto.
- Factores de reducción de riesgo que son una función directa de medidas de seguridad implementadas.

Estos factores pueden ser evaluados de forma cualitativa y cuantitativa con MAHERI, y por consiguiente, contribuye en la evaluación de los niveles de riesgo.

Para establecer el nivel de gravedad máximo de las consecuencias de una situación de riesgo se utiliza el análisis de los intereses implicados. Esto es típicamente un factor estructural, mientras que para evaluar los factores de reducción de riesgo se utilizará el diagnóstico de la seguridad.

- **Análisis de riesgos: metodología para la elaboración del plan de seguridad**

Esta metodología estructurada se fundamenta en una base de conocimientos de un escenario de riesgos y en procedimientos automatizados para la evaluación de los factores de disminución de riesgo, utilizando un software que evita al usuario hacer cálculos, y que también proporciona simulaciones y optimizaciones.

- **Análisis sistemático de situaciones de riesgo**

Una manera de gestión de la seguridad levemente diferente es: identificar todas las situaciones de riesgo potenciales, analizar las más críticas e identificar las acciones para reducir cada riesgo a un nivel aceptable. Las bases de conocimiento de MEHARI han sido desarrolladas para permitir este modelo de gestión. El objetivo es asegurar que se ha identificado cada situación de riesgo crítica y que ésta es cubierta por un plan de acción.

- **Análisis específico de situaciones de riesgo**

En los casos, donde la seguridad se administra a través de auditorías o marcos de referencia de seguridad, siempre habrá casos específicos por los cuales las reglas no podrán aplicarse. El análisis de riesgos específico se puede utilizar para decidir cuál es el mejor camino a seguir.

- **Análisis de riesgo en nuevos proyectos**

MEHARI pueden emplearse en la gestión de proyectos, para identificar los riesgos y decidir qué medidas son necesarias.

Descripción general de las aplicaciones de MEHARI

MEHARI ayuda a analizar y reducir riesgos con sus bases de conocimiento, mecanismos y herramientas que se han creado con este propósito (MEHARI, 2010). La necesidad de un método estructurado de análisis y reducción de riesgos puede ser, dependiendo de la organización:

- Un método de trabajo permanente la guía para un grupo especializado
- Un método de trabajo utilizado en paralelo junto a otras prácticas de gestión de la seguridad,
- Un método de trabajo utilizado ocasionalmente como complemento a las prácticas habituales.

MEHARI suministra un conjunto de conceptos, métodos y herramientas que permiten analizar los riesgos si es necesario, que comprende las bases de conocimiento, los manuales y las guías que describen los diferentes módulos (intereses implicados, riesgos, vulnerabilidades), ayuda al personal implicado en la gestión de la

seguridad (Responsables de Seguridad, gerentes de riesgos, auditores, CIOs..), en sus diferentes tareas y actividades.

2.3 Metodología MAGERIT

MAGERIT "Es la Metodología de Análisis y Gestión de Riesgos elaborada por el Consejo Superior de Administración Electrónica de España, es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. Magerit persigue los siguientes objetivos": (Dirección General de Modernización Administrativa, 2012)

Directos:

- Concienciar a los responsables de la información de las organizaciones la existencia de riesgos y de la necesidad de gestionarlos

- Proporcionar un método sistemático para analizar los riesgos provenientes del uso de tecnologías de la información y comunicaciones (TIC)

- Apoyar a descubrir y planificar el tratamiento adecuado para mantener los riesgos bajo control

Indirectos:

- Acondicionar a la Organización para procesos de evaluación, auditoría, certificación o acreditación.

Proceso de la Metodología MAGERIT

Las actividades que se realizan en la metodología MAGERIT cumplen con un proceso que tendrán un lineamiento para llegar a los resultados propuestos que será explicado a continuación:

1. Identificación de Activos: Se refiere los activos que posee la Organización categorizados de acuerdo a su función.
2. Valoración de Activos: Es la valoración establecida al activo de acuerdo a la criticidad.
3. Identificación de Amenazas: Son eventos que reducirían el valor de los activos.
4. Frecuencia: Se refiere a los eventos que se producen en un tiempo determinado.
5. Degradación: Es que tan perjudicado quedaría el activo al materializarse las amenazas.
6. Impacto: Es un indicador de qué puede suceder cuando ocurren las amenazas.
7. Riesgo: Es la probabilidad de materialización de amenazas sobre el activo.
8. Identificación y Valoración de Salvaguardas: Son las acciones concretas para reducir el riesgo;
9. Riesgo Residual: Es el riesgo remanente después de emplear las salvaguardas.

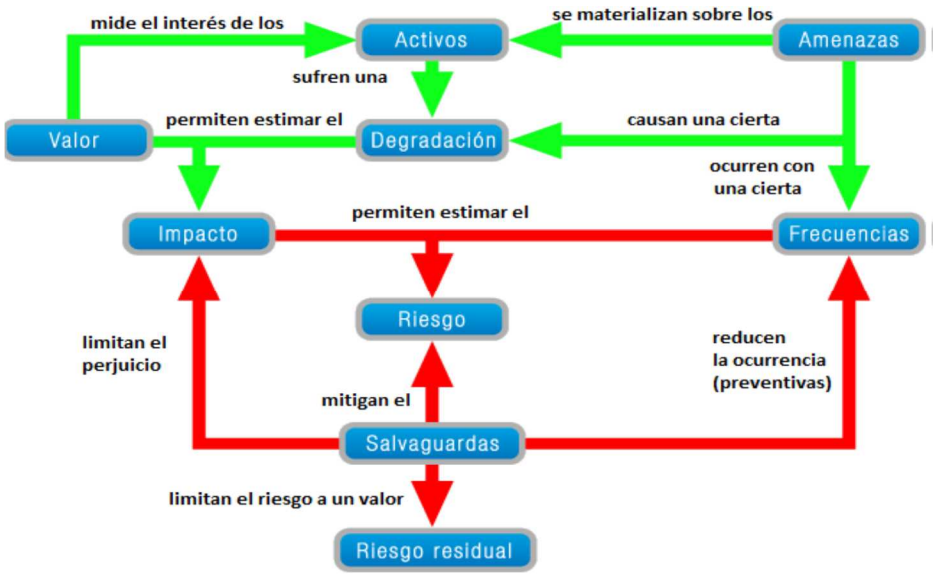


Gráfico 4: Proceso MAGERIT

Fuente: (Ramos, 2012)

2.3.1 Identificación de Activos

La organización identifica los activos, en el cual se puede distinguir 2 activos esenciales:

- La información que maneja

- Los servicios que presta.

Los requisitos de seguridad para todos los demás componentes del sistema están establecidos por los activos esenciales. Para el manejo de esta cantidad de información se utilizará matrices, las cuales nos permitirá manipular otros activos relevantes como:

- **Datos** que materializan la información.
- **Servicios** auxiliares que se necesitan para poder organizar el sistema.
- **Las aplicaciones informáticas** *(software)* que permiten manejar los datos.
- **Los equipos informáticos** *(hardware)* y que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar** que complementa el material informático.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
- **Las personas** que explotan u operan todos los elementos anteriormente citados.

Las amenazas y las salvaguardas son diferentes dependiendo del tipo de activo

2.3.2 Dependencias

La información y los servicios prestados son los activos esenciales, los cuales dependen de otros activos más comunes como: los equipos, las comunicaciones, las instalaciones y las personas que trabajan con aquellos.

Esta subordinación hace que la seguridad de los activos que se encuentran en la parte superior de la estructura depende de los activos que se encuentran en la parte inferior. En otras palabras se puede mencionar que los activos inferiores, son los cimientos en los que se apoya la seguridad de los activos superiores, ya que cuando se materializa una amenaza en un activo inferior tiene como resultado un daño sobre el activo superior.

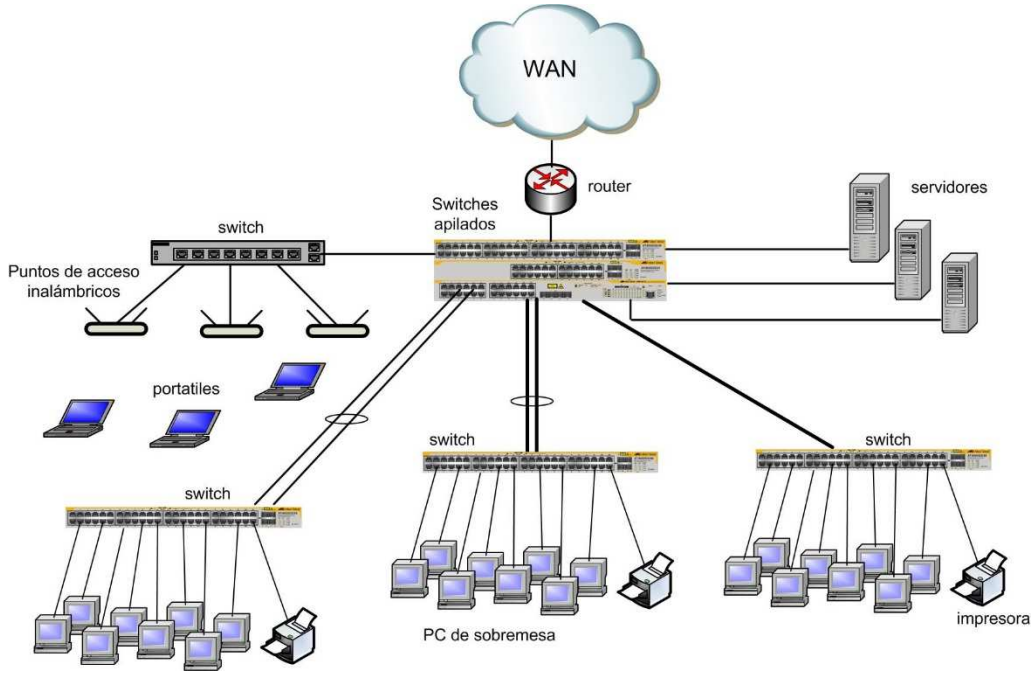


Gráfico 5: Dependencia de Servicios

Fuente: (redesinformatica, 2013)

2.3.3 Valoración

No se refiere a lo que cuestan las cosas, sino de lo que valen. La valoración se puede ver desde la punto de vista de la '**necesidad de proteger',** pues si el activo es más valioso, el nivel de protección que requiere es mayor según la dimensión de seguridad que sean oportunos. El valor que tiene un activo puede ser propio, o puede ser acumulado. Por lo que los activos inferiores en un modelo de dependencias, acumulan el valor de los activos superiores que se apoyan en ellos. En los activos esenciales el valor central frecuenta estar en la información que el sistema maneja y los servicios que se prestan.

La valoración puede ser cualitativa o cuantitativa.

- **Valoración cualitativa**

Permiten avanzar con rapidez las escalas cualitativas, ubicando el valor de cada activo en un orden coherente respecto de los demás. La restricción de las valoraciones cualitativas es que no admiten sumar valores.

- **Valoración cuantitativa**

Permiten sumar valores numéricos de forma "natural". Si la valoración es monetaria, se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución

Dimensiones

Se debe evaluar diferentes dimensiones de un activo:

- **Confidencialidad**: ¿qué daño produciría que lo supiera quien no debe? Esta valoración es típica de datos.
- **Integridad**: ¿qué inconveniente produciría si estuviera dañado? Esta valoración es característica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
- **Disponibilidad**: ¿qué inconveniente produciría no tenerlo o no poder utilizarlo? Esta valoración es característica de los servicios.

En los activos esenciales, es útil valorar continuamente:

- **Autenticidad:** ¿qué inconveniente produciría no conocer exactamente quien hace o ha hecho cada cosa?
- **Trazabilidad del uso del servicio**: ¿qué desperfecto produciría no conocer a quién se le suministra tal servicio? Es decir, quién hace qué y cuándo
- **Trazabilidad del acceso a los datos:** ¿qué desperfecto produciría no conocer quién accede a qué datos y qué hace con ellos?

2.3.4 Amenazas

Se debe determinar las amenazas que pueden dañar a cada activo. Las amenazas son sucesos que ocurren.

- **Identificación de las Amenazas**

En Magerit entre las amenazas más comunes se puede mencionar a las siguientes:

De origen natural

Hay accidentes naturales (terremotos, inundaciones, ...) frente a esos sucesos el sistema de información es víctima pasiva.

Del entorno (de origen industrial)

Hay desastres industriales (contaminación, fallos eléctricos, ...) frente a estos sucesos el sistema de información es víctima pasiva, pero no se debe permanecer indefensos.

Defectos de las aplicaciones

Hay inconvenientes que aparecen directamente en el equipamiento por errores en su diseño o en su implementación, que suelen tener consecuencias negativas sobre el sistema. A menudo se las conoce como vulnerabilidades técnicas.

Causadas por las personas de forma accidental

Los problemas no intencionados pueden ser ocasionados por personas que tienen acceso al sistema de información.

Causadas por las personas de forma deliberada

Los problemas intencionados pueden ser ocasionados por personas que tienen acceso al sistema de información, se los denomina ataques deliberados, cuya finalidad es beneficiarse ilegalmente y causar daños a los propietarios.

- **Valoración de las amenazas**

Luego de haber establecido que una amenaza puede dañar a un activo, se debe valorar su efecto en el valor del activo, en dos sentidos:

Degradación: que tan afectado resultaría el [valor del] activo

Probabilidad: que tan probable o improbable es que se plasme la amenaza

La degradación estima el daño ocasionado por un incidente en el supuesto de que sucediera.

La probabilidad de ocurrencia frecuentemente se presenta cualitativamente por medio de alguna escala nominal:

Tabla 2: Degradación de Valor

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Fuente: (Dirección General de Modernización Administrativa, 2012)

A veces se presenta numéricamente como una frecuencia de ocurrencia.

Tabla 3: Probabilidad de ocurrencia

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Fuente: (Dirección General de Modernización Administrativa, 2012)

Determinación del impacto potencial

Se denomina impacto al daño sobre el activo de una amenaza que se ha materializado. Tipos de impacto que puede tener un activo:

Impacto acumulado

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración tomando en cuenta: Su valor acumulado y las Amenazas a que está expuesto. Una vez que se ha realizado el cálculo del impacto acumulado se puede establecer las salvaguardas como protección de los equipos, copias de respaldo, etc.

Impacto repercutido

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración tomando en cuenta: Su valor propio y las amenazas a que están expuestos los activos de los que depende. Luego de haber realizado el cálculo del impacto repercutido ayudará a la gerencia a la toma de decisiones críticas de un análisis de riesgo y a aceptar un cierto nivel de riesgo.

Determinación del riesgo potencial

Una vez identificado el impacto de las amenazas sobre los activos, se puede determinar la probabilidad de ocurrencia.

En el grafico que se muestra a continuación se puede distinguir varias de zonas que se deben tomar en cuenta en el tratamiento del riesgo

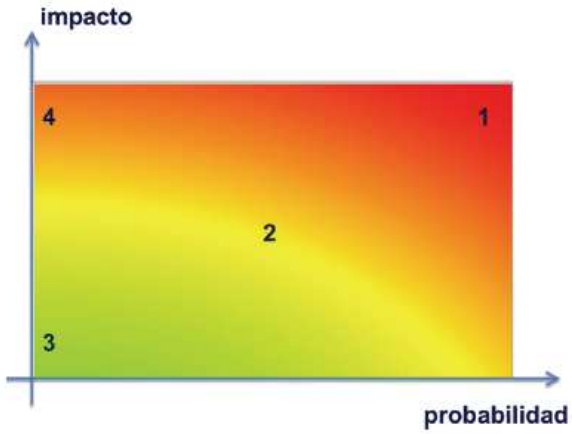


Gráfico 6: El riesgo en función del Impacto y la Probabilidad
Fuente: (Dirección General de Modernización Administrativa, 2012)

zona 1 – riesgos muy probables y de muy alto impacto
zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo
zona 3 – riesgos improbables y de bajo impacto
zona 4 – riesgos improbables pero de muy alto impacto

Riesgo acumulado

El Riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración tomando en cuenta: El impacto acumulado sobre un activo debido a una amenaza y La probabilidad de la amenaza. Una vez que se ha realizado

el cálculo del impacto acumulado se puede establecer las salvaguardas como protección de los equipos, copias de respaldo, etc.

Riesgo repercutido

El Riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración tomando en cuenta: El impacto repercutido sobre un activo debido a una amenaza y La probabilidad de la amenaza. Luego de haber realizado el cálculo del impacto repercutido ayudará a la gerencia a la toma de decisiones críticas de un análisis de riesgo y a aceptar un cierto nivel de riesgo.

2.3.5 Salvaguardas

En la actualidad no es frecuente encontrar sistemas desprotegidos, ya que las salvaguardas son mecanismos tecnológicos que reducen el riesgo.

Selección de salvaguardas

Existe un espectro extenso de las posibles salvaguardas que se pueden tomar en cuenta, por lo que se hace necesario realizar una selección de las salvaguardas más relevantes para lo que hay que proteger. En esta selección se deben tener en cuenta los siguientes aspectos:

1. Tipo de activos a proteger.
2. Dimensión o dimensiones de seguridad que requieren protección
3. Amenazas de las que necesitamos protegernos
4. Si existen salvaguardas alternativas

Además de todo el espectro de salvaguardas se debe excluir una cierta salvaguarda de acuerdo a las afirmaciones:

- **No aplica** cuando técnicamente no es adecuada al tipo de activo a proteger.
- **No se justifica** cuando la salvaguarda aplica, pero es excesiva al riesgo que se tiene que proteger

Tipos de Salvaguardas

Existen diferentes tipos de protección que ofrecen las salvaguardas, las cuales se relacionan con la reducción de degradación y de la probabilidad.

Tabla 4: Tipos de Salvaguardas

Efecto	**Tipo**
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: (Dirección General de Modernización Administrativa, 2012)

Eficacia de la salvaguarda

Además de por su existencia, las salvaguardas se caracterizan, por su eficacia frente al riesgo que procuran impedir. La salvaguarda ideal es 100% eficaz.

Entre una eficacia del 0% para aquellas que faltan y el 100% para aquellas que son idóneas y que están perfectamente implantadas, se estimará un grado de eficacia real en cada caso concreto.

Tabla 5: Eficacia de las salvaguardas

Factor	**Nivel**	**Significado**
0%	L0	inexistente

	L1	Inicial / ad hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso Definido
	L4	Gestionado y Medible
100%	L5	Optimizado

Fuente: (Dirección General de Modernización Administrativa, 2012)

2.3.6 Impacto

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de la amenaza, en otras palabras es un indicador de qué puede suceder cuando ocurren las amenazas.

Impacto Residual

Luego de haber implementado una o varias salvaguardas, el sistema permanece en un entorno de posible impacto que se denomina residual.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores

2.3.7 Riesgo

Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños a la organización, es decir, es lo que probablemente ocurra.

Riesgo Residual

Luego de haber implementado una o varias salvaguardas, el sistema permanece en un entorno de posible riesgo que se denomina residual.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

2.4 Metodología de Valoración de Riesgos OCTAVE

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) “es una metodología que mejora el proceso de toma de decisiones que tiene que ver con la

protección y gestión de recursos de una organización, así como una herramienta de análisis de riesgos" (Betolin, 2013). Se pueden identificar principalmente dos métodos

- OCTAVE: el utilizado para grandes empresas de trescientos o más empleados.
- OCTAVE-S para organizaciones con pocos empleados (PYMES).

2.4.1 Principales Aspectos de OCTAVE:

OCTAVE permite un distinto comienzo y fin en las actividades de gestión de riesgos de las organizaciones, puede realizarse tanto de forma puntual-eventual como de forma periódica.

- Es auto-dirigida, las personas de la organización realizan la evaluación ya que ellos conocen los requisitos y operaciones de la organización.
- Se enfoca en el riesgo de la organización y en las cuestiones estratégicas
- Utiliza un pequeño equipo de personas pertenecientes a unidades operacionales del giro del negocio y del departamento de tecnologías de la información.
- Se basa en las prácticas de seguridad y riesgo operacional, la tecnología sólo se examina en relación a las prácticas de seguridad.

OCTAVE tiene un enfoque de evaluación por activos. La valoración del riesgo se basan en tres principios básicos de administración de seguridad**: confidencialidad, integridad y disponibilidad.**

En el enfoque de OCTAVE incluyen principios, atributos y salidas:

Los principios. Son conceptos principales que direccionan la evaluación proporcionando una base para la misma. La auto-dirección es uno de los principios de OCTAVE, esto significa que las personas de la organización están aptos para liderar la evaluación y la toma de decisiones. Los requisitos de la evaluación se embeben en los atributos y salidas.

Los atributos. Definen lo que es necesario hacer para que la evaluación sea un éxito desde las perspectivas de procesos y organizacional.

Las salidas. Son los resultados que un equipo de análisis debe producir durante la evaluación.

2.4.2 Fases de la evaluación de riesgo con OCTAVE

OCTAVE es una metodología conducida por procesos para identificar, priorizar y gestionar los riesgos de seguridad de la información.
En el proceso de OCTAVE, se pueden establecer tres fases de evaluación de riesgos

Fase-1 (visión-evaluación organizacional).

Se trata de construir los perfiles de amenazas basados en los activos. Se identifican los activos importantes, lo que se debe hacer para proteger los activos y los requisitos de seguridad para cada activo. El equipo de análisis determina los activos críticos y que se hace actualmente para protegerlos. Se identifican los requisitos de seguridad para cada activo crítico. Finalmente se establecen las vulnerabilidades organizacionales con las prácticas existentes y el perfil de amenazas para cada activo crítico.

Fase-2 (visión-evaluación tecnológica).

El equipo de análisis identifica los caminos de acceso por red y las clases de componentes TIC relacionados con cada activo crítico. El equipo luego determina la extensión a la que cada clase de componente es resistente a los ataques de red y establece las vulnerabilidades tecnológicas que exponen a los activos críticos. Se trata de identificar las vulnerabilidades técnicas de infraestructura. Se examinan los caminos de acceso por red, las clases de componentes TIC para cada activo y se determina la resistencia a los ataques de red.

Fase-3 (desarrollo de planes y estrategia de seguridad).

El equipo de análisis establece-evalúa los riesgos a los activos críticos de la organización en base al análisis de la información recogida y decide qué hacer al respecto. El equipo crea una estrategia de protección para la organización y planes de mitigación para abordar los riesgos identificados. El equipo determina también las siguientes etapas requeridas para la implementación y para ganar la aprobación de la alta dirección al resultado de todo el proceso. Se identifican los riesgos de los activos críticos, se desarrollan estrategias de protección y planes de mitigación y el análisis se basa en las fases previas.

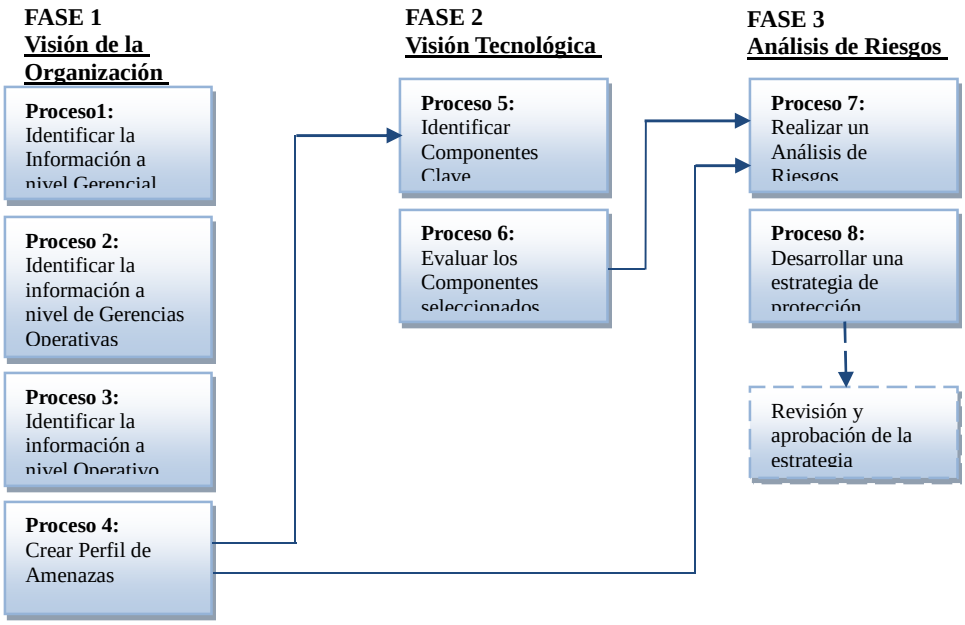


Gráfico 7: Esquema de Fases y Procesos de Octave

Fuente: (Gestion de Riesgos, 2013)

CUADRO COMPARATIVO DE METODOLOGÍAS PARA ANÁLISIS DE RIESGOS

Con lo revisado anteriormente se realizará un cuadro comparativo de las metodologías de análisis de riesgos:

Tabla 6*:* Comparación de metodologías para análisis de riesgos

CRITERIO DE COMPARACIÓN	MEHARI	MAGERIT	OCTAVE
Funcionalidad	Diagnóstico de Seguridad Análisis de los Intereses Implicados por la Seguridad Análisis de Riesgos	Análisis de Riesgos Gestión de Riesgos	Construcción de los Perfiles de Amenazas Basados en Activos Identificación de la Infraestructura de Vulnerabilidades Desarrollo de Planes y Estrategias de Seguridad
Elementos Principales	Niveles de categorías de controles Niveles de calidad de los servicios de seguridad Evaluación de la calidad del servicio por medio de cuestionarios Modelo de impactos	Escalas de valores cualitativos, cuantitativos y de indisponibilidad del servicio. Modelo de frecuencia de una amenaza como una tasa anual de ocurrencia. Escala alternativa de estimación del riesgo. Catálogos de amenazas Catálogos de medidas de control	Medidas de probabilidad considerando un rango de frecuencias. Análisis del límite entre niveles de probabilidad

2.5 Marco de Referencia COBIT

Misión

Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento. (IT Gobernance Institute, 2007)

Procesos

El marco de trabajo de COBIT proporciona un modelo de 34 procesos de referencia y un lenguaje común para que todos en la empresa visualicen y administren las actividades de TI. La incorporación de un modelo operativo y un lenguaje común para todas las parte de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno.

En la figura se ilustra el Marco de Trabajo General de COBIT

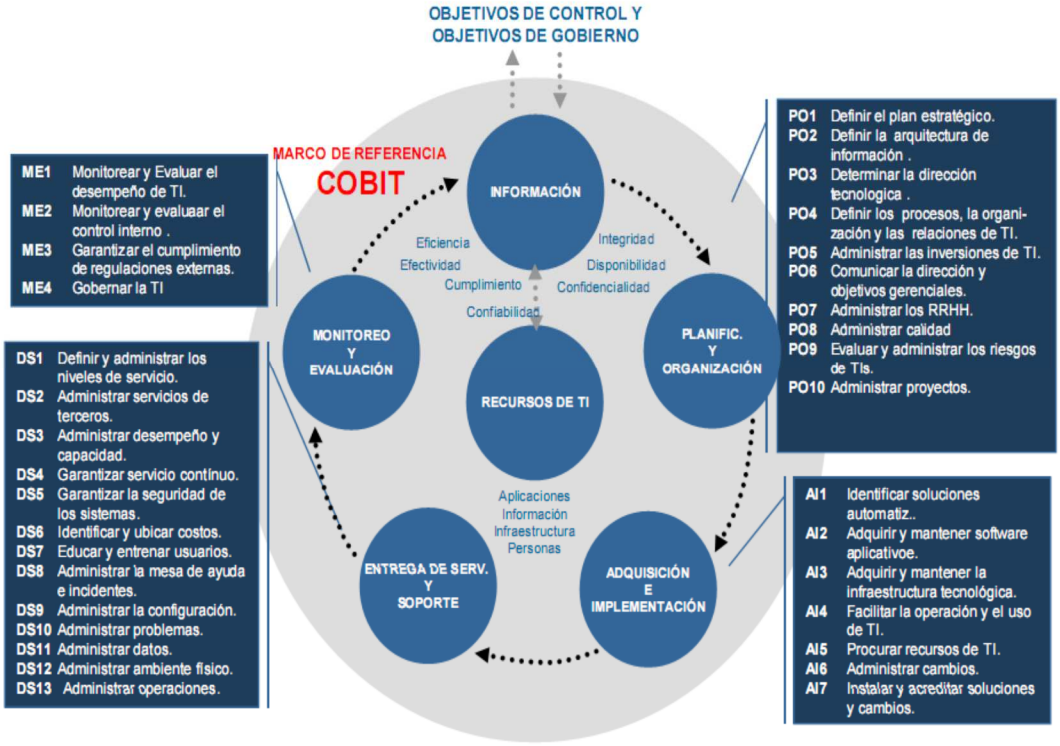


Gráfico 8: Marco de Trabajo General de COBIT

Fuente: (IT Gobernance Institute, 2007)

COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son:

- Planear y Organizar
- Adquirir e Implementar
- Entregar y Dar Soporte
- Monitorear y Evaluar.

Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

2.5.1 Planear y Organizar (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas.

2.5.2 Adquirir e Implementar (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

2.5.3 Entregar y Dar Soporte (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos.

2.5.4 Monitorear y Evaluar (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

2.5.5 Objetivos de Control

El control está definido como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proveer con una seguridad razonable que los objetivos de negocios serán alcanzados.

Los objetivos de control de COBIT son los requerimientos mínimos para el control efectivo de cada proceso de TI.

Los objetivos de control de TI de COBIT están organizados mediante procesos de TI, el marco de referencia provee un vínculo claro entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

El Marco de Referencia de Control COBIT contribuye a la necesidad de controlar la entrega satisfactoria de los servicios de TI en función de los objetivos de negocios:

- Vinculando TI a los requerimientos de negocios
- Organizando las actividades de TI en un modelo de proceso generalmente aceptado
- Identificando los principales recursos de TI a ser enfatizados
- Definiendo los objetivos de control de gestión a ser considerados.

2.5.6 Interrelaciones de los Componentes COBIT

Los componentes de COBIT se interrelacionan, ofreciendo soporte para las necesidades de gobierno, de administración, de control y de auditoría de los distintos interesados de acurdo a los requerimientos del negocio.

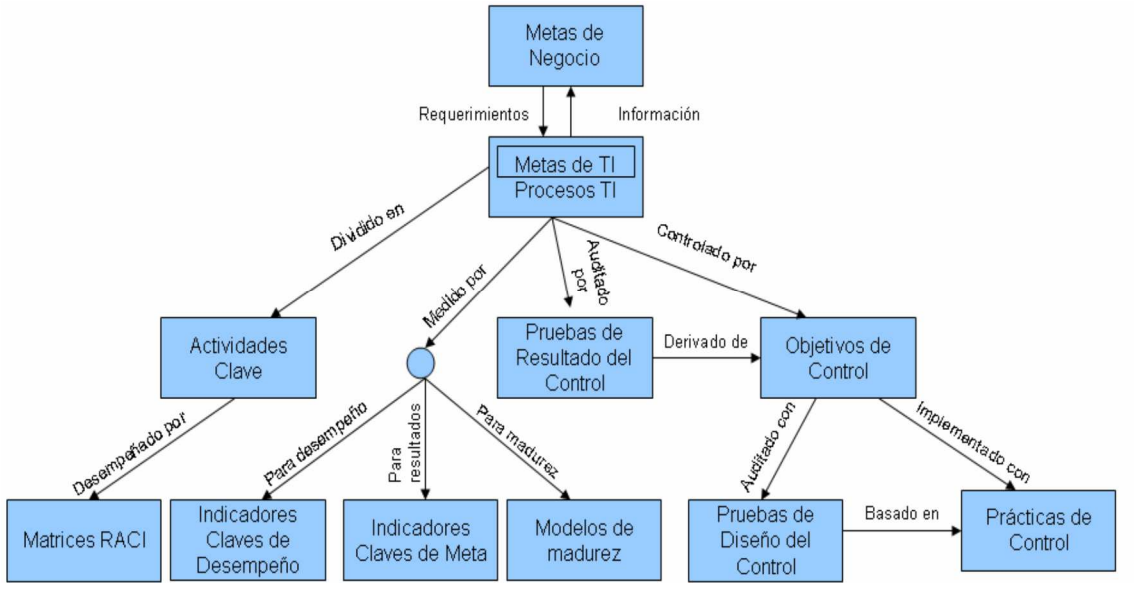


Gráfico 9: Interrelaciones componentes COBIT

Fuente: (IT Gobernance Institute, 2007)

2.5.7 Metas de Negocio y Metas de TI.

La definición de un conjunto de metas genéricas de negocios y TI provee una base más refinada para establecer requerimientos de negocios y desarrollar las métricas que permitan la medición contra estas metas.

Cada empresa usa TI para soportar iniciativas de negocios y estas pueden estar representadas como metas de negocio para TI

Si TI va a entregar exitosamente servicios para soportar la estrategia de la empresa, debería haber una propiedad y dirección claras de los requerimientos para el negocio (el cliente) y un claro entendimiento de qué necesita ser entregado y como por parte de TI (el proveedor).

Las empresas exitosas comprenden los riesgos, explotan los beneficios de TI para:

- Alinear la estrategia de TI con la estrategia del negocio
- Ir transmitiendo y conectando la estrategia de TI y las metas hacia abajo en la empresa
- Proveer estructuras organizacionales que faciliten la implementación de estrategias y metas
- Crear relaciones constructivas y comunicaciones efectivas entre los negocios y TI, y con socios externos

Las áreas de TI no pueden hacer una entrega eficaz en función de los objetivos de negocios y los requerimientos de gobierno sin adoptar e implementar un marco de referencia de gobierno y control de TI para:

Hacer un vínculo a los requerimientos de negocio

Hacer que el funcionamiento sea transparente en función de esos requerimientos

Organizar sus actividades en un modelo de procesos generalmente aceptado

Identificar los recursos principales a ser potenciados

Definir los objetivos de control de gestión a ser considerados

Las mejores prácticas de TI se han vuelto significativas por un número de factores:

- Los gestores de negocio y directores demandan un mejor retorno de las inversiones de TI

- La preocupación sobre el generalmente creciente nivel de gastos de TI
- La necesidad de cumplir requerimientos regulatorios para controles de TI en áreas tales como privacidad y reportes financieros, y en sectores específicos tales como finanzas, industria farmacéutica y salud
- La selección de proveedores de servicio y la gestión del outsourcing de servicios y compras.
- Riesgos, relacionados con TI, crecientemente complejos tales como seguridad de redes.
- Iniciativas de gobierno de TI que incluye la adopción de marcos de referencia de control y mejores prácticas para ayudar a monitorear y mejorar actividades críticas de TI para incrementar el valor del negocio y reducir los riesgos del mismo.
- La necesidad de optimizar costos siguiendo, si es posible, aproximaciones estándares en lugar de desarrollos especiales.
- La creciente madurez y consecuente aceptación de marcos de referencia bien considerados como COBIT, ITIL, ISO 17799, ISO 9001, CMM.
- La necesidad de las empresas de evaluar cómo están respecto de estándares generalmente aceptados y respecto a sus pares.

Como se asegura la empresa que TI alcanza los objetivos y soporta el negocio?

Definiendo objetivos de control que aseguren que:

- Se alcancen los objetivos de negocio.
- Se prevengan o detecten y corrijan eventos indeseados.

Estableciendo y monitoreando los controles y niveles de funcionamiento de TI apropiados mediante:

- Mediciones (Benchmarking) de capacidad de proceso de TI expresada como modelos de madurez.
- Metas y Métricas de los procesos de TI para definir y medir sus resultados y funcionamiento (Balanced ScoreCard).
- Metas de Actividad para tener estos procesos bajo control (COBIT).

Importancia de un Marco de Referencia de Control para el Gobierno de TI.

Cada vez más la alta dirección percibe el impacto significativo que la información puede tener en el destino de la empresa.

La alta dirección necesita conocer si la TI está siendo gestionada de manera que esta es:

- Adecuada para alcanzar los objetivos
- Suficientemente flexible para aprender y adaptarse
- Consecuente en la gestión de los riesgos que enfrenta
- Apropiada reconociendo oportunidades y actuando sobre ellas.

Quienes necesitarían de un Marco de Referencia de Control para el Gobierno de TI.

Un marco de referencia de gobierno y control necesita servir a una variedad de actores internos y externos:

Accionistas dentro de la empresa quienes tienen un interés en generar valor de las inversiones de TI:

- Aquellos que toman decisiones de inversión
- Aquellos que deciden sobre requerimientos
- Aquellos que usan los servicios de TI.

Accionistas internos y externos que proveen servicios de TI:

- Aquellos que gestionan la organización y los procesos de TI
- Aquellos que desarrollan capacidades
- Aquellos que operan los servicios

Accionistas internos y externos que tienen responsabilidades de control/riesgos:

- Aquellos con responsabilidades de seguridad, privacidad y/o riesgos
- Aquellos que realizan funciones de aprobación
- Aquellos que requieren o proveen servicios de garantía.

Criterios de información de COBIT.

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

- Eficacia
- Eficiencia
- Confidencialidad
- Integridad
- Disponibilidad
- Conformidad
- Confiabilidad

Eficacia: Información relevante a los procesos de negocios y su entrega en tiempo, correcta, consistente y usable.

Eficiencia: Provisión de información a través del óptimo uso de los recursos.

Confidencialidad: Protección de información sensible contra acceso no autorizado
Integridad: Exactitud y completitud de la información y su validez de acuerdo a los valores y expectativas de negocio.

Disponibilidad: Que la información esté disponible cuando sea requerida por el proceso de negocios ahora y en el futuro.

Conformidad: Se ocupa de cumplir con las leyes, regulaciones y contratos a los cuales se sujeta el proceso de negocios.

Confiabilidad: Provisión de información apropiada a la gerencia para operar la organización.

Recursos de TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio.

Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada (Ej., un sistema de planeación de recursos empresariales) para dar soporte a la capacidad del negocio (Ej., implementando una cadena de suministro) que genere el resultado deseado (Ej., mayores ventas y beneficios financieros)
Los recursos de TI identificados en COBIT se pueden definir como:

- Aplicaciones
- Información
- Infraestructura
- Personas

Aplicaciones: incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

Información: son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.

Infraestructura: es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

Personas: son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

Impacto de los objetivos de control COBIT sobre los recursos y criterios de TI

En la siguiente tabla se muestra el impacto de los objetivos de control COBIT sobre los recursos y criterios de TI. En los recursos de TI una X significa que ese objetivo de control tiene impacto sobre el recurso y un espacio en blanco que no tiene impacto. En los criterios de información se identifica el grado de impacto; Primario (P), para indicar impacto directo sobre el criterio de información, Secundario (S) impacto indirecto o en menor medida y espacio en blanco o vacío, que no tiene impacto alguno.

Tabla 7: Impacto de los objetivos de control COBIT sobre los recursos de TI

D	PROCESOS DE TI	Criterios de Información	Recursos de TI

			Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		Recursos Humanos	Sistemas de Información	Tecnología	Instalaciones	Datos
Planeación y Organización	PO1	Definir un Plan Estratégico de TI	P	S							X	**X**	**X**	**X**	**X**
	PO2	Definir la Arquitectura de Información	P	S	S	S						**X**			**X**
	PO3	Definir la Dirección Tecnológica	P	S									**X**	**X**	
	PO4	Definir la Organización y las Relaciones de TI	P	S							X				
	PO5	Administrar la Inversión de Tecnología de Información	P	P					S		X	**X**	**X**	**X**	
	PO6	Comunicar las Aspiraciones y Dirección de la Gerencia	P					S			X				
	PO7	Administrar Recursos Humanos	P	P							X				
	PO8	Asegurar el cumplimiento con los Rewuerimientos Externos	P					P	S		X	**X**			**X**
	PO9	Evaluar los Riesgos	S	S	P	P	P	S	S		X	**X**	**X**	**X**	**X**
	PO10	Administrar Proyectos	P	P							X	**X**	**X**	**X**	
	PO11	Administrar Calidad	P	P		P			S		X	**X**	**X**	**X**	
Adquisición e Implementación	AI1	Identificar Soluciones Automatizadas	P	S								**X**	**X**	**X**	
	AI2	Adquirir y Mantener Software de Aplicación	P	P		S		S	S			**X**			
	AI3	Adquirir y Mantener la Infraestructura Tecnológica	P	P		S							**X**		
	AI4	Desarrollar y Mantener los Procedimientos	P	P		S		S	S		X	**X**	**X**	**X**	
	AI5	Instalar y Acreditar Sistemas	P			S	S				X	**X**	**X**	**X**	**X**
	AI6	Instalar y Acreditar Sistemas	P	P		P	P		S		X	**X**	**X**	**X**	**X**
Entrega de Servicios y Soporte	DS1	Definir Niveles de Servicio	P	P	S	S	S	S	S		X	**X**	**X**	**X**	**X**
	DS2	Administrar los Servicios prestados por Terceras Partes	P	P	S	S	S	S	S		X	**X**	**X**	**X**	**X**
	DS3	Administrar el Desempeño y la Capacidad	P	P			S					X	X	X	X
	DS4	Asegurar el Servicio Continuo	P	S			P				X	X	X	X	X
	DS5	Garantizar la Seguridad en los Sistemas			P	P	S	S	S		X	X	X	X	X
	DS6	Identificar y Asignar Costos		P							X	**X**	**X**	**X**	**X**
	DS7	Educar y Capacitar Usuarios	P	S							X				
	DS8	Atender y Aconsejar a los Clientes	P								X	**X**			
	DS9	Administrar la Configuración	P									**X**	**X**	**X**	
	DS10	Administrar Problemas e Incidentes	P	P			P				X	**X**	**X**	**X**	**X**
	DS11	Administrar Datos				P			P						**X**
	DS12	Administrar Instalaciones				P	P							**X**	
	DS13	Administrar Operaciones	P	P		S	S				X	**X**	**X**	**X**	**X**
Monitoreo	M1	Monitorear los Procesos	P	S	S	S	S	S	S		X	X	X	X	X
	M2	Evaluar que tan adecuado es el Control Interno	P	P	S	S	S	S	S		X	X	X	X	X
	M3	Obtener el Aseguramiento Independiente	P	P	S	S	S	S	S		X	X	X	X	X
	M4	Colaborar en la Auditoría Independiente	P	P	S	S	S	S	S		X	X	X	X	X

Fuente: (IT Gobernance Institute, 2007)

En la elaboración de la tesis se utilizará el procesos PO9 y ME4 de COBIT que son "Evaluar y Administrar los Riesgos de TI" **y** "Proporcionar Gobierno de TI", con el objetivo de poder desarrollar una estrategia de mitigación de Riesgos reduciendo el Riesgo Residual hasta un nivel aceptable por la organización.

COBIT no establece ninguna metodología de Análisis de Riesgos en particular, por lo que deja a libre elección la metodología más adecuada. Aquí es donde se presenta una relación entre COBIT y Magerit ya que esta última es una metodología de administración de riesgos. Relación que esta expresada en el plan de tesis.

Cuando se realiza una evaluación basada en riesgos los procesos PO9 y ME4 son los más indicados para realizar la misma.

En la Guía13 de Auditoria realizadas por ISACA, sugiere utilizar los procesos PO9 y ME4 cuando se realiza una auditoria basada en riesgos, es por esta razón elegido estos procesos para realizar este trabajo.

2.5.8 PO9 Evaluar y Administrar los Riesgos de TI

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgo de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable.

Este Proceso de Control nos permite Evaluar y Administrar los riesgos de TI, para más tarde analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio.

Lo que se logra con este proceso es:

- La Garantía de que la administración de riesgos está incluida completamente en los procesos administrativos, tanto interna como externamente, y se aplica de forma consistente.
- La realización de evaluaciones de riesgo.
- La recomendación y comunicación de los planes de acción para remediar los riesgos

Objetivos de Control

1 Marco de Trabajo de Administración de Riesgos

Establecer un marco de trabajo de administración de los riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.

2 Establecimiento del Contexto del Riesgo

Determinar el contexto interno y externo de cada evaluación, en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados.

3 Identificación de Eventos

Identificar una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa, con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Lo anterior se lo va a establecer con Magerit.

4 Evaluación

Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. Para esta evaluación se utilizará la metodología Magerit.

5 Respuesta a los Riesgos

Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos de costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.

6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos

Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación

de costos, beneficios y la responsabilidad de la ejecución. Obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas están a cargo del dueño (s) de los procesos afectados.

Modelo De Madurez

Existen varios niveles de madurez que puede alcanzar una institución de acuerdo a la administración de los riesgos de TI.

0 No Existente

Cuando la organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI.

1 Inicial / Ad Hoc

Cuando se realizan evaluaciones informales de riesgos tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto, es decir, que existe un entendimiento emergente que los riesgos de TI son importantes y necesitan ser considerados.

2 Repetible pero Intuitivo

Cuando la administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas.

3 Definido

Cuando la administración de riesgos sigue un proceso definido, el cual está documentado.

4 Administrado y Medible

Cuando los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI, otorgando por

parte de la gerencia un presupuesto para un proyecto de administración de riesgo operativo para re-evaluar los riesgos de manera regular.

5 Optimizado

Cuando la administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI, está bien aceptada, y abarca a los usuarios de servicios de TI y cuando la dirección evalúa las estrategias de mitigación de riesgos de manera contínua.

ME4 Proporcionar Gobierno de TI

La instauración de un marco de trabajo de gobierno efectivo, comprende la definición de procesos, roles responsabilidades dentro de la institución para asegurar que las inversiones institucionales de TI estén alineadas a los objetivos del negocio.

Lo que se logra con este proceso es:

- La instauración de un marco de trabajo para el Gobierno de TI, que forme parte del Gobierno Corporativo.

Objetivos de Control

1 Establecimiento de un Marco de Gobierno de TI

Especificar, implantar y alinear el marco de Gobierno de TI y gobierno Corporativo, asegurando el cumplimiento de las leyes y regulaciones que están alineadas a los objetivos de la empresa.

2 Alineamiento Estratégico

El rol de TI, las características y capacidades propias sobre temas estratégicos para la institución deben estar completamente entendidos por el consejo directivo y los ejecutivos. Proporcionar la alineación de TI con el negocio fomentando una co responsabilidad en la toma de decisiones.

3 Entrega de Valor

Garantizar que los resultados de la institución estén en concordancia con los programas las inversiones hechos en TI, para que de esta manera se dé el mayor valor posible en la consecución del portafolio institucional optimizando los costos.

4 Administración de Recursos

Realizar evaluaciones periódicas de las inversiones, uso y asignaciones de los activos de TI, para garantizar los recursos y el alineamiento con los objetivos del negocio.

5 Administración de Riesgos

El nivel de riesgo de TI aceptable por la institución debe ser definido por el Consejo Directivo. Establecer responsabilidades referentes a la administración de riesgos, garantizando que se realicen frecuentemente evaluaciones de riesgos a los que están expuestas las TI y el impacto que ocasionarían.

6 Medición de Desempeño

Constatar que el portafolio que se planteó para TI se logró, o si el avance del portafolio tiene buenas perspectivas de que se cumpla.

7 Aseguramiento Independiente

Las políticas de la institución, estándares, buenas prácticas, la efectividad y eficiencia del desempeño de TI, deben ser garantizadas de forma independiente.

Modelo de Madurez

0 No Existe

Cuando la organización no tiene ningún proceso identificable de Gobierno de TI.

1 Inicial / Ad Hoc

Las decisiones de la Gerencia son de forma reactiva a los incidentes y la comunicación que existe es ocasional sobre los problemas y como solucionarlos.

2 Repetible pero intuitivo

Los procesos, los instrumentos, los indicadores para evaluar el Gobierno de TI están restringidos lo que podría ocasionar que no se las utilice a toda su capacidad, ya que no se tiene la experiencia en su funcionalidad.

3 Definido

Los procedimientos se han estandarizado y documentado y la Gerencia los ha comunicado, pero la mayoría de problemas se los resuelve por iniciativa individual.

4 Administrado y Medible

A todos los niveles se tiene un conocimiento completo de los temas de gobierno. Los parámetros de eficacia de todas las actividades de gobierno de TI se monitorean logrando con esto mejoras significativas para la institución.

5 Optimizado

Los procesos se han depurado hasta alcanzar un nivel de mejor práctica, tomando como base los resultados de las mejoras permanentes y el modelo de madures de otras instituciones. Cuando existe un problema se analiza las causas para luego solucionarlos de manera eficiente.

CAPITULO III
METODOLOGÍA DE INVESTIGACIÓN

Método de Investigación, Técnicas de Recolección y Procesamiento de Datos.

3.1 Metodología

Para esta evaluación se utilizarán las metodologías de investigación: deductivo - inductivo, ya que con estas metodologías de puede realizarla evaluación de los hechos institucionales del Centro de Datos objetos de estudio, partiendo de un conocimiento general de los mismos, para luego dividirlos en unidades menores que permitan una mejor aproximación a la realidad que los originó para luego mediante un proceso de síntesis emitir una opinión profesional. Todo este proceso requiere que el auditor utilice una serie de pasos realizados en forma sistemática, ordenada y lógica que permita luego realizar una crítica objetiva del o área examinada. (Cuellar)

Además para el presente proyecto, se utilizará COBIT como Marco de Referencia y MAGERIT como metodología para determinación de riesgos para realizar la auditoría.

3.2 Método Deductivo

La deducción va de lo general a lo particular. El método deductivo es aquél que parte los datos generales aceptados como valederos, para deducir por medio del razonamiento lógico, varias suposiciones, es decir; parte de verdades previamente establecidas como principios generales, para luego aplicarlo a casos individuales y comprobar así su validez.

Se puede decir también que el aplicar el resultado de la inducción a casos nuevos es deducción.

3.3 Método Inductivo

La inducción va de lo particular a lo general. Empleamos el método inductivo cuando de la observación de los hechos particulares obtenemos proposiciones

generales, o sea, es aquél que establece un principio general una vez realizado el estudio y análisis de hechos y fenómenos en particular.

Técnicas

Además se utilizará ciertas técnicas como:

Observación

Razonamiento

Recopilación de información.

Análisis

Encuesta

3.4 Modelo para la Evolución del Centro De Datos

El Centro de Datos (CD), es aquella ubicación donde se agrupan los recursos necesarios para el procesamiento de la información de una institución, los mismos que deben tener en cuenta algunas consideraciones especiales, dado que en ellos se concentran datos y aplicaciones informáticas en espacios muy reducidos, lo que los hace propensos a problemas potenciales, tanto lógicos como físicos, que pueden afectar a su seguridad y funcionamiento.

En el modelo que se plantea para la evaluación del Centro de Datos de la Universidad Nacional de Chimborazo, se tomará en cuenta las Seguridades Físicas y Lógicas

3.4.1 Parámetros para la evaluación Física

Entran dentro de esta categoría todas las medidas para asegurar la integridad física de los equipos almacenados, la forma de evaluar la seguridad física será mediante la observación y encuestas realizadas al Director de Tecnología de la Universidad Nacional de Chimborazo.

Tabla 8: Seguridades Físicas de un Centro de Datos

Seguridad Física	Ubicación y Construcción del Centro de Datos
	Piso Elevado o Cámara Plena
	Aire Acondicionado
	Instalación Eléctrica y Suministro de Energía
	Desastres Provocados por Agua
	Seguridad de Autorización de Accesos
	Detección de Humo y Fuego, Extintores

3.4.2 Parámetros para la evaluación Lógica

Son las condiciones lógicas de los distintos sistemas que componen la institución que se está evaluando.

La evaluación de la infraestructura se la realizará con Magerit que es una metodología de análisis basada en riesgos como se describió anteriormente.

- **Identificación de Activos**

Los activos más comunes que se van a encontrar en un Centro de Datos son los siguientes:

Tabla 9: Activos Generales

Clase de Activo	Entorno de TI	Nombre del Activo
Activos Esenciales	Información	Datos de interés para el negocio
		Datos de interés comercial
		Datos vitales (registros de la Organización)
		Datos de carácter personal
	Servicio	
	Proceso del Negocio	
Datos / Información	Fichero de Datos	
	Copias de Respaldo	
	Datos de Configuración	
	Datos de Gestión Interna	
	Credenciales (contraseñas)	
	Datos de validación de credenciales	

CONTINÚA ⟹

	Datos de control de acceso	
	Registro de Actividad (log)	
	Voz	
	Multimedia	

	Código Fuente	
	Datos de Prueba	
Claves Criptográficas	Protección de la Información	Encriptación de claves
		Clave privada de firma
	Protección de Comunicaciones	Claves de cifrado del Canal
		Claves de autenticación
		Certificados de Clave Publica
Servicios	Al público en General (sin relación contractual)	
	A usuarios externos (bajo relación contractual)	
	Interno (Usuarios y medios de la propia institución)	
	Acceso remoto a cuenta local (telnet)	
	Correo electrónico (email)	
	Voz sobre IP	
	Almacenamiento de Ficheros	
	Servicio de Impresión	
	Transferencia de Archivos	
	Servicio de Copias de Respaldo (backup)	
	Servicio de Directorio	
	Servidor de nombres de Dominio	
	Gestión de Identidades	
	Gestión de Privilegios	
	Servicios Criptográficos	Generación de claves
		Protección de la Integridad
		Cifrado
		Autenticación
		Firma Electrónica
	Infraestructura de clave publica	Autoridad de certificación
		Autoridad de registro
		Autoridad de validación
		Autoridad de fechado electrónico
	Otros	

CONTINÚA ⟹

Aplicaciones (SW)	Desarrollo Propio	
	Desarrollo Subcontratado	
	Estándar	Navegador Web
		Servidor de Aplicaciones
		Cliente de Correo Electrónico

		Servidor de Correo Electrónico
		Servidor de Directorio
		Servidor de Ficheros
		Sistema de Gestión de Base de Datos
		Ofimática
		Antivirus
		Sistema Operativo
		Hypervisor ()Gestor de Máquinas Virtuales
		Backup
		Sistema Académico
		Sistema de Educación Virtual
		Sistema Financiero
		Sistema de Bibliotecas
		Sistema de Recursos Humanos
		Sistema de Inventarios
		Sistema Médico
		Sistema de Seguimiento de Graduados
		Sistema de Evaluación a Docentes
		Sistema de Gestión de Incidentes
		Sistema de Firewall
		Otros
Equipamiento informático (HW)	Grandes Equipos (Servidores)	
	Equipos Medios	
	Informática Personal	
	Informática Móvil	
	Agendas Electrónicas (PDA)	
	Máquinas Virtuales	
	Cluster	
	Equipamiento de respaldo	
	Robots	De Cintas
		De Discos
	Soporte de la Red	
	Centralita Telefónica	
	Switches	
	Routers	
	Teléfono IP	
	Firewall	
	IDS	
	IPS	

CONTINÚA ⟹

Redes de Comunicaciones (COM)	Red Telefónica	
	Red de Datos	
	Red Inalámbrica	
	Wifi	
	Telefonía Móvil	

	Por Satélite	
	Red Local (LAN)	
	LAN Virtual (VLAN)	
	Red Metropolitana (MAN)	
	Red de Área Amplea (WAN)	
	Internet	
	Comunicaciones de Respaldo	
	Otros	
Equipamiento Auxiliar (AUX)	Fuentes de Alimentación	
	Sistema de alimentación ininterrumpida (UPS)	
	Generadores Eléctricos	
	Equipos de Climatización	
	Cableado de Datos	
	Cajas Fuertes	
	Otros	
Instalaciones	Edificio	
	Cuarto	
	Plataformas Móviles	
	Centro de Datos	
	Instalaciones de Respaldo	
Personal	Usuarios Externos	
	Usuarios Internos	
	Operadores	
	Administradores de Sistemas	
	Administrador de Comunicaciones	
	Administrador de Base de Datos	
	Administradores de Seguridad	
	Desarrolladores / Programadores	
	Subcontratados	
	Proveedores	
	Otros	

Fuente: (Dirección General de Modernización Administrativa, 2012)

- **Dependencia entre activos**

Luego de identificar los activos que posee el Centro de Datos a Evaluar se debe ver la dependencia que existe entre ellos.

Activos Inferiores son los pilares en los que se apoya la seguridad de los activos superiores, es decir, cuando una amenaza se llegase a materializar sobre los activos

inferiores, el perjuicio repercute sobre los superiores.

La Tabla que se muestra a continuación servirá para identificar las dependencias que regularmente son entre equipos, servicios y personas que manejan esta información:

Tabla 10: Dependencia de Activos

Dependencia de activos inferiores	
Activo:	Grado:
Activo:	Grado:

Fuente**:** (Dirección General de Modernización Administrativa, 2012)

- **Valoración de Activos**

Es la valoración establecida al activo de acuerdo a la criticidad.

Para asignar el valor a los activos se ha elegido una escala de cero (0) a diez (10), para valorar de forma homogénea los activos cuyo valor es importante por diferentes motivos MAGERIT presenta varias tablas

Tabla 11: Escala de valores

Valor		**Criterio**
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6 - 8	Alto	Daño grave
3 - 5	Medio	Daño importante
1 - 2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: (Dirección General de Modernización Administrativa, 2012)

Para identificar la valoración de la información se utilizarán las siguientes dimensiones de seguridad:

[I] Integridad

Impacto que tendría en la organización el hecho de que la información que se maneja para prestar el servicio fuera incorrecta o incompleta

[C] Confidencialidad

Impacto que tendría en la organización el hecho de que la información que se maneja para prestar el servicio fuera accedida por personas no autorizadas

[A] Autenticidad de los datos

Impacto que tendría en la organización el hecho de que no se pueda saber a ciencia cierta quien accedido a la información que se maneja para prestar el servicio.

[T] Trazabilidad de los datos, quién ha modificado qué

Impacto que tendría en la organización el hecho de que no se pueda saber que se a hecho con la información que se maneja para prestar el servicio.

Para identificar la valoración de los servicios se utilizarán en las siguientes dimensiones:

[D] Disponibilidad

Impacto que tendría en la organización el hecho de que se dejara de prestar el servicio.

[A] Autenticidad de quien accede al Servicio.

Impacto que tendría en la organización el hecho de no saber quien accede al servicio.

[T] Trazabilidad de quien accede al servicio, cuando y que hace.

Impacto que tendría en la organización el hecho de que no se pudiera conocer

quién hace qué y cuándo con el servicio.

La Tabla que se muestra a continuación servirá para valorar los activos de acuerdo a las dimensiones de seguridad mencionadas anteriormente.

Tabla 12: Valoración de los Activos

Activos		**Dimensiones de Seguridad**				
Clase de Activo	Entorno de TI	[D]	[I]	[C]	[A]	[T]

Fuente: (Dirección General de Modernización Administrativa, 2012)

Para realizar un valoración más homogénea Magerit proporciona un catálogo estándar el cual se encuentra en el Anexo 1 (Catalogo Magerit)

- **Identificación de Amenazas**

Para este objetivo Magerit proporciona un catálogo de amenazas posibles sobre los activos de un sistema de información. Entre las amenazas típicas se puede mencionar las siguientes.

Desastres naturales

Hay accidentes naturales (terremotos, inundaciones, ...).

Del entorno (De origen industrial)

Hay desastres industriales (contaminación, fallos eléctricos, ...)

Errores y Fallos no intencionados

Los problemas no intencionados, típicamente por error o por omisión, son ocasionados por personas con acceso al sistema de información.

Ataques deliberados

Son problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación

entre el tipo de activo y lo que le podría ocurrir.

La Tabla que se muestra más adelante servirá para valorar los activos de acuerdo a las dimensiones de seguridad mencionadas anteriormente.

Para realizar la identificación de las amenazas Magerit proporciona un catálogo, el cual se encuentra en el Anexo 2 (Catalogo Magerit)

Tabla 13: Identificación de Amenazas

	Activos			**Activos**			**Activos**		
Amenazas	**D**	**I**	**D**	**I**	**C**	**C**	**D**	**I**	**C**
[N] Desastres naturales									
[I] De origen industrial									
[E] Errores y fallos no intencionados									
[A] Ataques intencionados									

Fuente: (Dirección General de Modernización Administrativa, 2012)

- **Valoración de Amenazas**

Luego de haber establecido que una amenaza puede dañar a un activo, se debe valorar su efecto en el valor del activo:

Probabilidad: Cuán probable o improbable es que se materialice la amenaza

Degradación: Cuan perjudicado resultaría el [valor del] activo

Frecuencia o Probabilidad de Ocurrencia

Se refiere a los eventos que se producen en un tiempo determinado. Los valores típicos para determinar la frecuencia se muestran a continuación:

Tabla 14: Probabilidad de Ocurrencia

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años

MB	1/100	muy poco frecuente	siglos

Fuente: (Dirección General de Modernización Administrativa, 2012)

MA: Muy Alta

A: Alta

M: Media

B: Baja

MB: Muy Baja

Degradación

Es que tan perjudicado quedaría el activo al materializarse las amenazas.

Tabla 3.8: Degradación de Valor

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Fuente: (Dirección General de Modernización Administrativa, 2012)

La Tabla que se muestra a continuación servirá para valorar las amenazas con relación a la frecuencia con la ocurren y la degradación que sufrirían activos en cada una de lasa las dimensiones de seguridad.

Tabla 15: Valoración de las Amenazas

Activo			**Probabilidad de Ocurrencia**	**Degradación (% o nivel)**				
Capas	**Activos**	**Amenazas**	**Nivel**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**

Fuente: (Dirección General de Modernización Administrativa, 2012)

- **Salvaguardas**

Son las acciones concretas para reducir el riesgo, se hace necesario realizar una

selección de las salvaguardas más relevantes.

El aspecto que trata las salvaguardas como:

G para Gestión

T para Técnico

F para seguridad Física

P para gestión del Personal

Entre los tipos protección que ofrecen las salvaguardas tenemos:

Tabla 16: Tipos de protección de las Salvaguardas

Efecto	**Tipo**
preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias [EL] eliminatorias
acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: (Dirección General de Modernización Administrativa, 2012)

Peso Relativo de las Salvaguardas

Tabla 17: Peso de las Salvaguardas

	Máximo peso	Critica
	Peso alto	Muy importante
	Peso normal	Importante
	Peso bajo	interesante

✓	Aseguramiento: componentes certificados

Fuente: (Dirección General de Modernización Administrativa, 2012)

Nivel de Criticidad

- **Identificacion de las Salvaguardas**

Tabla 18: Identificación de las Salvaguardas

Aspecto	**Tipo**	**Peso Relativo**	**Salvaguarda**	**Nivel de Criticidad**

Fuente: (Dirección General de Modernización Administrativa, 2012)

Eficacia de las salvaguardas

Se estimará un grado de la eficacia en cada caso en la que el 100% es una salvagurada ideal.

Tabla 19: Eficacia de las Salvaguardas

Factor	**Nivel**	**Significado**
0%	L0	inexistente
	L1	Inicial / ad hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso Definido
	L4	Gestionado y Medible

100%	L5	Optimizado

Fuente: (Dirección General de Modernización Administrativa, 2012)

- **Valoracion de las Salvaguardas**

Tabla 20: Valoración de las Salvaguardas

Aspecto	**Tipo**	**Peso Relativo**	**Salvaguarda**	**Eficacia Salvaguarda**

Fuente: (Dirección General de Modernización Administrativa, 2012)

- **Impacto**

Determinación del Impacto

Es un indicador de qué puede suceder cuando ocurren las amenazas.

La escala siguiente útil para calificar la magnitud del impacto

Valor:

[9]: Muy alto

[8]: Muy alto

[7]: Alto

[6]: Alto

[5]: Medio

[4]: Medio

[3]: Bajo

[2]: Bajo

[1]: Despreciable

[0]: Despreciable

En el impacto se va evaluar a los activos en cada una de las dimensiones.

Tabla 21: Impacto sobre los Activos

Activo		**Dimensiones de Seguridad**				
Capas	Activos	[D]	[I]	[C]	[A]	[T]

Fuente: (Dirección General de Modernización Administrativa, 2012)

- **Riesgo**

La probabilidad de materialización de amenazas sobre el activo.

Los riesgos se muestran con la siguiente escala de colores según su valor:

{5} o más: Crítico

{4}: Muy alto

{3}: Alto

{2}: Medio

{1}: Bajo

{0}: Despreciable

{OFF}: Este activo, o uno del que depende, está marcado como "/indisponible

Tabla 22: Riesgos sobre los Activos

Activo		**Dimensiones de Seguridad**				
Capas	Activos	[D]	[I]	[C]	[A]	[T]

Fuente: (Dirección General de Modernización Administrativa, 2012)

3.4.3 Evaluación de Control Interno

La evaluación del control interno se la realizará con el marco de referencia COBIT con los procesos PO9, ME4.

PO9 Evaluar y Administrar los Riesgos de TI

Los atributos de la información más relevantes son:

- **Primarios:** Confidencialidad, Integridad, Disponibilidad

- **Secundarios:** Efectividad, Eficiencia, Cumplimiento y Fiabilidad

Tabla 23: Evaluación de los Objetivos Control del Proceso PO9

DOMINIO:	**Planeación y Organización**		
PROCESO:	**PO9 Evaluación y Gestión de Riesgos**		
OBJETIVOS DE CONTROL	**DETALLE**	**Cumplimiento**	
		SI	**NO**
PO9.1 Marco de Trabajo de Administración de Riesgos			
PO9.2 Establecimiento del Contexto del Riesgo			
PO9.3 Identificación de Eventos			
PO9.4 Evaluación de Riesgos de TI			
PO9.5 Respuesta a los Riesgos			
PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos			

Tabla 24: Indicadores Claves de Desempeño de las Actividades PO9

METAS E INDICADORES CLAVES DE DESEMPEÑO DE LAS ACTIVIDADES		
METAS	INDICADOR CLAVE DE DESEMPEÑO	VALOR
1.- Asegurarse de que la administración de riesgos esté totalmente incluida en los procesos administrativos.	Porcentaje del presupuesto de TI gastado en actividades de administración de los riesgos (evaluación y mitigación).	
	Frecuencia de la revisión del proceso de administración de riesgos de TI.	
	Porcentaje de evaluaciones de riesgo autorizadas # de reportes de monitoreo de riesgos activados dentro de la frecuencia acordada.	
	Porcentaje de eventos de TI identificados usados en evaluaciones de riesgo.	
2.- Realizar evaluaciones	Porcentaje de planes de acción de administración de riesgos aprobados para su implantación.	

de riesgo periódicas con los gerentes y con el personal clave.		

Tabla 25: Indicadores Claves de Desempeño de los Procesos PO9

METAS E INDICADORES CLAVES DE DESEMPEÑO DE LOS PROCESOS		
METAS	**INDICADOR CLAVE DE DESEMPEÑO**	**VALOR**
1.- Establecer y reducir la posibilidad y el impacto de los riesgos de TI.	Porcentaje de eventos críticos de TI Identificados que han sido evaluados.	
	Número de riesgos de TI recientemente identificados (comparados con el ejercicio previo).	
	Número de incidentes significativos causados por riesgos no identificados por el proceso de evaluación de riesgos.	
2.- Establecer planes de acción rentables para los riesgos críticos de TI.	Porcentaje de riesgos críticos de TI identificados con un plan de acción elaborado.	

Tabla 26: Indicadores Claves de Desempeño de TI PO9

METAS E INDICADORES CLAVES DE DESEMPEÑO DE TI		
METAS	INDICADOR CLAVE DE DESEMPEÑO	VALOR
1.- Proteger el logro de los objetivos de TI.	Porcentaje de objetivos críticos de TI cubiertos por la evaluación de riesgos.	
2.- Establecer claridad sobre el impacto en el negocio de los riesgos a los objetivos y recursos de TI. 3.- Responder por y proteger todos activos de TI.	Porcentaje de evaluaciones de riesgos de TI integrados en el enfoque de evaluación de riesgos de TI.	

Tabla 27: Nivel de Madurez del Proceso PO9

NIVEL DEL MODELO DE MADUREZ		
NIVEL	**DESCRIPCION**	**ESTADO ACTUAL**
0 No Existente	Cuando la organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI.	
1 Inicial / Ad Hoc	Cuando se realizan evaluaciones informales de riesgos tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto, es decir, que existe un entendimiento emergente que los riesgos de TI son importantes y necesitan ser considerados.	
2 Repetible pero Intuitivo	Cuando la administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas.	
3 Definido	Cuando la administración de riesgos sigue un proceso definido, el cual está documentado.	
4 Administrado y Medible	Cuando los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI, otorgando por parte de la gerencia un presupuesto para un proyecto de administración de riesgo operativo para re-evaluar los riesgos de manera regular.	
5 Optimizado	Cuando la administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI, está bien aceptada, y abarca a los usuarios de servicios de TI y cuando la dirección evalúa las estrategias de mitigación de riesgos de manera contínua.	

Fuente: (IT Gobernance Institute, 2007)

ME4 Proporcionar Gobierno de TI

Los atributos más relevantes son:

Primarios: Efectividad, Eficiencia.

Secundarios: Confidencialidad, Integridad, Disponibilidad, Cumplimiento, Confiabilidad

Tabla 28: Evaluación de los Objetivos Control del Proceso ME4

DOMINIO:	**Monitorear y Evaluar**		
PROCESO:	PO9 Evaluación y Gestión de Riesgos		
OBJETIVOS DE CONTROL	DETALLE	Cumplimiento	
		SI	NO
ME4.1 Establecimiento de un Marco de Gobierno de TI			
ME4.2 Alineamiento Estratégico			
ME4.3 Entrega de Valor			
ME4.4 Administración de Recursos			
ME4.5 Administración de Riesgos			
ME4.6 Medición del Desempeño			
ME4.7 Aseguramiento Independiente			

Tabla 29: Indicadores Claves de Desempeño de las Actividades ME4

METAS E INDICADORES CLAVES DE DESEMPEÑO DE LAS ACTIVIDADES		
METAS	**INDICADOR CLAVE DE DESEMPEÑO**	**VALOR**
1.-Establecer un marco de trabajo para el gobierno de TI integrado al gobierno corporativo.	Porcentaje del equipo entrenado en gobierno (ej. Códigos de Conducta)	
	Frecuencia en que el gobierno de TI es un punto de la agenda en las reuniones estratégicas/ de comité de TI	
2.-Obteber una garantía	Porcentaje de miembros del consejo directivo con entrenamiento o experiencia en gobierno de TI	
	Número de Obsolescencia de	

independiente respecto al estatus del gobierno de TI	recomendaciones acordadas	
	Frecuencia de reportes al consejo sobre encuestas de satisfacción a las terceras partes interesados.	

Tabla 30: Indicadores Claves de Desempeño de los Procesos ME4

METAS E INDICADORES CLAVES DE DESEMPEÑO DE LOS PROCESOS		
METAS	**INDICADOR CLAVE DE DESEMPEÑO**	**VALOR**
1.-Integrar el gobierno de TI a los objetivos del gobierno corporativo. 2.-Elaborar reportes completos y oportunos par ale consejo directivo sobre la estrategia, el desempeño y los riesgos de TI. 3.- Responder a las preocupaciones y consultas del consejo directivo respecto a la estrategia, desempeño y riesgos de TI. 4.- Procurar aseguramiento independiente respecto al cumplimiento de las políticas estándares y procedimientos de TI	Frecuencia de reportes provenientes de TI hacia el consejo directivo	
	Frecuencia de revisiones independientes del cumplimiento de TI	

Tabla 31: Indicadores Claves de Desempeño de TI ME4

METAS E INDICADORES CLAVES DE DESEMPEÑO DE TI		
METAS	**INDICADOR CLAVE DE DESEMPEÑO**	**VALOR**
1.-Responder a los requerimientos de gobierno de acuerdo con las directrices del consejo directivo. 2.- Garantizar que TI cumpla las leyes regulaciones. 3.-asegurar que TI demuestre una calidad de servicio eficiente en	Número de veces que TI se encuentra en la agenda del consejo directivo de Manera Proactiva	
	Frecuencia de reportes del consejo directivo sobre TI a las/os terceras partes interesadas (incluyendo el nivel de madurez)	

consto, mejora continua y presteza para cambios futuros.	Número de eventos recurrentes de TI en las agendas del consejo directivo.	

Tabla 32: Nivel de Madurez del Proceso ME4

NIVELES DEL MODELO DE MADUREZ		
NIVEL	**DESCRIPCION**	**ESTADO ACTUAL**
0 No Existente	Cuando la organización no tiene ningún proceso identificable de Gobierno de TI.	
1 Inicial / Ad Hoc	Las decisiones de la Gerencia son de forma reactiva a los incidentes y la comunicación que existe es ocasional sobre los problemas y como solucionarlos.	
2 Repetible pero Intuitivo	Los procesos, los instrumentos, los indicadores para evaluar el Gobierno de TI están restringidos lo que podría ocasionar que no se las utilice a toda su capacidad, ya que no se tiene la experiencia en su funcionalidad.	
3 Definido	Los procedimientos se han estandarizado y documentado y la Gerencia los ha comunicado, pero la mayoría de problemas se los resuelve por iniciativa individual.	
4 Administrado y Medible	A todos los niveles se tiene un conocimiento completo de los temas de gobierno. Los parámetros de eficacia de todas las actividades de gobierno de TI se monitorean logrando con esto mejoras significativas para la institución.	
5 Optimizado	Los procesos se han depurado hasta alcanzar un nivel de mejor práctica, tomando como base los resultados de las mejoras permanentes y el modelo de madures de otras instituciones. Cuando existe un problema se analiza las causas para luego solucionarlos de manera eficiente.	

Fuente: (IT Gobernance Institute, 2007)

CAPITULO IV

PLANIFICACION Y EJECUCIÓN DE LA EVALUACIÓN

4.1 Planificación de la Evaluación

La planificación de la Evaluación se la llevará a cabo como se detalla a continuación:

Objetivo de la Evaluación

Alcance de la Evaluación

Canales de Comunicación

Programa de Auditoria

Ejecución de la Auditoría

Evaluación de la información y redacción del informe final

4.2 Objetivo de la Evaluación

Determinar los riesgos a los que está expuesto el Centro de Datos de la Universidad Nacional de Chimborazo.

4.3 Alcance de la Evaluación

Revisión de Recomendaciones de Auditorias Anteriores.

Recopilación de información relacionada con el Centro de Datos de la Universidad Nacional de Chimborazo

Análisis de riesgos

Nivel de Madurez de los procesos inherentes al Centro de Datos

4.4 Canales de Comunicación

Personal Involucrado

Personal a nivel Gerencial

Director del Departamento de Tecnología (Ing. Jorge Delgado)

Personal a nivel Estratégico

Administrador Redes (Ing. Javier Haro)

Administrador (Ing. Javier Montalvo)

Miembros del Equipo Auditor

Ing. Cristian Viteri Silva

4.5 Programa de Auditoria

Estudio Inicial del Entorno a Evaluar

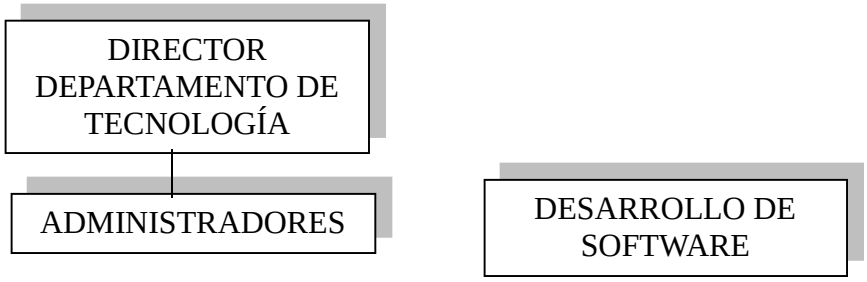
El evaluador realizará un estudio inicial de la situación actual de la unidad específica a ser evaluada. Para realizar dicho estudio se examinará de forma general lo siguiente:

- Unidad o dependencia.
- Entorno operacional.

Unidad o dependencia.

El Departamento de Tecnología está a cargo del Ing. Carlos Delgado y el administrador del Centro de Datos Institucional es el Ing. Javier Haro.
El orgánico funcional que tiene el Centro de Datos es el siguiente:

Organigrama



Los administradores de Centro de Datos Institucional se encargan de monitorear y gestionar los servicios de internet, intranet, telefonía, educación virtual que por el momento está brindando.

Sub Unidades o Jefaturas

Las Sub Unidades no se encuentran totalmente definidas ya que por políticas institucionales existe otra unidad de Desarrollo de Software pero no

forma parte del Departamento de Tecnología de la UNACH.

Entorno Operacional

Para poseer una referencia del entorno se va a determinar los siguientes aspectos:

Situación geográfica de los sistemas

El Centro de Datos de la Universidad Nacional de Chimborazo está ubicado en el Campus vía a Guano, en el Edificio del Departamento de Tecnologías, cuyo responsable del mismo es el Ing. Javier Haro.

Hardware y Software

El Hardware y Software que posee el Centro de Datos de la Universidad Nacional de Chimborazo se lo detallará más adelante donde están identificados estos elementos.

Comunicaciones y redes de comunicaciones

Las Redes de Comunicaciones que posee el Centro de Datos de la Universidad Nacional de Chimborazo se lo detallará más adelante donde están identificados estos elementos.

Determinación de Recursos para la Evaluación

Los recursos que se utilizarán en la Evaluación son:

Recursos materiales

Los recursos materiales del evaluador son:

Recursos materiales Software

Sistema Operativo. Windows 7

Ofimática

Recursos materiales Hardware

Computador Laptop Personal procesador i5, 4gb ram, 500Gb disco duro

Data Pen 4Gb

Internet

Recursos Humanos

Ing. Cristian Viteri Silva

Materialidad

Los Activos que se han identificado en el Centro de Datos de la Universidad de Chimborazo se muestran en la siguiente tabla:

Tabla 33: Activos Centro de Datos

Clase de Activo	**Entorno de TI**	**Nombre del Activo**
Activos Esenciales		Datos de interés comercial
	Servicio	
Datos / Información	Copias de Respaldo	
	Datos de control de acceso	
	Registro de Actividad (log)	
	Voz	
Claves Criptográficas	Protección de Comunicaciones	Claves de autenticación
Servicios	A usuarios externos (bajo relación contractual)	
	Interno (Usuarios y medios de la propia institución)	
	Correo electrónico (email)	
	Voz sobre IP	
	Almacenamiento de Ficheros	
	Servicio de Copias de Respaldo (backup)	
	Servidor de Nombres de Dominio	
	Servidor de Protocolo de Transferencia de Archivos (FTP)	
	Blearning	
	Hosting	

CONTINÚA ⟹

Aplicaciones (SW)	Desarrollo Subcontratado	
	Estándar	Navegador Web
		Servidor de Aplicaciones
		Cliente de Correo Electrónico
		Servidor de Correo Electrónico
		Servidor de Ficheros
		Sistema de Gestión de Base de Datos
		Ofimática
		Antivirus
		Sistema Operativo
		Hypervisor ()Gestor de Máquinas Virtuales
		Backup (Software de Respaldos Data Protector)
		Sistema de Educación Virtual
		Sistema de Firewall
Equipamiento informático (HW)	Grandes Equipos (Servidores) HP DL360p Gen8 E5-2630 Base US Svr (#2), HP BL460 c Gen8 10 Gb FLB CTO Blade (#5), Servidores Gen 7 (8)	
	Equipos Medios	
	Clúster	
	Equipamiento de respaldo HP MSL 2024 1 LTO -5 3000 FC Tape Lbry (Sistema de Respaldo de Cintas)	
	Robots	De Cintas
	Centralita Telefónica	
	Switches	
	Routers	
	Teléfono IP	
	Enclosure Blade System C7000 (2)	
	HP P6350 EVA FCSFF (sistema de almacenamiento)	
	HP B-serirs 8/12c BladeSystem SAN Switch	

CONTINÚA ⟹

	Cisco Call Manager Business Edition 6000(Telefonía)	
	Firewall	
Redes de Comunicaciones (COM)	Red Telefónica	
	Red de Datos	
	Red Inalámbrica	
	Wifi	
	Red Local (LAN)	
	LAN Virtual (VLAN)	
	Internet	
Equipamiento Auxiliar (AUX)	Fuentes de Alimentación	
	Sistema de alimentación ininterrumpida (UPS)	
	Generadores Eléctricos	
	Equipos de Climatización	
	Cableado de Datos	
	Sistema de Piso Falso	
	Puerta de Seguridad	
	Sistema de Detección y extinción de incendios	
	Control de Accesos	
Instalaciones	Edificio	
	Centro de Datos	
	Usuarios Internos	
	Operadores	
Personal	Administradores de Sistemas	
	Administrador de Redes	
	Proveedores	
	Seguridad (Guardianía)	

Fuente: Director de Tecnología UNACH

Una vez identificados los activos se llega a determinar que varias las aplicaciones como Sistema Académico, Sistema Financiero que ayudan al giro del negocio no están dentro de la infraestructura del Centro de Datos, por lo que la Evaluación se centrará en los activos que se muestran en la tabla anterior.

4.6 Ejecución de la Auditoria

4.6.1 Evaluación Física

A continuación se presentan los resultados de las encuestas realizadas al Director del Departamento de Tecnología en lo referente al cumplimiento o no de las normas de Seguridad Física que debe tener el Centro de Datos.

Las preguntas que se realizaron en estas encuetas se encontraran en el Anexo 3.

Cuestionario de Seguridades ante Incendios

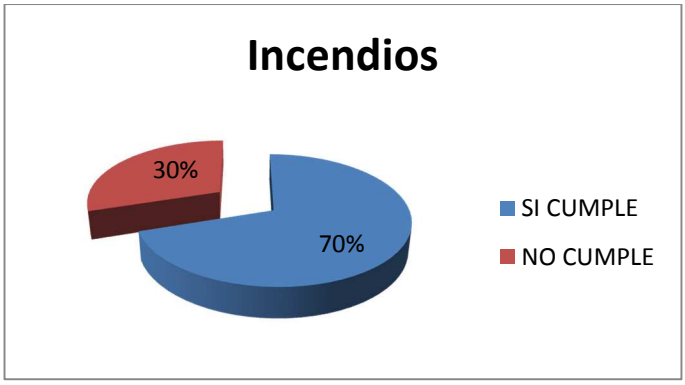


Gráfico 10: Resultado de Cuestionario de Seguridades ante Incendios

Cuestionario de Seguridades ante Inundaciones

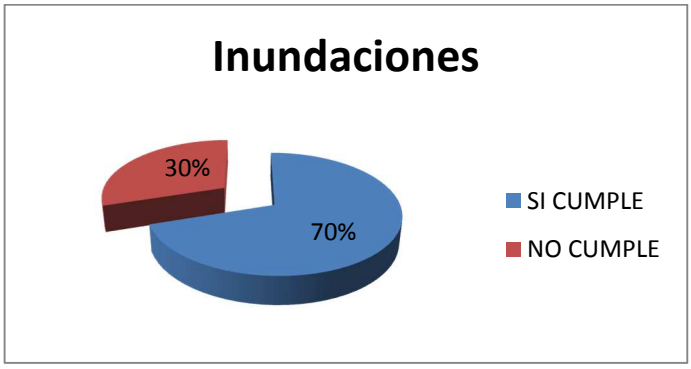


Gráfico 11: Resultado de Cuestionario de Seguridades ante Inundaciones

Cuestionario de Seguridad de Respaldos

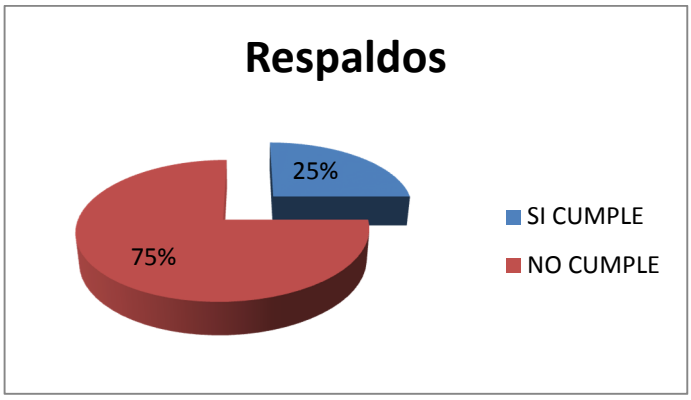


Gráfico 12: Resultado de Cuestionario de Seguridades de Respaldos

Cuestionario de Seguridades Eléctricas

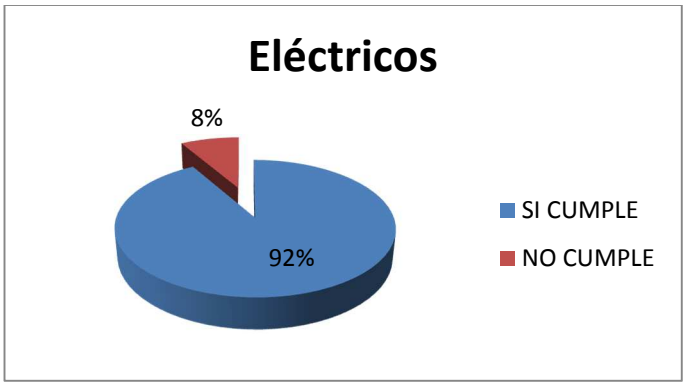


Gráfico 13: Resultado de Cuestionario de Seguridades Eléctricas

Cuestionario de Seguridades Ambientales

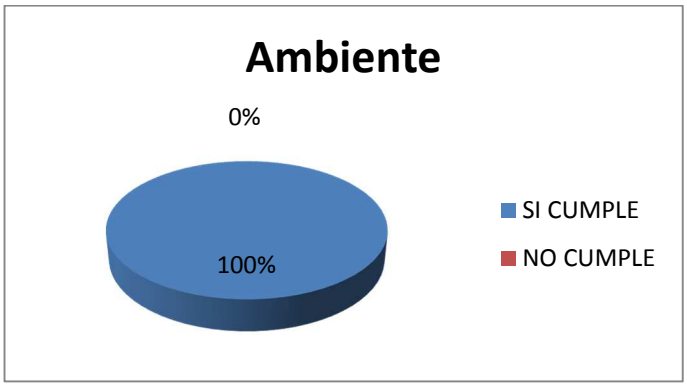


Gráfico 14: Resultado de Cuestionario de Seguridades Ambientales

Cuestionario de Seguridades de Control de Personal

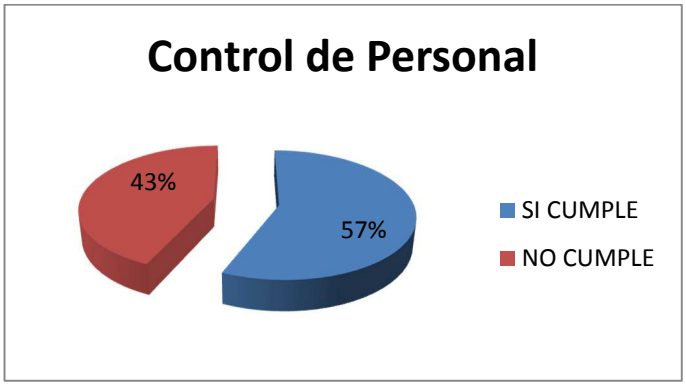


Gráfico 15: Resultado de Cuestionario de Seguridades de Control de Personal

Cuestionario de Seguridades de Control de Visitas

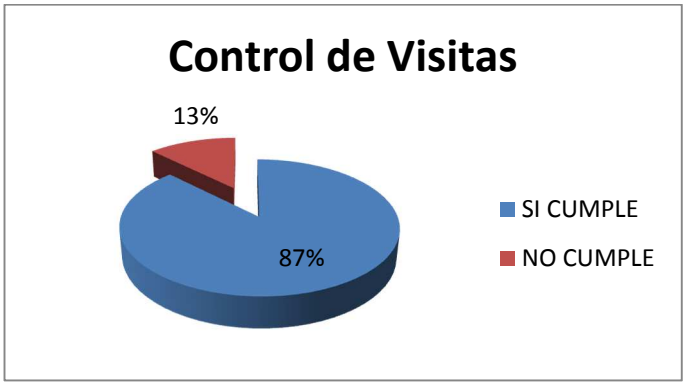


Gráfico 16: Resultado de Cuestionario de Seguridades de Control de Visitas

Cuestionario de Seguridades Secundarias

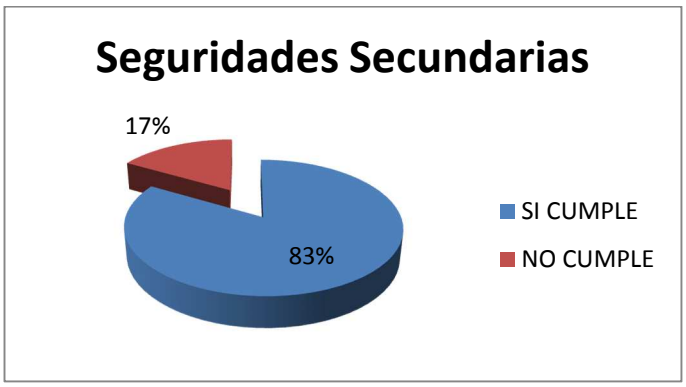


Gráfico 17: Resultado de Cuestionario de Seguridades Secundarias

Cuestionario de Seguridades Físicas de Servidores

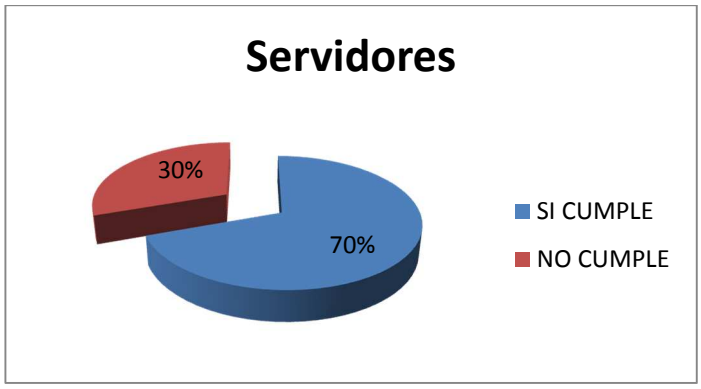


Gráfico 18: Resultado de Cuestionario de Físicas de Servidores

Cuestionario de Seguridades Físicas de Redes

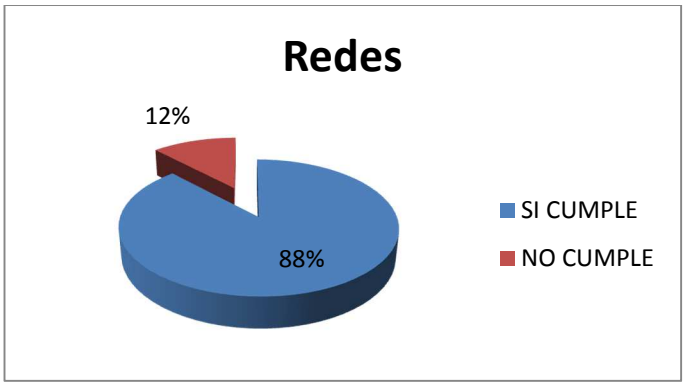


Gráfico 19: Resultado de Cuestionario de Físicas de Redes

Cuestionario de Seguridades Físicas de Telecomunicaciones

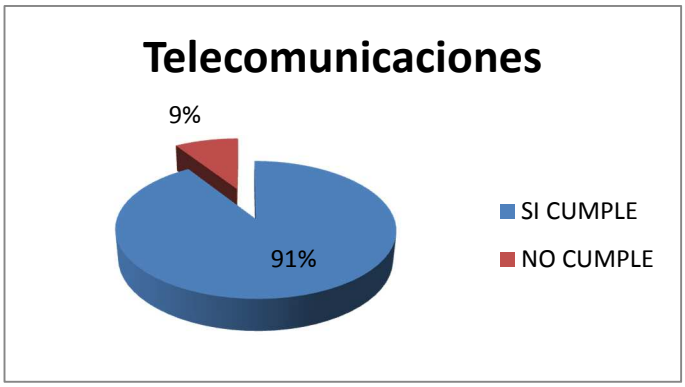


Gráfico 20: Resultado de Cuestionario de Físicas de Telecomunicaciones

Cuestionario de Seguridades Físicas Generales

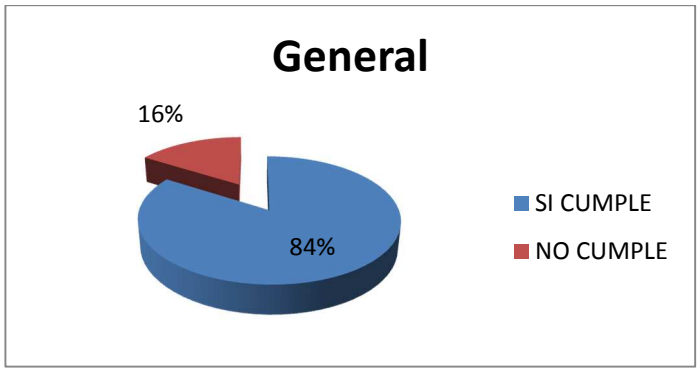


Gráfico 21: Resultado de Cuestionario de Seguridades Físicas Generales

4.6.2 Evaluación de Riesgos

De acuerdo a un análisis previo realizado se adoptará la guía G13 (Uso del riesgo de auditoria en la planeación de la auditoria) de ISACA, en la cual manifiesta que se debe elegir una metodología para la evaluación del riesgo. Como se detalló en Capítulo II la metodología elegida es MAGERIT la misma que tiene las siguientes actividades:

- **Identificación de Activos**

Tabla 34: Activos Centro de Datos UNACH

	Clase de Activo	Entorno de TI	Nombre del Activo
Activos Esenciales	Activos Esenciales	Información	Datos de interés comercial
		Servicio	
Servicios Internos	Datos / Información	Copias de Respaldo	
		Datos de control de acceso	
		Registro de Actividad (log)	
		Voz	
	Servicios	A usuarios externos (bajo relación contractual)	
		Interno (Usuarios y medios de la propia institución)	

CONTINÚA ⟹

		Correo electrónico (email)	
		Voz sobre IP	
		Almacenamiento de Ficheros	
		Servicio de Copias de Respaldo (backup)	
		Servidor de Nombres de Dominio	
		Servidor de Protocolo de Transferencia de Archivos (FTP)	
		Blearning	
		Hosting	
Equipamiento	Aplicaciones (SW)	Desarrollo Subcontratado	
		Estándar	Navegador Web
			Servidor de Aplicaciones
			Cliente de Correo Electrónico
			Servidor de Correo Electrónico
			Servidor de Ficheros
			Sistema de Gestión de Base de Datos
			Ofimática
			Antivirus
			Sistema Operativo
			Hypervisor ()Gestor de Máquinas Virtuales
			Backup (Software de Respaldos Data Protector)
			Sistema de Educación Virtual
			Sistema de Firewall
	Equipamiento informático (HW)	Grandes Equipos (Servidores) HP DL360p Gen8 E5-2630 Base US Svr (#2), HP BL460 c Gen8 10 Gb FLB CTO Blade (#5), Servidores Gen 7 (8)	
		Equipos Medios	
		Cluster	
		Equipamiento de respaldo HP MSL 2024 1 LTO -5 3000 FC Tape Lbry (Sistema de Respaldo de Cintas)	

CONTINÚA ⟹

	Robots	De Cintas
	Centralita Telefónica	
	Switches	
	Routers	
	Teléfono IP	
	Enclosure Blade System C7000 (2)	
	HP P6350 EVA FCSFF (sistema de almacenamiento)	
	HP B-serirs 8/12c BladeSystem SAN Switch	
	HP 8/24 Base 16- ports Enabled SAN switch.Conectividad	
	Cisco Call Manager Business Edition 6000(Telefonía)	
	Firewall	
Redes de Comunicaciones (COM)	Red Telefónica	
	Red de Datos	
	Red Inalámbrica	
	Wifi	
	Red Local (LAN)	
	LAN Virtual (VLAN)	
	Red Metropolitana (MAN)	
	Internet	
	Red Privada Virtual (VPN)	
	Comunicaciones de Respaldo	
Equipamiento Auxiliar (AUX)	Fuentes de Alimentación	
	Sistema de alimentación ininterrumpida (UPS)	
	Generadores Eléctricos	
	Equipos de Climatización	
	Cableado de Datos	
	Sistema de Piso Falso	
	Puerta de Seguridad	
	Sistema de Detección y extinción de incendios	
	Control de Accesos	
	Otros	

CONTINÚA ⟹

Instalaciones	Instalaciones	Edificio	
		Centro de Datos	
Personal	Personal	Usuarios Internos	
		Operadores	
		Administradores de Sistemas	
		Administrador de Redes	
		Proveedores	
		Seguridad (Guardianía)	

Fuente: Director de Tecnología UNACH

- **Dependencia de Activos**

Por el número de matrices que se utilizan para identificar la dependencia entre los Activos, a manera de ejemplo se muestran las matrices utilizadas para identificar la dependencia que existe entre los activos, por cada clase de activos se representa un activo. Las matrices restantes se encuentran en el Anexo 4.

Servicio

Las dependencias normalmente identifican equipamiento desplegado para prestar este servicio:

Aplicaciones (sw)

Equipos (hw)

Equipos de comunicaciones

Personas a cargo del servicio

Tabla 35: Dependencia de Aplicaciones SW (Servicio)

Aplicaciones SW			
Dependencia de Activos Inferiores			
Activo:	**Interno (Usuarios y medios de la propia institución)**	Grado:	
	Navegador Web		Alto
	Servidor de Aplicaciones		Alto
	Sistema de Educación Virtual		Alto

Tabla 36: Dependencia de Equipos HW (Servicio)

Equipos HW			
Dependencia de Activos Inferiores			
Activo:	**Interno (Usuarios y medios de la propia institución)**	Grado:	
	Grandes Equipos (Servidores) HP DL360p Gen8 E5-2630 Base US Svr (#2), HP BL460 c Gen8 10 Gb FLB CTO Blade (#5), Servidores Gen 7 (8)		Alto
	Equipamiento de respaldo HP MSL 2024 1 LTO - 5 3000 FC Tape Lbry (Sistema de Respaldo de Cintas)		Alto
	Enclosure Blade System C7000 (2)		Alto
	HP P6350 EVA FCSFF (sistema de almacenamiento)		Alto
	HP B-serirs 8/12c BladeSystem SAN Switch		Alto

Tabla 37: Dependencia de Equipos de Comunicaciones (Servicio)

Equipos de Comunicaciones			
Dependencia de Activos Inferiores			
Activo:	**Interno (Usuarios y medios de la propia institución)**	Grado:	
	Red Local (LAN)		Alto
	Red Metropolitana (MAN)		Alto
	Internet		Alto
	Red Privada Virtual (VPN)		Alto

Tabla 38: Dependencia de Personas a Cargo del Servicio (Servicio)

Personas a cargo del servicio.			
Dependencia de Activos Inferiores			
Activo:	**Interno (Usuarios y medios de la propia institución)**	Grado:	
	Administradores de Sistemas		Alto
	Administrador de Redes		Alto

Datos Información

Las dependencias que normalmente se identifican en este tipo de activos son:

Equipos que los hospedan

Líneas de Comunicación por las que se transfieren

Personas relacionadas: usuarios

Tabla 39: Dependencia de Equipos que los hospedan (Datos Información)

Equipos que los hospedan			
Dependencia de Activos Inferiores			
Activo:	**Copias de Respaldo**	Grado:	
	Equipamiento de respaldo HP MSL 2024 1 LTO -5 3000 FC Tape Lbry (Sistema de Respaldo de Cintas)		Alto
	HP P6350 EVA FCSFF (sistema de almacenamiento)		Alto

Tabla 40: Dependencia de Líneas de Comunicación (Datos Información)

Líneas de comunicación por las que se transfieren			
Dependencia de Activos Inferiores			
Activo:	**Copias de Respaldo**	Grado:	
	Red Local (LAN)		Alto
	Comunicaciones de Respaldo		Alto

Tabla 41: Dependencia de Personas Relacionadas (Datos Información)

Personas relacionadas: usuarios.			
Dependencia de Activos Inferiores			
Activo:	**Copias de Respaldo**	Grado:	
	Administradores de Sistemas		Alto
	Administrador de Redes		Alto

Aplicaciones

Las dependencias normalmente identifican:

Personas relacionadas con esta aplicación: operadores, administradores y desarrolladores.

Tabla 42: Dependencia de Personas Relacionadas con esta aplicación

Personas relacionadas con esta aplicación			
Dependencia de Activos Inferiores			
Activo:	**Servidor de Aplicaciones**	Grado:	
	Administradores de Sistemas		Alto

Equipamiento Informático HW

Las dependencias que normalmente se identifican en este tipo de activos son:

Personas relacionadas con este equipo: operadores, administradores

Instalaciones que lo acogen

Tabla 43: Dependencia de Personas Relacionadas con este equipo (Aplicaciones)

Personas relacionadas con este equipo			
Dependencia de Activos Inferiores			
Activo:	**Grandes Equipos (Servidores) HP DL360p Gen8 E5-2630 Base US Svr (#2), HP BL460 c Gen8 10 Gb FLB CTO Blade (#5), Servidores Gen 7 (8)**	Grado:	
	Administradores de Sistemas		Alto

Tabla 44: Dependencia de Instalaciones que los acogen (Aplicaciones)

Instalaciones que lo acogen			
Dependencia de Activos Inferiores			
Activo:	**Grandes Equipos (Servidores) HP DL360p Gen8 E5-2630 Base US Svr (#2), HP BL460 c Gen8 10 Gb FLB CTO Blade (#5), Servidores Gen 7 (8)**	Grado:	
	Centro de Datos		Alto

Redes y Comunicaciones

Las dependencias normalmente identifican

Personas relacionadas con este equipo: operadores, Administradores.

Instalaciones que lo acogen.

Tabla 45: Dependencia de Personas Relacionadas con este equipo (Redes y Comunicaciones)

Personas relacionadas con este equipo			
Dependencia de Activos Inferiores			
Activo:	**Red Telefónica**	Grado:	
	Administrador de Redes		Alto
	Usuarios Internos		Medio

Tabla 46: Dependencia de Instalaciones que lo acogen (Redes y Comunicaciones)

Instalaciones que lo acogen			
Dependencia de Activos Inferiores			
Activo:	**Red Telefónica**	Grado:	
	Centro de Datos		Alto
	Edificio		Alto

Equipamiento Auxiliar

Las dependencias normalmente identifican

Personas relacionadas con este equipo: operadores, administradores

Tabla 47: Personas relacionadas con este equipo (Equipamiento Auxiliar)

Personas relacionadas con este equipo			
Dependencia de Activos Inferiores			
Activo:	**Fuentes de Alimentación**	Grado:	
	Operadores		Alto

Instalaciones

Las dependencias normalmente identifican

Personas relacionadas con esta instalación guardias, encargados de mantenimiento.

Tabla 48: Personas relacionadas con este equipo (Instalaciones)

Personas relacionadas con este equipo			
Dependencia de Activos Inferiores			
Activo:	**Centro de Datos**	Grado:	
	Administradores de Sistemas		Alto
	Administrador de Redes		Alto
	Seguridad (Guardianía)		Alto

- **Valoración de Activos**

Tabla 49: Valoración de Activos

Clase de Activo	**Entorno de TI**	**Nombre del Activo**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Activos Esenciales	Información	Datos de interés comercial					
	Servicio						
Datos / Información	Copias de Respaldo			10	9	9	8
	Datos de control de acceso			8	8	8	8
	Registro de Actividad (log)			10	8	7	10
	Voz			6	6	5	5
Servicios	A usuarios externos (bajo relación contractual)		10			6	9
	Interno (Usuarios y medios de la propia institución)		7			8	8
	Correo electrónico (email)		6			5	8
	Voz sobre IP		3			8	8
	Almacenamiento de Ficheros		8			5	9
	Servicio de Copias de Respaldo (backup)		10			8	9
	Servidor de Nombres de Dominio		7			9	8
	Servidor de Protocolo de Transferencia de Archivos (FTP)		5			8	8
	Blearning		8			8	9
	Hosting		9			8	9

- **Identificación de Amenazas**

Por el tamaño de la matriz que se utiliza para identificar las amenazas a los que están expuestos los Activos, a manera de ejemplo se muestra una parte de la matriz. La matriz completa se encuentra en el Anexo 5.

Tabla 50: Identificación de Amenazas

	Clase de Activo	**Datos / Información**																			
	Entorno de TI	Copias de Respaldo				Datos de control de acceso				Registro de Actividad (log)				Voz				Protección de Comunicaciones			
	Nombre del Activo																				
Amenazas		**D**	**I**	**C**	**A**	**D**	**I**	**C**	**A**	**D**	**I**	**C**	**A**	**D**	**I**	**C**	**A**	**D**	**I**	**C**	**A**
[N] Desastres naturales																					
[N.1] Fuego																					
[N.2] Daños por agua																					
[N.*] rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc																					
[I] De origen industrial																					
[I.1] Fuego																					
[I.2] Daños por agua																					
[I.*] explosiones, derrumbes, contaminación química, sobrecarga eléctrica, etc																					
[I.3] Contaminación mecánica																					
[I.4] Contaminación electromagnética																					
[I.5] Avería de origen físico o lógico																					
[I.6] Corte del suministro eléctrico																					
[I.7] Condiciones inadecuadas de temperatura o humedad																					

CONTINÚA ⇨

[I.8] Fallo de servicios de comunicaciones																				
[I.9] Interrupción de otros servicios y suministros esenciales																				
[I.10] Degradación de los soportes de almacenamiento de la información																				
[I.11] Emanaciones electromagnéticas																				
[E] Errores y fallos no intencionados																				
[E.1] Errores de los usuarios	1	1	1		1	1	1		1	1	1		1	1	1		1	1	1	
[E.2] Errores del administrador	1	1	1		1	1	1		1	1	1		1	1	1		1	1	1	
[E.3] Errores de monitorización (log)																				
[E.4] Errores de configuración																				
[E.7] Deficiencias en la organización																				
[E.8] Difusión de software dañino																				
[E.9] Errores de [re-]encaminamiento																				
[E.10] Errores de secuencia																				
[E.14] Escapes de información																				
[E.15] Alteración accidental de la información		1				1				1				1				1		
[E.18] Destrucción de información	1				1				1				1				1			
[E.19] Fugas de información			1				1				1				1				1	
[E.20] Vulnerabilidades de los programas (software)																				
[E.21] Errores de mantenimiento / actualización de programas (software)																				
[E.23] Errores de mantenimiento / actualización de equipos (hardware)																				
[E.24] Caída del sistema por agotamiento de recursos																				
[E.25] Pérdida de equipos																				
[E.28] Indisponibilidad del personal																				

CONTINÚA ⟹

cionados																				
[A.3] Manipulación de los registros de actividad (log)									1											
[A.4] Manipulación de la configuración										1	1	1								
[A.5] Suplantación de la identidad del usuario		1	1	1		1	1	1		1	1	1		1	1	1		1	1	1
[A.6] Abuso de privilegios de acceso	1	1	1		1	1	1		1	1	1		1	1	1		1	1	1	
[A.7] Uso no previsto																				
[A.8] Difusión de software dañino																				
[A.9] [Re-]encaminamiento de mensajes																				
[A.10] Alteración de secuencia																				
[A.11] Acceso no autorizado		1	1			1	1			1	1			1	1			1	1	
[A.12] Análisis de tráfico																				
[A.13] Repudio										1										
[A.14] Interceptación de información (escucha)																				
[A.15] Modificación deliberada de la información		1				1				1				1				1		
[A.18] Destrucción de información	1				1				1				1				1			
[A.19] Divulgación de información			1				1				1				1				1	
[A.22] Manipulación de programas																				
[A.23] Manipulación de los equipos																				
[A.24] Denegación de servicio																				
[A.25] Robo																				
[A.26] Ataque destructivo																				
[A.27] Ocupación enemiga																				
[A.28] Indisponibilidad del personal																				
[A.29] Extorsión																				
[A.30] Ingeniería social (picaresca)																				

CONTINÚA ⟹

Valoración de las amenazas

Por el tamaño de la matriz que se utiliza para valorar las amenazas a los que están expuestos los Activos, a manera de ejemplo se muestra una parte de la matriz. La matriz completa se encuentra en el Anexo 6.

Tabla 51: Valoración de las Amenazas

ACTIVO				**PROBABILIDAD DE OCURRENCIA**	**DEGRADACION**				
CAPAS	**ACTIVOS**		**AMENAZAS**	**NIVEL**	**D**	**I**	**C**	**A**	**T**
Clase de Activo	**Entorno de TI**	**Nombre del Activo**							
Activos Esenciales	Información	Datos de interés comercial							
	Servicio								
Datos / Información	Copias de Respaldo								
			[E.1] Errores de los usuarios	**B**	**B**	**M**	**M**		
			[E.2] Errores del administrador	**B**	**A**	**A**	**M**		
			[E.15] Alteración accidental de la información	**B**		**M**			

CONTINÚA ⟹

			[E.18] Destrucción de información	**MB**	**B**				
			[E.19] Fugas de información	**B**			**M**		
			[A.5] Suplantación de la identidad del usuario	**B**		**A**	**A**	**A**	
			[A.6] Abuso de privilegios de acceso	**M**	**A**	**A**	**A**		
			[A.11] Acceso no autorizado	**B**			**A**	**M**	
			[A.15] Modificación deliberada de la información	**MB**		**A**			
			[A.18] Destrucción de información	**B**	**B**				
			[A.19] Divulgación de información	**M**			**M**		
	Datos de control de acceso								
			[E.1] Errores de los usuarios	**M**	**M**	**MB**	**B**		
			[E.2] Errores del administrador	**B**	**A**	**M**	**M**		
			[E.15] Alteración accidental de la información	**B**		**MA**			
			[E.18] Destrucción de información	**B**	**A**				
			[E.19] Fugas de información	**M**				**A**	
			[A.5] Suplantación de la identidad del usuario	**B**		**A**	**A**	**M**	
			[A.6] Abuso de privilegios de acceso	**B**	**M**	**M**	**M**		
			[A.11] Acceso no autorizado	**B**		**M**	**M**		
			[A.15] Modificación deliberada de la información	**B**		**M**			

CONTINÚA ⟹

		[A.18] Destrucción de información	**B**	**M**				
		[A.19] Divulgación de información	**B**				**M**	
Registro de Actividad (log)								
		[E.1] Errores de los usuarios	**B**	**M**	**M**	**M**		
		[E.2] Errores del administrador	**B**	**M**	**M**	**M**		
		[E.15] Alteración accidental de la información	**B**		**M**			
		[E.18] Destrucción de información	**B**	**A**				
		[A.3] Manipulación de los registros de actividad (log)	**B**		**A**			
		[A.4] Manipulación de la configuración	**M**		**M**	**M**	**M**	
		[A.5] Suplantación de la identidad del usuario	**M**		**A**	**A**	**M**	
		[A.6] Abuso de privilegios de acceso	**B**	**M**	**M**	**M**		
		[A.11] Acceso no autorizado	**B**		**M**	**M**		
		[A.13] Repudio	**B**		**M**			
		[A.15] Modificación deliberada de la información	**B**		**M**			
		[A.18] Destrucción de información	**B**		**M**			
		[A.19] Divulgación de información	**B**	**M**				
Voz								
		[E.1] Errores de los usuarios	**MB**	**MB**	**MB**	**MB**		
		[E.2] Errores del administrador	**B**	**M**	**MB**	**B**		

CONTINÚA ⟹

Voz								
		[E.1] Errores de los usuarios	**MB**	**MB**	**MB**	**MB**		
		[E.2] Errores del administrador	**B**	**M**	**MB**	**B**		
		[E.15] Alteración accidental de la información	**MB**		**B**			
		[E.18] Destrucción de información	**MB**	**MB**				
		[E.19] Fugas de información	**B**			**B**		
		[A.5] Suplantación de la identidad del usuario	**M**		**B**	**B**	**B**	
		[A.6] Abuso de privilegios de acceso	**M**	**B**	**B**	**B**		
		[A.11] Acceso no autorizado	**B**			**B**	**B**	
		[A.15] Modificación deliberada de la información	**MB**		**B**			
		[A.18] Destrucción de información	**MB**	**B**				
		[A.19] Divulgación de información	**MB**			**B**		

- **Impacto**

  Por el tamaño de la matriz que se utiliza identificar el impacto que tendrían los activos si ocurrieran las amenazas a continuación se muestra una matriz resumida. La matriz completa se encuentra en el Anexo 7.

Tabla 52: Identificación del Impacto

ACTIVO					
Clase de Activo	**D**	**I**	**C**	**A**	**T**
Activos Esenciales					
Datos / Información	4	6	4	4	0
Servicios	4	4	4	4	0
Aplicaciones (SW)	6	4	4	4	0
Equipamiento informático (HW)	6	4	4	3	0
Redes de Comunicaciones (COM)	4	4	4	3	0
Equipamiento Auxiliar (AUX)	4	2	2	0	0
Servicio Subcontratado	4	4	4	3	0
Instalaciones	3	0	2	0	0
Personal	3	3	3	3	0

- **Riesgos**

  Por el tamaño de la matriz que se utiliza identificar los riesgos no se muestra la matriz completa, a continuación se muestra una matriz resumida. La matriz completa se encuentra en el Anexo 8.

Tabla 53: Identificación del Riesgo

ACTIVO					
Clases de Activos	**D**	**I**	**C**	**A**	**T**
Datos / Información	{4,4}	{6,4}	{4,4}	{4,4}	
Servicios	{4,6}	{4,6}	{4,6}	{3,6}	
Aplicaciones (SW)	{6,4}	{4,4}	{4,4}	{4,4}	
Equipamiento informático (HW)	{6,4}	{4,4}	{4,4}	{4,2}	
Redes de Comunicaciones (COM)	{4,4}	{4,4}	{4,4}	{3,4}	
Equipamiento Auxiliar (AUX)	{4,2}	{2,2}	{2,2}	{0,2}	
Servicio Subcontratado	{4,4}	{4,4}	{4,4}	{3,4}	
Instalaciones	{4,2}	{3,2}	{3,2}	{0,2}	
Personal	{4,4}	{4,4}	{4,4}	{0,4}	

- **Identificación de Salvaguardas**

Tabla 54: Identificación de Salvaguardas

	ASPECTO	TIPO	PESO RELATIVO	SLAVAGUARDA	NIVEL DE CRITICIDAD
Protecciones generales u horizontales	**G**	**PR**	3	H Protecciones Generales	
	G	**EL**	3	H.IA Identificación y autenticación	**8**
	T	**EL**	3	H.AC Control de acceso lógico	**7**
	T	**IM**	2	H.ST Segregación de tareas	**8**
	G	**CR**	2	H.IR Gestión de incidencias	**5**
	T	**PR**	3	H.tools Herramientas de seguridad	**7**
	T	**EL**	3	H.tools.AV Herramienta contra código dañino	**7**
	T	**DC**	2	H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión	**6**
	T	**EL**	1	H.tools.CC Herramienta de chequeo de configuración	**6**
	T	**EL**	1	H.tools.VA Herramienta de análisis de vulnerabilidades	**6**
	T	**MN**	1	H.tools.TM Herramienta de monitorización de tráfico	**5**
	T	**DC**	1	H.tools.DLP DLP: Herramienta de monitorización de contenidos	**5**
	T	**MN**	1	H.tools.LA Herramienta para análisis de logs	**5**
	T	**DC**	0	H.tools.HP Honey net / honey pot	**5**
	T	**MN**	1	H.tools.SFV Verificación de las funciones de seguridad	**5**
	G	**DC**	1	H.VM Gestión de vulnerabilidades	**5**
	T	**CR**	2	H.AU Registro y auditoría	**7**
Protección de los datos / información	**G**	**PR**	3	D Protección de la Información	**7**
	G	**RC**	1	D.A Copias de seguridad de los datos (backup)	**5**
	G	**PR**	1	D.I Aseguramiento de la integridad	**6**
	G	**PR**	1	D.C Cifrado de la información	**5**
	G	**EL**	2	D.DS Uso de firmas electrónicas	**7**
	G	**IM**	2	D.TS Uso de servicios de fechado electrónico (time stamping)	**7**
Protección de las claves criptográficas	**G**	**EL**	3	K Gestión de claves criptográficas	**8**
	G	**EL**	3	K.IC Gestión de claves de cifra de información	
	G	**EL**	3	K.DS Gestión de claves de firma de información	**7**
	G	**EL**	3	K.disk Gestión de claves para contenedores criptográficos	
	G	**EL**	3	K.comms Gestión de claves de comunicaciones	**8**
	T	**EL**	1	K.509 Gestión de certificados	**4**

CONTINÚA ⟹

	G	**PR**	1	S Protección de los Servicios

Protección de los servicios	**G**	**IM**	1	S.A Aseguramiento de la disponibilidad
	G	**PR**	1	S.start Aceptación y puesta en operación
	T	**EL**	3	S.SC Se aplican perfiles de seguridad
	G	**EL**	2	S.op Explotación
	G	**EL**	1	S.CM Gestión de cambios (mejoras y sustituciones)
	G	**EL**	1	S.end Terminación
	G	**EL**	1	S.www Protección de servicios y aplicaciones web
	G	**EL**	1	S.email Protección del correo electrónico
	T	**EL**	2	S.dir Protección del directorio
	T	**PR**	1	S.dns Protección del servidor de nombres de dominio
	G	**EL**	1	S.TW Teletrabajo
	T	**EL**	1	S.voip Voz sobre IP
Protección de las aplicaciones (software)	**G**	**PR**	2	SW Protección de las Aplicaciones Informáticas
	G	**EL**	1	SW.A Copias de seguridad (backup)
	G	**EL**	1	SW.start Puesta en producción
	T	**EL**	3	SW.SC Se aplican perfiles de seguridad
	G	**EL**	1	SW.op Explotación / Producción
	G	**EL**	1	SW.CM Cambios (actualizaciones y mantenimiento)
	G	**PR**	1	SW.end Terminación
Protección de los equipos (hardware)	**G**	**PR**	2	HW Protección de los Equipos Informáticos
	G	**EL**	1	HW.start Puesta en producción
	T	**EL**	3	HW.SC Se aplican perfiles de seguridad
	G	**EL**	1	HW.A Aseguramiento de la disponibilidad
	G	**PR**	1	HW.op Operación
	G	**EL**	1	HW.CM Cambios (actualizaciones y mantenimiento)
	G	**PR**	1	HW.end Terminación
	G	**EL**	1	HW.PCD Informática móvil
	G	**EL**	1	HW.print Reproducción de documentos
	G	**EL**	1	HW.pabx Protección de la centralita telefónica (PABX)
Protección de las comunicaciones	**G**	**PR**	3	COM Protección de las Comunicaciones
	G	**EL**	1	COM.start Entrada en servicio
	T	**EL**	3	COM.SC Se aplican perfiles de seguridad
	G	**EL**	1	COM.A Aseguramiento de la disponibilidad
	T	**EL**	1	COM.aut Autenticación del canal
	T	**EL**	2	COM.I Protección de la integridad de los datos
	G	**EL**	2	COM.C Protección criptográfica de la confidencialidad de los datos intercambiados
	T	**EL**	1	COM.op Operación
	G	**EL**	1	COM.CM Cambios (actualizaciones y mantenimiento)
	G	**PR**	1	COM.end Terminación
	G	**EL**	2	COM.internet Internet: uso de ó acceso a
	G	**EL**	3	COM.wifi Seguridad Wireless (WiFi)
	G	**EL**	1	COM.mobile Telefonía móvil
	T	**EL**	2	COM.DS Segregación de las redes en dominios

CONTINÚA ⟹

Protección en los puntos de interconexión con otros sistemas	**G**	**PR**	1	IP Puntos de interconexión: conexiones entre zonas de confianza	**5**
	T	**EL**	3	IP.SPP Sistema de protección perimetral	**5**
	G	**EL**	1	IP.BS Protección de los equipos de frontera	**5**
Protección de los soportes de información	**G**	**PR**	2	MP Protección de los Soportes de Información	**7**
	T	**IM**	1	MP.A Aseguramiento de la disponibilidad	**5**
	G	**IM**	3	MP.IC Protección criptográfica del contenido	**7**
	G	**EL**	2	MP.clean Limpieza de contenidos	**5**
	G	**EL**	1	MP.end Destrucción de soportes	**5**
Protección de los elementos auxiliares	**G**	**PR**	1	AUX Elementos Auxiliares	**6**
	T	**CR**	1	AUX.A Aseguramiento de la disponibilidad	**5**
	F	**EL**	1	AUX.start Instalación	**4**
	F	**EL**	1	AUX.power Suministro eléctrico	**4**
	F	**PR**	1	AUX.AC Climatización	**5**
	F	**EL**	1	AUX.wires Protección del cableado	**6**
Seguridad física – Protección de las instalaciones	**F**	**PR**	2	Protección de las Instalaciones	**6**
	F	**EL**	2	L.design Diseño	**5**
	F	**PR**	3	L.depth Defensa en profundidad	**5**
	F	**EL**	3	L.AC Control de los accesos físicos	**6**
	F			L.A Aseguramiento de la disponibilidad	
	F	**PR**	1	L.end Terminación	**2**
Salvaguardas relativas al Personal	**P**	**PR**	2	PS Gestión del Personal	
	P	**AW**	2	PS.AT Formación y concienciación	
	P	**EL**	1	PS.A Aseguramiento de la disponibilidad	
Salvaguardas de tipo Organizativo	**G**	**AD**	1	G Organización	**6**
	G	**AD**	3	G.RM Gestión de riesgos	**3**
	G	**AD**	1	G Plan Planificación de la seguridad	**6**
	G	**CR**	1	G. Exam Inspecciones de seguridad	**4**
Continuidad de Operaciones	**G**	**RC**	2	BC Continuidad del negocio	**5**
	G	**AD**	1	BC.BIA Análisis de impacto (BIA)	**2**
	G	**RE**	3	BC.DRP Plan de Recuperación de Desastres (DRP)	**5**
Externalización	**G**	**AD**	1	E Relaciones Externas	**5**
	G	**AD**	1	E.1 Acuerdos para intercambio de información y software	**5**
	G	**EL**	1	E.2 Acceso externo	**3**
	G	**EL**	1	E.3 Servicios proporcionados por otras organizaciones	**4**
	G	**AD**	1	E.4 Personal subcontratado	
Adquisición y Desarrollo	**G**	**AD**	0	NEW Adquisición / desarrollo	**4**
	G	**AD**	1	NEW.S Servicios: Adquisición o desarrollo	**2**
	G	**AD**	2	NEW.SW Aplicaciones: Adquisición o desarrollo	**4**
	G	**EL**	1	NEW.HW Equipos: Adquisición o desarrollo	**4**
	T	**AD**	1	NEW.COM Comunicaciones: Adquisición o contratación	**3**
	G	**EL**	1	NEW.MP Soportes de Información: Adquisición	**4**
	G	**CERT**		NEW.C Productos certificados o acreditados	**4**

Fuente: (Dirección General de Modernización Administrativa, 2012)

- **Valoración de Salvaguardas**

Tabla 55: Valoración de Salvaguardas

	ASPECTO	TIPO	PESO RELATIVO	SALVAGUARDA	NIVEL DE CRITICIDAD	VALORACION DE
Protecciones generales u horizontales	**G**	**PR**	3	H Protecciones Generales		
	G	**EL**	3	H.IA Identificación y autenticación	**8**	**L2**
	T	**EL**	3	H.AC Control de acceso lógico	**7**	**L2**
	T	**IM**	2	H.ST Segregación de tareas	**8**	**L1**
	G	**CR**	2	H.IR Gestión de incidencias	**5**	**L1**
	T	**PR**	3	H.tools Herramientas de seguridad	**7**	**L2**
	T	**EL**	3	H.tools.AV Herramienta contra código dañino	**7**	**L0**
	T	**DC**	2	H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión	**6**	**L1**
	T	**EL**	1	H.tools.CC Herramienta de chequeo de configuración	**6**	**L1**
	T	**EL**	1	H.tools.VA Herramienta de análisis de vulnerabilidades	**6**	**L1**
	T	**MN**	1	H.tools.TM Herramienta de monitorización de tráfico	**5**	**L2**
	T	**DC**	1	H.tools.DLP DLP: Herramienta de monitorización de contenidos	**5**	**L1**
	T	**MN**	1	H.tools.LA Herramienta para análisis de logs	**5**	**L0**
	T	**DC**	0	H.tools.HP Honey net / honey pot	**5**	**L0**
	T	**MN**	1	H.tools.SFV Verificación de las funciones de seguridad	**5**	**L1**
	G	**DC**	1	H.VM Gestión de vulnerabilidades	**5**	**L1**
	T	**CR**	2	H.AU Registro y auditoría	**7**	**L2**
Protección de los datos / información	**G**	**PR**	3	D Protección de la Información	**7**	**L2**
	G	**RC**	1	D.A Copias de seguridad de los datos (backup)	**5**	**L3**
	G	**PR**	1	D.I Aseguramiento de la integridad	**6**	**L0**
	G	**PR**	1	D.C Cifrado de la información	**5**	**L0**
	G	**EL**	2	D.DS Uso de firmas electrónicas	**7**	**L1**
	G	**IM**	2	D.TS Uso de servicios de fechado electrónico (time stamping)	**7**	**L0**
Protección de las claves criptográficas	**G**	**EL**	3	K Gestión de claves criptográficas	**8**	**L2**
	G	**EL**	3	K.IC Gestión de claves de cifra de información		**L0**
	G	**EL**	3	K.DS Gestión de claves de firma de información	**7**	**L0**
	G	**EL**	3	K.disk Gestión de claves para contenedores criptográficos		**L0**
	G	**EL**	3	K.comms Gestión de claves de comunicaciones	**8**	**L1**
	T	**EL**	1	K.509 Gestión de certificados	**4**	**L1**
Protección de los servicios	**G**	**PR**	1	S Protección de los Servicios	**6**	**L2**
	G	**IM**	1	S.A Aseguramiento de la disponibilidad		**L3**
	G	**PR**	1	S.start Aceptación y puesta en operación	**4**	**L1**
	T	**EL**	3	S.SC Se aplican perfiles de seguridad	**6**	**L2**
	G	**EL**	2	S.op Explotación	**5**	**n.a.**

	G	EL	1	S.CM Gestión de cambios (mejoras y sustituciones)	3	L1
	G	EL	1	S.end Terminación	5	n.a.
	G	EL	1	S.www Protección de servicios y aplicaciones web		L1
	G	EL	1	S.email Protección del correo electrónico	3	L3
	T	EL	2	S.dir Protección del directorio	5	L1
	T	PR	1	S.dns Protección del servidor de nombres de dominio (DNS)	7	L3
	G	EL	1	S.TW Teletrabajo	4	n.a.
	T	EL	1	S.voip Voz sobre IP		L2
Protección de las aplicaciones (software)	G	PR	2	SW Protección de las Aplicaciones Informáticas	7	L1
	G	EL	1	SW.A Copias de seguridad (backup)	4	L2
	G	EL	1	SW.start Puesta en producción	4	L1
	T	EL	3	SW.SC Se aplican perfiles de seguridad	7	L2
	G	EL	1	SW.op Explotación / Producción	5	L1
	G	EL	1	SW.CM Cambios (actualizaciones y mantenimiento)	4	L2
	G	PR	1	SW.end Terminación	3	n.a.
Protección de los equipos (hardware)	G	PR	2	HW Protección de los Equipos Informáticos	7	L3
	G	EL	1	HW.start Puesta en producción	4	L1
	T	EL	3	HW.SC Se aplican perfiles de seguridad	7	L1
	G	EL	1	HW.A Aseguramiento de la disponibilidad	5	L1
	G	PR	1	HW.op Operación	5	L1
	G	EL	1	HW.CM Cambios (actualizaciones y mantenimiento)	4	L2
	G	PR	1	HW.end Terminación	3	n.a.
	G	EL	1	HW.PCD Informática móvil		L0
	G	EL	1	HW.print Reproducción de documentos		L0
	G	EL	1	HW.pabx Protección de la centralita telefónica (PABX)		L1
Protección de las comunicaciones	G	PR	3	COM Protección de las Comunicaciones	9	L2
	G	EL	1	COM.start Entrada en servicio	5	L1
	T	EL	3	COM.SC Se aplican perfiles de seguridad	9	L1
	G	EL	1	COM.A Aseguramiento de la disponibilidad	6	L2
	T	EL	1	COM.aut Autenticación del canal	5	L1
	T	EL	2	COM.I Protección de la integridad de los datos intercambiados	6	L1
	G	EL	2	COM.C Protección criptográfica de la confidencialidad de los datos intercambiados	6	L0
	T	EL	1	COM.op Operación	5	L1
	G	EL	1	COM.CM Cambios (actualizaciones y mantenimiento)	5	L2
	G	PR	1	COM.end Terminación	3	n.a.
	G	EL	2	COM.internet Internet: uso de ó acceso a	5	L3
	G	EL	3	COM.wifi Seguridad Wireless (WiFi)	7	L3
	G	EL	1	COM.mobile Telefonía móvil		n.a.
	T	EL	2	COM.DS Segregación de las redes en dominios	5	L3
Protección en los puntos de interconexión con otros sistemas	G	PR	1	IP Puntos de interconexión: conexiones entre zonas de confianza	5	L3
	T	EL	3	IP.SPP Sistema de protección perimetral	5	L2
	G	EL	1	IP.BS Protección de los equipos de frontera	5	L2

Protección de los soportes de información	**G**	**PR**	2	MP Protección de los Soportes de Información	**7**	**L2**
	T	**IM**	1	MP.A Aseguramiento de la disponibilidad	**5**	**L2**
	G	**IM**	3	MP.IC Protección criptográfica del contenido	**7**	**L0**
	G	**EL**	2	MP.clean Limpieza de contenidos	**5**	**L0**
	G	**EL**	1	MP.end Destrucción de soportes	**5**	**L0**
Protección de los elementos auxiliares	**G**	**PR**	1	AUX Elementos Auxiliares	**6**	**L3**
	T	**CR**	1	AUX.A Aseguramiento de la disponibilidad	**5**	**L3**
	F	**EL**	1	AUX.start Instalación	**4**	**L3**
	F	**EL**	1	AUX.power Suministro eléctrico	**4**	**L4**
	F	**PR**	1	AUX.AC Climatización	**5**	**L4**
	F	**EL**	1	AUX.wires Protección del cableado	**6**	**L3**
Seguridad física – Protección de las instalaciones	**F**	**PR**	2	Protección de las Instalaciones	**6**	**L3**
	F	**EL**	2	L.design Diseño	**5**	**L4**
	F	**PR**	3	L.depth Defensa en profundidad	**5**	**L3**
	F	**EL**	3	L.AC Control de los accesos físicos	**6**	**L4**
	F			L.A Aseguramiento de la disponibilidad		**L3**
	F	**PR**	1	L.end Terminación	**2**	**L3**
Salvaguardas relativas al Personal	**P**	**PR**	2	PS Gestión del Personal		**L3**
	P	**AW**	2	PS.AT Formación y concienciación		**L4**
	P	**EL**	1	PS.A Aseguramiento de la disponibilidad		**L3**
Salvaguardas de tipo Organizativo	**G**	**AD**	1	G Organización	**6**	**L2**
	G	**AD**	3	G.RM Gestión de riesgos	**3**	**L1**
	G	**AD**	1	G.plan Planificación de la seguridad	**6**	**L2**
	G	**CR**	1	G.exam Inspecciones de seguridad	**4**	**L2**
Continuidad de Operaciones	**G**	**RC**	2	BC Continuidad del negocio	**5**	**L0**
	G	**AD**	1	BC.BIA Análisis de impacto (BIA)	**2**	**L1**
	G	**RE**	3	BC.DRP Plan de Recuperación de Desastres (DRP)	**5**	**L0**
Externalización	**G**	**AD**	1	E Relaciones Externas	**5**	**L1**
	G	**AD**	1	E.1 Acuerdos para intercambio de información y software	**5**	**L2**
	G	**EL**	1	E.2 Acceso externo	**3**	**L1**
	G	**EL**	1	E.3 Servicios proporcionados por otras organizaciones	**4**	**L3**
	G	**AD**	1	E.4 Personal subcontratado		**L1**
Adquisición y Desarrollo	**G**	**AD**	0	NEW Adquisición / desarrollo	**4**	**L3**
	G	**AD**	1	NEW.S Servicios: Adquisición o desarrollo	**2**	**L3**
	G	**AD**	2	NEW.SW Aplicaciones: Adquisición o desarrollo	**4**	**L3**
	G	**EL**	1	NEW.HW Equipos: Adquisición o desarrollo	**4**	**L3**
	T	**AD**	1	NEW.COM Comunicaciones: Adquisición o contratación	**3**	**L3**
	G	**EL**	1	NEW.MP Soportes de Información: Adquisición	**4**	**L2**
	G	**CERT**		NEW.C Productos certificados o acreditados	**4**	**L1**

Fuente: (Dirección General de Modernización Administrativa, 2012)

4.6.3 Evaluación de Control Interno

Para llegar a determinar el nivel de madurez del proceso PO9 y ME4 en el que se encuentra de Centro de Datos de la Universidad Nacional de Chimborazo se realizó encuestas al Director del Departamento de Tecnología y a los Administradores mediante las matrices como Evaluación de los Objetivos de Control del Proceso, Metas e Indicadores Clave de Desempeño de las actividades, Metas e Indicadores Clave de Desempeño de los procesos, Metas e Indicadores Clave de Desempeño de TI que son parte de Control Interno, los resultados de las mismas se encuentran en el anexo 9, luego se tabulo la información con ayuda de la tabla de atributos de madurez del marco de referencia COBIT.

Tabla 56: Atributos de Madurez

Conciencia y Comunicación	Políticas, Estándares y Procedimientos	Herramientas y Automatizacón	Habilidades y Experiencia	Responsabilidad y Rendición de Cuentas	Establecimiento y Mediciòn de Metas
1 Suerge el reconocimiento de la necesidad del proceso. Existe Comunicación esporádica de los problemas.	Existen enfoques ad hoc hacia los procesos y las prácticas. Los procesos y las practicas no estan definidos.	Pueden existir algunas herramientas; el uso se basa en herramienta estándar de escritorio. No existe un enfoque planeado para el uso de herramientas.	No están definidas las habilidades requeridas para el proceso. No existe un plan de entrenamiento y no hay entrenamiento formal.	No exite definición de responsabilidades y de rendición de cuentas. Las personas toman la propiedad de los problemas con base a su propia iniciativa de manera reactiva.	Las metas no están claras y no existen las mediciones
2 Existe conciencia de la necesidad de actuar. La gerencia comunica los problemas generales.	Surgen procesos similares y comunes pero en su mayoría son intuitivos y parten de la experiencia individual. Algunos aspectos de los procesos son repetibles debido a la experiencia individual, y puede existir alguna documentación y entendimeinto informal de políticas y procedimientos.	Existen enfoques comunes para el uso de herramientas pero se basan en soluciones desarroladas por individuos clave. Pueden haberse adquirido herramientas de proveedores, pero probablemente no se aplican de forma correcta o incluso no usarse.	Se identifica los requerimientos mínimos de habilidades para áreas críticas. Se da entrenamiento como respuesta a las necesidades, en lugar de hacerlo con base en un plan acordado. Existe entrenamiento informal sobre la marcha.	Un individuo asume su responsabilidad, y por lo general debe rendir cuentas aún si esto no está acordado de modo formal. Existe confunsión acerca de la responsabilidad cuando ocurren problemas y una cultura de culpas tiende a existir.	Existen algunas metas, se establecen algunas mediciones financieras pero solo las conoce la alta dirección. Hay monitoreo inconsistente en áreas asiladas.
3 Existe el entendimiento de la necesidad de actuar. La gerencia es más formal y estructurada en su comunicación.	Surge el uso de buenas prácticas. Los procesos, políticas y procedimientos están definidos y documentados para todas las actividades clave.	Existe un plan para el uso y estandarización de las herramientas para automatizar el proceso. Se usan herramientas por su propósito básico, pero pueden no estar de acuerdo al plan acordado.	Se definen y documentan los requerimientos y habilidades para todas las áreas. Existen un plan de entrenamiento formal pero todavía se basa en iniciativas individuales.	La responsabilidad y la rendición de cuentas sobre los procesos están definidas y se han identificado a los dueños de los procesos del negocio. Es poco probable que el dueño del proceso tenga la autoridad plena.	Se establecn algunas mediciones y metas de efectividad, pero no se comunican, ya existe una relación clara co las metas del negocio. Surgen los procesos de medición pero no se aplican de modo consistente.
4 Hay entendimiento de los requerimientos completos. Se aplican técnicas maduras de comunicación y se usan herramientas estándar de comunicación.	El procesoo es solido y completo; se aplican las mejores prácticas internas. Todos los aspectos del proceso están documentados y son repetibles. La dirección ha terminado y aprobado las políticas. Se adoptan y siguen estándares para el desarrollo y mantenimiento.	Se implatan las herramientas de acuerdo a un plan estándar y algunas se han integrado con otras herramientas relacionadas. Se usan herramientas en las principales áreas para automatizar la administración del proceso y monitorear las actividades y controles.	Los requerimientos de habilidades se actualizan rutinariamente para todas las áreas, se asegura la capacidad para todas las áreas críticas y se fomenta la certificación. Se aplican técnicas maduras de entrenamiento de acuerdo al plan de entrenamiento y se fomenta la compartición del conocimiento.	Las responsabilidades y la rendición de cuentas sobre los procesos están aceptadas y funcionan de modo que se permite al dueño del proceso descargar sus responsabilidades. Existe una cultura de recompensas que activa la accioón positiva.	La eficiencia y la efectividad se miden y se comunican y estan ligadas a las metas del negocio y al plan estratégico de TI. Se implementa el balanced scorecard de TI en algunas áreas , con excepciones conocidas por la gerencia.
5 Existe un entendimiento avanzado y a futuro de los requerimientos. Existe una comunicación proactiva de los problemas, basada en las tendencias, se aplican técnicas maduras de comunicación y se usan herramientas integradas de comunicación.	Se aplican las mejores prácticas y estándares externos. La documentación de procesos ha evolucionado a flujos de trabajo automatizados. Los procesos, las políticas y los procedimientos están estandarizados e integrados para permitir una administración y mejora extremo a extremo.	Se usan juegos de herramientas estandarizadas a los largo de la empresa. Las herramientas están completamente integradas con otras herramientas relacionadas para permitir un soporte integral de los procesos. Se usan las herrmientas para dar soporte a la mejora de los procesos y automáticamente detectar excepciones a los controles.	La organización fomenta de manera formal la mejora continua de las habilidades, con base en metas personales y organizacionales claramente definidas. El entrenamiento y la eduación dna soporte a las mejoras prácticas externas y al uso de conceptos y técnicas. Compartir el conocimiento es una cultura empresarial, y se están desarrollando sistemas basados en el conocimiento. Expertos externos y líderes industriales se emplean como guía.	Los dueñois de procesos tienen la facultad de tomar decisiones y medidas. La aceptación de la responsabilidad ha descendido en cascada a través de la organización de forma consistnente.	Existe un sistema de medición de desempeño integrado que liga al desempeño de TI con las metas del negocio por la aplicación global del balanced scorecad de TI. La dirección nota las excepciones de forma global y consistente y el análisis de causas raíz.

Fuente: (IT Gobernance Institute, 2007)

Obteniéndose los resultados que se muestran en los gráficos siguientes:

Nivel de madurez del proceso PO9

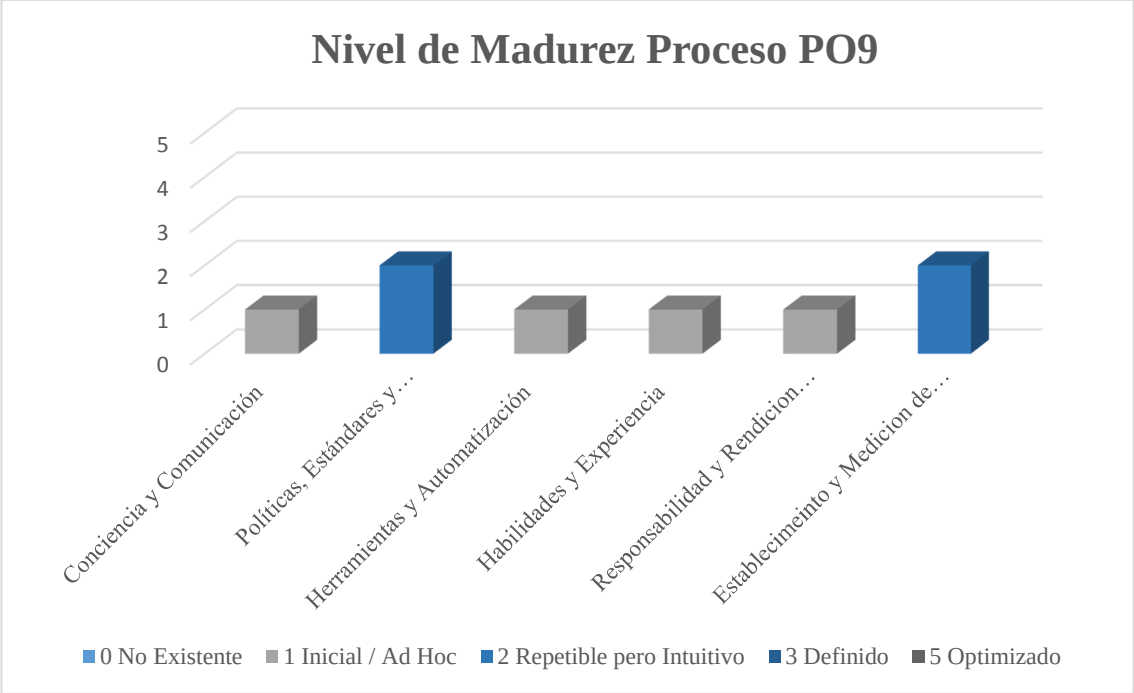


Gráfico 22: Resultado de la Evaluación del Control Interno

Tabla 57: Nivel de Madurez del Proceso PO9

NIVEL DEL MODELO DE MADUREZ		
NIVEL	**DESCRIPCION**	**ESTADO ACTUAL**
0 No Existente	Cuando la organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI.	
1 Inicial / Ad Hoc	Cuando se realizan evaluaciones informales de riesgos tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto, es decir, que existe un entendimiento emergente que los riesgos de TI son importantes y necesitan ser considerados.	X

CONTINÚA ⟹

2 Repetible pero Intuitivo	Cuando la administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas.	
3 Definido	Cuando la administración de riesgos sigue un proceso definido, el cual está documentado.	
4 Administrado y Medible	Cuando los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI, otorgando por parte de la gerencia un presupuesto para un proyecto de administración de riesgo operativo para re-evaluar los riesgos de manera regular.	
5 Optimizado	Cuando la administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI, está bien aceptada, y abarca a los usuarios de servicios de TI y cuando la dirección evalúa las estrategias de mitigación de riesgos de manera contínua.	

Fuente: (IT Gobernance Institute, 2007)

Nivel de Madurez del proceso ME4

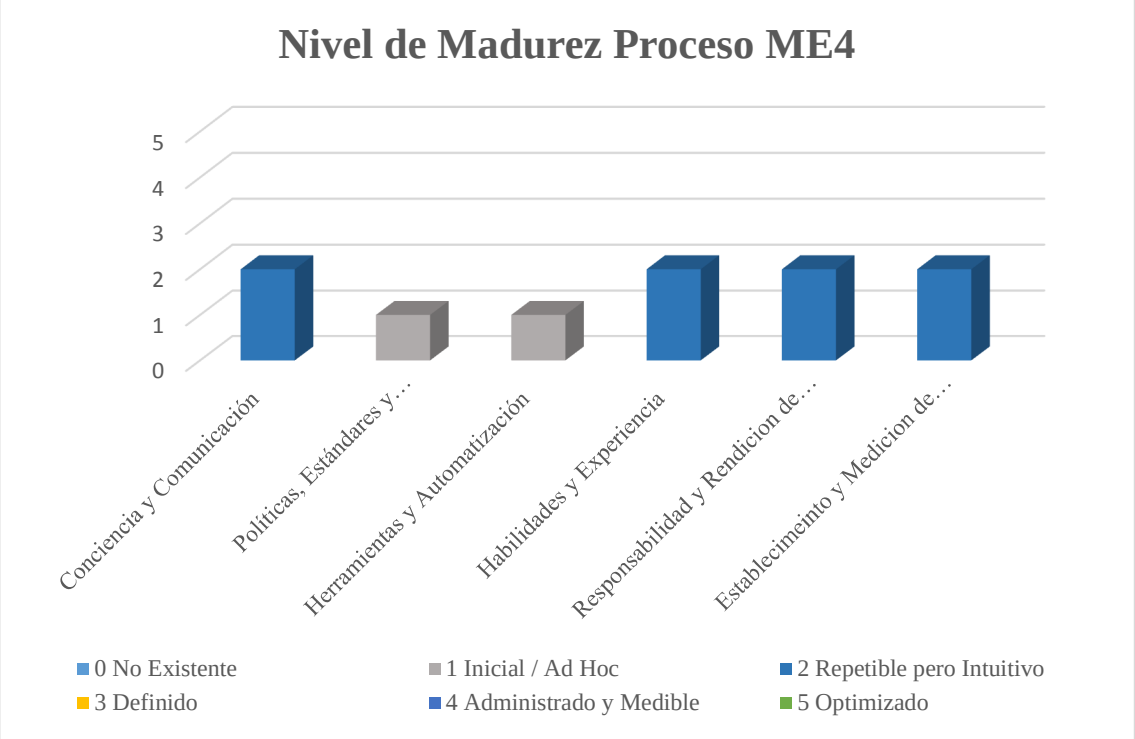


Gráfico 23: Resultado de la Evaluación del Control Interno

Tabla 58: Nivel de Madurez del Proceso ME4

NIVEL DEL MODELO DE MADUREZ		
NIVEL	**DESCRIPCION**	**ESTADO ACTUAL**
0 No Existente	Cuando la organización no tiene ningún proceso identificable de Gobierno de TI.	
1 Inicial / Ad Hoc	Las decisiones de la Gerencia son de forma reactiva a los incidentes y la comunicación que existe es ocasional sobre los problemas y como solucionarlos.	
2 Repetible pero Intuitivo	Los procesos, los instrumentos, los indicadores para evaluar el Gobierno de TI están restringidos lo que podría ocasionar que no se las utilice a toda su capacidad, ya que no se tiene la experiencia en su funcionalidad.	**X**
3 Definido	Los procedimientos se han estandarizado y documentado y la Gerencia los ha comunicado, pero la mayoría de problemas se los resuelve por iniciativa individual.	
4 Administrado y Medible	A todos los niveles se tiene un conocimiento completo de los temas de gobierno. Los parámetros de eficacia de todas las actividades de gobierno de TI se monitorean logrando con esto mejoras significativas para la institución.	
5 Optimizado	Los procesos se han depurado hasta alcanzar un nivel de mejor práctica, tomando como base los resultados de las mejoras permanentes y el modelo de madures de otras instituciones. Cuando existe un problema se analiza las causas para luego solucionarlos de manera eficiente.	

Fuente: (IT Gobernance Institute, 2007)

4.6.4 Confección y Redacción del Informe Final

Introducción

La Evaluación de Riesgos Tecnológicos del Centro de Datos de la Universidad Nacional de Chimborazo fue elaborada en base a la información proporcionada por el Director del Departamento de Tecnología, las observaciones realizadas y las evidencias encontradas durante las visitas realizadas.

Para la evaluación se elaboró un modelo en el cual para el análisis de riesgos se utilizó la metodología MAGERIT y para determinar el nivel de Madurez del proceso de gestión de riesgo se utilizó COBIT.

Hallazgos y Recomendaciones

El Comité Informático no ha sido creado.

Observación

La Universidad Nacional de Chimborazo no ha creado el Comité Informático. Actualmente.

Condición

Al no contar con el Comité Informático en la Universidad Nacional de Chimborazo, la Dirección de Tecnología se encarga de los procesos referentes a esta área, es decir, es la encomendada a definir y evaluar las políticas internas de tecnología, así como apoyar a las demás unidades administrativas que conforman esta institución.

Criterio

El Comité Informático debe estar a cargo de definir y evaluar las políticas internas referente a la tecnología de la Universidad Nacional de Chimborazo para que de esta manera el crecimiento tecnológico y la calidad de los servicios informáticos se los realice de forma ordenada y progresiva acorde las necesidades de la Institución y cumpliendo con las mejores prácticas establecidas.

Efecto

No poseer el Comité Informático ocasionaría que el alineamiento entre el Plan estratégico de la Institución y las actividades que realiza el área de Tecnología no sea el adecuado.

Causa

Falta de una política institucional para proceder a la creación del Comité Informático que especifique las políticas internas en el área tecnológica.

Recomendación

Por el tamaño de la Institución la máxima autoridad pertinente creará el Comité Informático, el cual definirá las funciones, su estatuto, roles y responsabilidades de cada miembro de dicho Comité, el cual deberá comenzar sus funciones seis meses posteriores a la entrega del informe final de la evaluación.

Garantizar la Seguridad

Observación

No se ha definido un plan de seguridad de TI, que garantice la consecución de los objetivos de la Universidad Nacional de Chimborazo.

Condición

La Universidad Nacional de Chimborazo no posee un plan de Políticas de Seguridad de TI, en el cual se encuentren definidos los requerimientos de seguridades físicas, lógicas relacionadas a TI.

Criterio

En el Plan de Políticas de Seguridad de TI, deben estar detallado los Acuerdos de niveles de Servicio, Acuerdos de niveles de Operación, además definir métricas e indicadores que permitan evaluar los niveles de seguridad físicos y lógicos.

Efecto

No poseer un plan de Políticas de Seguridad ocasionaría que los componentes de Tecnología estén expuestos a muchos riesgos, si una de las

amenazas se llegara a materializar la confianza de los usuarios disminuiría y la reputación institucional se vería afectada.

Causa

No tener identificados todos los riesgos a los cuales están expuestos los activos que poseen la Universidad de Chimborazo y la necesidad de gestionar los mismos.

Recomendación

Al no existir un Comité Informático u organismo equivalente en la Universidad Nacional de Chimborazo el Director del Departamento de Tecnología, elaborará un plan de Políticas de Seguridad en el cual se evidencie el alcance del plan de seguridad, estructura y responsables de los procesos y subprocesos de Gestión de Seguridad, Acuerdos de Niveles de Operación, indicadores que permitan monitorear los niveles de seguridad acordados, procedimientos de respaldo de la data de acuerdo a un cronograma específico y aprobado, esto durante los seis meses posteriores a la entrega del informe final de la evaluación, el mismo será valorado luego de la Creación del Comité Informático.

En el anexo 10 se encuentra un esquema básico de lo debe tener un plan de seguridad que coadyuve a gestionar los riesgos.

Garantizar la Seguridad de los Sistemas

Observación

La Universidad Nacional de Chimborazo no ha definido un plan de seguridad de los sistemas que forman parte del giro del negocio de la institución.

Condición

Al no contar con el Comité Informático, la Dirección de Tecnología se encarga de los procesos referentes a Políticas de Seguridad de los Sistemas, por lo que varios sistemas que se utilizan para el normal funcionamiento

de la Universidad Nacional de Chimborazo no están alojados en el Centro de Datos Institucional.

Criterio

El Comité Informático debe estar a cargo de precisar las políticas de seguridad para los sistemas en los cuales se soporta el funcionamiento de la Universidad Nacional de Chimborazo. Estas políticas deben ser actualizadas cuando existan cambios en las configuraciones, deben ser monitoreadas y evaluadas para de esta manera lograr un alineamiento entre los procedimientos de seguridad de TI a otras políticas y procedimientos que existan a nivel Institucional.

Efecto

La vulnerabilidad de los sistemas de la Universidad Nacional de Chimborazo sería mayor si no se toman en implementan políticas de seguridad.

Se tendrían interrupciones en los servicios informáticos, perdida de integridad de la información.

Causa

No se han definido políticas y normativas referentes a la seguridad de los sistemas internos.

Recomendación

Al no existir un Comité Informático u organismo equivalente en la Universidad Nacional de Chimborazo el Director del Departamento de Tecnología, definirá e elaborará políticas y procedimientos para administrar y monitorear la seguridad de los sistemas. Esto incluye trasladar los sistemas que se encuentran en otras unidades al Centro de Datos Institucional para proveerles de todas las prestaciones de seguridad lógica y física que brinda estas instalaciones durante los cinco meses posteriores a la definición de las políticas de seguridad.

Plan de Continuidad de TI

Observación

No se cuenta con un plan de continuidad de las operaciones de TI de la Universidad Nacional de Chimborazo.

Condición

La Universidad Nacional de Chimborazo no evidencia las políticas o algún procedimiento que se haya realizado por parte del Departamento de Tecnología, que pueda servir de base para el desarrollo del Plan de Continuidad de TI.

Criterio

El Director del Departamento de Tecnología deberá garantizar que el Plan de Continuidad de TI se encuentra alineado con el plan general de continuidad de funcionamiento de la Universidad Nacional de Chimborazo

Efecto

En el caso de una incidencia grave o un desastre la continuidad de las operaciones de TI de la Universidad Nacional de Chimborazo no podrá mantener un nivel adecuado o en el peor de los casos eliminación total de las mismas.

Al no poseer un plan de continuidad de TI se incrementarían los costos involucrados en la recuperación de la operatividad de los sistemas y la información.

Causa

Al no tener las alojadas en el Centro de Datos las aplicaciones sobre las cuales giran las actividades de la Universidad, no se ha visto la necesidad de elaborar una estrategia de continuidad de TI, que este alineada con estrategia de continuidad de la Universidad Nacional de Chimborazo.

Recomendación

Al no existir un Comité Informático u organismo equivalente en la Universidad Nacional de Chimborazo el Director del Departamento de Tecnología, definirá las políticas para la continuidad de TI internos durante los doce meses posteriores a la entrega del informe final de la evaluación.

En el anexo 11 se encuentra un esquema básico de lo debe tener un plan de Continuidad de TI que contribuya a gestionar los riesgos.

Continuidad de Servicios

Observación

La Universidad Nacional de Chimborazo no cuenta con un plan de continuidad de los servicios prestados por terceros.

Condición

La Universidad Nacional de Chimborazo no ha definido un plan de continuidad, en caso de que los servicios prestados por terceros se deterioren o no funcionen.

Criterio

En el plan de continuidad de los servicios prestados por terceros se debe definir las líneas base sobre las operaciones de la Universidad Nacional de Chimborazo, indicadores de capacidad, métricas para monitorear la los niveles de servicios acordados para tomar los correctivos que sean necesarios.

Efecto

No poseer un plan de continuidad de los servicios prestados por terceros puede ocasionar que al momento de presentarse un decremento o la ausencia total de él o los servicios no se puedan restaurar los mismos en un tiempo

adecuado de acuerdo a las necesidades de la Universidad Nacional de Chimborazo.

Causa

No se han definido un marco de trabajo, políticas y normativas de monitoreo referentes a la continuidad de los servicios prestados por terceros.

Recomendación

Al no existir un Comité Informático u organismo equivalente en la Universidad Nacional de Chimborazo el Director del Departamento de Tecnología, elaborará un plan sobre las políticas para la continuidad de los servicios prestados por terceros, en el cual se definirán los procedimientos, herramientas, frecuencia del monitoreo y presentación de informes del nivel de satisfacción durante los seis meses posteriores a la elaboración del plan de continuidad de TI, con el objetivo de que se identifiquen y se implementen gestiones correctivas del nivel de servicio prestado por terceros.

Almacenamiento de respaldo en un sitio alterno (Off-site)

Observación

No se ha contemplado el servicio de respaldos de información sensible en un sitio alterno de la Universidad Nacional de Chimborazo.

Condición

La Universidad Nacional de Chimborazo no ha contemplado la posibilidad de respaldar la información en un sitio alterno, basados en un análisis de la criticidad de la misma.

Criterio

El respaldo externo de información establecida como crítica debe ser implantado para soportar el plan de continuidad del negocio, además debe estar considerado dentro del plan de seguridad.

El sitio de almacenamiento externo debe tener un nivel de seguridad suficiente, que permita proteger los respaldos contra accesos no autorizados, robo o daño.

Efecto

No poseer un sitio externo para el respaldo de la información crítica ocasionaría que si una amenaza se materializara se perdería información vital para la continuidad de las operaciones de la Universidad Nacional de Chimborazo.

Causa

Falta de normativas de respaldo en sitios alternos. Falta del manual de políticas de seguridad.

Recomendación

Al no existir un Comité Informático u organismo equivalente en la Universidad Nacional de Chimborazo el Director del Departamento de Tecnología debe establecer normativas que determinen un sitio alterno para el respaldo de información sensible. Las instalaciones del sitio alterno deberán contar con niveles de seguridad suficiente, que permita proteger los recursos de respaldo, los acuerdos con el sitio alterno serán periódicamente analizados, al menos una vez al año, esto durante los seis meses posteriores a la elaboración del plan de continuidad de los Servicios.

Respaldo y Restauración

Observación

No se ha definido políticas para la administración de respaldos y recuperación de la información de la Universidad Nacional de Chimborazo.

Condición

La Universidad Nacional de Chimborazo no posee políticas para respaldar y restaurar la información de los servidores de la Universidad Nacional de Chimborazo. No se sigue un procedimiento para realizar los respaldos y restauración de los servicios prestados por Centro de Datos de la Universidad de Chimborazo que sirva para documentar las configuraciones de software y hardware. No se está utilizando de manera adecuada la infraestructura de Respaldos.

Criterio

Dentro de las políticas se deben definir procedimientos de elaboración periódica de respaldos en acuerdo a un cronograma aprobado, además se debe realizar una comprobación de los medios en los que se realizan los respaldos y el proceso de restauración para verificar la integridad de la información que se está respaldando.

Efecto

No poseer políticas de respaldos y restauración de la información sensible para la Universidad Nacional de Chimborazo puede ocasionar pérdida de datos y un riesgo en la continuidad de las operaciones del Centro de Datos.

Causa

A pesar de que el Centro de Datos de la Universidad Nacional de Chimborazo posee los equipos necesarios para realizar respaldos, no se están efectuando los mismas ya que aplicaciones como el sistema académico esta afuera del Centro de Datos y los administradores del mismo no tienen los accesos necesarios.

Recomendación

Al no existir un Comité Informático u organismo equivalente en la Universidad Nacional de Chimborazo el Director del Departamento de Tecnología, elaborará políticas para el respaldo y restauración de la información, en el cual esté definido la periodicidad con la que se van a realizar los mismos de acuerdo a un cronograma previamente aprobado.

Además se deberá comprobar los medios de respaldo y realizar una restauración para verificar la integridad de la información y su funcionalidad.

Administración de Configuración

Observación

No existe una administración de un repositorio de la configuración base del hardware y software de la Universidad Nacional de Chimborazo.

Condición

La Universidad Nacional de Chimborazo no posee evidencia de algún procedimiento para registrar la configuración base de los nuevos sistemas tanto.

Hardware como Software y de las modificaciones realizadas a los mismos para mantener una configuración raíz.

Criterio

Establecer y mantener un repositorio que contenga toda la información referente a los elementos de configuración tanto en Hardware como Software que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción. Se debe mantener una línea base de elementos de configuración para cada sistema y servicio, como un punto de control al cual regresar después de realizar cambios.

Efecto

No poseer un repositorio de los diagramas y configuraciones ocasionaría que al momento de implementar nuevas versiones de los sistemas hardware y software se pierda información crítica de la Universidad Nacional de Chimborazo que impida el normal funcionamiento de sus operaciones.

Causa

No se han definido un manual de diagramas y configuraciones referentes a la administración de la misma.

Recomendación

Al no existir un Comité Informático u organismo equivalente en la Universidad Nacional de Chimborazo el Director del Departamento de Tecnología, definirá un repositorio central que contenga toda la información relacionada a las configuraciones de cada uno de los activos tanto Hardware como Software que posee el Centro de Datos Institucional. Definir una línea base de la configuración para cada sistema y servicio, como un punto de control al cual regresar después de realizar cambios, lo anterior lo deberá realizar durante los diez meses posteriores a la entrega del informe final de la evaluación. Implementar un Service Desk con ITIL.

Manejo de Problemas e Incidentes

Observación

No ese ha definido un procedimiento de escalamiento de problemas e incidentes reportados al Departamento de Tecnología.

Condición

La Universidad Nacional de Chimborazo no posee un procedimiento de Soporte

Técnico cuando se presentan problemas e incidentes en los servicios prestados por el Departamento de Tecnología de la Universidad de Chimborazo.

No existe un registro en el que se incluyan los problemas escalados a otras unidades y a proveedores externos.

Criterio

La administración de los procedimientos de escalamiento de problemas e incidentes reportados por los usuarios, debe asegurar que sean resueltos por medio de mecanismos efectivos, eficientes, adecuados, los mismos que se deberán documentar.

Efecto

No poseer un manejo adecuado de los problemas e incidentes causaría pérdida de tiempo al momento de atender problemas reportados o identificados.

Causa

No se han definido normativas referentes al manejo de problemas e incidentes.

Recomendación

Al no existir un Comité Informático u organismo equivalente en la Universidad Nacional de Chimborazo el Director del Departamento de Tecnología establecerá el adecuado manejo de escalamiento de problemas, para garantizar que los problemas identificados sean resueltos de la manera eficiente.

Los procedimientos se deberán documentar para la activación del plan de continuidad de TI. Implementar un Service Desk con ITIL.

Control de Visitas

Observación

No existen procedimientos de acceso de visitantes al ingreso del Centro de Datos de la Universidad Nacional de Chimborazo.

Condición

La Universidad Nacional de Chimborazo carece de un procedimiento detallado para ingreso de las personas, registro en donde se evidencia el motivo de la visita, fechas, las actividades que se van a realizar en el Centro de Datos de la Universidad Nacional de Chimborazo.

Criterio

Deberán definirse procedimientos apropiados para las visitas al Centro de Datos, en los que se registrar el motivo de la visita, fechas y actividades que se realizaran en la visita (bitácora).

Efecto

No poseer procedimientos definidos de visitas puede ocasionar un riesgo ya que no se tendría una bitácora de las personas que visitan el Centro de Datos las mismas que podrían tener intensiones de sabotaje.

Causa

Falta de un manual de políticas de seguridad de acceso para los visitantes.

Recomendación

Al no existir un Comité Informático u organismo equivalente en la Universidad Nacional de Chimborazo el Director del Departamento de Tecnología elaborará el manual de políticas de visitas en el que entre otras cosas constará el control de acceso de los visitantes durante los doce meses posteriores a la entrega del informe final de la evaluación, además deberá mantenerse y revisarse regularmente una bitácora de visitantes.

CAPITUO V
CONCLUSIONES Y RECOMENDACIONES

5.1.1 Conclusiones

- En el desarrollo de la evaluación se evidenció que la Universidad Nacional de Chimborazo no tiene establecido un conjunto de buenas prácticas con estándares internacionales que sirvan para administrar y gestionar los riesgos de TI y generar valor al negocio.

- La Metodología MAGERIT elaborada por el Consejo Superior de Administración Electrónica de España, ha permitido realizar un análisis de los riesgos a los que están expuestos los diferentes activos del Centro de Datos de la Universidad de Chimborazo, evaluando cada uno de los activos a través de las dimensiones de seguridad como: Disponibilidad, Confidencialidad, Integridad, Autenticidad y Trazabilidad.

- Con las evaluaciones basadas en riesgos es probable prevenir incidentes posteriores no esperados, determinar las acciones que se va tomar con el objetivo de eliminar o minimizar los riesgos de caídas de los sistemas que ayudan al normal funcionamiento de la Universidad Nacional de Chimborazo.

- El Departamento de Tecnología de la Universidad Nacional de Chimborazo no posee un Plan de Continuidad de TI.

- El Departamento de Tecnología de la Universidad Nacional de Chimborazo no posee un manual de políticas de seguridad.

- Como constancia de la evaluación realizada al Centro de Datos de la Universidad Nacional de Chimborazo se adjunta el certificado de los

resultados de la misma en el Anexo 12.

5.1.2 Recomendaciones

- Integrar al Centro de Datos las aplicaciones que soportan el giro del negocio como el sistema académico, financiero, así como aplicaciones posteriores que planifique adquirir, o desarrollar por medio del personal la Universidad Nacional de Chimborazo para que tengan una mayor seguridad ante una probable amenaza.

- Elaborar e implementar un Plan de Continuidad de TI que permita disminuir el impacto en el funcionamiento normal de la Universidad Nacional de Chimborazo, en caso de un desastre o se materialice una amenaza.

- Capacitar a los funcionarios de la institución en aspectos de seguridad, control de tecnología y buenas prácticas para que en base a estos conocimientos se puedan plantear e implementar estrategias adecuadas de administración y gobierno de TI y se realicen evaluaciones tecnológicas frecuentes.

- Elaboración de un plan para ejecución de las recomendaciones de la presente evaluación para que el desenvolvimiento del Centro de Datos de la Universidad Nacional de Chimborazo más eficiente y eficaz.

- Elaboración de un manual de políticas de seguridad en el cual se definan y se formalicen las mismas, que permita al Departamento de Tecnología tener un adecuado control interno.

GLOSARIO DE TÉRMINOS

Actividad: Las medidas principales tomadas para operar el proceso COBIT.

Activo: Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

Amenaza: Eventos que pueden desencadenar un incidente de la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Análisis de Riesgo: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Autenticidad: Aseguramiento de la identidad u origen.

Centro de Datos: gran diversidad de sistemas, tanto lógicos como físicos, cuyo objetivo principal es administrar y salvaguardar la información que allí se encuentra alojada.

Cliente: Una persona o una entidad externa o interna que recibe los servicios.

COBIT: Objetivos de Control para Información y Tecnologías Relacionadas, es una guía de mejores prácticas presentado como framework, dirigida al control y supervisión de tecnología de la información.

Confidencialidad: Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

Continuidad: Prevenir, mitigar y recuperarse de una interrupción.

Degradación: Pérdida de valor de un activo como consecuencia de la materialización de una amenaza.

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Desempeño: La implantación real o el logro de un proceso.

Dominio: Agrupación de objetivos de control con etapas lógicas en el ciclo de vida de la inversión en TI.

Gobierno: Método por medio del cual una organización es administrada.

Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza.

Incidente: Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione una interrupción o una reducción de la calidad de ese servicio.

Infraestructura: La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.

Integridad: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

ITIL: Librería de Infraestructura de TI de Gobierno Gubernamental del reino Unido. Conjunto de lineamientos sobre la administración y procuración de servicios operativos de TI.

ISACA: Asociación de Auditoría y Control de Sistemas de Información, una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.

KPI: Indicador clave de desempeño.

Madurez: Indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar los objetivos y metas deseados.

MAGERIT: Es la Metodología de Análisis y Gestión de Riesgos elaborada por el Consejo Superior de Administración Electrónica de España.

MEHARI: Es un método para el análisis y gestión del riesgo.

OCTAVE: Es una metodología que mejora el proceso de toma de decisiones que tiene que ver con la protección y gestión de recursos de una organización, así como una herramienta de análisis de riesgos

Proceso: Un conjunto de procedimientos influenciados por las políticas y estándares de la organización.

Riesgo: El probabilidad de que una amenaza específica explote las debilidades de un activo o un grupo de activos para ocasionar perdida o daño a los activos.

Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo.

Usuario: Una persona que utiliza los sistemas empresariales.

TI: Tecnología de Información

Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

Vulnerabilidad: Estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada.

Bibliografía

IT Gobernance Institute. (2007). COBIT. United States of America.

Association, I. I. (s.f.). *(http://www.isaca.org)*.

Auditoriapublica. (2012). *auditoriaygestiondefondospublicos*. Obtenido de http://www.auditoriapublica.com/auditoriaygestiondefondospublicos

Betolin, D. A. (s.f.). *1*. Obtenido de Gestion de riesgos y de seguridad de la informacion: http://conectronica.com

C/Albasanz. (s.f.). *www.trc.es*. Recuperado el 29 de 01 de 2013

Cevallos, J. D. (2005). *Auditor en Control de Gestión* .

Cevallos, M. (2005). Administración de Riesgos de Tecnología de Información de una Empresa del Sector Informático. En J. D. 2005.

Comercio, O. M. (2013). Evalaucion de Riesgos.

Cuellar, G. (s.f.). Concepto Universal de Auditoria,.

Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Madrid.

Duarte, F. I. (2003). *Administracion de Riesgos de TI*. Manizales.

FOPAE. (2012). Fondo De Prevención Y Atención De Emergencias. Bogotá .

Gestion de Riesgos. (2013). Obtenido de http:// www.concetronica.com/gestionderiesgos1

González, A. C. (2005). Riesgos Informaticos.

Landeau, R. (2007). *Elaboracion de Trabajos de Investigacion*. Caracas.

Manslla, R. (2013). Obtenido de http://www.slideshare.net/riesgos

MEHARI. (Agosto de 2010). *www.mehari.info*. Obtenido de http://mehari.info/Security Stake Analysis and Classification Guide

Ortega, J. A. (s.f.).

publica, M. d. (2012). *Magerit*. Madrid.

Ramos, A. (2012). Magerit V3 nuevas guías STIC.

redesinformatica. (2013). Obtenido de http://redesinformatica1-2demm.com/

Troncoso, M. V. (Marzo de 1993). Santa Fe, Colomobia.

UNAL. (2012). *Procedimeinto de Adminsitracion del Riesgo*. Obtenido de

http://www.simege.unal.edu.co

www.clubensayo.com. (2013). Obtenido de http://clubensayos.com/Negocios/Metodologias-Del-Control-Interno/1223241.html