UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA SISTEMAS Y COMPUTACIÓN

"Trabajo de grado previo a la obtención del Título de Ingeniero en Sistemas y Computación"

TRABAJO DE GRADUACIÓN:

"APLICACIÓN DE PROCESOS Y POLÍTICAS DE LA INFORMÁTICA FORENSE EN LAS SEGURIDADES DE SERVIDORES. CASO PRÁCTICO SERVIDOR B-LEARNING DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO".

AUTOR:

FREDY ALEJANDRO FIERRO ZÚÑIGA

DIRECTORA:

ING. LIDA BARBA

RIOBAMBA – ECUADOR

2013

PÁGINA DE REVISIÓN

Los miembros del Tribunal de Graduación del proyecto de investigación de título **"Aplicación de procesos y políticas de la Informática Forense en las seguridades de servidores caso práctico servidor B-learning de la Universidad Nacional de Chimborazo"**, presentado por: Fredy Alejandro Fierro Zúñiga y dirigida por Ing. Lida Barba.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en la cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

Ing. Fernando Molina

Presidente del Tribunal _____

Firma

Ing. Lida Barba

Miembro del Tribunal _____

Firma

Ing. Danny Velasco

Miembro del Tribunal _____

Firma

AUTORÍA DE LA INVESTIGACIÓN

"La responsabilidad del contenido de este Proyecto de Graduación, corresponde exclusivamente a: Fredy Alejandro Fierro Zúñiga y del Director del Proyecto; Ing. Lida Barba y el patrimonio intelectual de la misma a la Universidad Nacional de Chimborazo.

AGRADECIMIENTO

Mi agradecimiento profundo a la Universidad Nacional de Chimborazo y a la carrera de Ingeniería en Sistemas y Computación por los conocimientos que me fueron impartidos en el transcurso de mi formación académica dentro de sus aulas, al Centro de Tecnología Educativa y a mi tutora de tesis por ayudarme a plasmar esta anhelada meta, también deseo agradecer a mis profesores y compañeros por formar parte de mi formación intelectual y personal. Pero de manera especial agradezco a mi Madre y mi hermana por darme las fuerzas y apoyo para terminar esta etapa de mi vida y hacerme ver que no hay mayor obstáculo en la vida que el que uno mismo se pone.

DEDICATORIA

Dedico el presente trabajo a mi familia, de sobremanera a mi madre que es el mayor ejemplo enseñanza y sacrificio, a mi hermana por estar junto a mí brindarme su apoyo y comprensión a pesar de la adversidad, está firme cuidándome de forma incondicional y no quiero olvidarme de muchos personas grandes amigos y amigas quienes me apoyaron para no caer en estos momentos, gracias Jimena, Rosa, Elbita, sin su apoyo este camino sería más largo y obscuro. Gracias a todos los que forman parte de mi existencia y recuerden que estoy aprovechando la segunda oportunidad por todos ustedes.

ÍNDICE GENERAL

Contenido

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

El presente trabajo tiene como objeto determinar la importancia que tiene la Informática Forense para identificar las fortalezas y vulnerabilidades del sistema de B-learning de la Universidad Nacional de Chimborazo, con el único fin de que se realice un seguimiento a este proceso para que se implementen y mejoren las normas de este servicio.

Durante el análisis se determinaron varios parámetros de investigación, se aplicó la metodología MAGERIT, que permite identificar los principales aspectos a tener en cuenta para la protección de los servicios informáticos que presta la Universidad Nacional de Chimborazo, poniendo énfasis en los de mayor acceso, con los cuales se ha logrado monitorearlos y detectar las diversas falencias que podrían presentarse y así evitar riesgos futuros.

Este trabajo tiene como fin el dar una pauta en cuanto a la utilización de la Informática Forense, la aplicación de normas y estándares de seguridad de la información, evaluación de métodos y la verificación de posibles riegos. El estudio conlleva a la implementación de planes de contingencia que fortalezcan al nuevo Centro de Tecnología Educativa con la visión de que éste se convierta en uno de los Centros de Datos pioneros en cuanto a seguridad y eficiencia dentro de la ciudad, provincia y el país, aportando en el posicionamiento de la Universidad Nacional de Chimborazo como una institución educativa de primer nivel.

Se puede considerar que la Informática Forense no puede ser la única herramienta para determinar falencias ocultas de los sistemas, esta debe ir acompañada de la actualización de metodologías, implementación de estándares y capacitación del personal a cargo de la administración del edificio Centro de Tecnología Educativa, la Informática Forense brinda una cantidad de posibilidades que nos permiten saber el estado del sistema que es objeto de investigación, por lo que se puede decir que se convierte en aliada para mejorar la seguridad de los sistemas informáticos.

SUMMARY

The following work aims to determine the importance that forensic informatics has to identify strengths and weakness into the B-learning system of the Chimborazo National University. Once done, it could help to make a follow up to this process in order to apply and also improve the parameters of this service.

During the analysis, some features of investigation were pointed out. After that, it was applied MAGERIT methodology, which allows identifying the mains aspects to take into consideration for protect those informatics services that the University gives to their students. A special emphasis was made into those services with more expanded use, monitoring them, so it could be detected possibilities of failures and avoiding future risks.

The objective of this work is to provide a guideline in the usage of Forensic Informatics, the application of norms and information security standards, the evaluation of methods and the evaluation of possible failures. The study entails the implementation of contingency plans that strengthens the new Educational Technology Center. The vision for this new center is to become one of the pioneer Data Center in the province and also nationwide for its security and efficiency, and in this way contributing to make the Chimborazo National University as first level education institution.

Forensic Informatics could be considered as one in many other tools to determine hidden failures in technological systems. It would be appropriate to make it work in complementation with other procedures such as methodologies update, standards implementation and also capacitation for the personal in charge of the administration of the center. Since Forensic Informatics gives a great number of possibilities to determine the current status of any studied system, we could catalogue it as a great ally to improve informatics systems security.

INTRODUCCIÓN

En los últimos años las tecnologías de la información y las comunicaciones, han tenido un crecimiento exponencial, éste crecimiento, si bien ofrece muchas posibilidades para tener nuevos servicios, también conforma el ambiente propicio, para que desaprensivos basados en el anonimato, intenten acceder a la información existente en nuestros sistemas, casi siempre con fines delictivos o destructivos.

Son muchas las violaciones que se pueden realizar en un sistema informático, por usuarios que, sin tener acceso permitido, logran entrar a los mismos para obtener información confidencial, pudiendo incluso manipularla en su beneficio, destruirla o usarla contra terceros.

La Seguridad Informática se puede clasificar en seguridad lógica y seguridad física y busca con la ayuda de políticas y controles mantener la seguridad de los recursos y la información manejando los riesgos, sin embargo cuando se habla de seguridad se debe tener en cuenta que no existe la seguridad total.

Este documento pretende, ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que la institución, prevenga, proteja y maneje los riesgos de seguridad en diversas circunstancias. Las normas y políticas expuestas en este documento servirán de referencia, en ningún momento pretenden ser normas absolutas, las mismas están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad.

En la Universidad Nacional de Chimborazo como parte del modelo enseñanza-aprendizaje se ha implementado la modalidad de enseñanza B-learning ya que en estos tiempos en donde la tecnología es parte de nuestra vida en todos los aspectos, también la actividad pedagógica empieza a incorporarse a esta tendencia y así empieza a sortear las diversas barreras y dificultades que existían tales como: costos, distancias, horarios, entre otros con esta modalidad.

El B-learning combina la educación presencial y a distancia y el e-learning, también llamado educación virtual o educación a distancia basada en el uso de computadoras. Los principales ingredientes de esta mezcla (*blend*) son la comunicación e intercambio de información cara-a-cara y mediada por tecnologías, experimentación, trabajo tele-colaborativo y la enseñanza presencial y a distancia.

En B-learning el docente desempeña su rol tradicional, pero usa en beneficio propio el material didáctico que la informática e internet le proporcionan, para ejercer su labor en dos frentes: como tutor on-line (tutorías a distancia) y como educador tradicional (cursos presenciales). La forma en que combine ambas estrategias depende de las necesidades específicas de ese curso, dotando así a la formación on-line de una gran flexibilidad.

CAPITULO I

1. FUNDAMENTACION TEÓRICA

1.1. PROBLEMATIZACIÓN

1.1.1. IDENTIFICACIÓN Y DESCRIPCIÓN DEL PROBLEMA

Actualmente en todo el mundo se han identificado casos de robo de información por medio de varios métodos tales como internet o ingresando físicamente a los equipos, interceptando paquetes desde la LAN, insertando dispositivos físicos, ejecutando software malicioso sin que el usuario tenga conocimiento, la Educación virtual o en línea no está exenta de este problema pues las instituciones que manejan información de carácter académico como universidades, colegios, centros de formación académica son directamente afectados por estos procedimientos. Estos ataques conllevan a consecuencias como:

- Estafas electrónicas
- Pérdidas económicas
- Daños a equipos
- Espionaje electrónico
- Pérdida de información confidencial
- Manipulación de información en caso de instituciones educativas cambio en calificaciones
- Saturación de los servicios que brindan los servidores

En el caso aplicativo a estudiar se va a investigar e identificar las diferentes vulnerabilidades existentes en el servidor B-learning que posee la Universidad Nacional de Chimborazo, lo que implica conocer las fortalezas y debilidades en cuanto a la ubicación física del servidor, hardware, software, políticas de seguridad implementadas dentro del Centro Cómputo y reglas que se estén aplicando en el servidor .La Informática forense permitirá identificar si existen vulnerabilidades en el servidor B-learning de la Universidad Nacional de Chimborazo de acuerdo a este análisis se podrá sugerir nuevos parámetros para mejorar la seguridad de la información.

1.1.2. ANÁLISIS CRÍTICO

Dentro de las políticas de seguridad informática en las diferentes instituciones públicas, privadas, educativas y en general no aplican estándares y normas de seguridad efectivas, por lo que se vuelven susceptibles a ataques, fallas y problemas, todos estos inconvenientes se solucionarían al aplicar debidamente las normas y políticas a nivel hardware, software y red.

En el momento de implementar un servicio en este caso Moodle se debe considerar la integridad, disponibilidad escalabilidad y otros aspectos importantes para abastecer de manera efectiva el acceso a la información, la demanda de usuarios simultáneos su crecimiento y mejoramiento continuo en el acceso del personal es imperativo aplicar políticas de seguridad a los equipos servidores, de los usuarios, respaldo de datos, control de tareas administrativas y comunes y monitorización en los equipos

1.1.3. PROGNOSIS

Al aplicar un estudio completo de análisis forense en los temas relacionados a la seguridad Informática podemos encontrar y prever los riesgos a los que está expuesto el medio en donde se aplique dicho estudio.

Con la obtención de los resultados del estudio forense permitirá al equipo técnico establecer políticas y estrategias de seguridad, que permita a través de una normativa el uso adecuado de los recursos informáticos en la red institucional e internet. Esto implica que a futuro se implemente nuevas tecnologías Informáticas en equipos y software que permitan optimizar y proteger la información. También se podrá sugerir capacitar a los usuarios en el uso y manejo de la información para que estén conscientes de la vulnerabilidad y la fragilidad de cómo manejar la información a la que acceden todos los días tanto en el ámbito laboral y personal.

Se podría también establecer parámetros internacionales de seguridad que se podrían aplicar en lo que es la Educación virtual, que facilitarían de gran manera que los administradores de esta aplicación precautelaran la información que genera el servicio B-learning con normas técnicas probadas y certificadas aplicando y mejorando muchos

servicios la posibilidad de expansiones futuras que se necesiten en el tema de la Educación virtual.

1.1.4. JUSTIFICACIÓN

En nuestros tiempos gracias a la tecnología se ha podido realizar muchísimos avances tecnológicos tanto en software, hardware, internet, intranet.

La mayor parte de las aplicaciones e información general inclusive financiera y en muchos de los casos importantes se halla en aplicaciones web. Debido a su facilidad de accesibilidad en cualquier momento y lugar sin estar permanentemente en un lugar de trabajo específico la accesibilidad y el administración de la información deben estar dispuesto a controlados y tener medidas de seguridad adecuadas.

Hoy en día es conocido que las aplicaciones web son susceptibles a los ataques, el mal manejo o inclusive la malversación de la información, que pudiese incluir desde la utilización estratégica de la información financiera de las instituciones, empresas competidoras o incluso la intervención de informaciones estatales y manipulación de información en nuestro caso información de índole educativo.

La Universidad Nacional de Chimborazo, se ha ido acoplando a las nuevas tecnologías existentes de la información, y dentro de su infraestructura posee varios servicios web para brindar a sus estudiantes, los mismos que podrían ser susceptibles a ataques, perdida y manipulación lo que haría que la información que estos poseen y brindan sean mal utilizados.

Debido a que la Universidad Nacional de Chimborazo posee información de suma importancia y de valor incalculable esta tiene que ser debidamente cuidada y protegida de personas externas que hagan mal uso de la misma, y mucha de esa información es digital y si no se aplican las seguridades debidas podrían ser objeto de algún ataque, vulnerabilidad o manipulación.

El objeto de este estudio de tesis que se va a realizar permitiría detectar si los servicios informáticos, que se encuentran en los servidores que posee la Universidad Nacional de Chimborazo se encuentran debidamente protegidos y si estos siguen normas o

estándares que se recomiendan a nivel de seguridad se usaría para esto la Informática Forense para identificarlos y ayudar a que dichas vulnerabilidades sean corregidas.

Para esto se realizara e implementara dentro del servidor B-learning todas las pruebas necesarias, aplicando normas y estándares. Los mismos que permitirán que estos parámetros sean aplicados en todos los servidores de la institución tomando en consideración todo lo anterior el tema de investigación y la aplicación de la Informática forense y su implementación e importancia en campo de la seguridad Informática a desarrollar pretende fomentar una visión autónoma sobre las vulnerabilidades, exposiciones, el nivel de diseño de controles y los riesgos informáticos, que puede sufrir esta información.

1.1.5. DELIMITACIÓN

Este trabajo de investigación delimita su alcance al estudio de la Informática forense su implementación e importancia en el campo de la seguridad Informática, en el servidor B-learning de la Universidad Nacional de Chimborazo

La investigación está dirigida al análisis de la seguridad de la información generada en las aulas virtuales por parte de docentes y estudiantes de la institución el cual mantiene un total 5275 usuarios registrados a la fecha de estudio año lectivo 2012 - 2013.

1.1.6. FORMULACIÓN DEL PROBLEMA

¿Cómo contribuye la Aplicación de Procesos y Políticas de la Informática Forense en las seguridades del Servidor B-learning de la Universidad Nacional de Chimborazo?

1.1.7. OBJETIVOS

GENERAL

- Analizar la importancia de la Aplicación de Procesos y Políticas de la Informática Forense y su contribución en la seguridad Informática en el servidor B-learning de la Universidad Nacional de Chimborazo.

ESPECÍFICOS

- Investigar la teoría de la Informática Forense, los procesos y normativas de seguridad de la información con la finalidad de salvaguardar la misma.
- Realizar un estudio de infraestructura, servicios y políticas de seguridad aplicadas al Servidor B-learning de la Universidad Nacional de Chimborazo.
- Desarrollar una guía de aplicación de la Informática Forense para garantizar la seguridad del sistema B-learning, en base a estándares informáticos internacionales.
- Aplicar medidas de seguridad basadas en la Informática Forense a nivel de infraestructura y servicios del servidor B-learning para determinar su contribución en el mejoramiento de la seguridad del sistema y de los datos.

1.1.8. HIPÓTESIS

- La aplicación de Procesos y Políticas de Informática Forense mejoran la Seguridad del Servidor B-learning de la Universidad Nacional de Chimborazo.

1.2. INFORMÁTICA FORENSE

1.2.1. CONCEPTO DE INFORMÁTICA FORENSE

La Informática Forense o Auditoria Informática, es un proceso realizado por personal experto, esta consiste en la recolección, agrupamiento y evaluación de evidencia que nos permitan determinar si el Sistema de Información que maneja una empresa, entidad o compañía protege de manera efectiva uno de sus activos más importantes que es la información.

El auditar nos permitirá estudiar los diferentes mecanismos de control que se encuentran implementados dentro en una empresa u organización permitiéndonos determinar si estos son los más adecuados y cumplen objetivos y estrategias por los que fueron elegidos. Los mecanismos de control implementados pueden ser de varios tipos tales como:

- Directivos
- Preventivos
- De detección

- Correctivos
- De contingencia

1.2.2. LA SEGURIDAD INFORMÁTICA

La seguridad informática es el área de la Informática que su principal objetivo es el de proteger la infraestructura computacional sea esta física como lógica poniendo énfasis en la información que se encuentra contenida dentro de este ambiente.

En la actualidad para lograr este propósito nos regimos a estándares, métodos, reglas, protocolos y leyes que nos permiten que el impacto y los riesgos sean mínimos tanto en la infraestructura o con la información que se encuentra almacenada.

La Seguridad Informática puede abarcar para su estudio e implementación la protección del software, archivos, bases de datos, metadatos en lo referente a los componentes lógicos que la organización valore como un activo y signifique un riesgo, su manipulación o perdida de la información es decir en cuanto al tipo de datos que sea considerada privilegiada, delicada o confidencial.

También la Seguridad Informática abarca todo lo referente a la infraestructura, equipos, que la organización posea podemos describir a esto como la parte Física a proteger.

La Seguridad de la Información: Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistema tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e Integridad de la misma.[1]

Hay que tomar en cuenta los siguientes términos que se usan en el estudio de la Informática Forense:

- **Activo:** Cualquier cosa que tenga valor para la organización.[2]
- **Amenaza**: Se considera una amenaza a cualquier cosa que puede suceder y que, cuando esta ocurra, tienen consecuencias de índole negativas sobre los activos que administramos.

---

[1] **Fuente:** Libro Informática; Glosario de Términos y Siglas, Antonio Baquero, Luis Joyanes, Mc.Grow Hill

[2] **Fuente: Norma ISO/IEC 13335-1:2004**

- **Impacto:** Denominamos impacto a las consecuencias que se dan en un activo luego de la ejecución y materialización de alguna amenaza.
- **Riesgo:** Es la estimación del grado a la que se está expuesto a que una amenaza se haga efectiva y materialice en los activos causando daños o perjuicios dentro de la organización.
- **Riesgo Residual:** es el riesgo que queda aún después de haberse tomado las medidas de seguridad implementadas.
- **Análisis de riesgos:** Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.
- **Gestión de riesgos:** Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.[3]
- **Disponibilidad:** Garantizar de que los usuarios autorizados tengan acceso cuando requieran tanto a la información como a los activos asociados.
- **Integridad:** La propiedad de salvaguardar la exactitud e integridad de los activos.[4]
- **Confidencialidad:** La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.[5]
- **Autenticidad:** Comprobación de que la fuente de datos recibidos es confiable y legitima.
- **Trazabilidad:** Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.[6]
- **Seguridad de la Información:** Es la preservación de la integridad de la confidencialidad, disponibilidad de la información; además también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad. [7]
- **Evento de seguridad de la Información:** es una recurrencia identificada en el estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación

---

[3] **Fuente:** Libro de MAGERIT 2 (Método)

[4] **Fuente:** Biblioteca PILAR

[5] **Fuente:** Norma ISO/IEC 13335-1:2004

[6] Biblioteca PILAR

[7] **Fuente:** Norma ISO/IEC 17799-1:2005

previamente desconocida que puede ser relevante para la seguridad.[8]

- **Incidente de Seguridad de la Información**: Es una serie de eventos en la seguridad de la información, no deseada o inesperada que tienen una significativa probabilidad de poner en riesgo las operaciones comerciales y amenazan la seguridad de la información.[9]

1.2.3. PROCESOS DE SEGURIDAD DE LA INFORMACIÓN

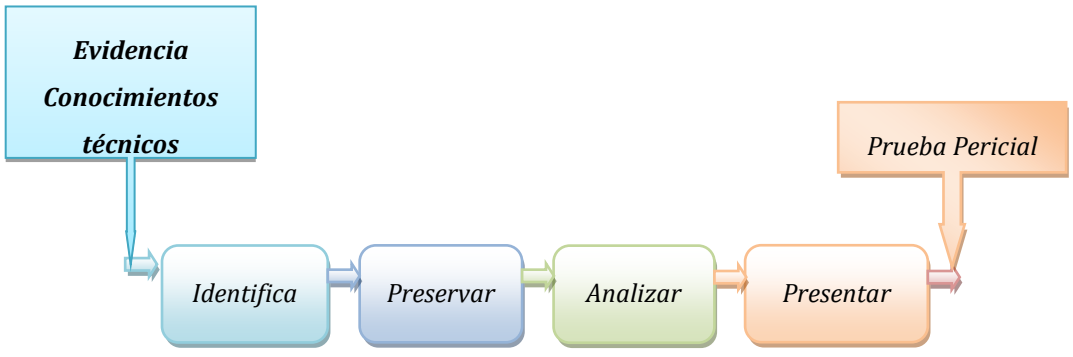
1.2.3.1. ANÁLISIS Y GESTIÓN DE RIESGOS

La información y activos se encuentran expuestos a un sinfín de amenazas que pueden destruir dichos recursos, produciendo un grave impacto dentro de la organización. Por ende es necesario minimizar el riesgo al que está expuesto el sistema.

Entonces se dispone de salvaguardas, que reducen la frecuencia de ocurrencia, o bien reducen o limitan el impacto. Dependiendo del grado de implantación de estas salvaguardas, el sistema pasa a una nueva estimación de riesgo que se denomina riesgo residual.

"Es el proceso de identificar, preservar, analizar y presentar evidencia digital, de manera que esta sea legalmente aceptable".[10]

Figura 1. Tratamiento de la Evidencia



[8] Norma ISO/IEC 13335-1:2004

[9] Norma ISO/IEC TR 18044:2004

[10] http://www.neuquen.gov.ar/seguridadinformatica/pdf/Informatica%20Forense%20-%20Hernan%20Herrera.pdf

1.2.3.2. LA IDENTIFICACIÓN DE LA EVIDENCIA DIGITAL

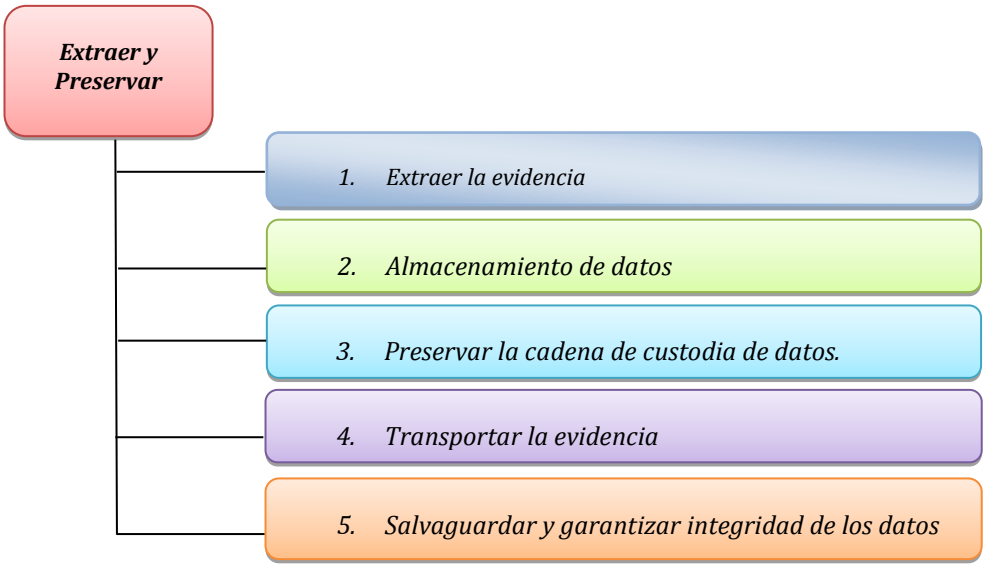
El identificar la evidencia digital es una tarea conocida por distintos aspectos. Entre los principales podemos indicar el factor humano, que realiza la obtención y manipulación del material informático. Muchas veces la identificación y recolección de la evidencia digital es realizada por personal sin muchos conocimientos para esta tarea, lo cual genera la omisión de algunos aspectos técnicos puede llevar a la perdida de datos.

Otro aspecto a tomar en cuenta es el relativo a la identificación de la evidencia digital se refiere a la correcta rotulación y detalle de los elementos informáticos a ser identificara extracción y preservación del material informático

Extraer y Preservar el material informático durante la investigación supone considerar la fragilidad que poseen los medios de almacenamiento de los datos y la delicadeza de la información. Sobre esto cabe indicar que existe una gran falencia en lo referente a la cadena de custodia, cuyo principal objetivo es el de mantener todo el registro de las operaciones que se realizan sobre la evidencia digital en cada uno de los pasos de la investigación.

Preservar implica los aspectos técnicos relativos a la no alteración (integridad) de la evidencia original, aquí se puede utilizar algún software que genere un valor a partir de un conjunto de datos es de gran ayuda.

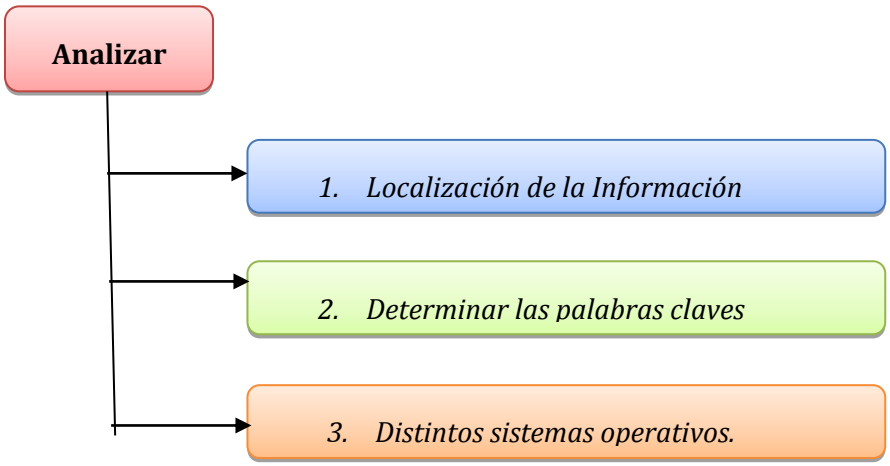
Figura 2. Elementos para la preservación de la evidencia



1.2.3.3. ANÁLISIS DE DATOS

El analizar involucra tareas referentes al extraer evidencia digital de los dispositivos o aparatos de almacenamiento. A la hora de analizar es necesario la localización de información específica vinculada con el objeto de la investigación, el análisis de datos en muchos casos requerirá de un trabajo interdisciplinario entre los sujetos que actúan dentro del proceso. Hay que determinar palabras claves al momento de la investigación y sobre todo hay que tener en cuenta que este proceso puede realizarse sobre distintos sistemas operativos.

Figura 3. Análisis de Datos



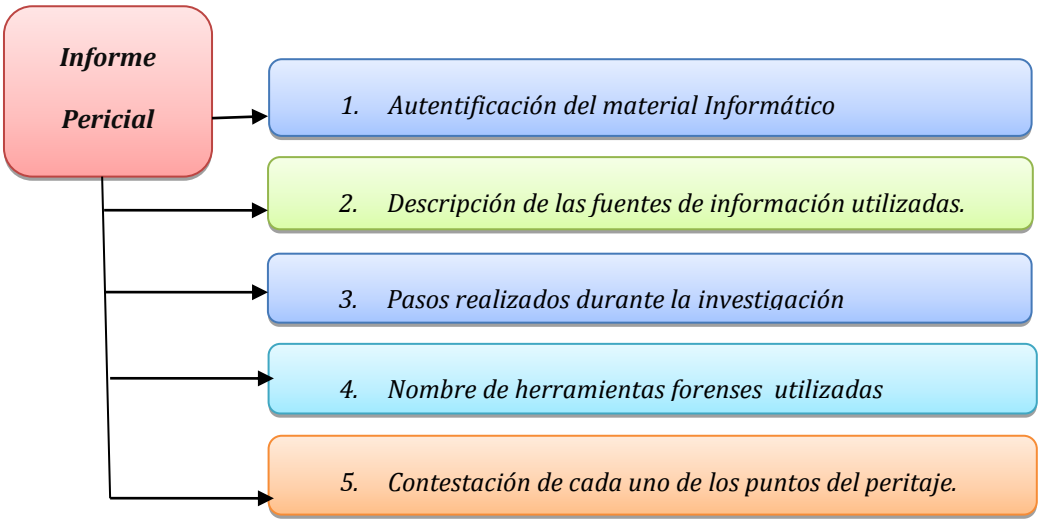
1.2.3.4. LA PRESENTACIÓN DEL DICTAMEN PERICIAL

El presentar consiste en elaborar el dictamen con los resultados que se obtuvieron en las etapas anteriores de la investigación.

La estructura básica de cualquier informe tendrían los siguientes elementos:

- Antecedentes.
- Documentos facilitados, recopilados y examinados.
- Inspecciones realizadas.
- Metodología del informe.
- Dictamen.
- Anexos.

Figura 4. Estructura del Informe



1.2.4. NORMATIVAS DE LA SEGURIDAD DE LA INFORMACIÓN

Son un conjunto de normas y criterios básicos que determinan lo relativo al uso de los recursos de una organización cualquiera. Se refiere a normas jurídicas necesarias para la prevención y sanción de las posibles conductas que puedan ir en contra de la integridad y seguridad de los sistemas informáticos.

Las siguientes normas de seguridad informática expuestas en este documento, sirven de referencia más no se pretende establecer como normas absolutas, a continuación se define los procedimientos más adecuados tomando en cuenta cuatro criterios.

1.2.4.1. SEGURIDAD ORGANIZACIONAL

Tratar establecer el marco formal de la seguridad que se debe implementar en la institución, incluyendo los servicios o contrataciones externas realizadas en la infraestructura de seguridad, y a su vez integrar el recurso humano con la tecnología implementada señalando las responsabilidades y las actividades complementarias que pueden darse ante situaciones anómalas de la seguridad.[11]

[11]Fuente: Manual de políticas y normas de seguridad informática

1.2.4.2. SEGURIDAD LÓGICA

Establece e integra mecanismos y procedimientos que permiten el monitoreo de los accesos a la información que incluyen los procedimientos de administración de usuarios, la definición de responsabilidades, los perfiles de seguridad a implementarse, el control de acceso a las aplicaciones alojadas en el sistema y a la documentación sobre sistemas, que van desde el control de los cambios ejecutados en la configuración de los equipos, el manejo de incidentes, la selección y aceptación de sistemas, hasta el control de software perjudicial.[12]

1.2.4.3. SEGURIDAD FÍSICA

Permite identificar los parámetros mínimos que se deben cumplir en cuanto al perímetro físico de seguridad, de tal forma que se puedan establecer controles en el manejo de equipos, transferencias y manipulación de información así como el control de los accesos a las distintas áreas que conforman la unidad donde se encuentran alojados los equipos o activos de la institución.[13]

1.2.4.4. SEGURIDAD LEGAL

Permite integrar los requerimientos que deben cumplir todos los administradores empleados y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos.[14]

1.2.5. NORMAS ISO - SEGURIDAD INFORMÁTICA

ISO es una organización no gubernamental que forma un puente entre los sectores públicos y privados y nació con el objetivo de "facilitar la coordinación internacional y la unificación de los estándares industriales."

---

[12]Fuente: Manual de políticas y normas de seguridad informática
[13]Fuente: Manual de políticas y normas de seguridad informática
[14]Fuente: Manual de políticas y normas de seguridad informática

La ISO ha reservado la serie ISO/IEC 27000 para una gama de normas de gestión de la seguridad de la información de manera similar a lo realizado con las normas de gestión de la calidad, la serie ISO 9000.

1.2.5.1. NORMA ISO 27000

La serie ISO 27000 es una serie de estándares publicados por la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional que contiene las normas para la Seguridad de la Información, utilizada por cualquier tipo de organización, pública o privada, grande o pequeña.

Las distintas normas que componen la serie ISO 27000; indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

Nota: La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) elegido. En general, es recomendable la ayuda de consultores externos.[15]

1.2.5.2. FAMILIAS DE LA NORMA ISO 27000

- **ISO 27001**: Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información.
- **ISO 27002**: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
- **ISO 27003**: guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.
- **ISO 27004**: Sistema de Gestión de Seguridad de Información y de los controles relacionados

[15]http://es.wikipedia.org/wiki/ISO/IEC_27001

- **ISO 27005**: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma
- **ISO/IEC 27001** y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

1.2.5.3. NORMA ISO 27001

La Norma ISO 27001, siendo la principal norma en requisitos de la serie, está dedicada a especificar los requerimientos necesarios para: establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.

Esta norma se basa en la gestión de riesgos y en el mejoramiento de los procesos, además para ser implantada el tiempo necesario es de 6 meses a 1 año.

La ISO 27001 contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma a la cual se certifican por auditores externos los SGSI (Sistema de Gestión de la Seguridad de la Información) de las organizaciones.

1.3. METODOLOGÍAS DE LA INFORMÁTICA FORENSE

El desarrollar las metodologías de análisis forense empezó con la investigación y el estudio pormenorizado de las principales metodologías existentes para al análisis de los riesgos informáticos. En éste trabajo se detallan las tres metodologías más usadas, con el fin de determinar en forma detallada sobre cómo es su funcionamiento y cuáles son sus fortalezas y debilidades. Las metodologías estudiadas son:

- MAGERIT
- Octave
- Mehari

1.3.1. OBJETIVOS DE LAS METODOLOGÍAS

Tanto las tres metodologías estudiadas como la que se desarrollará tienen por objetivo los siguientes puntos:

- Planificación de la reducción de riesgos
- Planificación de la prevención de accidentes
- Visualización y detección de las debilidades existentes en los sistemas
- Ayuda en la toma de las mejores decisiones en materia de seguridad de la información.

1.3.2. ANÁLISIS DE LA METODOLOGÍA BASE

Se realizó un estudio detallado de cada uno de los elementos funcionales que intervienen en cada etapa de la metodología a fin de determinar los puntos débiles que la misma presenta. En síntesis se obtuvo como resultado lo siguiente:

- Escasez de material teórico para cada una de las etapas.
- Ausencia de un procedimiento práctico que mida las debilidades y calidad de los servicios de seguridad.
- Las escalas de la probabilidad de ocurrencia, impacto y del riesgo presentan niveles simples de valoración.
- Ausencia de un análisis de la frecuencia de una amenaza.
- Ausencia de un método que registre el nivel del impacto y del riesgo en sus reales dimensiones.
- Falta de un mecanismo o procedimiento práctico que permita la interpretación de los resultados obtenidos.

1.3.3. ANÁLISIS FUNCIONAL DE LAS METODOLOGÍAS

MAGERIT

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes

para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

- Análisis de Riesgos
- Gestión de Riesgos

PRINCIPALES ELEMENTOS DE MAGERIT

- 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

OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation por sus siglas en ingles es una metodología de análisis y gestión de riesgos, donde el objetivo principal es garantizar los sistemas informáticos dentro de una organización es un conjunto de herramientas, técnicas y métodos para desarrollar análisis de riesgos basados en gestión y la planeación estratégica de la organización. Son todas las acciones que necesitan ser llevadas a cabo dentro de la organización para realizar la gestión de activos, conocer posibles amenazas y evaluar vulnerabilidades.

Existen 3 versiones de la metodología OCTAVE:

La versión original de OCTAVE

La versión para pequeñas empresa OCTAVE-S

La versión simplificada de la herramienta OCTAVE-ALLEGRO

Cuenta con 3 fases durante el proceso de desarrollo de la metodología:

La primera contempla la evaluación de la organización, se construyen los perfiles activo-amenaza, recogiendo los principales activos, así como las amenazas y requisitos como imperativos legales que puede afectar a los activos, las medidas de seguridad implantadas en los activos y las debilidades organizativas.
En la segunda se identifican las vulnerabilidades a nivel de infraestructura de TI.
En la última fase de desarrolla un plan y una estrategia de seguridad, siendo analizados los riesgos en esta fase en base al impacto que puede tener en la misión de la organización.

- Construcción de los Perfiles de Amenazas Basados en Activos
- Identificación de la Infraestructura de Vulnerabilidades
- Desarrollo de Planes y Estrategias de Seguridad

PRINCIPALES ELEMENTOS DE OCTAVE

- Medidas de probabilidad considerando un rango de frecuencias.
- Análisis del límite entre niveles de probabilidad.

MEHARI

Método Armonizado de Análisis de Riesgos esta metodología originalmente desarrollada por la comisión Métodos de Clusif[16], en 1996 es una metodología utilizada para apoyar a los responsables de la seguridad informática de una empresa mediante un análisis riguroso de los principales factores de riesgos evaluando cuantitativamente de acuerdo a la situación de la organización donde se requiere el análisis, acopla los objetivos estratégicos existentes con los nuevos métodos de funcionamiento de la empresa, esto se lo realiza mediante una política de seguridad y mantenimiento de los riesgos a un nivel convenido.

[16] CLUSIF = Club de la Seguridad de los Sistemas de Información Franceses

MEHARI propone un módulo para analizar los intereses implicados por la seguridad, y un método de análisis de riesgos con herramientas de apoyo. Estos dos son necesarios para evaluar de una manera exitosa los riesgos en una empresa.

Los diagnósticos de seguridad

Esta metodología propone dos módulos para realizar el análisis de riesgos dentro de una organización:

- Modulo rápido.
- Modulo detallado.

En los dos casos el objetivo es el mismo, es decir evaluar el nivel de seguridad de la organización. La diferencia radica en el nivel de profundidad de la evaluación, en este caso el módulo rápido resultara menos preciso y el módulo detallado más confiable.

El módulo rápido es utilizado generalmente para una primera evaluación en la cual se identifican las principales debilidades de una organización. En el módulo de análisis detallado se analiza todas las posibles debilidades de cada uno de los servicios de seguridad con los que cuenta la organización a evaluar, con lo cual se crea una base experta, la misma que podremos utilizar posteriormente para el análisis de riesgos.

Existe la opción de combinar estos dos módulos donde se puede comenzar con el módulo rápido y realizar un diagnóstico y luego profundizar los mismos con el módulo detallado.

Estos módulos se pueden utilizar de maneras diferentes:

- **El diagnóstico de seguridad**

El realizar un correcto diagnóstico de seguridad dentro de una organización representa la base primordial para asegurar la reducción de los riesgos dentro de la misma.

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

La manera correcta de gestionar la seguridad de una organización es estableciendo planes de acción en base a la evaluación del estado de los servicios de seguridad.

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

MEHARI identifica todas las situaciones de riesgo dentro de una organización de tal forma que también cubre aquellos riesgos no aceptables.

Esta metodología no se restringe solamente a realizar un análisis de la parte informática sino que también incluye en su análisis los sistemas de información, la organización en general, el entorno de trabajo además de aspectos legales y reglamentarios.

- **Síntesis sobre los módulos de diagnóstico**

Estos módulos nos ofrecen una vista amplia y relacionada con la seguridad, pudiéndose utilizar progresivamente de acuerdo a la madurez de la empresa u organización donde se vaya a .implementar.

- **Análisis de los intereses implicados por la seguridad**

En esta parte se debe tener claro los intereses de seguridad que la organización realmente requiere, ya que se debe mantener un equilibrio entre las inversiones de seguridad y el verdadero nivel de los interese implicados por la seguridad.

PRINCIPALES ELEMENTOS DE MAHARI

- Análisis de riesgos: metodología para la elaboración de un plan de seguridad institucional
- Análisis sistemático de situaciones de riesgo
- Análisis específico de situaciones de riesgo
- Análisis de riesgo en nuevos proyectos

CUADRO COMPARATIVO Y SELECCIÓN DE LA METODOLOGÍA PARA REALIZAR EL ANÁLISIS DE RIESGOS.

En esta parte nos centraremos en la comparación de las metodologías explicadas posteriormente en el análisis de riesgos.

Tabla 1. Cuadro comparativo de metodologías.

METODOLOGIA	DESCRIPCION	FASES
MAGERIT	Esta metodología consta de 5 fases bien definidas y correctamente identificadas para realizar un análisis de riesgo dentro de una organización y cuyos objetivos son generales para cualquier tipo de organización donde se ejecute la misma.	1. Identificar los activos de la empresa. 2. Determinar las amenazas 3. Establecer las respectivas salvaguardas 4. Estimar el impacto 5. Determinación del Riesgo
OCTAVE	Esta metodología consta de tres fases las cuales reúnen a ocho procesos, con el objetivo de organizar e identificar todos los riesgos en cada uno de los niveles de los que consta la empresa u organización donde se vaya a realizar dicho análisis de riesgos. Cada uno de los procesos tiene un objetivo específico que ayudará a identificar y mitigar las posibles amenazas y riesgos que pueda ocurrir en una empresa.	1. Identificar el conocimiento de los altos directivos. 2. Identificar el conocimiento de los directivos de áreas operativas. 3. Identificar el conocimiento del personal. 4. Crear perfiles de amenaza 5. Identificar componentes claves. 6. Evaluar componentes seleccionados. 7. Realizar un análisis de riesgos 8. Desarrollo de una estrategia de protección
MEHARI	Esta metodología consta 5 fases o pasos con los cuales ayudan a los responsables de mantener un control y prevención sobre cualquier imprevisto o amenaza que pueda darse sobre la infraestructura de tecnología e información de una empresa de tal forma que en el momento en el que la amenaza pase pueda guiarse en estas guías previamente identificadas para mitigar dichos riesgos.	1. Análisis de riesgos. 2. Análisis sistemático de situaciones de riesgo. 3. Análisis específico de situaciones de riesgo. 4. Análisis de riesgo en nuevos proyectos

1.4. HERRAMIENTAS PARA LA INVESTIGACIÓN FORENSE

Hoy en día existen una gran cantidad de sistemas y aplicaciones capases de detectar las diferentes falencias de seguridad a las que los servidores son vulnerables los cuales poseen información crítica perteneciente a empresas, instituciones de tipo público o privado.

Para nuestro análisis se consideró pertinente la herramienta MAGERIT 2.0 por lo que a continuación se detallará las características más importantes de MAGERIT 2.0.

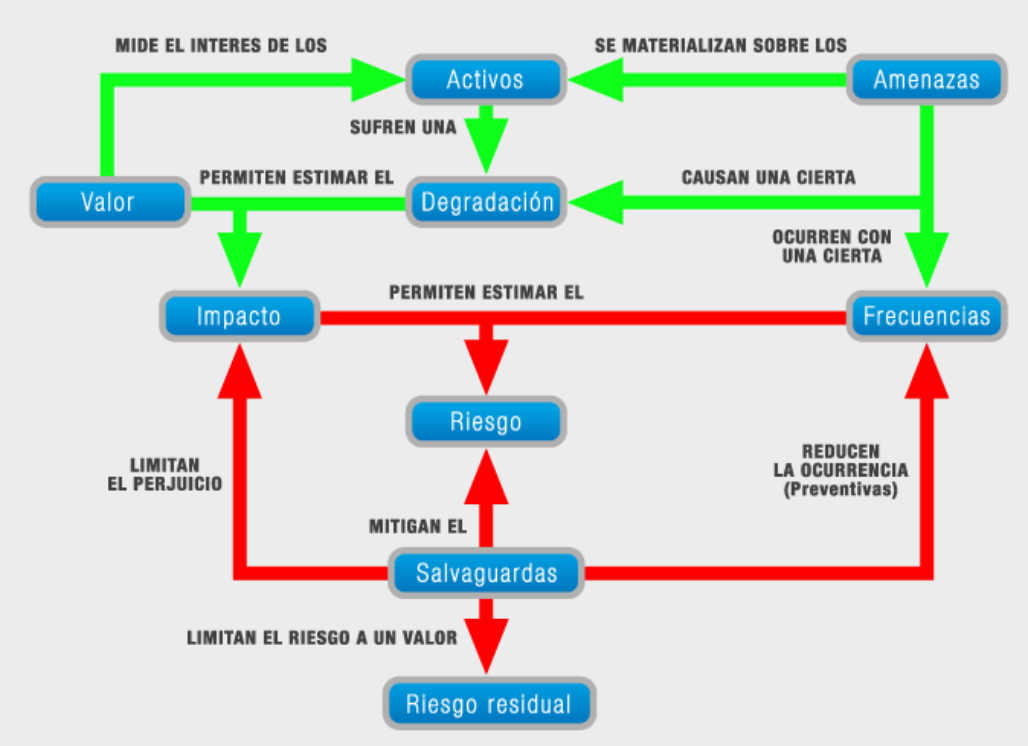
1.4.1. MAGERIT 2.0

MAGERIT 2, es la metodología formal para el análisis y gestión de riesgos que soportan los sistemas de información elaborada por el Consejo Superior de Administración Electrónica de España. MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de detenerlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

1.4.1.1. PROCESOS DE LA METODOLOGÍA MAGERIT[17]

Figura 4. Metodología MAGERIT.



1.4.1.2. IDENTIFICACIÓN DE ACTIVOS

Es en donde se identifican los activos de la organización. El activo esencial es la información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes para su manejo en PILAR:

- Los servicios que se pueden presentar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- 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.

[17]Fuente: http://seguridadinformaticaufps.wikispaces.com/MAGERIT

- 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.

1.4.1.3. CLASES DE ACTIVOS

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes. PILAR contiene una tabla de clases de activos, que abarca todos los aspectos concernientes a los recursos de procesamiento de la información. Se debe asociar cada activo a una o varias clases de las propuestas en la herramienta.

1.4.1.4. VALORACIÓN DE ACTIVOS

La valoración de un activo, se la hace de acuerdo a sus dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad). A cada una de estas dimensiones se le da un valor de acuerdo a la siguiente tabla 1:

Tabla 2. Valoración de Activos

VALOR		CRITERIO
10	Muy Alto	Daño muy grave a la organización
7 – 9	Alto	Daño grave a la organización
4 – 6	Medio	Daño importante a la organización
1 – 3	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

Para obtener el valor, PILAR dispone de una serie de criterios de valoración; este valor varía según la afectación que sufra activo, y que el usuario podrá escoger con la finalidad de obtener un valor preciso.

1.4.1.5. IDENTIFICACIÓN DE AMENAZAS

PILAR presenta un catálogo de posibles amenazas incluidas en su biblioteca, que se asocian al activo de acuerdo a la clase seleccionada para el mismo.

1.4.1.6. VALORACIÓN DE AMENAZAS

Una vez determinado que una amenaza puede perjudicar a un activo, PILAR estima cuán vulnerable es el activo, en dos sentidos

- **Degradación:** cuán perjudicado resultaría el activo
- **Frecuencia:** cada cuánto se materializa la amenaza

Tabla 3. Criterio de Valoración de Amenazas.

FRECUENCIA	DEGRADACIÓN
0,1 una vez cada 10 años	De 0% a 100% para los cinco pilares
1 todos los años	
10 todos los meses	
100 todos los días	

1.4.1.7. IMPACTO Y RIESGO.

El impacto es un indicador de qué puede suceder cuando ocurren las amenazas.

El riesgo es un indicador de lo que probablemente suceda por causa de las amenazas.

El pilar, se miden los impactos y los riesgos.

Tabla 4. Impacto y riesgo

CUALITATIVO	
Impacto	Nivel del valor
Riesgo	Novel de criticidad

El impacto acumulado se calcula tomando en cuenta la siguiente fórmula:

- Impacto acumulado = valor acumulado * degradación

Para calcular el riesgo acumulado que utilizamos el impacto acumulado y la probabilidad:

- Riesgo acumulado = impacto acumulado * probabilidad

1.4.1.8. ANÁLISIS MEDIANTE TABLAS

La nomenclatura utilizada se describe a continuación en la tabla siguiente.

Tabla 5. Estimación del Impacto

IMPACTO		DEGRADACIÓN		
		1%	10%	100%
Valor	MA	M	A	MA
	A	B	M	A
	MA	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB
	MB: Muy Bajo	B:Bajo	MA: Muy Alto	
	M: Medio	A: Alto		
Aquellos activos que reciben una calificación de impacto muy alto (MA) debería ser objetivo de atención inmediata				

Tabla 6. Estimación del riesgo

RIESGO		FRECUENCIA			
		PF	FN	F	MF
Impacto	MA	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M
	MF: Muy Frecuente (a diario)		FN: Frecuencia normal (anual)		
	F: Frecuencia		PF: Poco frecuente (cada varios años)		
Aquellos activos que realicen una calificación de riesgo muy alto (MA) deberían ser objeto de atención inmediata. Los que reciban una calificación de riesgo alto, deberían ser objeto de planificación inmediata de salvaguardas					

1.4.1.9. IDENTIFICACIÓN Y VALORACIÓN DE SALVAGUARDAS

PILAR en su biblioteca de trabajo contiene una colección de salvaguardas que están de acuerdo con los estándares internaciones de seguridad de la información. Se presenta una relación de salvaguardas adecuadas para cada tipo de activos.

La valoración de las salvaguardas depende de cuantas etapas existan en el proyecto. Por defecto existe la etapa actual y la objetivo. En cada etapa se realizara la evaluación del nivel de madurez de cada salvaguarda de acuerdo al progreso en ella con los siguientes criterios:

- **Eficacia de las Salvaguardas:** Todos los modelos requieren una evaluación de la eficacia de las salvaguardas que se despliegan para proteger un activo de una amenaza.

- **Paquete de salvaguardas**: Se define como el conjunto de salvaguardas acumuladas sobre un activo. Las diferentes Salvaguardas se pueden acumular de manera concurrente.
- **Eficacia de una Salvaguarda**: Cada salvaguarda se valora según su eficacia reduciendo el riesgo del activo que protege. La eficacia de un paquete de salvaguardas es un número real entre 0,0 y 1,0:

Si una salvaguarda es idónea (100% eficaz), se dice que e = 1

- si una salvaguarda es insuficiente, se dice que e< 1
- si una salvaguarda no sirve, se dice que e= 0
- si una salvaguarda no tiene sentido en este contexto, se dice que e = na.

1.4.2. HERRAMIENTAS PILAR.

Pilar es un software que utiliza la metodología MAGERIT de análisis y gestión de riesgos. Además tiene una biblioteca estándar de propósito general, y permite evaluar con puntaje la seguridad respecto:

Normas ISO 27000, Criterios de Seguridad, Normalización y Conservación del Consejo Superior de Informática, entre otras. Con la utilización de esta herramienta se pretende:

- Analizar los riesgos de acuerdo a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- También dispone de salvaguardas, normas y procedimientos de seguridad para el análisis del riesgo residual en el proceso de tratamiento.
- Para un análisis de riesgos adecuado, es necesario tener conocimiento sobre el entorno Pilar en cuanto a:
- Identificar los Activos, dependencias, valoración de activos, identificación amenazas, valoración de amenazas, identificación y valoración de salvaguardas.

1.4.3. DIAGRAMA DE UTILIZACIÓN DE PILAR

Figura 5. Diagrama Pilar

1.5. PLATAFORMA MOODLE

Es una aplicación web de tipo Ambiente Educativo Virtual, un sistema de gestión de cursos, de distribución libre, que ayuda a los educadores a crear comunidades de aprendizaje en línea. Este tipo de plataformas tecnológicas también se conoce como LMS (*Learning Management System*).

1.5.1. ASPECTOS BÁSICOS DE SEGURIDAD

La plataforma tiene varios niveles de seguridad que deben tenerse en cuenta, desde ella y desde el servidor se pueden configurar algunos aspectos básicos para tener un nivel aceptable de protección ante amenazas. Moodle dispone del sitio web de en el cual se puede analizar la seguridad y sus posibles soluciones.

El administrador principal debe ser el responsable de la seguridad de la plataforma las configuraciones básicas en los niveles más delicados: servidor, autenticación, contraseñas y roles.

1.5.1.1. SEGURIDAD DEL SERVIDOR

El servidor es independiente de la plataforma, es función del administrador del sistema tener bien configurado el servidor donde está alojada.

Para establecer un buen nivel de seguridad en el servidor basta con disponer de:

- Un antivirus actualizado.
- Control sobre las actualizaciones del sistema operativo, especialmente contra *rootkis* (Software para esconderse a sí mismo o a otras herramientas) y *exploits* (Software desarrollado para automatizar errores) que podrían dañar el equipo.
- Control sobre servicios de Internet abiertos que no vayan a usarse.
- Contraseñas complejas y diferentes para MySQL administrador de sistemas y administrador de la plataforma.
- Separación entre la carpeta de datos Moodle y la plataforma principal e imposibilidad de acceso vía web.
- Configurar el servidor Web (Apache, IIS, etc.) para que impida el acceso a direcciones IP no autorizadas (Si se trabaja con red privada).

1.5.1.2. SEGURIDAD EN AUTENTICACIÓN

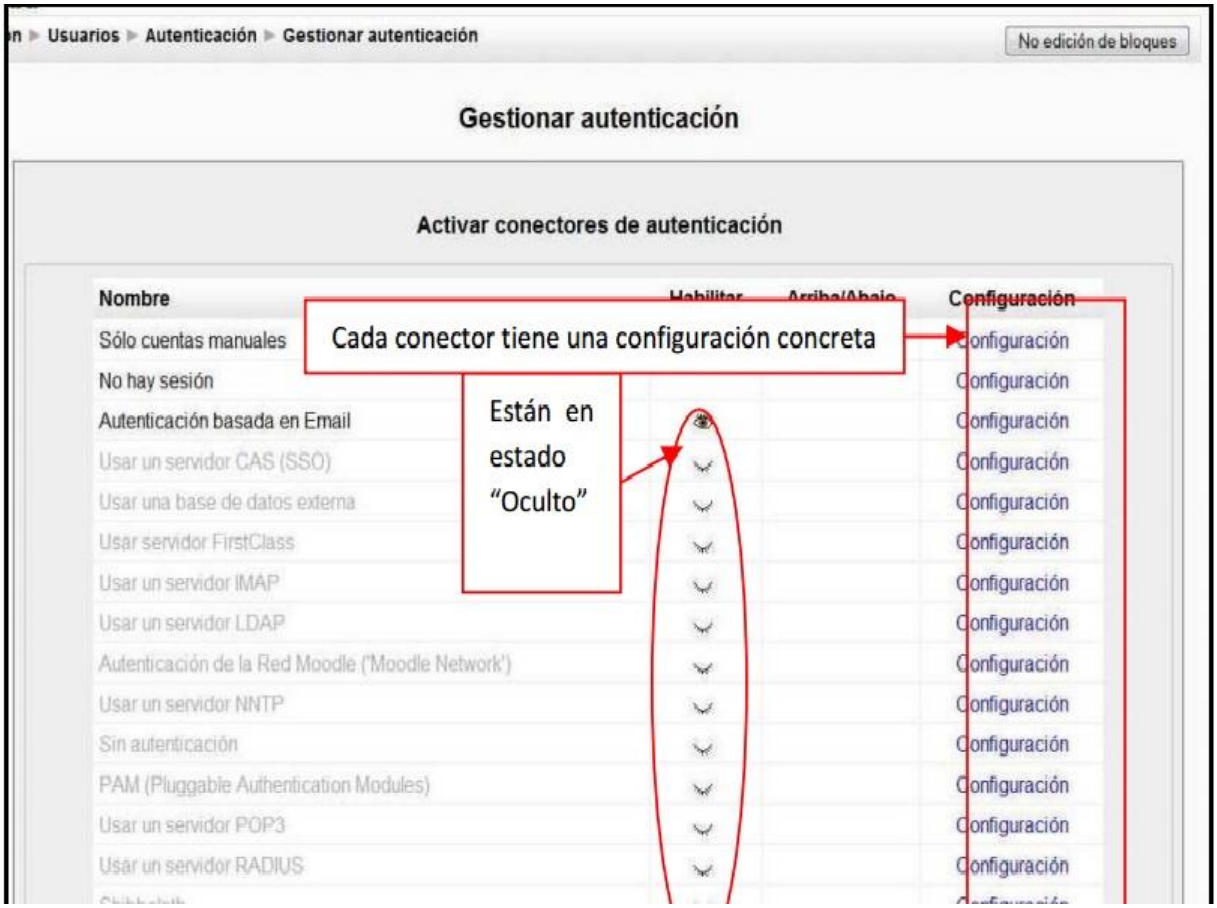
Los métodos de autenticación de un nuevo usuario pueden ser de diversos, usando la autenticación por defecto de Moodle o usando un *plugin* compatible con la plataforma como, LDAP, etc. En la figura siguiente se puede ver que hay varias maneras de autenticación del usuario, ya se ha comentado la creación de cuentas manual, basadas en email y no hay uso de *login* (inicio de sesión). De estas el nivel más seguro es el que contempla la creación de cuentas de forma manual, el administrador será el encargado de darlas de alta.

Con esto se evita el acceso de bots (Programa informático que realiza distintos cometidos y que trata de simular a un humano) y spam porque se tiene control absoluto de quienes son los admitidos a la plataforma. Es la opción más recomendada para grupos pequeños de uso pero puede ser un trabajo tedioso para plataformas masivas, así que la opción recomendada será la autenticación basada en email bien configurado.

Para una buena gestión de autenticación basada en e-mail es recomendable seguir estos pasos:

- Dejar bien claro en el campo instrucciones los pasos necesarios para una buena autenticación del usuario, así como la buena construcción de una contraseña de usuario.
- Bloquear cuentas de usuario que considere importantes, como por ejemplo la dirección de correo y el nombre. Así se evita la suplantación de identidad del usuario. Si se bloquean campos requeridos por Moodle, se deben asegurar que se proporcionan esos datos de forma manual al crear las cuentas de usuario, sino estas cuentas no podrán ser usadas para ello existen la opción de desbloqueado si está vacío que evita este problema.

Figura 6. Gestionar Autenticación en Moodle



1.5.2. SEGURIDAD CON LAS CONTRASEÑAS

Uno de los cometidos del administrador podría ser forzar a los usuarios autenticados de la plataforma a que usen una contraseña segura para su inicio de sesión, para evitar el robo de contraseñas, no hay un estándar para la configuración de las contraseñas aunque se recomiendan las normas.

- Una longitud mínima de 8 caracteres.
- Incluir letras, números y caracteres especiales.
- Debe incluir mayúsculas y minúsculas.

Desde Moodle se puede configurar los patrones que debe tener la contraseña de los usuarios. Estos se configuran desde administración/seguridad/ políticas del sitio. Desde

allí se pueden definir la longitud de caracteres, los caracteres mínimos no alfanumérico cantidad de mayúsculas, minúsculas, caracteres, etc.

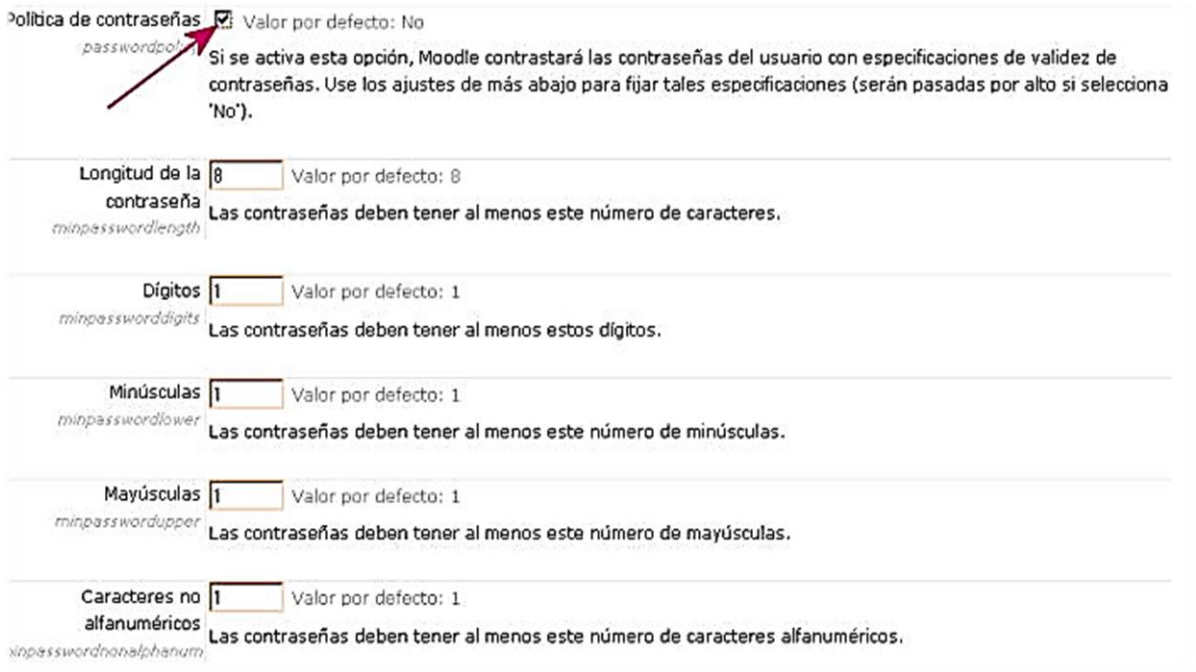
1.5.3. SEGURIDAD EN DEFINICIÓN DE ROLES

Los roles bien definidos, pueden ser una herramienta magnifica para la gestión de los permisos de los usuarios autenticados y de la seguridad general de la plataforma a la hora de definir perfectamente que es lo que puede hacer un usuario o que es lo que no puede hacer.

Mal gestionado puede provocar ataques internos, pudiendo incluso provocar que usuarios no autorizados tengan permisos administrativos poniendo en peligro toda la gestión del sistema.

Moodle tiene configurado por defecto siete roles básicos que son de mayor nivel de permiso a menor: Administrador, Creador de recursos, Profesor, Profesor no editor, Estudiante, Invitado y usuario no autenticado. Cada grupo es englobado en un tipo de rol y estos a su vez tienen una serie de permisos definidos. Cada rol se puede asignar fe forma global y también de forma específica para cada curso, los permisos de los roles son heredados. Por ejemplo, si tenemos permisos de creador de cursos de rol global podemos tener también el rol de estudiante en un curso determinado, de los permisos de estudiantes en el curso y los permisos heredados de creador de cursos que no sean incompatibles entre ellos.

Figura 7. Política de contraseñas en Moodle



Lo que se debe de tomar en cuenta a la hora de seguridad en roles es:

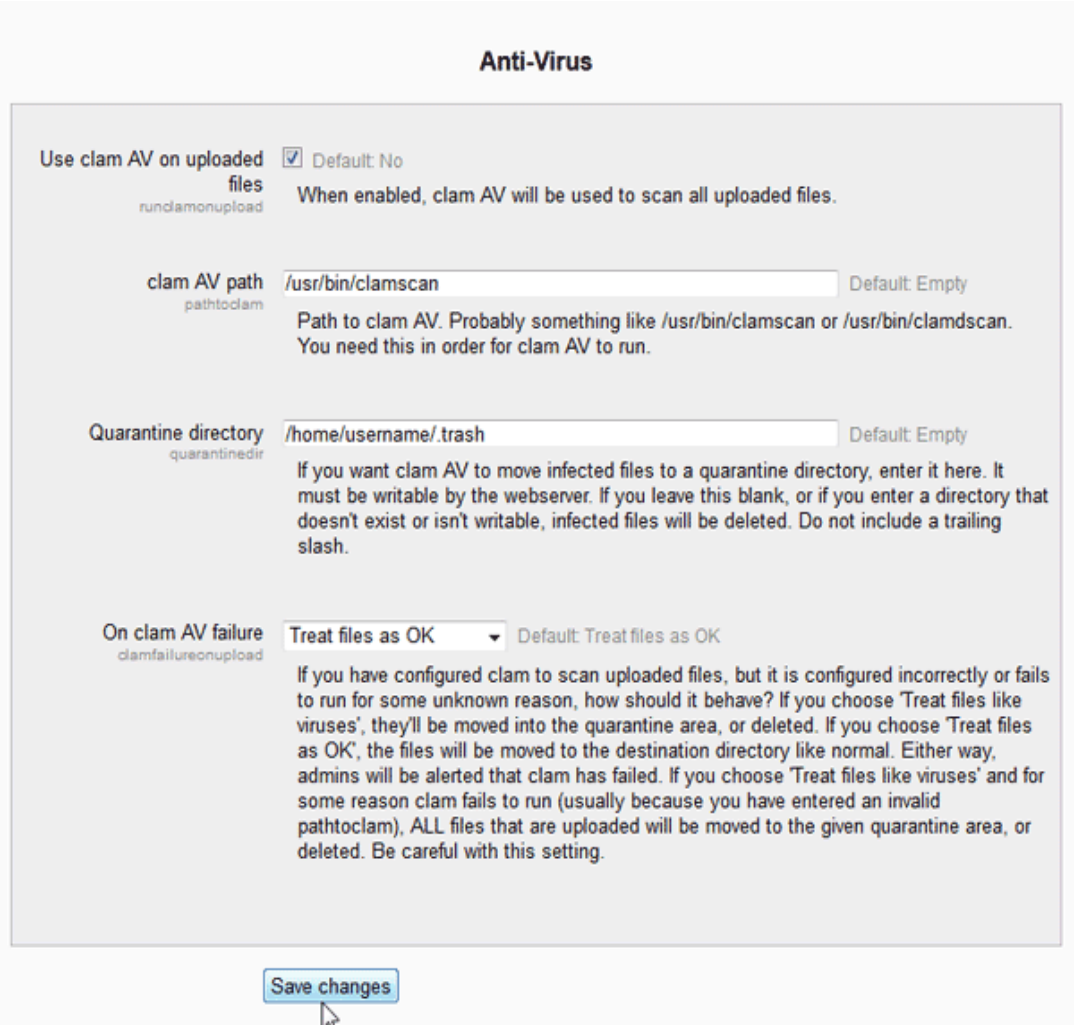
- Solo debe haber un usuario con permisos de administrador, normalmente el creador de la plataforma. Si se necesita se puede crear un rol nuevo como administrador secundario que sea heredado de administrador y gestionar los permisos correctamente.
- Solo el administrador debe tener este permiso de Moodle/Site: *do anything* (permiso para todo).
- Solo se debe dar roles globales al administrador y al creador de cursos el resto se deja con el rol por defecto usuario autenticado. Una vez que estén los cursos creados se pueden asignar roles a los usuarios.
- No dar privilegios al rol de invitados.
- No modificar los roles predefinidos de la plataforma Moodle, estos roles están ben gestionados y cada rol tiene bien definidos los tipos de permisos. Si se necesita modificar un rol para que se ajuste a lo deseado es mejor crear un nuevo rol que herede del rol que se desee modificar.
- Evitar en lo posible asignar roles a los usuarios.

1.5.4. ANTIVIRUS

Se puede descargar e instalar el antivirus ClamAV que es GPL. Una vez instalado y configurado el antivirus se conecta automáticamente con Moodle si activamos las opciones. El antivirus es muy útil si queremos que se analicen los archivos que se suben al servidor, evitando así la inserción de virus o cualquier otro archivo nocivo para el sistema.

Para configurar el antivirus es necesario especificar la ruta donde está instalado el programa.

Figura 8. Antivirus recomendado.



1.5.5. VISOR DE SUCESOS DE MOODLE.

Desde Moodle se puede configurar el visor de sucesos de la plataforma. Toda actividad de cualquier usuario se guarda en los registros del sistema. Se pueden visualizar los ficheros *logs* desde dentro de la plataforma en la carpeta Informes y luego Registros desde el bloque de administración. Nos saldrá una pantalla que nos indicará el día que queremos ver los registros, si queremos ver un curso en concreto o toda la plataforma, los participantes y las acciones a ver.

Estos registros se pueden descargar en formato ODT, en formato de texto plano o en formato Excel para almacenarlos.

Los ficheros *logs* no es necesario almacenarlos, ya se almacenan directamente cuando se hace una copia de seguridad de la base de datos. Si queremos tener copias de seguridad específicas de los *logs*, se tiene que salvar la tabla log de la base de datos Moodle. Esto se puede hacer con el *phpmyadmin* u otro programa de gestión de MySQL.

Si se tiene activada las estadísticas se pueden ver un informe con las estadísticas generales del sitio Moodle. Este informe estadístico se puede enviar por correo a los usuarios elegidos. Desde estos informes se puede acceder con facilidad a los registros que deseemos. Cada vez que se genera un informe estadístico se consumen muchos recursos del sistema, así que es conveniente que se automatice a unas horas donde no haya tráfico de usuarios.

CAPITULO II

2. METODOLOGÍA

2.1. TIPO DE ESTUDIO

La investigación que se va a desarrollar es una investigación descriptiva. Con la finalidad de proponer posibles soluciones para las diferentes vulnerabilidades, y fallos de seguridad que se encuentren en el proceso de auditoría Informática.

- **Método Científico:** la investigación se basa en el análisis de la información recopilada de los diferentes procesos informáticos que se desarrollan en la institución.

2.1.1. SEGÚN EL OBJETIVO DE ESTUDIO

Investigación Aplicada: este tipo de investigación tiene como propósitos resolver o mejorar una situación específica o particular, para comprobar un método o modelo mediante la aplicación innovadora y creativa de una propuesta de intervención, en este caso de índole Orientadora, en un grupo, persona, institución o empresa que lo requiera.

2.1.2. SEGÚN LA FUENTE DE INFORMACIÓN

Investigación bibliográfica: este conjunto de técnicas y estrategias son utilizadas para localizar, y acceder a aquella información y documentos, la misma que contienen la información adecuada para la utilización del proyecto en curso.

2.1.3. SEGÚN LAS VARIABLES

Descriptiva Aplicada: a través de la descripción y análisis del objeto que se va a estudiar se determina su forma de aplicación en un entorno real.

2.2. POBLACIÓN MUESTRA

POBLACIÓN: Para implementar una auditoria Informática forense se ha considerado a la Universidad Nacional de Chimborazo de la ciudad de Riobamba.

MUESTRA: Para la muestra se ha considerado la los 1234 usuarios estudiantes, 100 docentes de la Facultad de Ingeniería de la Universidad Nacional de Chimborazo los cuales utilizan el servicios de B-learning implementado en la institución.

Se procederá a realizar las encuestas aplicadas a los dos administradores del servidor B-learning de la Universidad Nacional de Chimborazo.

Muestra para usuarios alumnos.

Tamaño Muestra= $\frac{N\,z^2pq}{r^2(N-1)+z^2pq}$

Dónde:

N: Tamaño de la población, número de total de historias,

z: Valor de z, 1.96 para α=0.05 y 2.58 para α=0.01.

p: Prevalecía esperada del parámetro a evaluar. En Caso de desconocerse aplicar la opción más desfavorable (p = 0.5), que hace mayor el tamaño de la muestra.

q: 1 – p

i: Error que se prevé cometer

$$\frac{1234 * (1.96)^2(0.5)(0.5)}{(0.1)^2(1234-1)+(1.96)^2(0.5)(0.5)}$$

$$n = \frac{1234 * (3.84)(0.25)}{(0.01)(1233)+(3.84)(0.25)}$$

$$n = \frac{1184.64}{13.29}$$

$n = 89$ Estudiantes

89 es la muestra total de alumnos a los que se procederá aplicar la encuesta.

Muestra para usuarios docentes.

Tamaño Muestra$= \frac{N\, z^2 pq}{r^2(N-1)+z^2 pq}$

$$\frac{100 * (1.96)^2(0.5)(0.5)}{(0.1)^2(100-1)+(1.96)^2(0.5)(0.5)}$$

$$n = \frac{100 * (3.84)(0.25)}{(0.01)(100)+(3.84)(0.25)}$$

$$n = \frac{96}{1{,}96}$$

$n = 48$

48 es el número total de docentes a los que se procederá aplicar las encuestas.

En el caso de los administradores se tomó como referencia a toda la población que es 2.

2.3. OPERACIONALIZACIÓN DE VARIABLES

Tabla 7. Operacionalización de Variables.

VARIABLE	TIPO	DEFINICION CONCEPTUAL	DIMENSIONES	INDICADORES
Procesos y políticas de Seguridad Informática	Independiente	Técnicas científicas y analíticas que permiten identificar, preservar, analizar y presentar datos.	Cumplimiento Porcentual	Políticas de seguridad aplicados Normas de seguridad de software Normas de seguridad de hardware Estándares ISO Seguridad WEB Seguridad en los servicios
Seguridades en el servidor B-learning	Dependiente	La seguridad se enfoca a la protección de la infraestructura computacional existen estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad comprende software, bases de datos, metadatos, archivos y todo lo que la se valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Información privilegiada o confidencial.	Cumplimiento Porcentual Unidad	Accesos de usuarios Protección, control de acceso Niveles y categorías de usuarios Rendimiento de servidores Firewalls Físicos y Lógico Períodos Backup

2.4. PROCEDIMIENTOS

Para la recopilación de la información se realizaran algunos procedimientos.

a) La técnica de investigación que se empleará:

Entrevista: a los usuarios del sistema, trabajadores de la institución que manejan el sistema.

Encuesta: trabajadores de la institución que manejan el sistema para conocer las políticas de seguridad implementadas en el mismo.

Observación. Data Center, Servidores, Firewall físicos, instalaciones físicas de *router* y *switch*.

b) Organización y tabulación de la información.

2.4.1. PROCESAMIENTO Y ANÁLISIS

La investigación comprende un análisis de la plataforma Moodle implementada en la Universidad Nacional de Chimborazo para lo cual se procederá de la siguiente manera:

- Análisis del funcionamiento de la plataforma Moodle.
- Recopilación de información de acceso de usuarios y administrador del sistema Moodle y equipos.
- Análisis de las herramientas más apropiadas a utilizarse en el análisis forense de la plataforma Moodle.
- Investigación y estudio de guías, estándares que forman parte de la Informática forense.
- Realizar un diagnóstico de los procesos administrativos y de información que se llevan a cabo en el Centro de Cómputo para la manipulación del equipo en donde se ejecuta la plataforma Moodle.

Diagnóstico de la situación actual del Centro de Tecnología Educativa basado en los controles de la norma ISO 27004 y aplicación de la metodología MAGERIT.

SITUACIÓN ACTUAL DEL CENTRO DE TECNOLOGÍA EDUCATIVA

La información sobre la situación actual del Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo se basa en las observaciones tomadas durante las visitas realizadas a la institución durante la investigación para realizar el presente documento.

A continuación se detalla el diagnostico que se obtuvo en los resultados de las encuestas y cuestionarios aplicados al personal responsable del Centro de Tecnología Educativa de la UNACH, basado en la norma ISO 27004 y documentado en las fechas establecidas.

El resultado que se obtuvo de las encuestas aplicadas en lo que respecta a seguridad de la información abarca 11 puntos estratégicos como lo indica la Norma ISO 27001 y 27002.

ACTIVOS SEGÚN MAGERIT.

Tabla 8. Aplicaciones Software

[SW] APLICACIONES (SOFTWARE)
○ **Portal Web**
○ **Sistema de Base de Datos de Respaldo**
○ **Sistema de Acceso de Centros de Datos**
• **Sistema Académico**

Tabla 9. Servicios

[S] SERVICIOS
○ **Acceso Seguro de Usuario**
○ **Mensajería Electrónica**
○ **Archivo histórico central**
○ **Operaciones de Gestión Interna**
• **Servicio Técnico Auxiliares**
○ **Ficheros en Red**
○ **Acceso a Internet**

Tabla 10. Redes de comunicaciones

[COM] REDES DE COMUNICACIONES
○ **red LAN**

Tabla 11. Equipamiento auxiliar

[AUX] EQUIPAMIENTO AUXILIAR
○ **Proyector Digital**
○ **Equipo Multimedia**

Tabla 12. Instalaciones

[L] INSTALACIONES
○ **Oficina Principal Área UTIC**
○ **Oficina Unach – Digital**
○ **Cuarto de Servidores – Principal**
○ **Fibra Óptica**

Tabla 13. Activos según MAGERIT

[HW] EQUIPOS INFORMÁTICOS (HARDWARE)
○ **Puestos de Trabajo**
○ **Racks de Piso - Servidores SUN**
• **Servidores Centro de Tecnología Educativa.**
○ **Servidor Base de Datos del Sistema B-learning**
○ **Servidor de Respaldo de Base de Datos**
○ **Servidor Base de Datos Académico**
○ **Servidor Base de Datos Portal Web Institucional**
○ **Servidor Autoservicio (SelfService Banner)**
○ **Servidor Portal Web**
○ **Servidor Digitalización de Documentos**
○ **Portal Web Institucional**
○ **Servidor Educativa Respaldos, Aplicaciones Área de Desarrollo**
○ **Servidor Sistema Financiero Sistema RRHH**
○ **Exchange Administrativos**
○ **Active Directory Principal Administrativos**
○ **Active Directory Secundario Administrativos**
○ **Exchange Alumnos**
○ **Active Directory Principal Alumnos**
○ **Servidor Educativa Principal**

CAPITULO III

3. RESULTADOS

3.1. RESULTADOS FINALES.

Los resultados obtenidos están basados en la investigación teórica sobre los servidores existentes en el Centro de Tecnologías Educativas de la Universidad Nacional de Chimborazo, enfocado a la plataforma B-learning desarrollado para el ambiente educativo.

Estos resultados son producto de la aplicación de los indicadores descritos anteriormente en la Operacionalización de variables, mismos que han sido analizados bajo ciertos parámetros que permiten determinar en forma comparativa el desempeño del servidor B-learning tanto en administradores, usuarios docentes y usuarios alumnos de la escuela de sistemas y computación de la Universidad Nacional de Chimborazo.

En esta investigación se pretende dar a conocer el nivel de seguridad informática que la Universidad Nacional de Chimborazo posee. Considerando estándares, normas, guías de seguridad informática.

Para el análisis de resultados se trabajó con las siguientes tablas de valoración de riesgos:

Tabla 14. Valoración del Riesgo

NIVEL DE RIESGO	EQUIVALENCIA
1% – 30 %	Alto
31 % – 60 %	Medio
61 % – 100 %	Bajo

Nota: Para el análisis se consideró como 1% - 30% de cumplimiento el nivel de riesgo es alto. De 31% - 60% de cumplimiento se define el nivel de riesgo medio. De 61% - 100% de cumplimiento se define como nivel de riesgo bajo.

3.1.1. ANÁLISIS COMPARATIVO RESULTADOS ENCUESTAS ADMINISTRADORES, PROFESORES Y ESTUDIANTES DE LA FACULTAD DE INGENIERÍA EN SISTEMAS DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO

RESULTADOS ANTES DE LA INVESTIGACION ADMINISTRATIVOS

El estudio inicio en el año 2012. El Centro de Computo de la Universidad Nacional de Chimborazo funcionaba en el Edificio Administrativo de la institución. Se realizó las encuestas y mediciones pertinentes para conocer el grado de seguridad en la infraestructura informática en la cual obtuvimos los siguientes resultados:

Tabla 15. Antes Indicadores y Parámetros

VARIABLE	INDICADORES	CUMPLIMIENTO	NO CUMPLIMIENTO
Procesos y políticas	Políticas de Seguridad aplicadas	37%	63%
	Normas de seguridad de software	43%	57%
	Normas de seguridad de hardware	40%	60%
	Estándares ISO	0%	100%
	Seguridad WEB	58%	42%
	Seguridad en los servicios	37%	63%
Seguridad Informática	Accesos de usuarios	37%	63%
	Protección control niveles de usuarios	43%	57%
	Rendimiento de servidores	25%	75%
	Firewalls Físicos y Lógico	38%	62%
	Períodos Backup	50%	50%

RESULTADOS DESPUÉS DE LA INVESTIGACION ADMINISTRATIVOS

Las encuestas realizadas después de cinco meses de que los servidores se trasladaran al edificio inteligente donde el Centro de Tecnología Educativa cuenta una nueva infraestructura nueva se obtuvieron los siguientes resultados:

Resultados posteriores a la aplicación de indicadores y parámetros

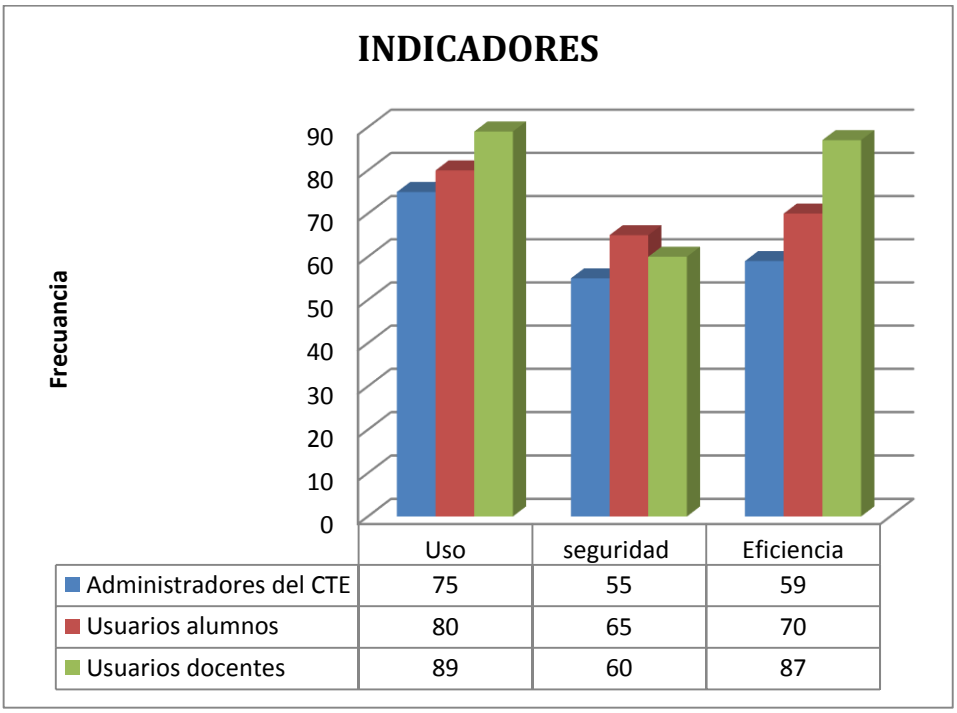
Tabla 16. Después Indicadores y Parámetros

VARIABLE	INDICADORES	CUMPLIMIENTO	NO CUMPLIMIENTO
Procesos y políticas	Políticas de Seguridad aplicadas	62%	38%
	Normas de seguridad de software	57%	43%
	Normas de seguridad de hardware	60%	40%
	Estándares ISO	0%	100%
	Seguridad WEB	64%	36%
	Seguridad en los servicios	50%	50%
Seguridad Informática	Accesos de usuarios	56%	44%
	Protección control niveles de usuarios	57%	43%
	Rendimiento de servidores	58%	42%
	Firewalls Físicos y Lógico	62%	38%
	Períodos Backup	67%	33%

Tabla 17. Tipos de Usuarios

TIPO DE USUARIO	USO	SEGURIDAD	EFICIENCIA
Administradores del CTE	75	55	59
Usuarios alumnos	80	65	70
Usuarios docentes	89	60	87

Gráfico 1. Indicadores del análisis



3.1.2. ANÁLISIS DE RESULTADOS

Los resultados se presentan en forma de porcentajes como se lo detalla a continuación:

Al aplicar las encuestas a los administradores del Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo, se obtuvieron los siguientes resultados:

- Seguridad de 62,4% seguro.
- Accesibilidad 66% Accesible
- Rendimiento 53%

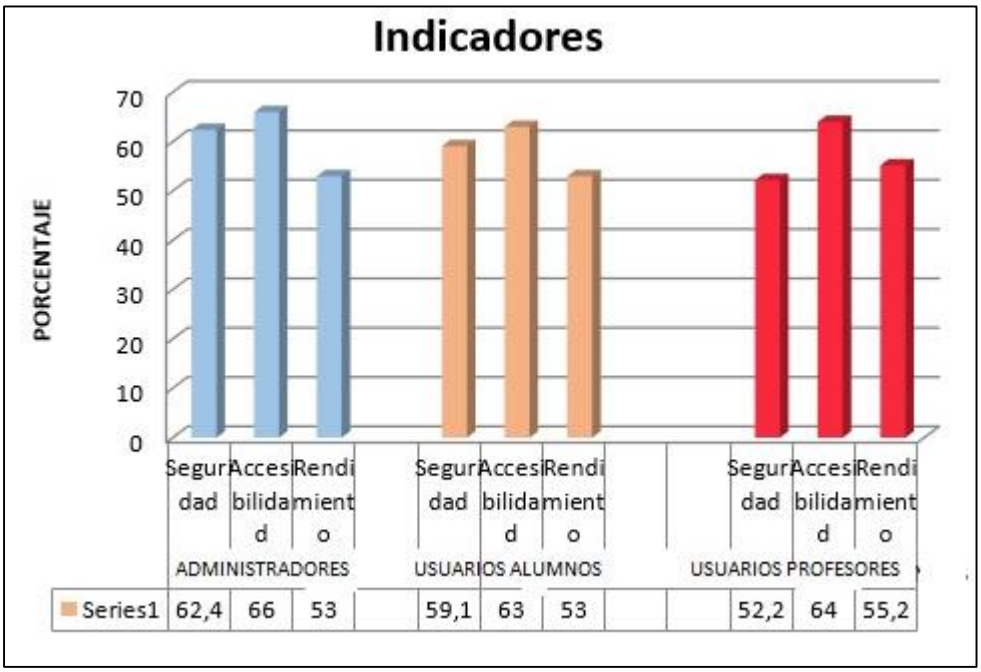
- Los resultados de las encuestas aplicadas a los usuarios estudiantes determinaron los siguientes resultados.

- Seguridad de 59.1% seguro.
- Accesibilidad 63% Accesible
- Rendimiento 53%

- Resultados obtenidos por los usuarios profesores.

- Seguridad de 52,2% seguro.
- Accesibilidad 64% Accesible
- Rendimiento 55,2%

Figura: Indicadores.



3.2. COMPROBACIÓN DE LA HIPÓTESIS

En los temas tratados anteriormente, se han podido identificar la falta de implementación de normas de seguridad internacional dentro de los servidores del Centro de tecnologías educativas, enfocadas en el servidor B-learning, para lo cual se comprobará estadísticamente con Chi^2

3.2.1. HIPÓTESIS GENERAL

Mediante la aplicación de Procesos y Políticas de Informática Forense mejoran la Seguridad y los datos del Servidor B-learning de la Universidad Nacional de Chimborazo.

3.2.2. HIPÓTESIS ESPECÍFICA

3.2.3. HIPÓTESIS DE INVESTIGACIÓN.

Hi: El porcentaje de parámetros aplicados en la investigación a través de las encuestas realizadas a los diferentes usuarios, de las plataforma B-learning supera los índices de confidencialidad esperados referentes a la seguridad.

Ho: El porcentaje de parámetros aplicados en la investigación a través de las encuestas realizadas a los diferentes usuarios, de las plataforma B-learning no supera los índices de confidencialidad esperados referentes a la seguridad.

Tabla 18. Hipótesis de investigación.

INDICADOR	ADMINISTRADORES	ALUMNOS	PROFESORES
Seguridad	62,4%	59.1%	52,2%
Accesibilidad	66%	63%	64%
Rendimiento	53%	53%	55,2%

Para el cálculo del Chi^2 aplicamos la siguiente fórmula:

$$\chi^2 = \sum \frac{(Fo - Fe)^2}{Fe}$$

Partimos de las frecuencias observadas que se plasman en el siguiente cuadro:

Tabla 19. Frecuencias Observadas

CATEGORÍA	SEGURO	ACCESIBLE	TOTAL
Administradores	62%	66%	128%
Usuarios	59%	63%	122%
Total	121%	129%	250%

Posteriormente se calcula las frecuencias esperadas:

El Cálculo se obtuvo de la tabla general de resultados que se encuentra en la parte superior, donde se aplica la constante del X^2 y de ésta manera se obtiene la siguiente tabla.

Tabla 20. Frecuencias Esperadas

CATEGORÍA	SEGURO	ACCESIBLE	TOTAL
Administradores	61,952%	66,048%	128%
Usuarios	59,048%	62,952%	122%
Total	121%	129%	250%

CÁLCULO MANUAL

Tabla 21. Calculo Manual

CÁLCULO MANUAL		
fo	**Fe**	$x^2 = \sum \frac{(Fo - Fe)^2}{Fe}$
62	61,952%	3,71901E-05
66	66,048%	3,48837E-05
59	59,048%	3,90191E-05
63	62,952%	3,65993E-05
250	250%	0,000147692

CÁLCULO EXCEL

Tabla 22. Cálculo en Excel

CÁLCULO EXCEL	
Prueba Chi	**0,990303652**
Prueba Chi Inv.	**0,000147692**

Al ser el cálculo del Chi^2 superior, 0.990303652 al $Chi^2\ inverso$, 0,000147692 se comprueba el **Hi,** debido a que el porcentaje de parámetros aplicados en la investigación a través de las encuestas realizadas a los diferentes usuarios, de la plataforma B-learning supera los índices de confidencialidad esperados referentes a la seguridad.

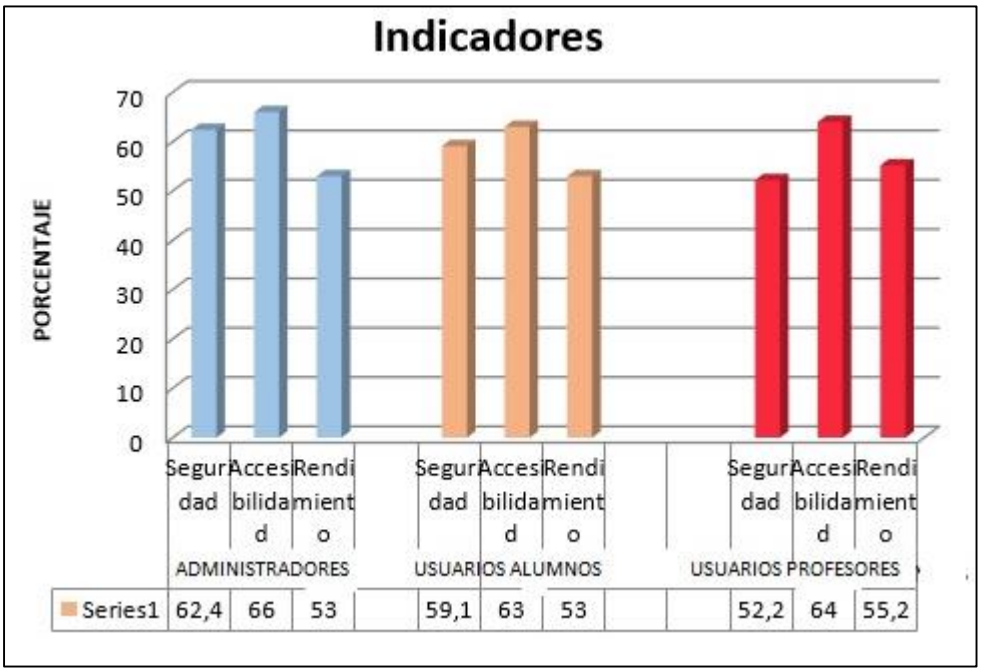
Descartando de ésta manera la hipótesis nula: Ho.

CAPITULO IV

4. DISCUSIÓN

DISCUSIÓN DE RESULTADOS DE LA ENCUESTA APLICADA A DOCENTES, ESTUDIANTES Y ADMINISTRADORES USUARIOS

Figura 4. 1 Indicadores



Elaborado por: Alejandro Fierro

ANÁLISIS

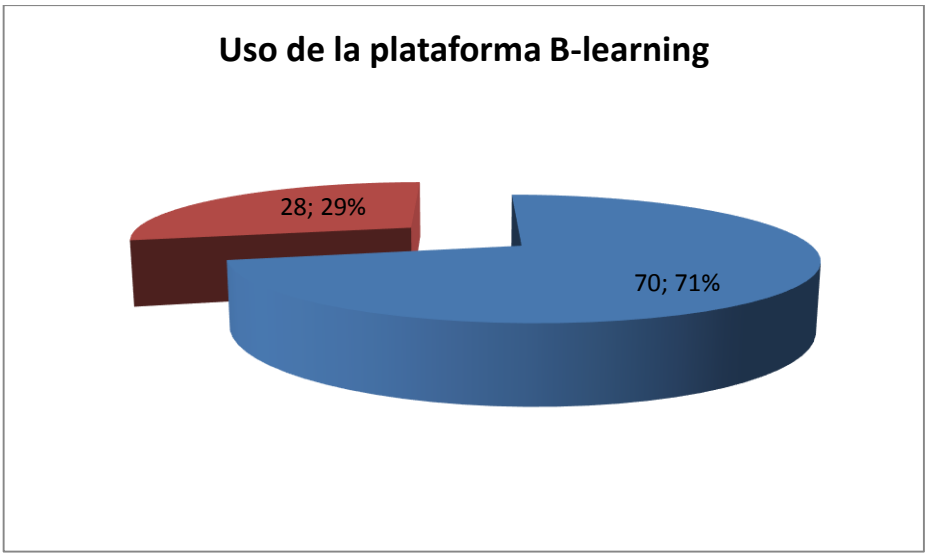
La mayoría de los Administradores, el 62,4% cree que existe seguridad, en tanto que en referencia a accesibilidad se obtuvo el 66% y finalmente el 53% está de acuerdo con el rendimiento, por lo que el 37,6%, 44% y 47% opinan lo contrario, de igual manera los estudiantes en lo que a seguridad se refiere el 59,1% cree que si existe seguridad, el 63% de estos creen que si es accesible, en tanto que el 53% está de acuerdo con el rendimiento, por otra parte los docentes, el 52,2% cree que el sistema es seguro, el 64% cree que es accesible y el 55% están conformes con el rendimiento, en tanto que los demás no están de acuerdo con las opciones planteadas.

INTERPRETACIÓN

En general la mayoría de encuestados está de acuerdo con los procesos y políticas de la informática forense en las seguridades de servidores, caso práctico servidor B-learning de la Universidad Nacional de Chimborazo, debido a que la mayoría de la población en estudio posterior a la aplicación de la propuesta está de acuerdo con el servidor.

USO B-LEARNING

Figura 4.2 Uso de la plataforma B-learning



Elaborado por: Alejandro Fierro

Análisis

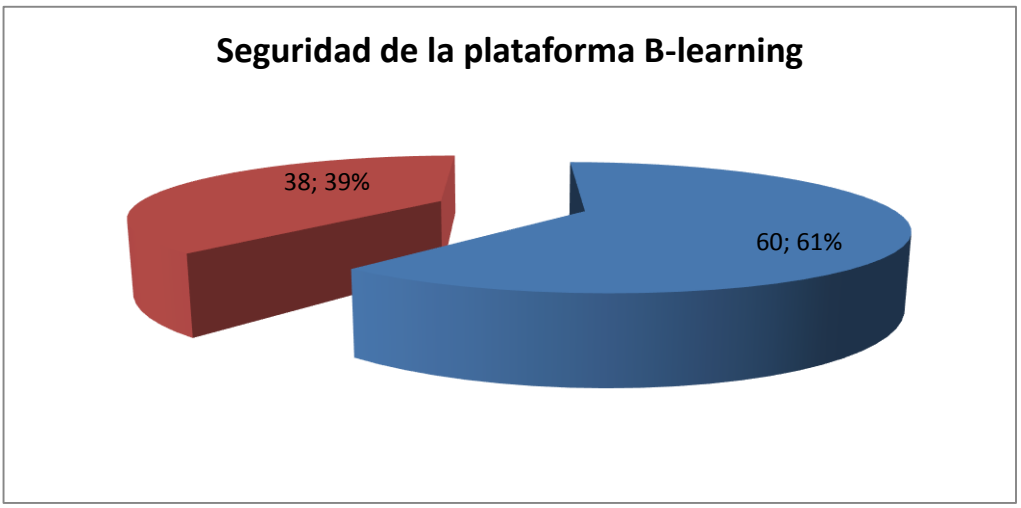
La mayoría de personas de la universidad ocupan la plataforma B-learning, es así que se denota con el 71% de encuestados que sí lo han hecho, en tanto que el 29% no lo ha utilizado.

Interpretación

Hoy en la actualidad es necesario el uso de plataformas virtuales como soporte al proceso educativo por lo que es necesaria la capacitación sobre el uso de la plataforma B-learning como mecanismo de aprendizaje.

SEGURIDAD

Figura 4.3 Seguridad de la plataforma B-learning



Elaborado por: Alejandro Fierro

Análisis

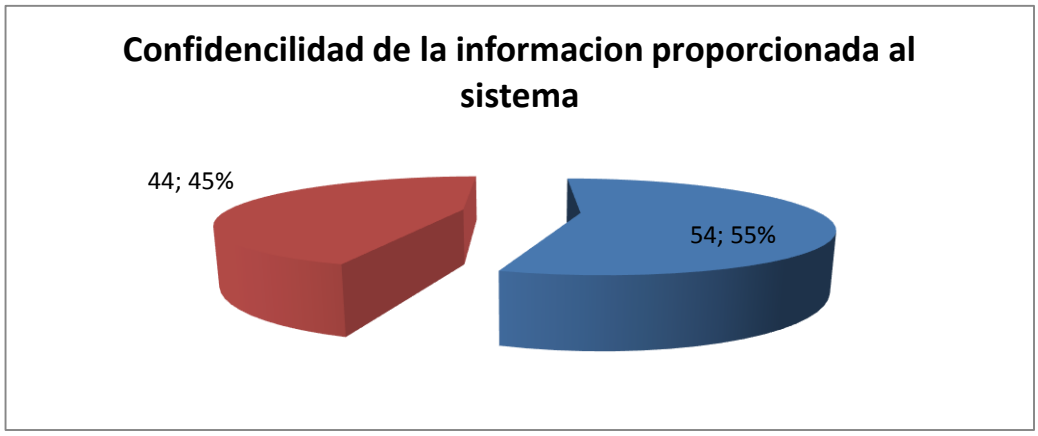
En lo que refiere a seguridad de la plataforma B-learning, las opiniones de los encuestados no distan mucho debido a que el 39% de personas argumenta que no son muy seguras éstas, mientras que el 61% aduce estar de acuerdo con la seguridad.

Interpretación

Hoy en la actualidad algunos sistemas informáticos han sido vulnerados por los piratas informáticos, esto se ve a diario en el mundo, es así que un porcentaje considerable considera que la plataforma no es muy segura, mientras que la mayoría cree que si lo es.

CONFIDENCIALIDAD DEL SISTEMA

Figura 4.4 Confidencialidad del sistema



Elaborado por: Alejandro Fierro

Análisis

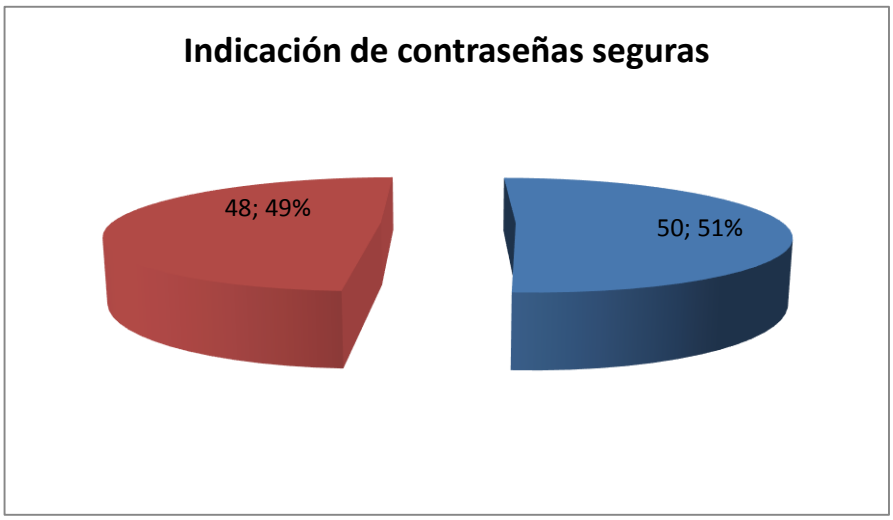
La confidencialidad en la actualidad es cuestionada por el 45% de encuestados debido a múltiples razones argumentadas por ellos, frente al 55% que aduce sí existe confidencialidad, como se puede observar hay una ínfima diferencia entre la diferencia de opiniones.

Interpretación

El sistema posee políticas de confiabilidad en sus servidores y la información que éstos ingresan, los puntos de vista discrepan de acuerdo a experiencias pasadas en referencia al uso de algunas plataformas virtuales.

CONTRASEÑAS SEGURAS

Figura 4.5 Contraseñas seguras



Elaborado por: Alejandro Fierro

Análisis

La plataforma B-learning posee condiciones seguras en base a sus contraseñas, esto argumenta el 51% de los encuestados, es ínfima la diferencia de resultados puesto que el 49 % de servidores aclara que las contraseñas de la plataforma no son seguras, dejando entrever para ellos la vulnerabilidad del sistema.

Interpretación

Casi en iguales condiciones se encuentran las opiniones vertidas en la encuesta de servidores de la plataforma, debido a que solamente diferencia dos por ciento de la mayoría que está conforme o de acuerdo con la seguridad de sus claves.

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- La Seguridad Informática permite proteger la infraestructura computacional incluyendo también la información que aquí se encuentre, por esto se la debe tratar con la mayor responsabilidad en todas las áreas del Centro de Tecnología Educativa para que así sea uno de los factores de éxito dentro de la institución; un recurso humano organizado con Normas y Políticas establecidas y apoyado en las herramientas informáticas permite la prevención de amenazas y disminución de Riesgos en Seguridad.

- Mediante la Informática Forense se logró identificar las principales vulnerabilidades con las que cuenta el Centro de Tecnología Educativa, tanto en su seguridad física como lógica lo cual permitió elaborar una guía de seguridad que contienen normas y estándares que puede servir como un referente para la implementación de un reglamento de uso dentro de la Universidad Nacional de Chimborazo.

- Con la nueva infraestructura que posee la Universidad Nacional de Chimborazo a partir de la construcción del Edificio Inteligente en el campus MS. Edison Riera Rodríguez, en donde hoy se encuentra instalado el Centro de Tecnología Educativa, ha permitido de manera extraordinaria reforzar muchas de los estándares internacionales que se deben seguir al poseer y administrar un Centro de Datos ya que se crearon, implementaron, reforzaron muchas de las políticas de seguridad que en el anterior Centro de Cómputo no se aplicaban por diversas razones, pero gracias a la inversión en recursos tecnológicos de vanguardia por parte de la institución hoy se han logrado.

- La utilización de la plataforma B-Learning en la Universidad Nacional de Chimborazo en la actualidad permite que la educación mejore en gran medida pues el acceso y aplicación está estandarizado dentro de la institución y su aceptación por parte de los estudiantes y docentes es muy alta, esto da a entender que con el paso del tiempo se convertirá en una herramienta más de aprendizaje e implicará que se manejen elevados volúmenes de información y datos por lo que la seguridad y accesibilidad del sistema B-learning será vital en este caso.

- Con relación a la seguridad que ofrece la plataforma B-Learning a los alumnos y profesores de la Universidad Nacional de Chimborazo, se detectó luego del estudio que existen aún falencias en el sistema que si se aplican normativas y estándares puntuales pueden ser resultas y así poder garantizar la confidencialidad y el buen uso de la información que se registra y almacena dentro del servidor.

- La Metodología MAGERIT ha permitido en el transcurso de esta investigación la identificación, el análisis y la gestión de riesgos que soportan los sistemas de información de la Universidad Nacional de Chimborazo; con la ayuda del software Pilar se pudo conocer y evaluar la información a través de los Pilares en Seguridad Informática como: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, esto ayuda a tener resultados más reales y que pueden ser discutidos y aplicados a la realidad del entorno de la Universidad Nacional de Chimborazo con el fin de mejorar e implementar políticas de seguridad Informática.

- La implementación de políticas de seguridad se puede efectuar conociendo e identificando los riesgos basados en la estimación del grado a que está expuesto el sistema a que una amenaza se materialice sobre uno o más activos y que causen daños o perjuicios a la institución, para que se puedan minimizar al máximo mediante la aplicación de los mecanismos de control y salvaguardas para evitar que se materialicen.

5.2. RECOMENDACIONES

- Aprovechar al máximo las nuevas instalaciones e infraestructura que posee el Centro de Tecnología Educativa, pues no basta que se conformen con la adquisición de equipos y software de última generación también se debe ahondar en el desarrollo e implementación de normas, políticas, estrategias y estándares de seguridad que permitan que optimizar los nuevos recursos adquiridos por la Universidad Nacional de Chimborazo.
- Indagar detallamente que tipo de herramientas de Informática Forense se podrían aplicar y normalizar de manera permanente dentro de la institución para lograr mejorar y efectivizar las políticas de seguridad informática internas que se en la actualidad se posee para lograr una eficiente administración de recursos y seguridad.
- Resaltar los beneficios que la plataforma B-learning tiene dentro del nuevo modelo pedagógico de Educación Superior, así como mejorar estándares de acceso al sistema que permitan que los usuarios se encuentren seguros que la información que generan se encuentra segura.
- Realizar capacitaciones relacionadas con la configuración acerca de la plataforma B-Learning, tanto en lo referente a uso, beneficios, funcionamiento, seguridad y demás servicios que esta plataforma puede ofrecer a los usuarios así como al personal que se encuentran a cargo de su administración.
- Implementar las normas de seguridad faltantes, con la finalidad de ofrecer un mejor servicio que presta el Centro de Tecnología Educativa con respecto a la información almacenada de los diferentes usuarios del sistema.
- Desarrollar un Plan de Seguridad Informático tomando en cuenta los parámetros que aporta en seguridad informática la metodología MAGERIT empleada en el estudio aunque este no es la única metodología existente en el mercado puede ser una guía para iniciar un estudio más profundo de los requerimientos que se tiene en el Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo.
- Se deben aplicar las salvaguardas mencionadas en la guía que se adjunta dentro del presente documento para proteger de mejor manera los activos de la Institución frente a las posibles amenazas detectadas y así mitigar el riesgo encontrado.

CAPITULO VI

6. PROPUESTA

6.1 ANÁLISIS Y DESARROLLO DE UNA GUÍA DE SEGURIDAD APLICADA A LOS SERVIDORES INFORMATICOS DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO

6.2 INTRODUCCIÓN

En la actualidad es muy importante tener en cuenta que la información que se maneja dentro de una institución, empresa o en este caso en particular de la Universidad Nacional de Chimborazo, contiene datos altamente importantes y confidenciales los mismos que se deben proteger y resguardar apropiadamente teniendo en cuenta normas, procedimientos y políticas que permitan alcanzar este objetivo.

En la propuesta de la guía se presenta las normas y políticas de seguridad, que integran esfuerzos, conocimientos y análisis de una manera conjunta. Para que esta metodología funcione se deben establecer reglas, normas, controles y procedimientos que regulen la forma en que la Universidad Nacional de Chimborazo, proteja, prevenga y maneje los riesgos de seguridad que se puedan presentar o suscitar dentro del Centro de Tecnología Educativa que se encuentra implementado en esta prestigiosa institución.

6.3 OBJETIVOS

6.3.1. OBJETIVOS GENERALES

Desarrollar una guía de Políticas de Seguridad Informática para el Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo.

6.3.2. OBJETIVOS ESPECÍFICOS

- Elaborar una guía de Políticas de Seguridad Informática adaptado a las necesidades de la Universidad Nacional de Chimborazo.
- Identificar las principales amenazas a la que está expuesto el Centro de Tecnología Educativa en cuanto a la seguridad informática.
- Establecer niveles de seguridad en base a normas y recomendaciones internacionales, a través de un guía de seguridad que se enfoque en los objetivos y en la situación de la institución.

6.4 FUNDAMENTACIÓN CIENTÍFICO – TÉCNICA

6.4.1. SEGURIDAD INFORMÁTICA

Es el área que se encarga de la protección de la infraestructura computacional, incluyendo la información contenida. Maneja la protección de aspectos tales como confidencialidad, integridad, autenticidad y disponibilidad la seguridad informática protege software, base de datos archivos, dato, etc. De que caiga en manos de personas inescrupulosas o no autorizadas.

La Seguridad Informática (S.I.) es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos. La decisión de aplicarlos es responsabilidad de cada usuario. Las consecuencias de no hacerlo también. Tema: Seguridad informática.

6.4.2. PRINCIPIOS DE SEGURIDAD INFORMÁTICA

Para lograr sus objetivos, la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático:

- Confidencialidad
- Integridad
- Disponibilidad

6.4.2.1. PRINCIPIOS DE SEGURIDAD INFORMÁTICA: CONFIDENCIALIDAD

Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben proteger al sistema de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

6.4.2.2. PRINCIPIOS DE SEGURIDAD INFORMÁTICA: INTEGRIDAD

Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es particularmente importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

6.4.2.3. PRINCIPIOS DE SEGURIDAD INFORMÁTICA: DISPONIBILIDAD

Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de Seguridad Informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran. Este principio es particularmente importante en sistemas informáticos cuyo compromiso con el usuario, es prestar servicio permanente.

6.4.2.4. FACTORES DE RIESGO TECNOLÓGICO.

Tales como fallas de hardware y/o software, fallas en el aire acondicionado, falla en el servicio eléctrico, ataque por virus informáticos, etc.

- **Ambientales:** factores externos, lluvias, inundaciones, terremotos, tormentas, rayos, suciedad, humedad, calor, entre otros.

- **Humanos**: hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, intrusión, alteración, etc. Impredecibles - Inciertos Predecibles Tema: Seguridad informática.

6.4.2.5. FACTORES TECNOLÓGICOS DE RIESGO: VIRUS INFORMÁTICOS

Definición: Un virus informático es un programa (código) que se replica, añadiendo una copia de sí mismo a otro(s) programa(s). Los virus informáticos son particularmente dañinos porque pasan desapercibidos hasta que los usuarios sufren las consecuencias, que pueden ir desde anuncios inocuos hasta la pérdida total del sistema.

Características: Auto-reproducción: Es la capacidad que tiene el programa de replicarse (hacer copias de sí mismo), sin intervención o consentimiento del usuario.

Infección: Es la capacidad que tiene el código de alojarse en otros programas, diferentes al portador original.

6.4.3. ANÁLISIS DE RIESGOS.

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta: "lo que no está permitido debe estar prohibido" y ésta debe ser la meta perseguida.

Los medios para conseguirlo son:

- Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.

- Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
- Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
- Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

6.4.4. ELEMENTOS DE UN ANÁLISIS DE RIESGO

Cuando se pretende diseñar o crear una técnica para implementar un análisis de riesgo informático se pueden tomar los siguientes puntos como referencia a seguir:

- Planes para reducir los riesgos.

Análisis del impacto al negocio.

El reto es asignar estratégicamente los recursos para cada equipo de seguridad y bienes que intervengan, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver. Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un valor relativo a cada sistema y la información sobre ella. Dentro de los Valores para el sistema se pueden distinguir: Confidencialidad de la información, la Integridad (aplicaciones e información) y finalmente la Disponibilidad del sistema. Cada uno de estos valores es un sistema independiente del negocio, supongamos el siguiente ejemplo, un servidor Web público pueden poseer los requisitos de confidencialidad de baja (ya que toda la información es pública),pero de alta disponibilidad y los requisitos de integridad. En contraste, un sistema de planificación de recursos empresariales (ERP), sistema puede poseer alto puntaje en los tres variables. Los incidentes individuales pueden variar ampliamente en términos de alcance e importancia.

I

6.4.5. PUESTA EN MARCHA DE UNA POLÍTICA DE SEGURIDAD

Actualmente las legislaciones nacionales de los Estados, obligan a las empresas, instituciones públicas a implantar una política de seguridad.

Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza.

Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión
- Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad informática.

6.5 DESCRIPCIÓN DE LA PROPUESTA

6.5.1. ANÁLISIS DE REQUISITOS.

Para el análisis de cada uno de los requerimientos relacionados con los indicadores que se plantearon y se aplicaron durante el proceso de investigación, se inició con una visita de observación cuyo objetivo fue observar de manera directa la situación en la que se desarrolla y desenvuelve el Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo.

Mediante la aplicación de encuestas dirigidas a los usuarios recurrentes tales como administradores responsables, alumnos, profesores, se recopilo información sobre la visión que poseen los usuarios a cerca de los sistemas existentes en el Centro de Tecnología Educativa, permitiendo detectar las necesidades y falencias que se pueden presentar en base a la seguridad que se maneja dentro del CTE. basados en las normas de seguridad Internacionales

6.5.2. MONITOREO Y EVALUACIÓN DE LA PROPUESTA

Mediante la aplicación de las encuestas realizadas a los técnicos administradores del Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo.

6.5.3. VERIFICACIÓN DEL CUMPLIMIENTO MEDIDAS DE SEGURIDAD.

Las encuestas se dividen en grupos que componen la seguridad es decir, marco organizativo, marco operacional, y medidas de protección.

Por cada uno de los componentes de los grupos se indicará cómo verificar el correcto cumplimiento con las medidas indicadas en el ENS, haciendo referencia a aquellas guías que proporcionan información sobre las medidas a aplicar en cada caso.

Tabla 23. Tabulación de las medidas de seguridad

APTDO.	CATEGORÍA-DIMENSIONES	REQUISITO	APLICABILIDAD-AUDITADO	COMENTARIOS
Org.	**Marco organizativo**			
Org. 1	Política de seguridad			
1	Básica	Marco organizativo de seguridad	Cumple ( )si (x)no	Requisitos ( )Documentos (x)Muestreo
2	Básica	Arquitectura de seguridad	Cumple ( )si (x)no	Requisitos ( )Documentos (x)Registros
3	Baja	Control de acceso	Cumple ( )si (x)no	Requisitos ( )Documentos (x)Muestreo
4	Baja	Acceso local (Local logon)	Cumple (x)si ( )no	Requisitos ( )Documentos (x)Muestreo
5	Media	Mantenimiento	Cumple (x)si ( )no	Requisitos (x)Documentos ( )Muestreo
6	Baja	Protección frente a código dañino	Cumple ( )si (x)no	Requisitos ( )Documentos (x)Muestreo
7	Media	Registro de actividad de los usuarios	Cumple ( )si (x)no	Requisitos ( )Documentos (x)Muestreo
8	Media	Protección de los riesgos de actividad	Cumple ( )si (x)no	Requisitos ( )Documentos (x)Muestreo
9	Baja	Monitorización del sistema	Cumple ( )si (x)no	Requisitos ( )Documentos (x)Muestreo
10	Alta	Protección de las instalaciones e infraestructuras	Cumple (x)si ( )no	Requisitos (x)Documentos ( )Muestreo
11	Media	Protección de las comunicaciones y confidencialidad	Cumple (x)si ( )no	Requisitos (x)Documentos ( )Muestreo
12	Baja	Copias de seguridad (backup)	Cumple ( )si (x)no	Requisitos ( )Documentos (x)Muestreo
13	Media	Protección de los servicios	Cumple (x)si ( )no	Requisitos (x)Documentos ( )Muestreo
14	Baja	Seguridad de funciones y tareas	Cumple ( )si (x)no	Requisitos ( )Documentos (x)Muestreo

6.5.4. FUNCIONALIDAD DE LOS SERVICIOS OFRECIDOS POR EL SERVIDOR B-LEARNING.

Tabla 24. Resultados de los servicios ofrecidos a los usuarios de la Universidad Nacional de Chimborazo.

N°	DESCRIPCIÓN SERVICIO	CUMPLIMIENTO	
		SI%	NO%
1	Ha utilizado usted antes una plataforma B-learning	70	28
2	Utilizas con frecuencia la plataforma B-learning	62	36
3	Utilizas la plataforma B-learning como método de enseñanza	66	32
4	La enseñanza a través de la plataforma B-learning ayuda a mejorar el desempeño del desarrollo académico	64	34
5	Recibió usted una introducción previa sobre el servicio que ofrece la plataforma B-learning.	64	34
6	Existe documentación de ayuda sobre el funcionamiento del sistema.	64	34
7	Ha aplicado algún examen mediante esta plataforma.	64	34
8	Cree la plataforma B-learning cuenta con una interface de usuario amigable	64	34
9	¿Crees usted que la plataforma B-learning cuenta con las seguridades adecuadas como para proteger su información?	60	38
10	Sabe usted si la información que proporciona al sistema es confidencial	54	44
11	El funcionamiento durante las horas picos es satisfactorio	60	38
12	Usted accede a los servicios del B-learning desde la universidad	58	40
13	Usted accede a los servicios del B-learning desde la universidad	50	48
14	Existe un Periodo en el que el sistema le pide cambiar su contraseña	34	64

Si bien en la Universidad Nacional de Chimborazo se utiliza con frecuencia la plataforma B-learning, los resultados obtenidos a través de las encuestas realizadas a los usuarios estudiantes, se concluye que su servicio como método de aprendizaje es aceptable en un 65%, sus servicios y funcionamientos son satisfactoriamente aceptables, no así su seguridad con la que se maneja la confidencialidad que se le proporciona al sistema.

6.6 ELABORACIÓN DE LA PROPUESTA

GUIA DE SEGURIDAD APLICADA AL SISTEMA B-LEARNING DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO

En la actualidad es muy importante tener en cuenta que la información que se maneja dentro de una institución, empresa o en este caso en particular de la Universidad Nacional de Chimborazo, contiene datos altamente importantes y confidenciales los mismos que se deben proteger y resguardar apropiadamente teniendo en cuenta normas, procedimientos y políticas que permitan alcanzar este objetivo.

En la siguiente guía se presenta las normas y políticas de seguridad, que integran esfuerzos, conocimientos y análisis de una manera conjunta. Para que esta metodología funcione se deben establecer reglas, normas, controles y procedimientos que regulen la forma en que la Universidad Nacional de Chimborazo, proteja, prevenga y maneje los riesgos de seguridad que se puedan presentar o suscitar dentro del Centro de Tecnología Educativa que se encuentra implementado en esta prestigiosa institución.

El documento elaborado a continuación servirá como referencia, mas no pretenderá ser una normativa absoluta, pues la misma está sujeta a cambios que se pueden realizar en cualquier momento, teniendo en cuenta que tengan como prioridad alcanzar los objetivos de seguridad para lo que fue desarrollada la presente guía.

Todo usuario que utilice los servicios que ofrece el Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo, a través de su red debe conocer, aceptar y aplicar el reglamento para su uso, el hecho de no conocer esta normativa por parte del usuario, no lo exonerara ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

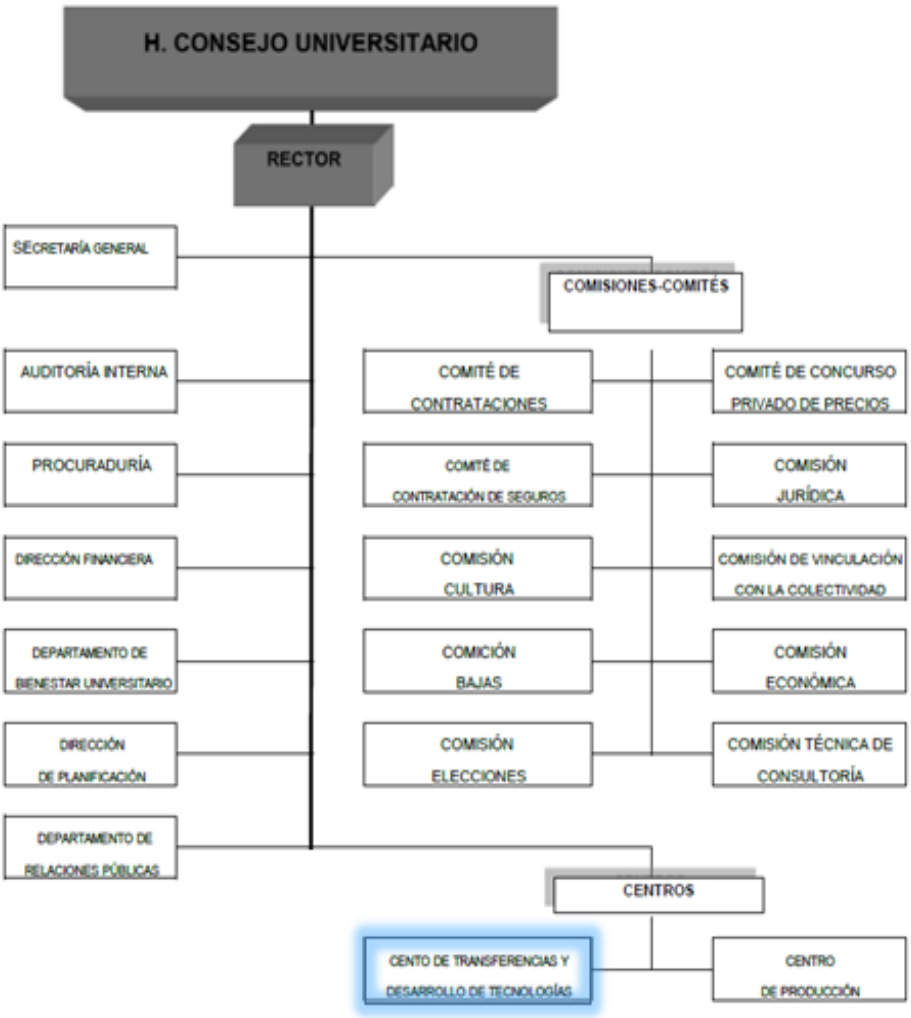
En términos generales el manual de normas y políticas de seguridad informática abarca los principales procedimientos que deben tomarse en cuenta los lineamientos que se explican a continuación.

6.7 SEGURIDAD ORGANIZACIONAL DEL CENTRO DE TECNOLOGÍA EDUCATIVA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO

Organización del Centro de Tecnología Educativa dentro de la Universidad Nacional de Chimborazo.

La Universidad Nacional de Chimborazo consta con un organigrama general dentro del cual se poseciona el Centro de Tecnología Educativa.

Figura 9. Diagrama organizacional del Centro de trasferencia de Tecnología Educativa de la Universidad Nacional de Chimborazo.



6.7.1. SITUACIÓN ACTUAL

La Universidad Nacional de Chimborazo encuentra ubicada en el barrio San Antonio brinda a la sociedad la formación de profesionales de tercer y cuarto nivel, actualmente tiene una población estudiantil de 7000 estudiantes distribuidos en los campus MsC. Edison Riera y La Dolorosa.

En el Campus Central "La Dolorosa", cuya superficie es de 35.588,44 m², funcionan: El Vicerrectorado de Postgrado e Investigación, la Facultad de Ciencias de la Educación y parte de la Facultad de Ciencias Políticas, mientras que el Edificio Central Administrativo y las Facultades de Ingeniería, Ciencias de la Salud y Ciencias Políticas se encuentran ubicadas en el Campus Norte "Edison Riera Rodríguez" ubicado en km. 1 1/2 de la vía a Guano. Este campus tiene una superficie de 129.092,67 m².

La Facultad de Ciencias de la Educación: está ubicada en el campus central sector La Dolorosa, cuenta con 1 edificio con oficinas, 1 biblioteca, 2 bloques para 37 aulas destinadas a la docencia, 4 aulas virtuales, 8 laboratorios de cómputo y 11 puestos de trabajo para profesores.

La Facultad de Ciencias Políticas y Administrativas tiene: Campus Centro: 1 edificio con 5 oficinas, 16 aulas, 1 aula virtual, 3 laboratorios varios y 4 puestos de trabajo para profesores. En el campus Norte: 22 aulas campus norte, 3 aulas virtuales, 5 centros de cómputo, 1 biblioteca y 5 puestos de trabajo para profesores.

La Facultad de Ciencias de la Salud cuenta con 3 edificios que tienen 14 oficinas, 33 aulas, 6 aulas virtuales, 1 auditórium, 2 centros de cómputo, 13 laboratorios varios, 1 biblioteca y 6 puestos de trabajo para profesores.

La Facultad de Ingeniería cuenta con 3 edificios que tienen 10 oficinas, 36 aulas, 2 aulas virtuales, 1 auditórium, 5 centros de cómputo, 1 biblioteca, 16 laboratorios varios y 5 puestos de trabajo para profesores

El Centro de Tecnología Educativa concentra los siguientes ambientes: 9 laboratorios de cómputo, 3 salas de videoconferencia, 3 salas de internet, 1 sala red inalámbrico, bibliotecas.

6.7.2. MISIÓN CTE

Ser agente transformador en el ámbito de las TIC y sus aplicaciones, potenciando la innovación tecnológica, cultivando el desarrollo de talento y atrayendo recursos financieros; generando así reconocimiento al apoyar y promover la cooperación, el desarrollo, competitividad y calidad de la UNACH.

6.7.3. VISIÓN CTE

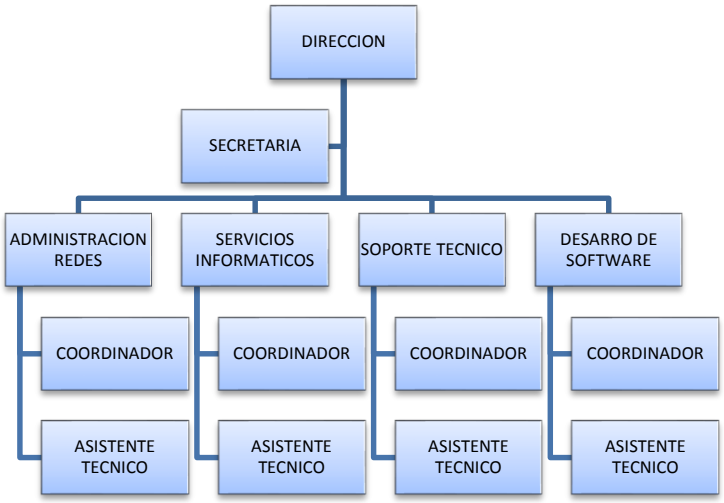
CTE tiene la visión ser un referente en la investigación, innovación y prestación de servicios en el ámbito de las TICs, tanto a nivel local, regional, y nacional, contribuyendo a posicionar a la UNACH como institución líder en el ámbito de la educación superior

6.7.4. VALORES

- La vocación del servicio: Todas las actuaciones de CTE estarán orientadas al cumplimiento de la misión que es compromiso de servicio a la UNACH. Ello implica una vocación de servicio en todas y cada una de las actuaciones que CTE realice con las unidades administrativas y académicas de la institución.
- La aportación de valor añadido: CTE, en su relación con las unidades administrativas y académicas de la institución deberá ser siempre percibido muy positivamente en su afán de no escatimar esfuerzos para la búsqueda o desarrollo de soluciones que redunden en la mejora de sus servicios.
- La honestidad profesional: deberá ser un valor de todos los trabajadores de CTE, tanto hacia los compañeros de trabajo como hacia las unidades administrativas y académicas de la institución, que sabrán apreciar en justa medida, y en términos de confianza, la honradez de CTE a la hora de dimensionar de forma correcta si tiene competencia técnica o no para satisfacer una necesidad.
- La transparencia en la gestión.
- El compromiso de la organización con el trabajo bien hecho.

6.7.5. ORGANIGRAMA CTE

Figura 10. Organigrama del CTE (Centro de Tecnología Educativa)



6.7.6. VISIÓN DE GESTIÓN

Antes de realizar un análisis minucioso de los riesgos, hay que considerar dos tareas importantes a realizar:

Análisis de riesgos: Mediante esta tarea se determinara lo que tiene la organización, para así poder estimar lo que podría pasar en un futuro.

Dentro del análisis de riesgos se considera los elementos siguientes:

Activos: Son elementos del sistema de información (o están estrechamente relacionados con este) que soportan la misión de la organización.

Amenazas: Son las cosas que les puede pasar a los activos causando un perjuicio a la organización.

Salvaguardas: (Contramedidas) son medidas de protección desarrolladas para que aquellas amenazas no causen tanto daño.

Mediante estos elementos se pueden estimar lo siguiente:

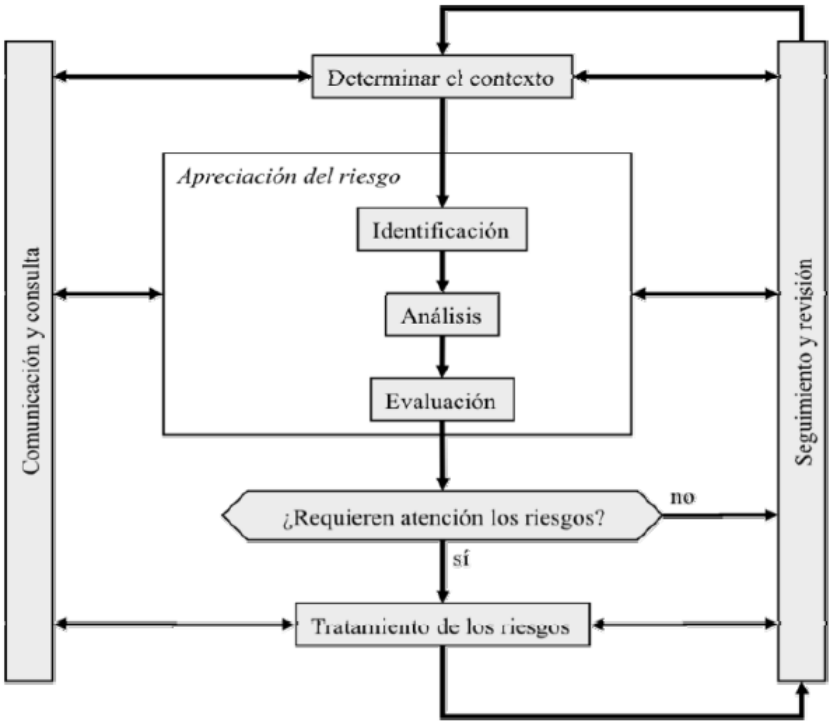
- **Impacto**: lo que podría pasar.
- **Riesgo**: lo que probablemente pase.

El análisis de riesgo permite analizar estos elementos de forma ordenada para llegar a una conclusión, y proceder a la fase de tratamiento.

De manera informal se dice que la gestión de seguridad de un sistema de información es la gestión de sus riesgos, mientras que el análisis permite racionalizar dicha gestión.

De manera formal, la gestión de los riesgos está estructurada de forma metódica en las normas ISO.

Figura 11. Proceso de gestión de riesgos (ISO 31000).



Determinar contexto: lleva a una determinación de los parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para gestionar los riesgos. Un elemento a destacar es el alcance del análisis, incluyendo obligaciones propias y obligaciones contraídas, así como las relaciones con otras organizaciones, sean para intercambio de información y servicios o proveedoras de servicios subcontratados. Norma (ISO 31000) para un mayor desarrollo de los factores que determinan el contexto.

Identificación de los riesgos: busca una relación de los posibles puntos de peligro. Lo que se identifique será analizado en la siguiente etapa. Lo que no se identifique quedará como riesgo oculto o ignorado.

Análisis de los riesgos: busca calificar los riesgos identificados, bien cuantificando sus consecuencias (análisis cuantitativo), bien ordenando su importancia relativa (análisis

cualitativo). De una u otra forma, como resultado del análisis tendremos una visión estructurada que nos permita centrarnos en lo más importante.

Evaluación de los riesgos: va un paso más allá del análisis técnico y traduce las consecuencias a términos de negocio. Aquí entran factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuáles no, así como de en qué circunstancias podemos aceptar un riesgo o trabajar en su tratamiento.

Tratamiento de los riesgos: recopila las actividades encaminadas a modificar la situación de riesgo. Es una actividad que presenta numerosas opciones.

Comunicación y consulta: Es importante no olvidar nunca que los sistemas de información deben ser soporte de la productividad de la Organización. Es absurdo un sistema muy seguro pero que impide que la Organización alcance sus objetivos. Siempre hay que buscar un equilibrio entre seguridad y productividad y en ese equilibrio hay que contar con la colaboración de varios interlocutores:

- Los usuarios cuyas necesidades deben ser tenidas en cuenta y a los que hay que informar para que colaboren activamente en la operación del sistema dentro de los parámetros de seguridad determinados por la Dirección.
- los proveedores externos, a los que hay proporcionar instrucciones claras para poder exigirles tanto el cumplimiento de los niveles de servicio requeridos, como la gestión de los incidentes de seguridad que pudieran acaecer.
- Los órganos de gobierno para establecer canales de comunicación que consoliden la con-fianza de que el sistema de información responderá sin sorpresas para atender a la misión de la Organización y que los incidentes serán atajados de acuerdo el plan previsto

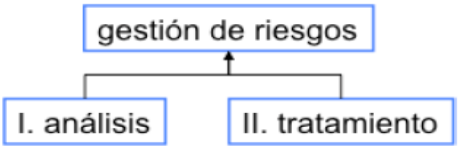
Seguimiento y revisión: Es importante no olvidar nunca que el análisis de riesgos es una actividad de despacho y que es imprescindible ver qué ocurre en la práctica y actuar en consecuencia, tanto reaccionando diligentemente a los incidentes, como mejorando continuamente nuestro conocimiento del sistema y de su entorno para mejorar el análisis y ajustarlo a la experiencia.

Tratamiento de los riesgos: en este tratamiento se determina una defensa meticulosa y prudente, preparándose para que nada malo pase para tratar de evitar las emergencias,

sobrevivir a los incidentes y seguir operando en mejores condiciones; tomado en cuenta de que nada es perfecto, el riesgo se reduce a un nivel residual que la dirección.

Estad dos actividades análisis y tratamiento de riesgos se combinan en el proceso denominado gestión de riesgos.

Figura 12. Visión de Riesgos



6.8 MÉTODO DE ANÁLISIS DE RIESGOS

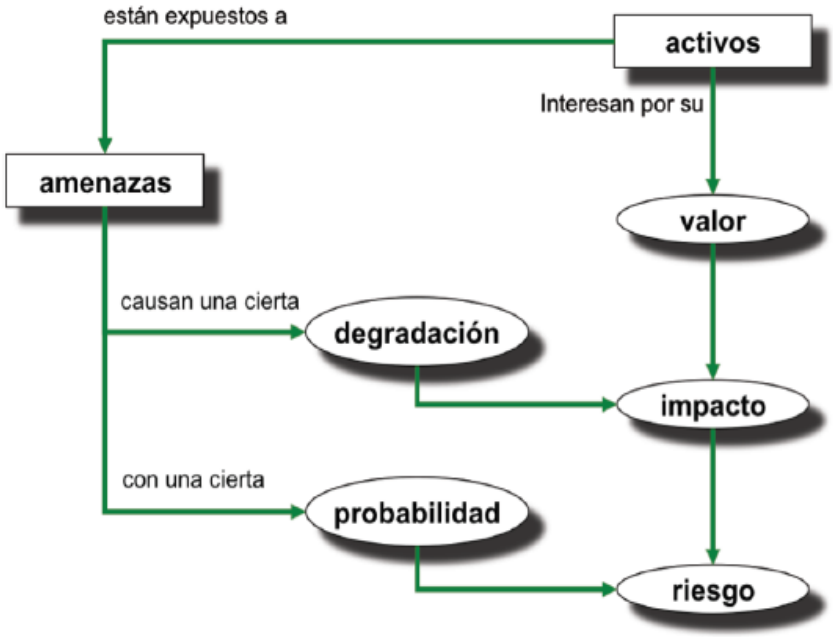
Antes de monitorear las fallas encontradas en el Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo, se realizara un análisis de gestión de riego, cuya finalidad es seguir un esquema lógico para determinar los problemas que se presenten en las diferentes etapas de gestión. El análisis de riesgo consiste en seguir un conjunto de pasos ordenados, pautados con el fin de determinar el riesgo.

- Determinar los activos relevantes para la Universidad Nacional de Chimborazo, su interrelación y su valor su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- Determinar a qué amenazas están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Con el objeto de organizar la presentación, se introducen los conceptos de “impacto y riesgo potenciales” entre los pasos 2 y 3. Estas valoraciones son “teóricas”: en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas del paso 3, derivando estimaciones realistas de impacto y riesgo.

La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

Figura 13. Elementos del análisis de riesgos Potenciales



6.8.1. PASO 1: ACTIVOS

Es un componente o una funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la Universidad Nacional de Chimborazo. Incluye información, datos, servicios, aplicaciones (Software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Un sistema de información consta de dos aspectos esenciales.

- La información que maneja.
- Los servicios que presta.

Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Subordinados a dicha esencia se pueden identificar otros activos relevantes:

- **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.

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes.

DEPENDENCIAS

Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más ligeros como pueden ser los equipos, las comunicaciones, las instalaciones y las frecuentemente olvidadas personas que trabajan con aquellos.

De manera que los activos vienen a formar árboles o grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en la estructura o 'superiores' depende de los activos que se encuentran más abajo o 'inferiores'. Estas estructuras reflejan de arriba hacia abajo las dependencias, mientas que de abajo hacia arriba la propagación del daño caso de materializarse las amenazas.

Por ello aparece como importante el concepto de "dependencias entre activos" o la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior.

Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Informalmente puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

Aunque en cada caso hay que adaptarse a la Organización objeto del análisis, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

ACTIVOS ESENCIALES

- Información que se maneja.
- Servicios Prestados.

SERVICIOS INTERNOS

Que estructuran ordenadamente el sistema de Información.

EL EQUIPAMIENTO INFORMÁTICO

- Aplicaciones (Software).
- Equipos Informáticos (Hardware).
- Comunicaciones.
- Soportes de información: discos, cintas, etc.

EL ENTORNO

Activos que se precisan para garantizar las siguientes capas:

- Equipamiento y suministros: energía, climatización, etc.
- Mobiliario.

LOS SERVICIOS SUBCONTRATADOS A TERCEROS

LAS INSTALACIONES FÍSICAS

EL PERSONAL

- Usuarios.
- Operadores y administradores
- Desarrolladores.

VALORACIÓN

¿Por qué interesa un activo? Por lo que vale.

No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial.

Por otra parte, los sistemas de información explotan los datos para proporcionar servicios, internos a la Organización o destinados a terceros, apareciendo una serie de datos necesarios para prestar un servicio. Sin entrar en detalles técnicos de cómo se hacen las cosas, el conjunto de información y servicios esenciales permite caracterizar funcionalmente una organización. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios.

DIMENSIONES

Un activo puede interesar calibrar diferentes dimensiones:

- **Su confidencialidad**: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- **Su integridad**: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falso o, incluso faltar datos.
- **Su disponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

En sistemas dedicados a servicios de la sociedad de la información como puedan ser los de administración electrónica o comercio electrónico, el conocimiento de los actores es fundamental para poder prestar el servicio correctamente y poder perseguir los fallos (accidentales o deliberados) que pudieran darse. Así pues, en los activos esenciales, frecuentemente es útil valorar:

LA AUTENTICIDAD

¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?

Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)

LA TRAZABILIDAD

Del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

LA TRAZABILIDAD DEL USO DEL SERVICIO

¿Qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?

Se reconocen habitualmente como dimensiones básicas la confidencialidad, integridad y disponibilidad. En esta metodología se han añadido la autenticidad y el concepto de trazabilidad (del inglés, *accountability*), que a efectos técnicos se traducen en mantener la integridad y la confidencialidad de ciertos activos del sistema que pueden ser los servicios de directorio, las claves de firma digital, los registros de actividad, etc.

En un árbol de dependencias, donde los activos superiores dependen de los inferiores, es imprescindible valorar los activos superiores, los que son importantes por sí mismos. Automáticamente este valor se acumula en los inferiores, lo que no es impedimento para que también puedan merecer, adicionalmente, su valoración propia.

¿CUÁNTO VALE LA "SALUD" DE LOS ACTIVOS?

Una vez determinadas qué dimensiones (de seguridad) interesan de un activo hay que proceder a valorarlo. La valoración es la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo. Hay muchos factores a considerar:

- Coste de reposición: adquisición e instalación.
- Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo.
- Lucro cesante: pérdida de ingresos.
- Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas.
- Sanciones por incumplimiento de la ley u obligaciones contractuales.

- Daño a otros activos, propios o ajenos.
- Daño a personas.
- Daños medioambientales.

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes a respetar son:

La homogeneidad: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra.

La relatividad: es importante poder relativizar el valor de un activo en comparación con otros activos

Ambos criterios se satisfacen con valoraciones económicas (coste dinerario requerido para "curar" el activo) y es frecuente la tentación de ponerle precio a todo. Si se consigue, excelente. Incluso es fácil ponerle precio a los aspectos más tangibles (equipamiento, horas de trabajo, etc.); pero al entrar en valoraciones más abstractas (intangibles como la credibilidad de la Organización) la valoración económica exacta puede ser escurridiza y motivo de agrias disputas entre expertos.

Valoración cualitativa

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como "órdenes de magnitud" y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

Valoración cuantitativa

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente "natural". La interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es dineraria, además se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución respondiendo a las preguntas:

- ¿Vale la pena invertir tanto dinero en esta salvaguarda?

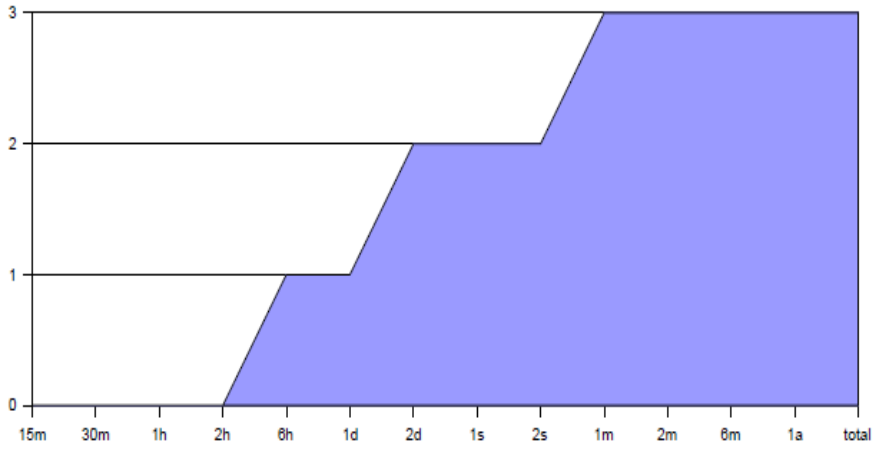
- ¿Qué conjunto de salvaguardas optimizan la inversión?
- ¿En qué plazo de tiempo se recupera la inversión?
- ¿Cuánto es razonable que cueste la prima de un seguro?

Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad.

No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido suponga la terminación de la actividad. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias.

En consecuencia, para valorar la (interrupción de la) disponibilidad de un activo hay que usar una estructura más compleja que se puede resumir en algún gráfico como el siguiente:

Figura 14. Coste de la interrupción de la disponibilidad



Donde aparece una serie de escalones de interrupción que terminan con la destrucción total o permanente del activo. En el ejemplo anterior, paradas de hasta 6 horas se pueden asumir sin consecuencias. Pero a las 6 horas se disparan las alarmas que aumentan si la parada supera los 2 días. Y si la parada supera el mes, se puede decir que la Organización ha perdido su capacidad de operar: ha muerto. Desde el punto de vista de los remedios, la gráfica dice directamente que no valiera la pena.

6.8.2. PASO 2: AMENAZAS

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son "cosas que ocurren". Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

AMENAZA

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

IDENTIFICACIÓN DE LAS AMENAZAS

Se presenta una relación de amenazas típicas.

DE ORIGEN NATURAL

Hay accidentes naturales (terremotos, inundaciones). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

DEL ENTORNO (DE ORIGEN INDUSTRIAL)

Hay desastres industriales (contaminación, fallos eléctricos) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

DEFECTOS DE LAS APLICACIONES

Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, vulnerabilidades.

CAUSADAS POR LAS PERSONAS DE FORMA ACCIDENTAL

Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

CAUSADAS POR LA PERSONAS DE FORMA DELIBERADA

Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de 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.

VALORACIÓN DE LAS AMENAZAS

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

Degradación: cuán perjudicado resultaría el (valor del) activo.

Probabilidad: cuán probable o improbable es que se materialice la amenaza.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera.

La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o "degradado en una pequeña fracción". Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

Tabla 25. Degradación del 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

A veces se modela numéricamente como una frecuencia de ocurrencia. Es habitual usar 1 año como referencia, de forma que se recurre a la tasa anual de ocurrencia como medida de la probabilidad de que algo ocurra. Son valores típicos:

Tabla 26. 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

6.8.3. DETERMINACIÓN DEL IMPACTO POTENCIAL

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias.

IMPACTO ACUMULADO: Es el calculado sobre un activo teniendo en cuenta.

SU VALOR ACUMULADO (el propio mas el acumulado de los activos que dependen de él).

LAS AMENAZAS a que está expuesto.

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada. El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado. El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

IMPACTO REPERCUTIDO

Es el calculado sobre un activo teniendo en cuenta

- Su valor propio.
- Las amenazas a que están expuestos los activos de los que depende.

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio de un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.

El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

AGREGACIÓN DE VALORES DE IMPACTO

Anteriormente se determinó los activos que podría estar expuestos a ciertas amenazas estos diferentes impactos se pueden agregar bajo ciertas condiciones.

- Puede agregarse el impacto repercutido sobre diferentes activos.
- Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común.
- No debe agregarse el impacto acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el impacto al incluir varias veces el valor acumulado de activos superiores.

- Puede agregarse el impacto de diferentes amenazas sobre un mismo activo, aunque con-viene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes.
- Puede agregarse el impacto de una amenaza en diferentes dimensiones.

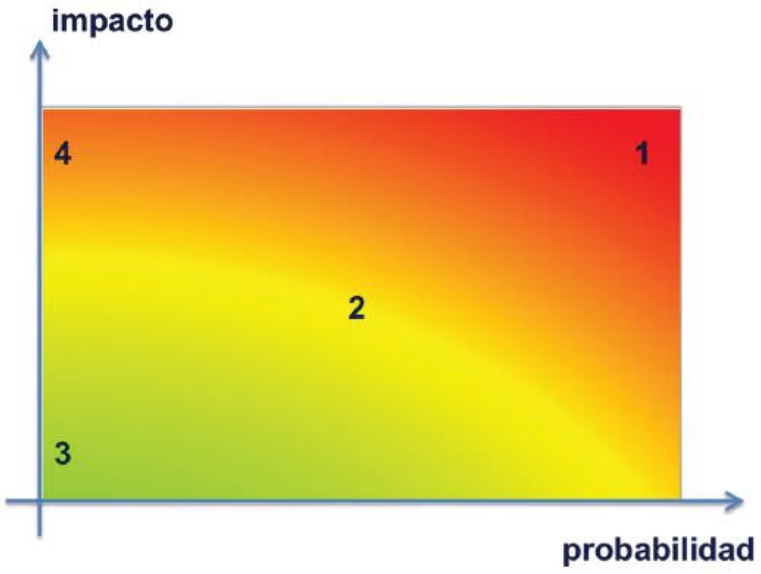
DETERMINACIÓN DEL RIESGO POTENCIAL

Un riesgo implica la medida del daño probable sobre un sistema, conociendo el impacto de las amenazas sobre los activos es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo (que veremos más adelante):

- **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.

Figura 15. El riesgo en función del impacto y la probabilidad



RIESGO ACUMULADO

Es el calculado sobre un activo tomando en cuenta los siguientes aspectos:

- El impacto acumulado sobre un activo debido a una amenaza.
- La probabilidad de la amenaza.

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza.

El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

RIESGO REPERCUTIDO

Es el calculado sobre un activo teniendo en cuenta.

- El impacto repercutido sobre un activo debido a una amenaza.
- La probabilidad de la amenaza.

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la probabilidad de la amenaza.

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

AGREGACIÓN DE RIESGOS

Anteriormente se determinó el riesgo que sobre un activo tendría una amenaza en una cierta dimensión. Estos riesgos singulares pueden agregarse bajo ciertas condiciones:

- Puede agregarse el riesgo repercutido sobre diferentes activos.
- Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común.

- No debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores.
- Puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes.
- Puede agregarse el riesgo de una amenaza en diferentes dimensiones

6.8.4. PASO 3: SALVAGUARDAS

En los pasos anteriores no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridades físicas y, por último, está la política de personal.

SELECCIÓN DE SALVAGUARDAS

Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

- Tipo de activos a proteger, pues cada tipo se protege de una forma específica.
- Dimensión o dimensiones de seguridad que requieren protección.
- Amenazas de las que necesitamos protegernos.
- Si existen salvaguardas alternativas

Hay que establecer un principio de proporcionalidad y tener en cuenta.

- El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante.

- La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes (ver zonas de riesgo).
- La cobertura del riesgo que proporcionan salvaguardas alternativas.

Esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar:

- **No aplica**: se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración
- **No se justifica**: se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger

Como resultado de estas consideraciones dispondremos de una "declaración de aplicabilidad" o relación de salvaguardas que deben ser analizadas como componentes nuestro sistema de protección.

EFECTO DE SALVAGUARDAS

Las salvaguardas entran en el cálculo del riesgo de dos formas.

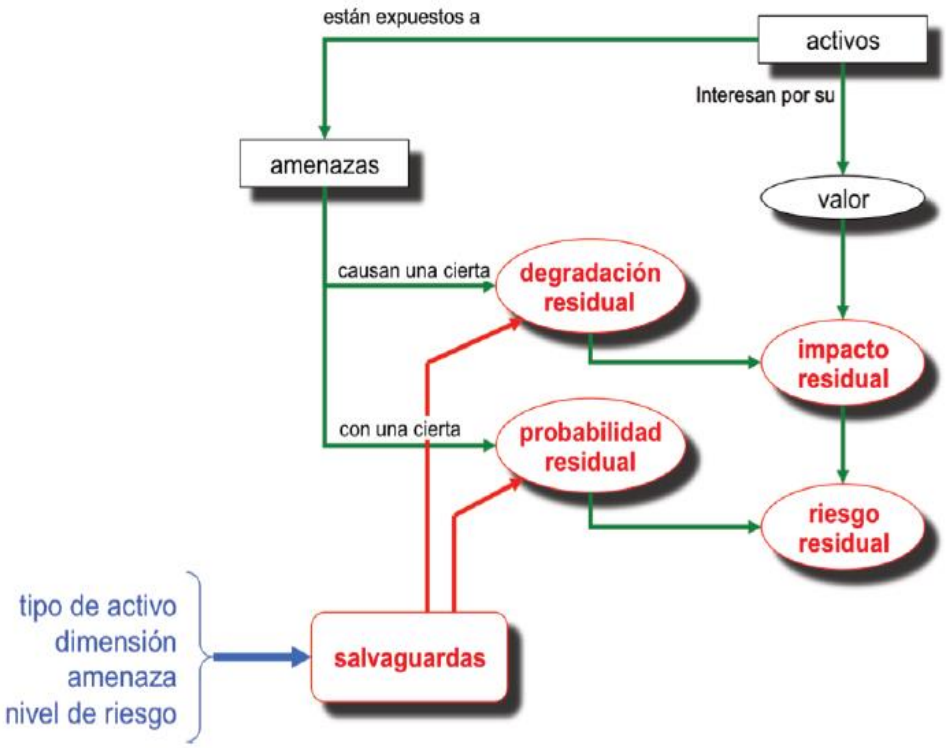
REDUCIENDO LA PROBABILIDAD DE LAS AMENAZAS

Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

LIMITANDO EL DAÑO CAUSADO

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las con-secuencias se limitan.

Figura 16. Elementos de análisis de riesgo residual



TIPO DE PROTECCIÓN

Esta aproximación a veces resulta un poco simplificadora, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

[PR] PREVENCIÓN: Diremos que una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos. Ejemplos: autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, metodología segura de desarrollo de software, pruebas en pre-producción, segregación de tareas,

[DR] DISUASIÓN: Diremos que una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados caso de que el atacante realmente se atreva. Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente.

[EL] ELIMINACIÓN: Diremos que una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

Ejemplos: eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, en general, todo lo que tenga que ver con la fortificación o bastionado, cifrado de la información, armarios ignífugos.

[IM] MINIMIZACIÓN DEL IMPACTO / LIMITACIÓN DEL IMPACTO: Se dice que una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente.

Ejemplos: desconexión de redes o equipos en caso de ataque, detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente

[CR] CORRECCIÓN: Diremos que una salvaguarda es correctiva cuando, habiéndose producido un daño, lo repara. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.

Ejemplos: gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes.

[RC] RECUPERACIÓN: Diremos que una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo.

Ejemplos: copias de seguridad (back-up).

[MN] MONITORIZACIÓN: Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posterior, podemos aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro.

Ejemplos: registros de actividad, registro de descargas de web.

[DC] DETECCIÓN: Diremos que una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí

permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños.

Ejemplos: antivirus, IDS, detectores de incendio.

[AW] CONCIENCIACIÓN: Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación.

Ejemplos: cursos de concienciación, cursos de formación.

[AD] ADMINISTRACIÓN: Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que haya puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo.

Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad.

La siguiente tabla relaciona cada uno de estos tipos de protección con el modelo anterior de reducción de la degradación y de la probabilidad:

Tabla 27. Tipos de salvaguarda

EFECTO	TIPO
Preventivas: Reducen la probabilidad	[PR] preventivas. [DR] disuasorias. [EL] eliminatorias.
Acortan 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.

EFICACIA DE LA PROTECCIÓN: Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, eficacia que combina 2 factores: desde el punto de vista técnico.

- Es técnicamente idónea para enfrentarse al riesgo que protege.
- Se emplea siempre.

Desde el punto de vista de operación de salvaguardas.

- Está perfectamente desplegada, configurada y mantenida.
- Existen procedimientos claros de uso normal y en caso de incidencias.
- Los usuarios están formados y concienciados.
- Existen controles que avisan de posibles fallos.

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. Para medir los aspectos organizativos, se puede emplear una escala de madurez que recoja en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda:

Tabla 28. Eficacia y madurez de las salvaguardas

FACTOR	NIVEL	SIGNIFICADO
0%	**L0**	Inexistente
	L1	Inicial/add hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso definido
	L4	Gestionado y medible
100%	**L5**	Optimizado

VULNERABILIDADES

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

Traducido a los términos empleados en los párrafos anteriores, son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre un activo. A veces se emplea el término “insuficiencia”

para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza.

6.8.5. PASO 4: IMPACTO RESIDUAL

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

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

6.8.6. PASO 5: RIESGO RESIDUAL

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

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

6.9 FORMALIZACIÓN DE LAS ACTIVIDADES

Este conjunto de actividades tiene los siguientes objetivos:

- Levantar un modelo del valor del sistema, identificando y valorando los activos relevantes.
- Levantar un mapa de riesgos del sistema, identificando y valorando las amenazas sobre aquellos activos.
- Levantar un conocimiento de la situación actual de salvaguardas.
- Evaluar el impacto posible sobre el sistema en estudio, tanto el impacto potencial (sin salvaguardas), como el impacto residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).
- Evaluar el riesgo del sistema en estudio, tanto el riesgo potencial (sin salvaguardas), como el riesgo residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).
- Informar de las áreas del sistema con mayor impacto y/o riesgo a fin de que se puedan tomar las decisiones de tratamiento con motivo justificado.

Por medio de las siguientes tareas se lleva a cabo el análisis de los riesgos.

Tabla 29. Análisis de riesgo caracterización.

MAR - MÉTODO DE ANÁLISIS DE RIESGOS.
MAR. 1- Caracterización de los activos
MAR.11 - Identificación de los activos.
MAR.12 – Dependencias entre activos.
MAR.13 – Valoración de los activos.
MAR. 2 – Caracterización de las amenazas.
MAR.21 – Identificación de las amenazas.
MAR.22 – Valoración de las amenazas.

MAR. 3 – Caracterización de las salvaguardas.

MAR.31 – Identificación de las salvaguardas impertinentes.

MAR.32 – Valoración de las salvaguardas.

MAR. 4 – Estimación del estado de riesgo.

MAR.41 – Estimación del impacto.

MAR.42- Estimación del riesgo.

MAR. 1- CARACTERIZACIÓN DE LOS ACTIVOS

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

El resultado de esta actividad es el informe denominado "modelo de valor".

Sub-tareas:

Tarea MAR.11: Identificación de los activos.

Tarea MAR.12: Dependencias entre activos.

Tarea MAR.13: Valoración de los activos.

El objetivo de estas tareas es reconocer los activos que componen el sistema, definir las dependencias entre ellos, y determinar que parte del valor del sistema se soporta en cada activo. Podemos resumirlo en la expresión "conócete a ti mismo".

Tabla 30. Análisis de Riesgos Objetivos.

MAR: Análisis de riesgos **MAR.1: Caracterización de los activos** **MAR.11: Identificación de los activos**
Objetivos • Identificar los activos que componen el sistema, determinando sus características, atributos y clasificación en los tipos determinados

Productos de entrada
Inventario de datos manejados por el sistema. Inventario de servicios prestados por el sistema. Procesos de negocio. Diagramas de uso. Diagramas de flujo de datos. Inventarios de equipamiento lógico. Inventarios de equipamiento físico. Locales y sedes de la Organización. Caracterización funcional de los puestos de trabajo.

Tabla 31. Análisis de riesgos de los activos

MAR: ANÁLISIS DE RIESGO. **MAR. 1: CARACTERIZACIÓN DE LOS ACTIVOS.** **MAR. 11: IDENTIFICACIÓN DE LOS ACTIVOS.**
Productos de salida • Relación de activos a considerar. • Caracterización de los activos: valor propio y acumulado. • Relaciones entre activos.
Técnicas, prácticas y pautas • Diagramas de flujo de datos • Diagramas de procesos • Entrevistas • Reuniones

Esta tarea es crítica. Una buena identificación es importante desde varios puntos de vista:

- Materializa con precisión el alcance del proyecto.
- Permite la interlocución con los grupos de usuarios: todos hablan el mismo lenguaje.
- Permite determinar las dependencias precisas entre activos.
- Permite valorar los activos con precisión.
- Permite identificar y valorar las amenazas con precisión.

- Permite determinar qué salvaguardas serán necesarias para proteger el sistema.

Para cada activo hay que determinar una serie de características que lo definen:

- Código, típicamente procedente del inventario.
- Nombre (corto).
- Descripción (larga).
- Tipo (o tipos) que caracterizan el activo.
- Unidad responsable. A veces hay más de una unidad. Por ejemplo, en el caso de aplicaciones cabe diferenciar entre la unidad que la mantiene y la que la explota.
- Persona responsable. Especialmente relevante en el caso de datos. A veces hay más de un responsable. Por ejemplo en caso de datos de carácter personal cabe diferenciar entre el responsable del dato y el operador u operadores que lo manejan.
- Ubicación, técnica (en activos intangibles) o geográfica (en activos materiales).
- Cantidad, si procede como puede ser en el caso de la informática personal (por ejemplo 350 equipos de sobremesa).
- Otras características específicas del tipo de activo.

Tabla 32. Proyecto de análisis de riesgos

MAR: Análisis de riesgos. **MAR.1: Caracterización de los activos.** **MAR.12: Dependencias entre activos.**
Objetivos • Identificar y valorar las dependencias entre activos, es decir la medida en que un activo de orden superior se puede ver perjudicado por una amenaza materializada sobre un activo de orden inferior.
Productos de entrada • Resultados de la tarea T1.2.1, Identificación. • Procesos de negocio. • Diagramas de flujo de datos. • Diagramas de uso.
Productos de salida • Diagrama de dependencias entre activos

Técnicas, prácticas y pautas • Diagramas de flujo de datos. • Diagramas de procesos. • Entrevistas • Reuniones.

Para cada dependencia conviene registrar la siguiente información:

- Estimación del grado de dependencia: hasta un 100%.
- Explicación de la valoración de la dependencia.
- Entrevistas realizadas de las que se ha deducido la anterior estimación

Tabla 33. Registro de información

MAR: Análisis de riesgos. **MAR.1: Caracterización de los activos.** **MAR.12: Dependencias entre activos.**
Objetivos • Identificar en qué dimensión es valioso el activo. • Valorar el coste que para la Organización supondría la destrucción del activo.
Productos de entrada • Resultados de la tarea MAR.11, Identificación de los activos. • Resultados de la tarea MAR.12, Dependencias entre activos.
Productos de salida • Modelo de valor: informe de valor de los activos
Técnicas, prácticas y pautas • Entrevistas • Reuniones

Para la adquisición de este conocimiento puede ser necesario entrevistar a diferentes colectivos dentro de la Organización:

- Dirección o gerencia, que conocen las consecuencias para la misión de la Organización.

- Responsables de los datos, que conocen las consecuencias de sus fallos de seguridad.
- Responsables de los servicios, que conocen las consecuencias de la no prestación del servicio o de su prestación degradada.
- Responsables de sistemas de información y responsables de operación, que conocen las consecuencias de un incidente

Para cada valoración conviene registrar la siguiente información.

- Dimensiones en las que el activo es relevante.
- Estimación de la valoración en cada dimensión.
- Explicación de la valoración.
- Entrevistas realizadas de las que se han deducido las anteriores estimaciones

MAR. 2 – CARACTERIZACIÓN DE LAS AMENAZAS

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

El resultado de esta actividad es el informe denominado “mapa de riesgos”.

Sub-tareas:

Tarea MAR.21: Identificación de las amenazas

Tarea MAR.22: Valoración de las amenazas

El objetivo de estas tareas es caracterizar el entorno al que se enfrenta el sistema, qué puede pasar, qué consecuencias se derivarían y cómo de probable es que pase. Podemos resumirlo en la expresión “conoce a tu enemigo”.

Tabla 34. Caracterización de las amenazas

MAR: Análisis de riesgos **MAR.2: Caracterización de las amenazas** **MAR.21: Identificación de las amenazas**
Objetivos • Identificar las amenazas relevantes sobre cada activo
Productos de entrada • Resultados de la actividad MAR.1, Caracterización de los activos • Informes relativos a defectos en los productos. Esto es, informes de vulnerabilidades.
Productos de salida • Relación de amenazas posibles.
Técnicas, prácticas y pautas • Catálogos de amenazas. • Árboles de ataque. • Entrevistas. • Reuniones

En esta tarea se identifican las amenazas significativas sobre los activos identificados, tomando en consideración:

- El tipo de activo.
- Las dimensiones en que el activo es valioso.
- La experiencia de la Organización.
- Los defectos reportados por los fabricantes y organismos de respuesta a incidentes de seguridad (CERTS)

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- Explicación del efecto de la amenaza.
- Entrevistas realizadas de las que se ha deducido la anterior estimación.
- Antecedentes, si los hubiera, bien en la propia Organización, bien en otras organizaciones que se haya considerado relevantes.

Tabla 35. Amenazas identificadas.

MAR: Análisis de riesgos **MAR.2: Caracterización de las amenazas** **MAR.21: Identificación de las amenazas**
Objetivos • Estimar la frecuencia de ocurrencia de cada amenaza sobre cada activo • Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse
Productos de entrada • Resultados de la tarea MAR2.1, Identificación de las amenazas. • Series históricas de incidentes. • Informes de defectos en los productos. • Antecedentes: incidentes en la Organización
Productos de salida • Mapa de riesgos: informe de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos
Técnicas, prácticas y pautas Árboles de ataque. Entrevistas. Reuniones

En esta tarea se valoran las amenazas identificadas en la tarea anterior, tomando en consideración:

- La experiencia (historia) universal.
- La experiencia (historia) del sector de actividad.
- La experiencia (historia) del entorno en que se ubican los sistemas.
- La experiencia (historia) de la propia Organización.
- Los informes anexos a los reportes de defectos proporcionados por los fabricantes y organismos de respuesta a incidentes de seguridad (CERTS).

Para cada amenaza sobre cada activo conviene registrar la siguiente información:

- Estimación de la frecuencia de la amenaza
- Estimación del daño (degradación) que causaría su materialización
- Explicación de las estimaciones de frecuencia y degradación
- Entrevistas realizadas de las que se han deducido las anteriores estimaciones

MAR. 3 – CARACTERIZACIÓN DE LAS SALVAGUARDAS

Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar.

El resultado de esta actividad se concreta en varios informes:

- Declaración de aplicabilidad.
- Evaluación de salvaguardas.
- Insuficiencias (o vulnerabilidades del sistema de protección).

Sub-tareas:

Tarea MAR.31: Identificación de las salvaguardas pertinentes

Tarea MAR.32: Valoración de las salvaguardas.

El objetivo de estas tareas es doble: saber qué necesitamos para proteger el sistema y saber si tenemos un sistema de protección a la altura de nuestras necesidades.

Tabla 36. Necesidades para la protección del sistema

MAR: Análisis de riesgos. **MAR.3: Caracterización de las salvaguardas.** **MAR.31: Identificación de las salvaguardas pertinentes.**
Objetivos • Identificar las salvaguardas convenientes para proteger el sistema
Productos de entrada • Modelo de activos del sistema. • Modelo de amenazas del sistema. • Indicadores de impacto y riesgo residual. • Informes de productos y servicios en el mercado.
Productos de salida • Declaración de aplicabilidad: relación justificada de las salvaguardas necesarias. • Relación de salvaguardas desplegadas.
Técnicas, prácticas y pautas • Catálogos de salvaguardas. • Árboles de ataque. • Entrevistas. • Reuniones.

Para cada salvaguarda conviene registrar la siguiente información:

- Descripción de la salvaguarda y su estado de implantación.
- Descripción de las amenazas a las que pretende hacer frente.
- Entrevistas realizadas de las que se ha deducido la anterior información.

Para determinar las salvaguardas pertinentes es frecuente recurrir a catálogos de salvaguardas o al consejo de personas expertas. De una u otra forma dispondremos de una colección de salva-guardas para elegir, de forma que el complejo problema de encontrar lo que necesitamos se reduce al problema más sencillo de descartar lo que no necesitamos.

En el proceso de descarte hay varias razones para eliminar una salvaguarda propuesta.

- Porque no es apropiada para el activo que necesitamos defender
- Porque no es apropiada para la dimensión de seguridad que necesitamos defender
- Porque no es efectiva oponiéndose a la amenaza que necesitamos contrarrestar
- Porque es excesiva para el valor que tenemos que proteger (desproporcionada)
- Porque disponemos de medidas alternativas.

Tabla 37. Salvaguardas.

MAR: Análisis de riesgos **MAR.3: Caracterización de las salvaguardas** **MAR.32: Valoración de las salvaguardas**
Objetivos • Determinar la eficacia de las salvaguardas pertinentes.
Productos de entrada • Inventario de salvaguardas derivado de la tarea MAR.31.
Productos de salida • Evaluación de salvaguardas: informe de salvaguardas desplegadas, caracterizadas por su grado de efectividad. • Informe de insuficiencias (o vulnerabilidades): relación de salvaguardas que deberían estar pero no están desplegadas o están desplegadas de forma insuficiente.
Técnicas, prácticas y pautas • Entrevistas. • Reuniones. • Valoración Delphi.

En esta tarea se valora la efectividad de las salvaguardas identificadas en la tarea anterior, tomando en consideración:

- La idoneidad de la salvaguarda para el fin perseguido.
- La calidad de la implantación.
- La formación de los responsables de su configuración y operación.
- La formación de los usuarios, si tienen un papel activo.
- La existencia de controles de medida de su efectividad.
- La existencia de procedimientos de revisión regular

Para cada salvaguarda conviene registrar la siguiente información:

- Estimación de su eficacia para afrontar aquellas amenazas.
- Explicación de la estimación de eficacia.
- Entrevistas realizadas de las que se ha deducido la anterior estimación.

MAR. 4 – ESTIMACIÓN DEL ESTADO DE RIESGO

Esta actividad procesa todos los datos recopilados en las actividades anteriores para.

- Realizar un informe del estado de riesgo: estimación de impacto y riesgo.
- Realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas.

Sub-tareas:

Tarea MAR.41: Estimación del impacto.

Tarea MAR.42: Estimación del riesgo.

Es frecuente que las tareas relacionadas con los activos (MAR.1) se realicen concurrentemente con las tareas relacionadas con las amenazas sobre dichos activos (MAR.2) e identificación de las salvaguardas actuales (MAR.3), simplemente porque suelen coincidir las personas y es difícil que el interlocutor no tienda de forma natural a tratar cada activo “verticalmente”, viendo todo lo que le afecta antes de pasar al siguiente.

El objetivo de estas tareas es disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo).

Tabla 38. Análisis de la estimación del estado de riesgo.

MAR: Análisis de riesgos. **MAR.4: Estimación del estado de riesgo.** **MAR.41: Estimación del impacto.**
Objetivos • Determinar el impacto potencial al que está sometido el sistema. • Determinar el impacto residual al que está sometido el sistema.
Productos de entrada • Resultados de la actividad MAR.1, Caracterización de los activos. • Resultados de la actividad MAR.2, Caracterización de las amenazas. • Resultados de la actividad MAR.3, Caracterización de las salvaguardas.
Productos de salida • Informe de impacto (potencial) por activo. • Informe de impacto residual por activo.
Técnicas, prácticas y pautas • Análisis mediante tablas. • Análisis algorítmico.

En esta tarea se estima el impacto al que están expuestos los activos del sistema:

- El impacto potencial, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas
- El impacto residual, al que está expuesto el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas

Tabla 39. Estimación del Estado de riesgo

MAR: Análisis de riesgos. **MAR.4: Estimación del estado de riesgo.** **MAR.42: Estimación del riesgo.**
Objetivos • Determinar el riesgo potencial al que está sometido el sistema • Determinar el riesgo residual al que está sometido el sistema
Productos de entrada • Resultados de la actividad MAR.1, Caracterización de los activos. • Resultados de la actividad MAR.2, Caracterización de las amenazas. • Resultados de la actividad MAR.3, Caracterización de las salvaguardas. • Resultados de la actividad MAR.4, Estimaciones de impacto.

Tabla 40. Estimación del riesgo Objetivos.

MAR: Análisis de riesgos. **MAR.4: Estimación del estado de riesgo.** **MAR.42: Estimación del riesgo.**
Objetivos • Informe de riesgo (potencial) por activo. • Informe de riesgo residual por activo.
Técnicas, prácticas y pautas • Análisis mediante tablas. • Análisis algorítmico.

En esta tarea se estima el riesgo al que están sometidos los activos del sistema:

- El riesgo potencial, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas
- El riesgo residual, al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como la eficacia de las salvaguardas actualmente desplegadas.

6.10 DOCUMENTACIÓN

6.10.1. DOCUMENTACIÓN INTERMEDIA

- Resultados de las entrevistas.
- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Información existente utilizable por el proyecto (por ejemplo inventario de activos)
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.
- Informes y evaluaciones de defectos de los productos, procedentes de fabricantes o de centros de respuesta a incidentes de seguridad (CERTs).

6.10.2. DOCUMENTACIÓN FINAL

MODELO DE VALOR: Informe que detalla los activos, sus dependencias, las dimensiones en las que son valiosos y la estimación de su valor en cada dimensión.

MAPA DE RIESGOS: Informe que detalla las amenazas significativas sobre cada activo, caracterizándolas por su frecuencia de ocurrencia y por la degradación que causaría su materialización sobre el activo.

DECLARACIÓN DE APLICABILIDAD: Informe que recoge las contramedidas que se consideran apropiadas para defender el sistema de información bajo estudio.

EVALUACIÓN DE SALVAGUARDAS: Informe que detalla las salvaguardas existentes calificándolas en su eficacia para reducir el riesgo que afrontan.

INFORME DE INSUFICIENCIAS O VULNERABILIDADES: Informe que detalla las salvaguardas necesarias pero ausentes o insuficientemente eficaces.

ESTADO DE RIESGO: Informe que detalla para cada activo el impacto y el riesgo, potenciales y residuales, frente a cada amenaza.

Es fundamental entender las razones que llevan a una valoración determinada de riesgo para que el proceso de gestión de riesgos esté bien fundamentado. El proceso de gestión de riesgos partirá de estas valoraciones para atajar el riesgo o reducirlo a niveles aceptables.

Tabla 41. Identificación de estado de riesgos

γ	Actividad	Tarea
	Se han identificado los activos esenciales: información que se trata y servicios que se prestan.	MAR.11
	Se han valorado las necesidades o niveles de seguridad requeridos por cada activo esencial en cada dimensión de seguridad.	MAR.13
	Se han identificado los demás activos del sistema.	MAR.11
	Se han establecido el valor (o nivel requerido de seguridad) de los demás activos en función de su relación con los activos esenciales (por ejemplo, mediante identificación de las dependencias).	MAR.12
	Se han identificado las amenazas posibles sobre los activos.	MAR.21
	Se han estimado las consecuencias que se derivarían de la materialización de dichas amenazas.	MAR.22

	Se ha estimado la probabilidad de que dichas amenazas se materialicen,	MAR.23
	Se han estimado los impactos y riesgos potenciales, inherentes al sistema.	MAR.4
	Se han identificado las salvaguardas apropiadas para atajar los impactos y riesgos potenciales.	MAR.31
	Se ha valorado el despliegue de las salvaguardas identificadas.	MAR.32
	Se han estimado los valores de impacto y riesgo residuales, que es el nivel de impacto y riesgo que aún soporta el sistema tras el despliegue de las salvaguardas	MAR.4

6.11 PROCESO DE GESTIÓN DE RIESGO

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por diversos factores:

- La gravedad del impacto y/o del riesgo.
- Las obligaciones a las que por ley esté sometida la Organización.
- Las obligaciones a las que por reglamentos sectoriales esté sometida la Organización.
- Las obligaciones a las que por contrato esté sometida la Organización.

Dentro del margen de maniobra que permita este marco, pueden aparecer consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible tales como:

- Imagen pública de cara a la Sociedad.
- Política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etc.
- Relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.
- Relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia.
- Relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, etc.

- Nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad.
- Acceso a sellos o calificaciones reconocidas de seguridad.

Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose:

- Es **crítico** en el sentido de que requiere atención urgente.
- Es **grave** en el sentido de que requiere atención.
- Es **apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento.
- Es **asumible** en el sentido de que no se van a tomar acciones para atajarlo.

La opción 4.5, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:

- Cuando el impacto residual es asumible.
- Cuando el riesgo residual es asumible.
- Cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales.

La calificación de los riesgos tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones.

6.11.1. CONCEPTOS

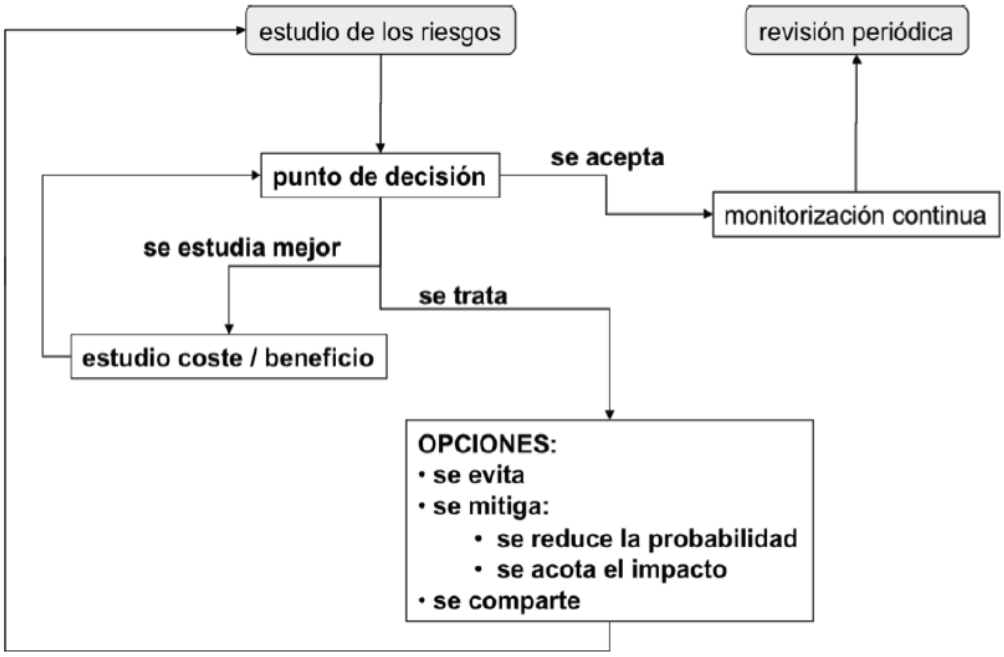
Mediante el análisis de riesgos se determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio, el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible (lo peor que puede ocurrir), mientras que el riesgo refleja el daño probable (lo que probablemente ocurra).

El resultado del análisis es sólo un análisis. A partir del disponemos de información para tomar decisiones conociendo lo que queremos proteger (activos valorados=, de qué lo queremos proteger (amenazas valoradas) y qué hemos hecho por protegerlo (salvaguardas valoradas). Todo ello sintetizado en los valores de impacto y riesgo.

A partir de aquí, las decisiones son de Órganos de administradores de Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo que actuara en dos pasos.

A continuación se resume las posibles decisiones que se pueden tomar tras haber estudiado los riesgos.

Figura 17. Decisiones de tratamiento de los riesgos.



6.11.2. EVALUACIÓN: INTERPRETACIÓN DE LOS VALORES DE IMPACTO Y RIESGO RESIDUALES

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables. Los párrafos siguientes se refieren conjuntamente a impacto y riesgo. Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer. Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho; es decir, de las vulnerabilidades que presenta el sistema. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a

esta relación de tareas pendientes, que se denomina Informe de Insuficiencias o de vulnerabilidades

6.11.3. ACEPTACIÓN DEL RIESGO

La Dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión).

6.11.4. TRATAMIENTO

La Dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información. Hay dos grandes opciones:

- Reducir el riesgo residual (aceptar un menor riesgo).
- Ampliar el riesgo residual (aceptar un mayor riesgo).

Para tomar una u otra decisión hay que enmarcar los riesgos soportados por el sistema de información dentro de un contexto más amplio que cubre un amplio espectro de consideraciones de las que podemos apuntar algunas sin pretender ser exhaustivos:

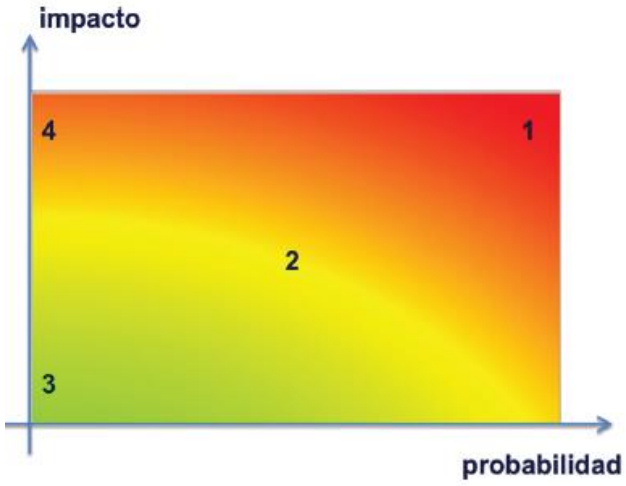
- Cumplimiento de obligaciones; sean legales, regulación pública o sectorial, compromisos internos, misión de la Organización, responsabilidad corporativa, etc.
- Posibles beneficios derivados de una actividad que en sí entraña riesgos condicionantes técnicos, económicos, culturales, políticos, etc.
- Equilibrio con otros tipos de riesgos: comerciales, financieros, regulatorios, medioambientales, laborales.

En condiciones de **riesgo residual extremo**, casi la única opción es reducir el riesgo.

En condiciones de **riesgo residual aceptable**, se optar entre aceptar el nivel actual o ampliar el riesgo asumido. En cualquier caso hay que mantener una monitorización

continua de las circunstancias para que el riesgo formal cuadre con la experiencia real y reaccionemos ante cualquier desviación significativa.

Figura 18. Zona de riesgo



En condiciones de **riesgo residual medio**, podemos observar otras características como las pérdidas y ganancias que pueden verse afectadas por el escenario presente, o incluso analizar el estado del sector en el que operamos para compararnos con la "norma".

En términos de las zonas de riesgo que se expusieron anteriormente.

- **Zona 1** – riesgos muy probables y de muy alto impacto; posiblemente nos planteemos sacarlos de esta zona
- **Zona 2** – riesgos de probabilidad relativa e impacto medio; se pueden tomar varias opciones
- **Zona 3** – riesgos improbables y de bajo impacto; o los dejamos como están, o permitimos que suban a mayores si ello nos ofreciera alguna ventaja o beneficio en otro terreno.
- **Zona 4** – riesgos improbables pero de muy alto impacto; suponen un reto de decisión pues su improbabilidad no justifica que se tomen medidas preventivas, pero su elevado impacto exige que tengamos algo previsto para reaccionar; es decir, hay que poner el énfasis en medidas de reacción para limitar el daño y de recuperación del desastre si ocurriera.

También conviene considerar la incertidumbre del análisis. Hay veces que sospechamos las consecuencias, pero hay un amplio rango de opiniones sobre su magnitud

(incertidumbre en el impacto). En otras ocasiones la incertidumbre afecta a la probabilidad. Estos escenarios suelen afectar a las zonas 4 y 3, pues cuando la probabilidad es alta, normalmente adquirimos experiencia, propia o ajena, con rapidez y salimos de la incertidumbre. En cualquier caso, toda incertidumbre debe considerarse como mala y debemos hacer algo:

- Buscar formas de mejorar la previsión, típicamente indagando en foros, centros de respuesta a incidentes o expertos en la materia.
- Evitar el riesgo cambiando algún aspecto, componente o arquitectura del sistema
- Tener preparados sistemas de alerta temprana y procedimientos flexibles de contención, limitación y recuperación del posible incidente.

A veces que estos escenarios de incertidumbre ocurren en un terreno en el que hay obligaciones de cumplimiento y la propia normativa elimina o reduce notablemente las opciones disponibles; es decir, el sistema se protege por obligación más que por certidumbre del riesgo.

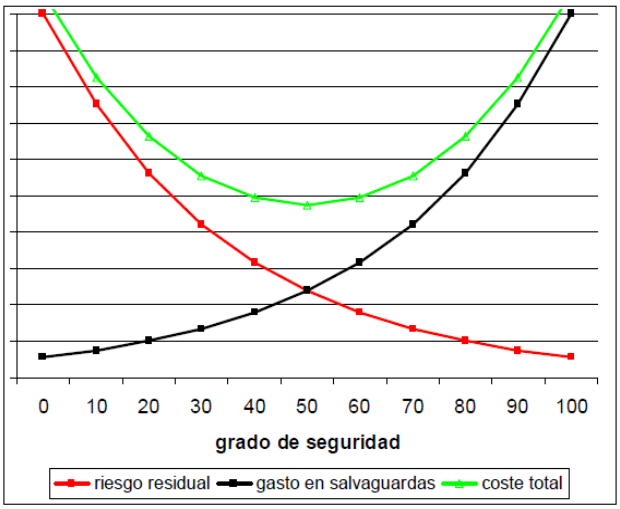
A la vista de estas consideraciones se tomarán las decisiones de tratamiento.

6.11.5. ESTUDIO CUANTITATIVO DE COSTES / BENEFICIOS

Es de sentido común que no se puede invertir en salvaguardas más allá del valor que queremos proteger.

Aparecen en la práctica gráficos como el siguiente que ponen uno frente al otro el coste de la in-seguridad (lo que costaría no estar protegidos) y el coste de las salvaguardas.

Figura 19. Relación entre el gasto en seguridad y el riesgo residual



Esta grafica refleja cómo al avanzar de un grado de seguridad 0 hacia un grado de seguridad del 100%, el coste de la inseguridad (el riesgo) disminuye, mientras que el coste de la inversión en salvaguardas aumenta. Es intencionado el hecho de que el riesgo caiga fuertemente con pequeñas inversiones y que el coste de las inversiones se dispare para alcanzar niveles de seguridad cercanos al 100%. La curva central suma el coste para la Organización, bien derivado del riesgo (baja seguridad), bien derivado de la inversión en protección. De alguna forma existe un punto de equilibrio entre lo que se arriesga y lo que se invierte en defensa, punto al que hay que tender si la única consideración es económica.

Pero llevar el sentido común a la práctica no es evidente, ni por la parte del cálculo del riesgo, ni por la parte del cálculo del coste de las salvaguardas. En otras palabras, la curva anterior es conceptual y no se puede dibujar en un caso real.

En la práctica, cuando hay que protegerse de un riesgo que se considera significativo, aparecen varios escenarios hipotéticos:

E0: si no se hace nada.

E1: si se aplica un cierto conjunto de salvaguardas

E2: si se aplica otro conjunto de salvaguardas

Y así N escenarios con diferentes combinaciones de salvaguardas.

El análisis económico tendrá como misión decidir entre estas opciones, siendo E0 (seguir como estamos) una opción posible, que pudiera estar justificada económicamente.

En cada escenario hay que estimar a lo largo del tiempo el coste que va a suponer. Para poder agregar costes, se contabilizan como valores negativos las pérdidas de dinero y como valores positivos las entradas de dinero. Considerando los siguientes componentes:

- (Recurrente) riesgo residual.

- (Una vez) coste de las salvaguardas.

- (Recurrente) coste anual de mantenimiento de las salvaguardas

+ (Recurrente) mejora en la productividad.

+ (Recurrente) mejoras en la capacidad de la Organización para prestar nuevos servicios, conseguir mejores condiciones de los proveedores, entrar en asociación con otras organizaciones, etc.

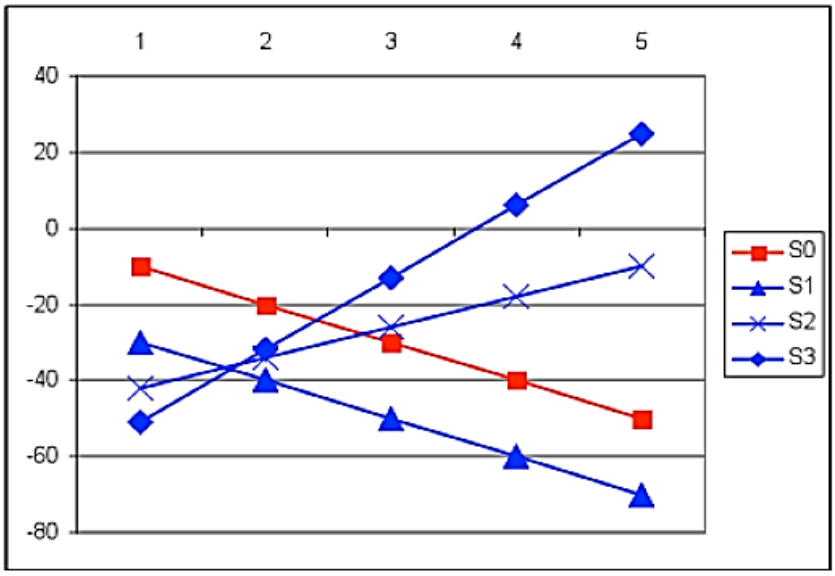
El escenario E0 es muy simple: todos los años se afronta un gasto marcado por el riesgo, que se acumula año tras año.

En los demás escenarios, hay cosas que suman y cosas que restan, pudiendo darse varias situaciones como las recogidas en la gráfica siguiente. Se presentan valores acumulados a lo largo de un periodo de 5 años. La pendiente de la recta responde a los costes recurrentes. El valor el primer año corresponde a los costes de implantación.

Figura 20. Tratamiento de riesgos.

						año				
	riesgo (anual)	coste (inicial)	coste (anual)	mejora (anual)	otros (anual)	1	2	3	4	5
E0	10	0	0	0	0	-10	-20	-30	-40	-50
E1	5	20	5	0	0	-30	-40	-50	-60	-70
E2	2	50	10	20	0	-42	-34	-26	-18	-10
E3	1	70	15	35	0	-51	-32	-13	6	25

Figura 21. Decisiones de tratamiento de riesgos.



- En E0 se sabe lo que cada año (se estima que) se pierde
- El escenario E1 aparece como mala idea, pues supone un gasto añadido el primer año; pero este gasto no se recupera en años venideros.
- No así el escenario E2 que, suponiendo un mayor desembolso inicial, empieza a ser rentable a partir del cuarto año.
- Más atractivo aún es el escenario E3 en el que a costa de un mayor desembolso inicial, se empieza a ahorrar al tercer año, e incluso se llega a obtener beneficios operativos a partir del quinto año. Se puede decir que en escenario E3 se ha hecho una buena inversión.

6.11.6. ESTUDIO CUALITATIVO DE COSTES / BENEFICIOS

Cuando el análisis es cualitativo, en la balanza de costes beneficios aparecen aspectos intangibles que impiden el cálculo de un punto numérico de equilibrio.

Entre los aspectos intangibles se suelen contemplar:

- Aspectos reputaciones o de imagen
- Aspectos de competencia: comparación con otras organizaciones de mismo ámbito de actividad
- Cumplimiento normativo, que puede ser obligatorio o voluntario
- Capacidad de operar

- Productividad

Estas consideraciones llevan a contemplar diversos escenarios para determinar el balance neto. Por ejemplo, el no adoptar medidas puede exponernos a un cierto riesgo que causaría mala imagen; pero si la solución preventiva causa también mala imagen o supone un merma notable de oportunidades o de productividad, hay que buscar un punto de equilibrio, eligiendo una combinación de medidas que sea asumible.

6.11.7. ESTUDIO MIXTO DE COSTES / BENEFICIOS

En análisis de riesgos meramente cualitativos, la decisión la marca el balance de costes y beneficios intangibles, si bien siempre hay que hacer un cálculo de lo que cuesta la solución y cerciorarse de que el gasto es asumible. De lo contrario, la supuesta solución no es una opción. Es decir, primero hay que pasar el filtro económico y luego elegir la mejor de las soluciones factibles.

6.11.8. OPCIONES DE TRATAMIENTO DEL RIESGO: ELIMINACIÓN

La eliminación de la fuente de riesgo es una opción frente a un riesgo que no es aceptable.

En un sistema podemos eliminar varias cosas, siempre que no afecten a la esencia de la Organización. Es extremadamente raro que podamos prescindir de la información o los servicios esenciales por cuanto constituyen la misión de la Organización. Cambiar estos activos supone reorientar la misión de la Organización.

Más viable es prescindir de otros componentes no esenciales, que están presentes simple y llanamente para implementar la misión, pero no son parte constituyente de la misma. Esta opción puede tomar diferentes formas:

- Eliminar cierto tipo de activos, emplean otros en su lugar. Por ejemplo: cambiar de sistema operativo, de fabricante de equipos.
- Reordenar la arquitectura del sistema (el esquema de dependencias en nuestra terminología) de forma que alteremos el valor acumulado en ciertos activos expuestos a grandes amenazas. Por ejemplo: segregar redes, desdoblar equipos para atender a necesidades concretas, alejando lo más valioso de lo más expuesto.

6.11.9. OPCIONES DE TRATAMIENTO DEL RIESGO: MITIGACIÓN

La mitigación del riesgo se refiere a una de dos opciones:

- Reducir la degradación causada por una amenaza (a veces se usa la expresión 'acotar el impacto')
- Reducir la probabilidad de que una amenaza de materializa

En ambos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas. En términos de madurez de las salvaguardas: subir de nivel.

Algunas salvaguardas, notablemente las de tipo técnico, se traducen en el despliegue de más equipamiento que se convierte a su vez en un activo del sistema. Estos nuevos activos también acumularán valor del sistema y estarán a su vez sujetos a amenazas que pueden perjudicar a los activos esenciales.

Hay pues que repetir el análisis de riesgos, ampliándolo con el nuevo despliegue de medios y, por supuesto, cerciorarse de que el riesgo del sistema ampliado es menor que el del sistema original; es decir, que las salvaguardas efectivamente disminuyen el estado de riesgo de la Organización.

6.11.10. OPCIONES DE TRATAMIENTO DEL RIESGO: COMPARTICIÓN

Tradicionalmente se ha hablado de 'transferir el riesgo'. Como la transferencia puede ser parcial o total, es más general hablar de 'compartir el riesgo'.

Hay dos formas básicas de compartir riesgo:

- **Riesgo cualitativo**: se comparte por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el componen-te técnico; y otras legales según el acuerdo que se establezca de prestación del servicio.
- **Riesgo cuantitativo:** se comparte por medio de la contratación de seguros, de forma que a cambio de una prima, el tomador reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias. Hay multitud de tipos y cláusulas de seguros para concretar el grado de responsabilidad de cada una de las partes.

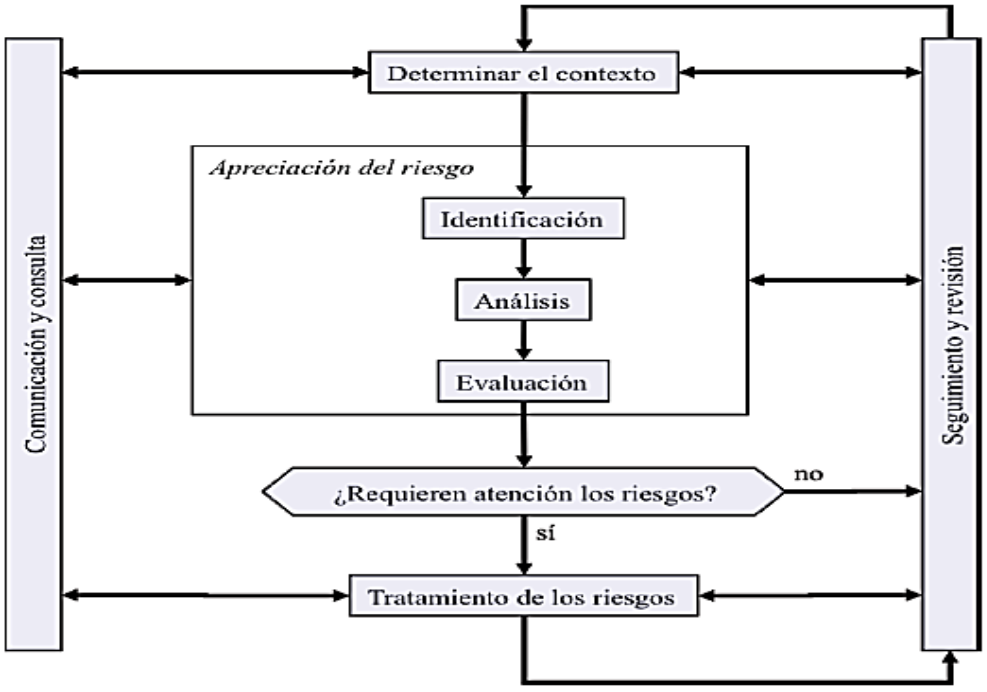
Cuando se comparten riesgos cambia, bien el conjunto de componentes del sistema, bien su valoración, requiriéndose un nuevo análisis del sistema resultante.

6.11.11. OPCIONES DE TRATAMIENTO DEL RIESGO: FINANCIACIÓN

Cuando se acepta un riesgo, la Organización hará bien en reservar fondos para el caso de que el riesgo se concrete y haya que responder de sus consecuencias. A veces de habla de ‘fondos de contingencia’ y también puede ser parte de los contratos de aseguramiento. Normalmente esta opción no modifica nada del sistema y nos vale el análisis de riesgos disponible.

6.12 FORMALIZACIÓN DE LAS ACTIVIDADES

Figura 22. Proceso de gestión de riesgos.



6.12.1. ROLES Y FUNCIONES

En el proceso de gestión de riesgos aparecen varios actores. Los siguientes párrafos intentan identificarlos de forma superficial y explicitar cuáles son sus funciones y responsabilidades.

6.12.2. ÓRGANOS DE GOBIERNOS

En este título se incluyen aquellos órganos colegiados o unipersonales que deciden la misión y los objetivos de la Organización.

Típicamente se incluyen en esta categoría los altos cargos de los organismos.

Cuando existe un Comité de Seguridad de la Información, suele aparecer en este nivel.

Estos órganos tienen la autoridad última para aceptar los riesgos con que se opera. Se dice que son los "propietarios del riesgo".

6.12.3. DIRECCIÓN EJECUTIVA

Este aspecto toma decisiones que concretan cómo alcanzar los objetivos de negocio marcados por los órganos de gobierno.

Aquí se incluye los responsables de unidades de negocio, los responsables de la calidad de los servicios prestados por la organización, etc.

6.12.3.1. DIRECCIÓN OPERACIONAL

Toman decisiones prácticas para materializar las indicaciones dadas por los órganos ejecutivos.En esta categoría incluyen los responsables de operaciones de producción de explotación y similares.

6.12.4. ESQUEMA NACIONAL DE SEGURIDAD

En el Esquema Nacional de Seguridad se identifican ciertos roles que pueden verse involucrados en el proceso de gestión de riesgos:

6.12.4.1. RESPONSABLE DE LA INFORMACIÓN

Típicamente a nivel de gobierno. Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por la Universidad Nacional de Chimborazo.

A este nivel se suele concretar la responsabilidad sobre datos de carácter personal y sobre la clasificación de la información.

6.12.4.2. RESPONSABLE DEL SERVICIO

Típicamente a nivel de gobierno, aunque a veces baja a nivel ejecutivo. Tiene la responsabilidad última de determinar los niveles de servicio aceptables por la Universidad Nacional de Chimborazo.

A veces este role lo asume el Comité de Seguridad de la Información.

6.12.4.3. RESPONSABLE DE LA SEGURIDAD

Típicamente a nivel ejecutivo, actuando como engranaje entre las directrices emanadas de los responsables de la información y los servicios, y el responsable del sistema. A su vez funciona como supervisor de la operación del sistema y vehículo de reporte al Comité de Seguridad de la Información.

A veces se denomina a esta figura CISO (*Chief Information Security Officer*).

En lo que respecta al proceso de gestión de riesgos, es la persona que traslada la valoración de los activos esenciales, que aprueba la declaración de aplicabilidad de salvaguardas, los procedimientos operativos, los riesgos residuales y los planes de seguridad. En esta función de informante, suele ser la persona encargada de elaborar los indicadores del esto de seguridad del sistema.

6.12.4.4. RESPONSABLE DEL SISTEMA

A nivel operacional. Toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día. En lo que respecta al proceso de gestión de riesgos, es la persona que propone la arquitectura de seguridad, la declaración de aplicabilidad de salvaguardas, los procedimientos operativos y los planes de seguridad. También es la persona responsable de la implantación y correcta operación de las salvaguardas.

6.12.4.5. ADMINISTRADORES Y OPERADORES

Son las personas encargadas de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.

6.12.5. MATRIZ RACI

La matriz de la asignación de responsabilidades (RACI por las iniciales, en inglés, de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo). De esta manera se logra asegurar que cada una de las tareas esté asignada a un individuo o en este caso aplicado al Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo.

Tabla 42. Roles en procesos distribuidos.

ROL		DESCRIPCION.
R	*Responsible.*	Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista sólo un R, si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RASCI. Es quien debe ejecutar las tareas.
A	*Acconuntable.*	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las tareas.
C	*Consulted.*	Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I	*Informed.*	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Tabla 43. Tareas relacionadas con la gestión de riesgo.

Tarea	Direc-ción	RINFO	RSERV	RSEG	RSIS	ASS
niveles de seguridad requeridos por la informa-ción		A	I	R	C	
niveles de seguridad requeridos por el servicio		I	A	R	C	
análisis de riesgos		I	I	A/R	C	
declaración de aplicabilidad		I	I	A/R	C	
aceptación del riesgo residual	I	A	A	R	I	
implantación de las medidas de seguridad		I	I	C	A	R
					C	R

Tarea	Direc-ción	RINFO	RSERV	RSEG	RSIS	ASS
estado de seguridad del sistema	I	I	I	A	I	R
planes de mejora de la seguridad				A	C	
planes de concienciación y formación				A	C	
planes de continuidad				C	A	
seguridad en el ciclo de vida				C	A	

Donde

- Dirección – Alta Dirección, Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo.
- RINFO – Responsable de la Información.
- RSERV – Responsable del Servicio.
- RSEG – Responsable de la Seguridad.
- RSIS – Responsable (operacional) del Sistema.
- ASS – Administrador(es) de la Seguridad del Sistema.

6.12.5.1. CONTEXTO

Hay que documentar el entorno en el que se desenvuelve el Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo, esto incluye aspectos internos como externos.

Dentro de este tema se identifica obligaciones, reglamentarias como las que se destacan a continuación.

- Tratamiento de datos de carácter personal.
- Tratamiento de información clasificada.
- Tratamiento de información y productos sometidos a derechos de propiedad intelectual Prestación de servicios públicos.
- Operación de infraestructuras críticas.

6.12.5.2. CRITERIOS

Múltiples aspectos relacionados con los riesgos son objeto de estimaciones. Conviene que las estimaciones sean lo más objetivas que sea posible o. al menos, que sean

repetibles, explicables y comparables. En particular conviene establecer escalas de valoración para

- Valorar los requisitos de seguridad de la información.
- Valorar los requisitos de disponibilidad de los servicios.
- Estimar la probabilidad de una amenaza.
- Estimar las consecuencias de un incidente de seguridad.
- Estimar el nivel de riesgo a partir de las estimaciones de impacto y probabilidad.

Establecer reglas y/o criterios para tomar decisiones de tratamiento.

- Umbrales de impacto.
- Umbrales de probabilidad.
- Umbrales combinados de impacto y probabilidad.
- Umbrales de nivel de riesgo.
- Impacto en la reputación de la Organización o de las personas responsables.
- Impacto en la posición de competencia.
- Impacto comparado con otras áreas de riesgo: financiero, regulatorio, medioambiental, seguridad industrial, etc.
- Amenazas especialmente sensibles (puede ser por motivos técnicos, porque adolecen de una amplia incertidumbre o porque su ocurrencia causaría una notable alarma social con grave daño para la reputación o la continuidad de las operaciones de la Organización, incluso si sus consecuencia técnicas o materiales son modestas)

6.12.5.3. DECISIÓN DE TRATAMIENTOS

Hay múltiples formas de reducir el riesgo:

- Eliminar el riesgo eliminando sus causas: información tratada, servicios prestados, arquitectura del sistema.
- Reducir o limitar el impacto.
- Reducir la probabilidad de que la amenaza ocurra.
- En el caso de amenazas derivadas de defectos de los productos (vulnerabilidades técnicas): reparar el producto (por ejemplo, aplicar los parches del fabricante).
- Implantar nuevas salvaguardas o mejorar la calidad de las presentes.
- Externalizar partes del sistema.
- Contratar seguros de cobertura

A veces la decisión consiste en aceptar un incremento del riesgo:

- Aceptando trabajar con nueva información o prestar nuevos servicios.
- Alterando la arquitectura del sistema
- Reduciendo las salvaguardas presentes
- Reduciendo la calidad de las salvaguardas presentes (es decir, dedicando menos recursos)

6.12.5.4. COMUNICACIÓN Y CONSULTA

Antes de tomar ninguna decisión relativa al tratamiento de un riesgo hay que entender para qué se usa el sistema y cómo se usa.

Esto quiere decir mantener un contacto fluido con varios actores.

- Los organismos administrativos y decisión, pues toda decisión debe estar alineada con la misión del Centro de Tecnología Educativa.
- Los usuarios y técnicos de sistemas, pues toda decisión debe tener en cuenta su impacto en la productividad y sobre la usabilidad del sistema.
- Los proveedores, pues toda decisión debe contar con su colaboración

Hay que tener en cuenta que cualquier medida de seguridad que merme la productividad, dificulte la operación del sistema, o requiera una elaborada formación de los usuarios, está condenada al fracaso.

Toda medida de seguridad debe estar.

- Apoyada por la Dirección.
- Amparada por la Política de Seguridad de la Organización.
- Apoyada por normativa clara y legible, ampliamente divulgada.
- Explicada de forma breve, clara y directa en procedimientos operativos de seguridad

Por último es interesante disponer de indicadores que midan el grado de aceptación por parte de los usuarios, identificando tanto el grado de cumplimiento como los problemas que causa su seguimiento.

6.12.5.5. SEGUIMIENTO Y REVISIÓN

El análisis de los riesgos es un ejercicio formal, basado en múltiples estimaciones y valoraciones que pueden no compadecerse con la realidad. Es absolutamente necesario

que el sistema esté bajo monitorización permanente. Los indicadores de impacto y riesgo potenciales son útiles para decidir qué puntos deben ser objeto de monitorización.

Y debe estar preparado un sistema de detección precoz de posibles incidentes (en base a indicadores predictivos) así como un sistema de reacción a incidentes de seguridad.

Se procurará disponer de un conjunto de indicadores clave de riesgo (KRI – *Key Risk Indicators*).

Estos indicadores:

- Son propuestos por el Responsable de la Seguridad.
- Su definición es acordada por el Responsable de la Seguridad y el propietario del riesgo; la definición indicará exactamente:

✓ En qué medidas se basan.
✓ Cuál es el algoritmo de cálculo.
✓ La periodicidad de evaluación y.
✓ Los umbrales de aviso y alarma (atención urgente).

- Se le presentan al responsable correspondiente.

✓ Rutinariamente, con la periodicidad establecida.
✓ Puntualmente, por demanda del propietario del riesgo medido.
✓ Y extraordinariamente cuando se supera un umbral de riesgo

- Estos indicadores estarán a disposición de los auditores.

6.12.5.6. SERVICIOS SUBCONTRATADOS

Esto se da cuando se depende de terceros, es esencial conocer el desempeño de los proveedores contando con un buen sistema de reporte, escalado y resolución de los incidentes de seguridad, como en el establecimiento de los indicadores predictivos

Del análisis de dependencias realizado durante el análisis de riesgos, se toma la información de en qué medida y en qué dimensiones de seguridad se depende de cada proveedor externo. De esta información se sigue qué elementos debemos monitorizar para asegurarnos que satisfacen nuestros requisitos de seguridad.

6.12.6. DOCUMENTACIÓN DEL PROCESO

DOCUMENTACIÓN INTERNA

- Definición de roles, funciones y esquemas de reporte
- Criterios de valoración de la información
- Criterios de valoración de los servicios
- Criterios de evaluación de los escenarios de impacto y riesgo

DOCUMENTACIÓN PARA OTROS

- Plan de seguridad.

6.13 PROYECTO DE ANÁLISIS DE RIESGOS

Las actividades de análisis de riesgo son recurrentes dentro del proceso de gestión, ya que hay que estar continuamente revisando el análisis y manteniéndolo al día. Podemos llamar 'análisis de riesgos marginales' a las salidas de estas actividades que, generalmente, requieren poco volumen de trabajo en cada iteración.

Pero antes de pasar a las iteraciones marginales, hay que disponer de un análisis de riesgos que sirva de plataforma de trabajo. Esto ocurre la primera vez que se realiza un análisis de riesgos y cuando la política de la organización marque que se prepare una nueva plataforma, sea por razones formales o porque los cambios acumulados justifican una revisión completa.

En esta sección se presentan las consideraciones que se deben tener en cuenta para que este proyecto llegue a buen término.

- PAR.1 – Actividades preliminares
- PAR.2 – Elaboración del análisis de riesgos
- PAR.3 – Comunicación de resultados

6.13.1. ROLES Y FUNCIONES

Durante la ejecución del proyecto es frecuente que se creen algunos roles específicos para llevar el proyecto a buen fin.

6.13.2. COMITÉ DE SEGUIMIENTO

Está constituido por los responsables de las unidades afectadas por el proyecto; así como por los responsables de la informática y de la gestión dentro de dichas unidades. También será importante la participación de los servicios comunes de la Organización (planificación, presupuesto, recursos humanos, administración, etc.) En cualquier caso la composición del comité depende de las características de las unidades afectadas.

Las responsabilidades de este comité consisten en:

- Resolver las incidencias durante el desarrollo del proyecto.
- Asegurar la disponibilidad de recursos humanos con los perfiles adecuados y su participación en las actividades donde es necesaria su colaboración.
- Aprobar los informes intermedios y finales de cada proceso.
- Elaborar los informes finales para el comité de dirección.

6.13.3. EQUIPO DE PROYECTO

Formado por personal experto en tecnologías y sistemas de información y personal técnico cualificado del dominio afectado, con conocimientos de gestión de seguridad en general y de la aplicación de la metodología de análisis y gestión de riesgos en particular. Si el proyecto se hace con asistencia técnica mediante contratación externa, el subsiguiente personal especialista en seguridad de sistemas de información se integrará en este equipo de proyecto.

Este equipo tiene a su cargo las siguientes responsabilidades.

- Llevar a cabo las tareas del proyecto
- Recopilar, procesar y consolidar datos
- Elaborar los informes

El Equipo de Proyecto reporta al Comité de Seguimiento a través del Director del Proyecto.

6.13.4. GRUPOS DE INTERLOCUTORES

Está formado por usuarios representativos dentro de las unidades afectadas por el proyecto. Lo constituyen varios posibles subgrupos:

- Responsables de servicio, conscientes de la misión de la Organización y sus estrategias a medio y largo plazo.
- Responsables de servicios internos.
- Personal de explotación y operación de los servicios informáticos, conscientes de los medios desplegados (de producción y salvaguardas) y de las incidencias habituales.

A más de esto hay que identificar unos roles adicionales.

6.13.4.1. PROMOTOR

Es una figura singular que lidera las primeras tareas del proyecto, perfilando su oportunidad y alcance para lanzar el proyecto de análisis de riesgos propiamente dicho. Debe ser una persona con visión global de los sistemas de información y su papel en las actividades de la Organización, sin necesidad de conocer los detalles; pero si al tanto de las incidencias.

6.13.4.1.1. DIRECTOR DEL PROYECTO

Con responsabilidades en seguridad dentro de la Organización, de sistemas de información o, en su defecto, de planificación, de coordinación o de materias, servicios o áreas semejantes. Es la cabeza visible del equipo de proyecto e interlocutor con el Responsable de la Seguridad de la Organización.

6.13.4.1.2. ENLACE OPERACIONAL

Está representada por una persona de la Organización con buen conocimiento de las personas y de las unidades implicadas en el proyecto, que tenga capacidad para conectar al equipo de proyecto con el grupo de usuarios.

Es el interlocutor visible del comité de seguimiento con los grupos de usuarios.

Un proyecto de análisis de riesgos siempre es mixto por su propia naturaleza; es decir, requiere la colaboración permanente de especialistas y usuarios tanto en las fases preparatorias como en su desarrollo. La figura del enlace operacional adquiere una relevancia permanente que no es habitual en otro.

Tabla 44. Proyecto de análisis de riesgo

PAR – Proyecto de Análisis de Riesgos
PAR.1 – Actividades preliminares
PAR.11 – Estudio de oportunidad
PAR.12 – Determinación del alcance del proyecto
PAR.13 – Planificación del proyecto
PAR.14 – Lanzamiento del proyecto
PAR.2 – Elaboración del análisis de riesgos
PAR.3 – Comunicación de resultados

6.14. PLAN DE SEGURIDAD

Planes de seguridad, entendiendo por tales proyectos para materializar las decisiones adoptadas para el tratamiento de los riesgos.

Estos planes reciben diferentes nombres en diferentes contextos y circunstancias

- Plan de mejora de la seguridad
- Plan director de seguridad
- Plan estratégico de seguridad
- Plan de adecuación.

Se identifican tres tareas:

Tabla 45. Plan de mejora de seguridad

PS – Plan de Seguridad.
PS1- Identificación del proyecto de seguridad.
PS2- Plan de ejecución.
PS3- Ejecución.

6.14.1. TAREA PS.1: IDENTIFICACIÓN DE PROYECTOS DE SEGURIDAD

Decisiones de tratamiento de los riesgos en acciones concretas

Tabla 46. Identificación del Plan de seguridad

PS: Plan de seguridad **PS.1: Identificación de proyectos de seguridad**
Objetivos **• Elaborar un conjunto armónico de programas de seguridad.**
Productos de entrada • **Resultados de las actividades de análisis y tratamiento de riesgos** • **Conocimientos de técnicas y productos de seguridad** • **Catálogos de productos y servicios de seguridad**
Productos de salida • **Relación de programas de seguridad.**
Técnicas, prácticas y pautas • **Planificación de proyectos.**
Participantes • **El equipo de proyecto** • **Especialistas en seguridad** • **Especialistas en áreas específicas de seguridad**

En última instancia se trata de implantar o mejorar la implantación de una serie de salvaguardas que lleven impacto y riesgo a los niveles residuales determinados por la Dirección. Este tratamiento de las salvaguardas se materializa en una serie de tareas a llevar a cabo.

Los programas de seguridad deben detallar lo siguiente:

- Su objetivo genérico.
- Las salvaguardas concretas a implantar o mejorar, detallando sus objetivos de calidad, eficacia y eficiencia.
- La relación de escenarios de impacto y/o riesgo que afronta: activos afectados, tipos de activos, amenazas afrontadas, valoración de activos y amenazas y niveles de impacto y riesgo.
- La unidad responsable de su ejecución.
- Una estimación de costes, tanto económicos como de esfuerzo de realización, teniendo en cuenta:
- Costes de adquisición (de productos), o de contratación (de servicios), o de desarrollo (de soluciones llave en mano), pudiendo ser necesario evaluar diferentes alternativas.

- Costes de implantación inicial y mantenimiento en el tiempo.
- Costes de formación, tanto de los operadores como de los usuarios, según convenga al caso.
- Costes de explotación.
- Impacto en la productividad de la Organización.
- Una relación de subtareas a afrontar, teniendo en cuenta cambios en la normativa y desarrollo de procedimientos.
- Solución técnica: programas, equipos, comunicaciones e instalaciones.
- Plan de despliegue.
- Plan de formación.
- Una estimación del tiempo de ejecución desde su arranque hasta su puesta en operación.
- Una estimación del estado de riesgo (impacto y riesgo residual a su compleción).
- Un sistema de indicadores de eficacia y eficiencia que permitan conocer en cada momento la calidad del desempeño de la función de seguridad que se desea y su evolución temporal.

Típicamente un plan de seguridad se planifica en tres niveles de detalle.

Plan director (uno)

A menudo denominado "plan de actuación", trabaja sobre un periodo largo (típicamente entre 3 y 5 años), estableciendo las directrices de actuación.

Plan anual (una serie de planes anuales)

Trabaja sobre un periodo corto (típicamente entre 1 y 2 años), estableciendo la planificación de los programas de seguridad.

A continuación se detallara los elementos que pueden intervenir en el análisis de gestión y riego estos elementos son los siguientes:

- Facilitar la labor de las personas que realizan el proyecto, en el sentido de ofrecerles ítem estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
- Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios que permitan comparar e incluso integrar análisis realizados por diferentes equipos

6.14.2. TIPOS DE ACTIVOS

La tipificación de los activos es tanto una información documental de interés como un criterio de identificación de amenazas potenciales y salvaguardas apropiadas a la naturaleza del activo.

A continuación se destaca la clasificación de los activos dentro de una jerarquía, determinando para cada uno un código que refleja su posición jerárquica, un nombre y una breve descripción de las características que recoge el epígrafe. Nótese que la pertenencia de un activo a un tipo no es excluyente de su pertenencia a otro tipo; es decir, un activo puede ser simultáneamente de varios tipos.

6.14.3. ACTIVOS ESCÁNCIALES

En un sistema de información hay 2 cosas esenciales:

- La **información** que se maneja y.
- Los **servicios** que prestan.

Los activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

Dentro de la información que se maneja, puede ser interesante considerar algunas características formales tales como si son de carácter personal, con requisitos legales, o si están sometidos a alguna clasificación de seguridad, con requisitos normativos:

Datos de carácter personal

Existen leyes relativas a los datos de carácter personal que, en función de su naturaleza y las circunstancias, establecen una serie de obligaciones a los sistemas de información que los tratan.

La aplicación de leyes concierne al criterio de responsabilidad por parte de los directivos del Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo.

Arquitectura del sistema

Propiamente que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.

Tabla 47. Arquitectura del sistema

[arch] Arquitectura del sistema
[sap] punto de [acceso al] servicio (1) **[ip] punto de interconexión (2)** **[ext] proporcionado por terceros (3)**
1. **Establece una frontera entre la prestación de un servicio (proveedor) y el usuario (consumidor). Los requisitos de seguridad del usuario se convierten en obligaciones del prestatario, mientras que los incidentes de seguridad en el proveedor repercuten en el usuario.** 2. **Establece una frontera inter-pares: cuando dos sistemas se interconectan para intercambiar información.** 3. **Establece una frontera inferior, cuando para la prestación de nuestros servicios recurrimos a un tercero.**

6.14.4. [D] DATOS / INFORMACIÓN

Los datos es la parte central del Centro de Tecnología Educativa, esta información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

Tabla 48. Datos y copias de respaldo.

[D] Datos / Información.
[files] ficheros **[backup] copias de respaldo** **[conf] datos de configuración (1)** **[int] datos de gestión interna** **[password] credenciales (ej. contraseñas)** **[auth] datos de validación de credenciales** **[acl] datos de control de acceso [log] registro de actividad (2)**

Tabla 49. Datos y Registros de la información.

[D] Datos / Información.
[source] código fuente **[exe] código ejecutable** **[test] datos de prueba**
• **Los datos de configuración son críticos para mantener la funcionalidad de las partes y del conjunto del sistema de información.** • **Los registros de actividad sustancian los requisitos de trazabilidad.**

6.14.5. [K] CLAVES CRIPTOGRÁFICAS

La criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.

Tabla 50. Claves criptográficas.

[keys] Claves criptográficas
[info] protección de la información
[encrypt] claves de cifra
[shared_secret] secreto compartido (clave simétrica) (1)
[public_encryption] clave pública de cifra (2)
[public_decryption] clave privada de descifrado (2)
[sign] claves de firma
[shared_secret] secreto compartido (clave simétrica)
[public_signature] clave privada de firma (2)
[public_verification] clave pública de verificación de firma (2)
[com] protección de las comunicaciones
[channel] claves de cifrado del canal
[authentication] claves de autenticación
[verification] claves de verificación de autenticación
[disk] cifrado de soportes de información
[encrypt] claves de cifra
[x509] certificados de clave pública

6.14.6. [S] SERVICIOS.

Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.

Tabla 51. Servicios.

[S] Servicios
[anon] anónimo (sin requerir identificación del usuario)
[pub] al público en general (sin relación contractual)
[ext] a usuarios externos (bajo una relación contractual)
[int] interno (a usuarios de la propia organización)

Tabla 52. Servicios Web.

[S] SERVICIOS
[www] world wide web **[telnet] accesoremoto a cuenta local** **[email] correo electrónico [file] almacenamiento de ficheros** **[ftp] transferencia de ficheros** **[edi] intercambio electrónico de datos** **[dir] servicio de directorio (1)** **[idm] gestión de identidades (2)** **[ipm] gestión de privilegios** **[pki] PKI - infraestructura de clave pública (3)**
• **Localización de personas (páginas blancas), empresas o servicios (páginas amarillas); permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado.** • **Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización.** • **Servicios asociados a sistemas de criptografía de clave pública, incluyendo especialmente la gestión de certificados.**

6.14.7. [SW] SOFTWARE

Aplicaciones informáticas prácticamente se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

Tabla 53. Aplicaciones.

[SW] Aplicaciones (software)
[prp] desarrollo propio (in house)
[sub] desarrollo a medida (subcontratado)
[std] estándar (off the shelf).
[browser] navegador web
[www] servidor de presentación
[app] servidor de aplicaciones
[email_client] cliente de correo electrónico
[email_server] servidor de correo electrónico
[file] servidor de ficheros
[dbms] sistema de gestión de bases de datos
[tm] monitor transaccional

[office] ofimática

[av] anti virus

[os] sistema operativo

[hypervisor] gestor de máquinas virtuales

[ts] servidor de terminales

backup] sistema de backup

6.14.8. [HW] EQUIPAMIENTO INFORMÁTICO (HARDWARE)

Los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

Tabla 54. Equipamiento informático

[HW] Equipos informáticos (hardware)
[host] grandes equipos (1) **[mid] equipos medios (2)** **[pc] informática personal (3)** **[mobile] informática móvil (4)** **[pda] agendas electrónicas** **[vhost] equipo virtual** **[backup] equipamiento de respaldo (5)** **[peripheral] periféricos** **[print] medios de impresión (6)** **[scan] escáneres** **[crypto] dispositivos criptográficos** **[bp] dispositivo de frontera (7)** **[network] soporte de la red (8)** **[modem] módems** **[hub] concentradores** **[switch] conmutadores** **[router] encaminadores** **[bridge] pasarelas** **[firewall] cortafuegos** **[wap] punto de acceso inalámbrico** **[pabx] centralita telefónica** **[ipphone] teléfono IP**
1. Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente gravosos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción.

2. **Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción.**
3. **Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción.**
4. **Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar.**
5. **Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción.**
6. **Dícese de impresoras y servidores de impresión.**
7. **Son los equipos que se instalan entre dos zonas de confianza**
8. **Dícese de equipamiento necesario para transmitir datos: routers, módems, etc.**

6.14.9. [COM] REDES DE COMUNICACIONES

Dentro de estas se incluyen instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

Tabla 55. Redes de comunicaciones.

[COM] Redes de comunicaciones
[PSTN] red telefónica
[ISDN] rdsi (red digital)
[X25] X25 (red de datos)
[ADSL] ADSL [pp] punto a punto
[radio] comunicaciones radio
[wifi] red inalámbrica
[mobile] telefonía móvil
[sat] por satélite
[LAN] red local
[MAN] red metropolitana
[Internet] Internet

6.14.10. [MEDIA] SOPORTES DE INFORMACIÓN

Este aspecto considera los dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

Tabla 56. Soporte de información.

[Media] Soportes de información
[electronic] electrónicos **[disk] discos** **[vdisk] discos virtuales** **[san] almacenamiento en red** **[disquette] disquetes** **[cd] cederrón (CD-ROM)** **[usb] memorias USB** **[dvd] DVD** **[tape] cinta magnética** **[mc] tarjetas de memoria** **[ic] tarjetas inteligentes.** **[non_electronic] no electrónicos** **[printed] material impreso** **[tape] cinta de papel** **[film] microfilm** **[cards] tarjetas perforadas**

6.14.11. [AUX] EQUIPAMIENTO AUXILIAR

Dentro de este tema seconsideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

Tabla 57. Equipamiento Auxiliar.

[AUX] Equipamiento auxiliar
[power] fuentes de alimentación **[ups] sistemas de alimentación ininterrumpida** **[gen] generadores eléctricos** **[ac] equipos de climatización** **[cabling] cableado** **[wire] cable eléctrico** **[fiber] fibra óptica** **[robot] robots** **[tape] ... de cintas** **[disk] ... de discos** **[supply] suministros esenciales** **[destroy] equipos de destrucción de soportes de información** **[furniture] mobiliario: armarios, etc** **[safe] cajas fuertes.**

6.14.12. [L] INSTALACIONES

Dentro de las instalaciones se consideran los lugares donde se hospedan los sistemas de información y comunicaciones.

Tabla 58. Instalaciones.

[L] Instalaciones
[site] recinto
[building] edificio
[local] cuarto
[mobile] plataformas móviles
[car] vehículo terrestre: coche, camión, etc.
[plane] vehículo aéreo: avión, etc.
[ship] vehículo marítimo: buque, lancha, etc.
[shelter] contenedores
[channel] canalización
[backup] instalaciones de respaldo

6.14.13. [P] PERSONAL

Son las personas relacionadas con los sistemas de información.

Tabla 59. Personal

[P] Personal
[ue] usuarios externos
[ui] usuarios internos
[op] operadores
[adm] administradores de sistemas
[com] administradores de comunicaciones [dba] administradores de BBDD
[sec] administradores de seguridad
[des] desarrolladores / programadores
[sub] subcontratas
[prov] proveedores

6.15. DIMENSIONES DE VALORACIÓN

Toda característica o atributo que le hacen valioso a un activo, es decir una dimensión es una faceta o aspecto de un activo independiente de otras facetas, se pueden hacer los análisis de riesgos centrados en una sola faceta, independientemente delo que ocurra con otros aspectos.

Estas dimensiones se utilizaran para valorar las consecuencias de la materialización de una amenaza.

6.15.1. [D] DISPONIBILIDAD

Tabla 60. Disponibilidad.

[D] DISPONIBILIDAD
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

¿Qué importancia tendría que el activo no estuviera disponible?

Un activo tiene un gran valor desde el punto de vista de disponibilidad cuando si una amenaza afectara a su disponibilidad, las consecuencias serían graves.

Y recíprocamente, un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodos de tiempo sin por ello causar mayor daño.

La disponibilidad es una característica que afecta a todo tipo de activos.

A menudo la disponibilidad requiere un tratamiento por escalones pues el coste de la indisponibilidad aumenta de forma no lineal con la duración de la interrupción, desde breves interrupciones sin importancia, pasando por interrupciones que causan daños considerables y llegando a interrupciones que no admiten recuperación: la organización está acabada.

6.15.2. INTEGRIDAD DE LOS DATOS

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. (ISO/IEC 13335-1:2004)

¿Qué importancia tendría que los datos fueran modificados fuera de control?

Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna.

6.15.3. CONFIDENCIALIDAD DE LA INFORMACIÓN

Tabla 61. Confidencialidad.

[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. (UNE-ISO/IEC 27001:2007)

¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

6.15.4. [A] AUTENTICIDAD

Tabla 62. Autenticidad.

[A] Autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que Garantiza la fuente de la que proceden los datos. (UNE 71504:2008)

¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?

La autenticidad de los usuarios de un servicio es lo contrario de la oportunidad de fraude o uso no autorizado de un servicio.

Así, un servicio recibe una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para la organización.

Y, recíprocamente, un servicio carece de un valor apreciable desde el punto de vista de autenticidad cuando su acceso por cualquiera no supone preocupación alguna.

¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?

Los datos reciben una elevada valoración desde el punto de vista de autenticidad del origen cuando un defecto de imputación causaría graves quebrantos a la organización. Típicamente, se habilita la oportunidad de repudio.

Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de autenticidad del origen cuando ignorar la fuente es irrelevante.

6.15.5. [T] TRAZABILIDAD

Tabla 63. Trazabilidad.

[T] Trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]

¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?

Abriría las puertas al fraude, incapacitaría a la Organización para perseguir delitos y podría suponer el incumplimiento de obligaciones legales.

¿Qué importancia tendría que no quedara constancia del acceso a los datos?

Abriría las puertas al fraude, incapacitaría a la Organización para perseguir delitos y podría suponer el incumplimiento de obligaciones legales.

6.15.6. AMENAZAS

A continuación se muestra un listado de amenazas posibles sobre los activos de un sistema de información. Para cada amenaza se presenta un cuadro como el siguiente:

Tabla 64. Amenazas.

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

6.15.7. [N] DESASTRES NATURALES

Que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Origen:

Natural (accidental).

6.15.8. [N.1] FUEGO

Tabla 65. Fuego.

[N.1] Fuego	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	**Dimensiones:** [D]disponibilidad
Descripción: Incendios: posibilidad de que el fuego acabe con recursos del sistema.	

6.15.9. [N.2] DAÑOS POR AGUA

Tabla 66. Daños por agua.

[N.2] Daños por agua.	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	**Dimensiones:** [D]disponibilidad
Descripción: inundaciones: posibilidad de que el agua acabe con recursos del sistema	

6.15.10. [I] DE ORIGEN INDUSTRIAL

Ocurren de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

Tabla 67. Fuego de origen industrial

[N.1] Fuego	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	**Dimensiones:** [D]disponibilidad
Descripción: Incendios: posibilidad de que el fuego acabe con recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

6.15.11. [I.2] DAÑOS POR AGUA

Tabla 68. Daños por agua.

[N.2] Daños por agua.	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	**Dimensiones:** [D]disponibilidad
Descripción: Inundaciones: posibilidad de que el agua acabe con recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

6.15.12. [I.8] FALLO DE SERVICIOS DE COMUNICACIONES

Tabla 69. Fallo de servicios de comunicaciones

[I.8] Fallo de servicios de comunicaciones	
Tipos de activos: [COM] redes de comunicaciones	**Dimensiones:** [D]disponibilidad
Descripción: Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

6.15.13. [E] ERRORES Y FALLOS NO INTENCIONADOS

Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.

Origen:

Humano (accidental).

6.15.14. [E.1] ERRORES DE LOS USUARIOS

Tabla 70. Errores de los usuarios

[E.1] Errores de los usuarios	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [Media] soportes de información	**Dimensiones:** [I] integridad [C] confidencialidad [D] disponibilidad
Descripción: Equivocaciones de las personas cuando usan los servicios, datos, etc.	

6.15.15. [E.2] ERRORES DEL ADMINISTRADOR

Tabla 71. Errores del administrador.

[E.2] Errores del administrador.	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [Media] soportes de información	**Dimensiones:** [I] integridad [C] confidencialidad [D] disponibilidad
Descripción: Equivocaciones de personas con responsabilidades de instalación y operación	

6.15.16. [E.3] ERRORES DE MONITORIZACIÓN (LOG)

Tabla 72. Errores de monitorización.

[E.3] Errores de monitorización (log)	
Tipos de activos: [D.log] registros de actividad	**Dimensiones:** [I] integridad (trazabilidad)
Descripción: Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos,	

6.15.17. [E.4] ERRORES DE CONFIGURACIÓN

Tabla 73. Errores de configuración.

[E.4] Errores de configuración	
Tipos de activos: [D.conf] datos de configuración	**Dimensiones:** [I] integridad
Descripción: Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	

6.15.18. [E.8] DIFUSIÓN DE SOFTWARE DAÑINO

Tabla 74. Difusión de software dañino

[E.8] Difusión de software dañino	
Tipos de activos: [SW] aplicaciones (software)	**Dimensiones:** [D] disponibilidad [I] integridad [C] confidencialidad
Descripción: Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	

6.15.19. [E.9] ERRORES DE [RE-] ENCAMINAMIENTO

Tabla 75. Errores de re encaminamiento de la información.

[E.9] Errores de [re-]encaminamiento	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones	**Dimensiones:** [C] confidencialidad
Descripción: Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	

6.15.20. [E.15] ALTERACIÓN ACCIDENTAL DE LA INFORMACIÓN

Tabla 76. Alteración accidental de la información.

[E.15] Alteración accidental de la información	
Tipos de activos: [D] datos / información [keys] claves criptográficas • [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones	**Dimensiones:** [I] integridad
Descripción: Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

6.15.21. [E.18] DESTRUCCIÓN DE INFORMACIÓN

Tabla 77. Destrucción de información.

[E.18] Destrucción de información.	
Tipos de activos: [D] datos / información [keys] claves criptográficas • [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones (tránsito) [Media] soportes de información [L] instalaciones	**Dimensiones:** [I] integridad
Descripción: Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	

6.15.22. [E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)

Tabla 78. Vulnerabilidades de los programas

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos: [SW] aplicaciones (software)	**Dimensiones:** [I] integridad [D] disponibilidad [C] confidencialidad
Descripción: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	

6.15.23. [E.21] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE PROGRAMAS (SOFTWARE)

Tabla 79. Errores de mantenimiento / actualización de programas (software).

[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos: [SW] aplicaciones (software)	**Dimensiones:** [I] integridad [D] disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.	

6.15.24. [E.23] ERRORES DE MANTENIMIENTO / ACTUALIZACIÓN DE EQUIPOS (HARDWARE)

Tabla 80. Errores de mantenimiento / actualización de equipos

[E.23] Errores de mantenimiento / actualización de equipos (hardware).	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes electrónicos [AUX] equipamiento auxiliar	**Dimensiones:** [D] disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	

6.15.25. [E.24] CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS

Tabla 81. Caída del sistema por agotamiento de recursos.

[E.24] Caída del sistema por agotamiento de recursos	
Tipos de activos: [S] servicios [HW] equipos informáticos (hardware) [COM] redes de comunicaciones	**Dimensiones:** [D] disponibilidad
Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	

6.15.26. [E.25] PÉRDIDA DE EQUIPOS

Tabla 82. Pérdida de equipos.

[E.25] Pérdida de equipos	
Tipos de activos: [HW] equipos informáticos (hardware) [Media] soportes electrónicos [AUX] equipamiento auxiliar	**Dimensiones:** [D] disponibilidad. [C] confidencialidad
Descripción: La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	

6.16. [A] ATAQUES INTENCIONADOS

Fallos deliberados causados por las personas.

La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.

Origen:

Humano (deliberado).

6.16.1. [A.3] MANIPULACIÓN DE LOS REGISTROS DE ACTIVIDAD (LOG)

Tabla 83. Manipulación de los registros de actividad (log).

[A.3] Manipulación de los registros de actividad (log).	
Tipos de activos: [D.log] registros de actividad	**Dimensiones:** [I] integridad (trazabilidad)
Descripción:	

6.16.2. [A.4] MANIPULACIÓN DE LA CONFIGURACIÓN

Tabla 84. Manipulación de la configuración.

[A.4] Manipulación de la configuración	
Tipos de activos: [D.log] registros de actividad	**Dimensiones:** [I] integridad [C] confidencialidad [A] disponibilidad
Descripción: Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	

6.16.3. [A.5] SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO

Tabla 85. Suplantación de la identidad del usuario.

[A.5] Suplantación de la identidad del usuario.	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones	**Dimensiones:** [C] confidencialidad [A] autenticidad 3 [I] integridad
Descripción: Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	

6.16.4. [A.6] ABUSO DE PRIVILEGIOS DE ACCESO

Tabla 86. Abuso de privilegios de acceso.

[A.6] Abuso de privilegios de acceso	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [COM] redes de comunicaciones	**Dimensiones:** [C] confidencialidad [D] disponibilidad [I] integridad
Descripción: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	

6.16.5. [A.7] USO NO PREVISTO

Tabla 87. Uso no previsto

[A.7] Uso no previsto	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware [COM] redes de comunicaciones [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	**Dimensiones:** [C] confidencialidad [D] disponibilidad [I] integridad
Descripción: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	

6.16.6. [A.8] DIFUSIÓN DE SOFTWARE DAÑINO.

Tabla 88. Difusión de software dañino.

[A.8] Difusión de software dañino	
Tipos de activos: [SW] aplicaciones (software)	**Dimensiones:** [C] confidencialidad [D] disponibilidad [I] integridad
Descripción: Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	

6.16.7. [A.11] ACCESO NO AUTORIZADO

Tabla 89. Acceso no autorizado

[A.11] Acceso no autorizado.	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos (hardware [COM] redes de comunicaciones [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	**Dimensiones:** [C] confidencialidad [I] integridad
Descripción: El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	

6.16.8. [A.12] ANÁLISIS DE TRÁFICO

Tabla 90. Análisis de tráfico.

[A.12] Análisis de tráfico.	
Tipos de activos: [COM] redes de comunicaciones	**Dimensiones:** [C] confidencialidad
Descripción: El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina "monitorización de tráfico".	

6.16.9. [A.22] MANIPULACIÓN DE PROGRAMAS

Tabla 91. Manipulación de los programas.

[A.22] Manipulación de programas.	
Tipos de activos: [SW] aplicaciones (software)	**Dimensiones:** [C] confidencialidad [D] disponibilidad [I] integridad
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	

6.16.10. [A.23] MANIPULACIÓN DE LOS EQUIPOS

Tabla 92. Manipulación de los equipos y activos.

[A.23] Manipulación de los equipos.	
Tipos de activos: [Media] soportes de información [AUX] equipamiento auxiliar [HW] equipos informáticos	**Dimensiones:** [C] confidencialidad [D] disponibilidad
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	

CAPITULO VII

7. BIBLIOGRAFIA

7.1 LIBROS

- Delgado, M. L. (2010). *Análisis Forense Digital* . Madrid: CRIPTORED.
- Gómez., L. S. (2009). *El tratamiento de la evidencia digital.* JAIIO.
- Gutiérrez, G. Z.–J. (2010|). *Informática Forense* . Colombia: Universidad de los Andes.
- Kano, J. A.-A.-J. (2005). *Evidencia Digital.* Colombia: Universidad de los Andes.
- Kano, J. J. (2008). *Introducción a la Informática Forense.* Colombia: Universidad de los Andes.
- Keith J. Jones, R. B. (2005). *Real digital forensics.* Addison - Wesley Education Publishers inc.
- Miguel, L. D. (2007). *Análisis Forense Digital.* CRIPORED.
- Óscar López, H. A. (2009). *INFORMÁTICA FORENSE: GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS.* Buenos Aires: CRPTORED.
- P.Leonard, W. (2005). *La evaluación de la gestión: Una evaluacion de los métodos de gestión y desempeño.* Ennglewood Clifs: McGraw-Hill.
- Pino, D. S. (2011). *Introducción a la Informática Forense.* Pontifica Universidad del Ecuador.
- Venema, D. F.-W. (2005). *Forensic Discovery.*Addison - Wesley Professional.

7.2 LINKOGRAFIA

- 27001, E. I. (2009). *El portal de ISO 27001*. Obtenido de http://www.iso27000.es/iso27000.html
- España, P. d. (s.f.). *Libro de MAGERIT 2*. Obtenido de http://administracionelectronica.gob.es/: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General
- Standard, I. 2. (2009). *Estándar Internacional ISO/IEC 27002 International Standard*. Obtenido de http://www.iso27000.es/sgsi.html#section2d
- Venema, D. F.-W. (2005). *Forensic Discovery*. Addison - Wesley Professional.
- Wikipedia. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Moodle

CAPITULO VIII

APÉNDICES Y ANEXOS

ANEXO 1.- ENCUESTA APLICADA A LOS ADMINISTRADORES DEL CENTRO DE TECNOLOGÍA EDUCATIVA DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO.

Objetivo: conocer el estado en el que se desenvuelve el Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo, sus características, políticas y normas de seguridad, con la finalidad de poner a disposición de las personas responsables las falencias, amenazas existentes en la forma de proteger la información de los sistemas.

Marco Organizativo de seguridad.

1. ¿Dispone de una política de seguridad escrita, impresa o guardada en formato electrónico?

   Si ( ) No ( ).

2. ¿Precisa los objetivos y misión del Centro de Tecnología Educativa?

   Si ( ) No ( ).

3. Cumple con la Norma ISO 27004 (Sistema de Gestión de Seguridad de Información y de los controles relacionados).

   Si ( ) No ( ).

4. ¿Existen documento(s) de políticas de seguridad de S.I.?

   Si ( ) No ( ).

5. ¿Existen políticas o normas sobre que personas pueden acceder a la documentación del sistema y su acceso?

   Si ( ) No ( ).

6. ¿Existen normativas sobre el uso correcto de equipos, servicios e instalaciones?

Si ( ) No ( ).

7. ¿Existen normativas acerca del uso indebido de los equipos, los servicios, las instalaciones, la información etc.?

Si ( ) No ( ).

8. ¿Precisa la responsabilidad del personal con respecto al cumplimiento o violación de estas normas?

Si ( ) No ( ).

9. ¿Precisan cómo identificar y reportar comportamientos anómalos?

Si ( ) No ( ).

10. ¿Existe un proceso formal para las autorizaciones respecto a los sistemas de información?

Si ( ) No ( ).

11. ¿Existen normativa contempla el proceso de autorización de utilización de soportes de información?

Si ( ) No ( ).

12. ¿Dispone de un análisis de riesgos, al menos, informal?

Si ( ) No ( ).

13. ¿Dicho análisis identifica los activos más valiosos del sistema?

Si ( ) No ( ).

14. ¿Identifica las amenazas más probables (incendio, robo, virus informático, ataque informático, etc.)?

Si ( ) No ( ).

15. ¿Identifica las salvaguardas que protegen de dichas amenazas (extintor, puerta con cerradura, antivirus, cortafuegos)?

Si ( ) No ( ).

16. ¿Dispone de un análisis de riesgos formal (lenguaje específico y con un fundamento metodológico reconocido internacionalmente)?

Si ( ) No ( ).

17. ¿Este análisis formal Identifica y valora cualitativamente los activos más valiosos del sistema?

Si ( ) No ( ).

18. ¿Identifica y cuantifica las amenazas posibles?

Si ( ) No ( ).

19. ¿Identifica y valora el riesgo al que están expuestos los servicios (bajo, medio o alto)?

Si ( ) No ( ).

20. ¿Identifica y valora cualitativamente los activos más valiosos del sistema?

Si ( ) No ( ).

Arquitectura de seguridad.

21. ¿Dispone de documentación de las instalaciones?

Si ( ) No ( ).

22. ¿Dispone de un inventario de los sistemas de información?

Si ( ) No ( ).

23. ¿Este inventario describe los activos del sistema (ejemplo: servidor de correo archivos de backup, etc.)?

Si ( ) No ( ).

24. ¿Describe las redes existentes (ejemplo: red local con direccionamiento 192.168.0.0/24, DMZ con direccionamiento 172.16.0.0/24, etc.) y los elementos de conexión al exterior (ejemplo: la red local está separada de Internet mediante un firewall, etc.)?

Si ( ) No ( ).

25. ¿Precisa los puntos de acceso al sistema?

Si ( ) No ( ).

26. ¿Disponen de un inventario donde se describe los sistemas de seguridad de que disponen (firewalls, antivirus, *antispam*, *antiphishing*, etc)?

Si ( ) No ( )

27. ¿Describe los elementos de defensa en las conexiones a otras redes?

Si ( ) No ( )

28. ¿Utilizan tecnologías de seguridad diferentes (el antivirus del firewall es diferente del antivirus del servidor de correo, el sistema operativo del *router* es diferente del sistema operativo del firewall, etc.)?

Si ( ) No ( )

29. ¿Dispone de un documento que detalla los sistemas de identificación y autenticación de usuarios para cada sistema o servicio?

Si ( ) No ( )

30. ¿Detalla el mecanismo de autenticación a cada sistema o servicio?

Si ( ) No ( )

31. ¿Detalla dónde se almacenan las contraseñas (las claves se almacenan cifradas en el fichero /etc/shadow en Linux, *Active Directory* en Windows, etc.)?

Si ( ) No ( )

32. ¿Detalla cómo se controlan los datos una vez en los sistemas?

Si ( ) No ( )

33. ¿Precisa la validación de datos de entrada, salida y datos intermedios?

Si ( ) No ( )

Control de acceso

34. ¿El Centro de Tecnología Educativa dispone de un procedimiento documentado para la creación de nuevos usuarios del sistema que especifica que no se puede crear un identificador para varios usuarios?

Si ( ) No ( ).

35. ¿El Centro de Tecnología Educativa dispone de una normativa documentada que especifica que los usuarios no pueden compartir su identificador con nadie?

Si ( ) No ( ).

36. ¿Se puede conocer un registro de las entidades responsables de cada identificador. Existe una relación de los identificadores con sus usuarios?

Si ( ) No ( ).

37. ¿Usted puede saber qué derechos tiene?

Si ( ) No ( ).

38. ¿Identifica el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad, procedimiento que indica que debe llevarse a cabo en los sistemas previos a su puesta en explotación?

Si ( ) No ( ).

39. ¿Se protegen los recursos del sistema con algún mecanismo que impida su utilización?

Si ( ) No ( ).

40. ¿Se dispone de evidencia documental (manual de administración, documento desarrollado internamente, etc.) donde se especifica cuáles son los componentes del sistema y sus ficheros o registros de configuración, así como los permisos de usuario que deben establecerse de forma que sólo los usuarios autorizados tengan acceso?

Si ( ) No ( ).

41. La política y normativa de seguridad del sistema especifican quién es el responsable de cada recurso y, por lo tanto, es también responsable de la asignación de autorización y nivel de acceso a cada recurso.

Si ( ) No ( ).

Segregación de funciones y tareas

42. ¿Dispone de un documento en el que se detallan cuáles son las tareas críticas?

Si ( ) No ( ).

43. ¿Dispone de un esquema de funciones y tareas en el que se contemplan las tareas críticas que son incompatibles en una misma persona?

Si ( ) No ( ).

44. ¿Contempla la incompatibilidad de tareas de auditoría o supervisión con las de cualquier otra función relacionada con el sistema?

Si ( ) No ( ).

45. ¿Se limitan los privilegios de cada usuario al mínimo estrictamente necesario para acceder a la información requerida y para cumplir sus obligaciones?

Si ( ) No ( ).

Mecanismo de autenticación

46. ¿Se encuentra identificado el mecanismo de autenticación en cada recurso?

Si ( ) No ( ).

47. Si utilizan contraseñas ¿cumplen las reglas básicas de calidad?

Si ( ) No ( ).

48. ¿Dicha política o normativa establece que la cuenta del usuario no se habilita hasta que éste haya confirmado la recepción del autenticador?

Si ( ) No ( ).

49. ¿Están los autenticadores bajo el control exclusivo del usuario?

Si ( ) No ( ).

50. ¿Se cambian los autenticadores con la periodicidad marcada por la política de la organización (atendiendo a la categoría del sistema al que se accede)?

Si ( ) No ( ).

51. ¿Se utilizan claves concertadas?

Si ( ) No ( ).

52. Si utilizan contraseñas ¿cumplen las políticas rigurosas de calidad y renovación?

Si ( ) No ( ).

Acceso local (local logon)

53. ¿Dispone de una política o normativa documentada que especifica que los sistemas antes de entrar en explotación o los ya existentes son configurados de forma que no revelen información del sistema antes de un acceso autorizado?

Si ( ) No ( ).

54. ¿Se limita el número de intentos fallidos de acceso?

Si ( ) No ( ).

55. ¿Se registran los accesos con éxito y los fallidos?

Si ( ) No ( ).

56. ¿Informa el sistema al usuario de sus obligaciones inmediatamente después de obtener el acceso?

Si ( ) No ( ).

57. ¿Informa el sistema al usuario del último acceso con su identidad con éxito?

Si ( ) No ( ).

58. ¿Se limita el horario, fechas y lugar desde donde se accede?

Si ( ) No ( ).

59. ¿Se garantiza la seguridad del sistema cuando acceden remotamente usuarios u otras entidades?

Si ( ) No ( ).

60. ¿Dispone de una política o normativa documentada que regula las actividades que pueden realizarse remotamente?

Si ( ) No ( ).

61. ¿Los accesos remotos deben ser autorizados previamente, indicando la persona que puede autorizar el acceso?

Si ( ) No ( ).

62. ¿Dispone de un inventario del sistema?

Si ( ) No ( ).

63. ¿Dispone de un procedimiento documentado que especifica el responsable y la frecuencia de su revisión y/o actualización?

Si ( ) No ( ).

Mantenimiento

64. ¿Dispone de un plan de mantenimiento del equipamiento físico y lógico?

Si ( ) No ( ).

65. ¿Atiende a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas?

Si ( ) No ( ).

66. ¿Dispone de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones, teniendo en cuenta el cambio en el riesgo de cara a su priorización?

Si ( ) No ( ).

Protección frente a código dañino

67. ¿Dispone de mecanismos de prevención y reacción frente a código dañino (virus, gusanos, troyanos, programas espía y "malware" en general)?

Si ( ) No ( ).

68. ¿Dispone de un proceso integral para hacer frente a incidentes que puedan tener un impacto en la seguridad del sistema?

Si ( ) No ( ).

69. ¿Incluye la toma de medidas urgentes, contemplando la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros (según convenga al caso)?

Si ( ) No ( ).

70. ¿Incluye la asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente?

Si ( ) No ( ).

71. ¿Incluye en los procedimientos de usuario la identificación y forma de tratar el incidente?

Si ( ) No ( ).

Registro de la actividad de los usuarios

72. ¿Dispone de mecanismos que garanticen la corrección de la hora a la que se realiza el registro?

Si ( ) No ( ).

73. ¿Se registran todas las actividades de los usuarios en el sistema?

Si ( ) No ( ).

74. ¿Indican quién realiza la actividad, cuándo la realiza y sobre qué información, sea cual sea el usuario?

Si ( ) No ( ).

75. ¿Incluye la actividad de los operadores y administradores del sistema?

Si ( ) No ( ).

76. ¿La determinación de las actividades a registrar y su nivel de detalle se determinan en base al análisis de riesgos del sistema?

Si ( ) No ( ).

Protección de los registros de actividad

77. ¿Se encuentran protegidos los registros del sistema?

Si ( ) No ( ).

78. ¿Se encuentran protegidos frente a su modificación o eliminación por personal no autorizado?

Si ( ) No ( ).

79. ¿Las copias de seguridad, si existen, se ajustan a los mismos requisitos?

Si ( ) No ( ).

Monitorización del sistema

80. ¿Dispone de un conjunto de indicadores que midan el desempeño real del sistema en materia de seguridad?

Si ( ) No ( ).

81. ¿Miden la eficacia y eficiencia de las medidas de seguridad?

Si ( ) No ( ).

82. ¿Miden el impacto de los incidentes de seguridad?

Si ( ) No ( ).

Protección de las instalaciones e infraestructuras

83. ¿El equipamiento ha sido instalado en áreas separadas específicas para su función?

Si ( ) No ( ).

84. ¿El acceso a las áreas separadas se encuentra controlado?

Si ( ) No ( ).

85. ¿El control de acceso a los locales donde hay equipamiento que forme parte del sistema de información se encuentra gestionado?

Si ( ) No ( ).

86. ¿Se identifican a todas las personas que accedan a estos locales?

Si ( ) No ( ).

87. ¿Los locales donde se ubican los sistemas de información y sus componentes disponen de las adecuadas condiciones de temperatura y humedad?

Si ( ) No ( ).

88. ¿Cuentan con protección del cableado frente a incidentes fortuitos o deliberados?

Si ( ) No ( ).

89. ¿Existe equipamiento redundante en caso de fallo de los equipos principales de acondicionamiento?

Si ( ) No ( ).

90. ¿Se encuentra actualizado el etiquetado de los cables?

Si ( ) No ( ).

91. ¿Se protegen los locales donde se ubiquen los sistemas de información y sus componentes frente a incendios fortuitos o deliberados?

Si ( ) No ( ).

92. ¿Se protegen los locales donde se ubiquen los sistemas de información y sus componentes frente a incidentes fortuitos o deliberados causados por el agua?

Si ( ) No ( ).

93. ¿Está garantizada la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles?

Si ( ) No ( ).

Protección de las comunicaciones y confidencialidad

94. ¿Dispone de cortafuegos que separe la red interna del exterior?

Si ( ) No ( ).

95. Respecto a dichos cortafuegos ¿Consta de dos o más equipos de diferente fabricante dispuestos en cascada?

Si ( ) No ( ).

96. ¿Se emplean redes privadas virtuales cuando la comunicación discurre por redes fuera del propio dominio de seguridad?

Si ( ) No ( ).

Segregación de redes

97. ¿Se encuentra la red segmentada?

Si ( ) No ( ).

98. ¿Existe control de entrada de los usuarios que llegan a cada segmento?

Si ( ) No ( ).

99. ¿Existe control de salida de la información disponible en cada segmento?

Si ( ) No ( ).

100. ¿Está el punto de interconexión particularmente asegurado, mantenido y monitorizado?

Si ( ) No ( ).

101. ¿Se ha establecido un tiempo máximo para que los equipos alternativos entren en funcionamiento?

Si ( ) No ( ).

Copias de seguridad (backup)

102. ¿Realizan copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad determinada?

Si ( ) No ( ).

103. ¿Estas copias de seguridad Abarcan la información de trabajo de la organización?

Si ( ) No ( ).

104. ¿Abarcan las aplicaciones en explotación, incluyendo los sistemas operativos?

Si ( ) No ( ).

105. ¿Existe un proceso de autorización para la recuperación de información de las copias de seguridad?

Si ( ) No ( ).

106. ¿Se verifica regularmente que la información respaldada está correctamente dispuesta para ser recuperada en caso de necesidad?

Si ( ) No ( ).

Protección de los servicios

107. ¿La información que se distribuye por medio de correo electrónico se protege, tanto en el cuerpo de los mensajes como en los anexos?

Si ( ) No ( ).

108. ¿Se protege la información de encaminamiento de mensajes y establecimiento de conexiones?

Si ( ) No ( ).

109. ¿Se protege frente a programas dañinos (virus, gusanos, troyanos, espías u otros de naturaleza análoga)?

Si ( ) No ( ).

110. ¿Se encuentran protegidos los subsistemas dedicados a la publicación de información frente a las amenazas que les son propias?

Si ( ) No ( ).

111. Cuando la información tenga algún tipo de control de acceso ¿se garantiza la imposibilidad de acceder a la información obviando la autenticación?

Si ( ) No ( ).

112. ¿Se previenen ataques de manipulación de URL?

Si ( ) No ( ).

113. ¿Se previenen ataques de manipulación de las cookies de los usuarios?

Si ( ) No ( ).

114. ¿Se previenen ataques de manipulación de “proxys” o “cachés”?

Si ( ) No ( ).

115. ¿Se realizan auditorías de seguridad y pruebas de penetración?

Si ( ) No ( ).

ANEXO 2.- ENCUESTAS APLICADAS A LOS USUARIOS ESTUDIANTES.

Objetivo: El objetivo de realizar esta encuesta es conocer los servicios que ofrece el Servidor B- learning de la Universidad Nacional de Chimborazo. Si la funcionalidad del sus servicios son satisfactorias.

Indicaciones: Marque con una x su respuesta.

1. ¿Ha utilizado usted antes una plataforma B-learning.?

   Si ( ) No ( ).

En caso de ser afirmativa la repuesta indique cual es……

2. ¿Utilizas con frecuencia la plataforma B-learning?

   Si ( ) No ( ).

3. ¿Utilizas la plataforma B-learning como método de enseñanza?

   Si ( ) No ( ).

4. ¿La enseñanza a través de la plataforma B-learning ayuda a mejorar el desempeño del desarrollo académico?

   Si ( ) No ( ).

5. Recibió usted una introducción previa sobre el servicio que ofrece la plataforma B-learning.

   Si ( ) No ( ).

6. Existe documentación de ayuda sobre el funcionamiento del sistema.

   Si ( ) No ( ).

7. Ha aplicado algún examen mediante esta plataforma.

   Si ( ) No ( ).

8. ¿Cree la plataforma B-learning cuenta con una interface de usuario amigable?

   Si ( ) No ( ).

9. ¿Crees usted que la plataforma B-learning cuenta con las seguridades adecuadas como para proteger su información?

   Si ( ) No ( ).

10. ¿Sabe usted si la información que proporciona al sistema es confidencial?

    Si ( ) No ( ).

11. ¿El funcionamiento durante las horas picos es satisfactorio?

    Si ( ) No ( ).

12. Usted accede a los servicios del B-learning desde la universidad

    Si ( ) No ( ).

13. ¿Al crear su contraseña el sistema, le pide crear una contraseña segura (utilización de mayúsculas, minúsculas, números, caracteres especiales)?

    Si ( ) No ( ).

14. ¿Existe un Periodo en el que el sistema le pide cambiar su contraseña?

    Si ( ) No ( ).

ANEXO 3.- ENCUESTA APLICADA A LOS USUARIOS PROFESORES.

Objetivo: El objetivo de realizar esta encuesta es conocer los servicios que ofrece el servidor B-learning a los docentes de la universidad nacional de Chimborazo. Si la funcionalidad del sus servicios son satisfactorias.

Indicaciones: Marque con una x su respuesta.

1. ¿Ha utilizado usted antes una plataforma B-learning?

Si ( ) No ( ).

En caso de ser afirmativa la repuesta indique cual es……

2. ¿Utiliza con frecuencia la plataforma B-learning?

Si ( ) No ( ).

3. ¿Utilizas la plataforma B-learning como método de aprendizaje?

Si ( ) No ( ).

4. ¿La enseñanza a través de la plataforma B-learning ayuda a mejorar el desempeño del desarrollo académico?

Si ( ) No ( ).

5. Recibió usted una introducción previa sobre el servicio que ofrece la plataforma B-learning.

Si ( ) No ( ).

6. Existe documentación de ayuda sobre el funcionamiento del sistema.

Si ( ) No ( ).

7. Ha realizado algún examen mediante esta plataforma.

Si ( ) No ( ).

8. ¿La educación mediante la plataforma B-learning cuenta con una interface de usuario amigable?

Si ( ) No ( ).

9. ¿Crees usted que la plataforma B-learning cuenta con las seguridades adecuadas como para proteger su información?

Si ( ) No ( ).

10. ¿Sabe usted si la información que proporciona al sistema es confidencial?

Si ( ) No ( )

ANEXO 4.- TABULACIÓN DE LAS ENCUESTAS REALIZADAS A LOS ADMINISTRADORES DEL CENTRO DE TECNOLOGÍA EDUCATIVA.

Marco Organizativo de seguridad.

1. ¿Dispone de una política de seguridad escrita, impresa o guardada en formato electrónico?

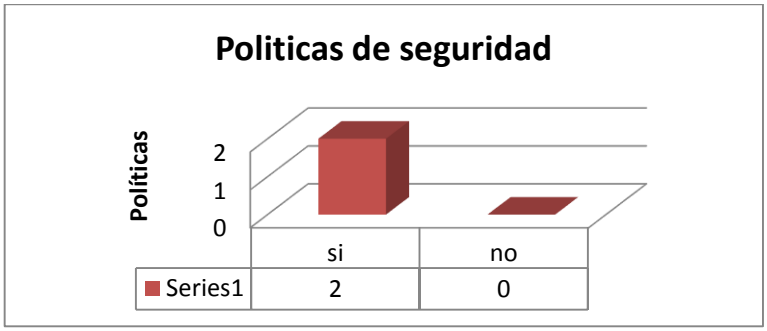


Gráfico 2. Políticas de Seguridad.

2. ¿Precisa los objetivos y misión del Centro de Tecnología Educativa?

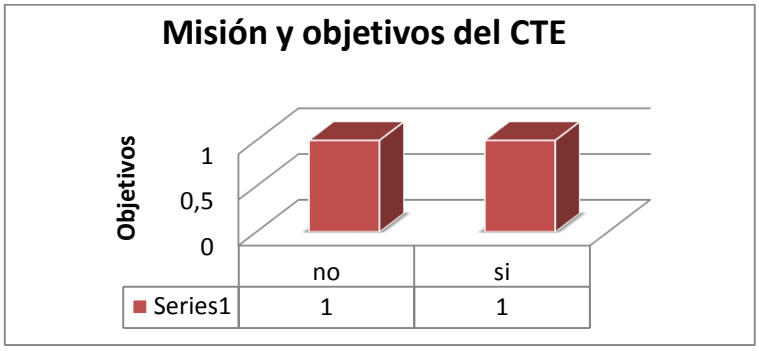


Gráfico 3. Misión y objetivos del Centro de Tecnología Educativa.

3. Cumple con la Norma ISO 27004 (Sistema de Gestión de Seguridad de Información y de los controles relacionado).

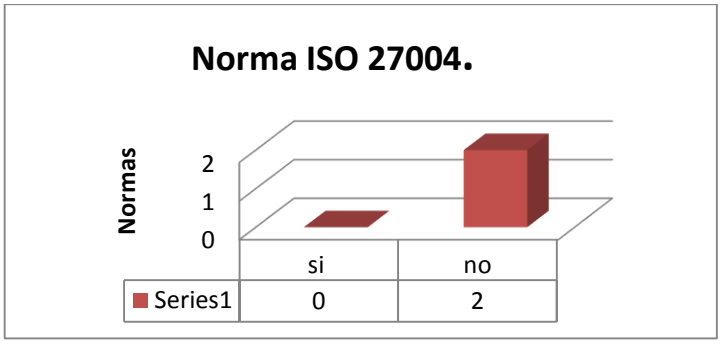


Gráfico 4. Norma ISO 27004

4. ¿Existen documentos de políticas de seguridad de S.I.?

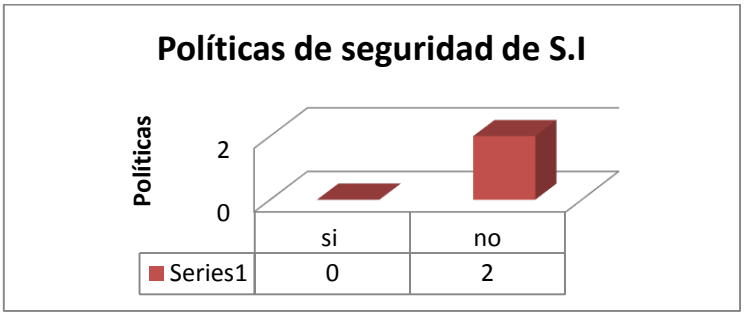


Gráfico 5. Documentos de S.I.

5. ¿Existen políticas o normas sobre que personas pueden acceder a la documentación del sistema y su acceso?

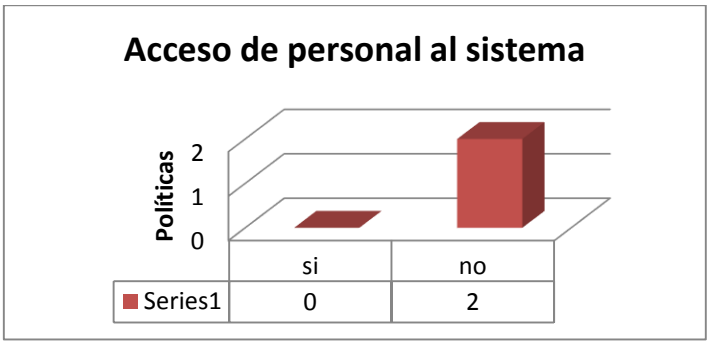


Gráfico 6. Acceso de personal al sistema.

6. ¿Existen normativas sobre el uso correcto de equipos, servicios e instalaciones?

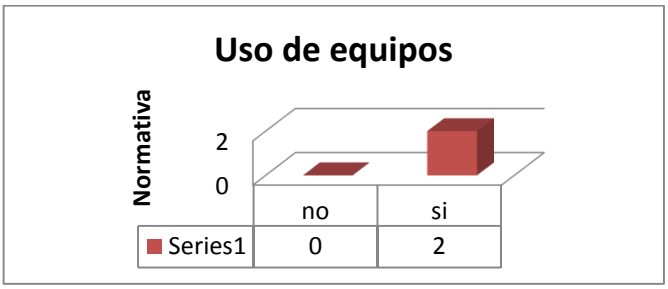


Gráfico 7. Normativas de uso de equipos.

7. ¿Existen normativas acerca del uso indebido de los equipos, los servicios, las instalaciones, la información etc.?

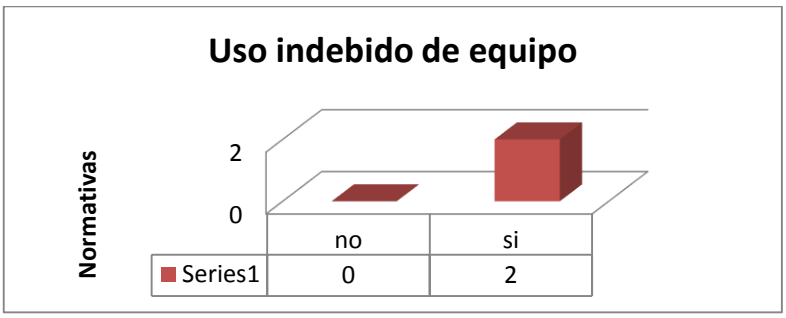


Gráfico 8. Normativas uso indebido de equipos

:.

8. ¿Precisa la responsabilidad del personal con respecto al cumplimiento o violación de estas normas?

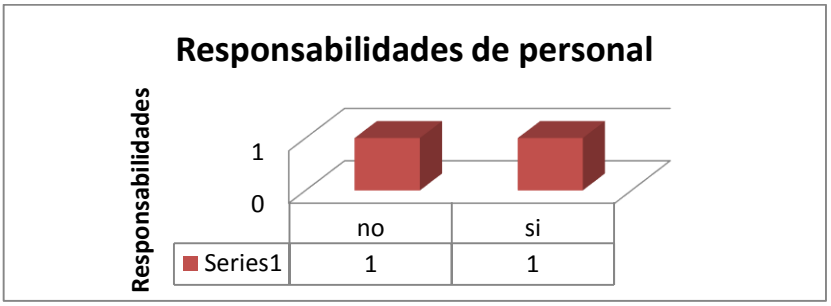


Gráfico 9. Responsabilidades del personal.

9. ¿Precisan cómo identificar y reportar comportamientos anómalos?

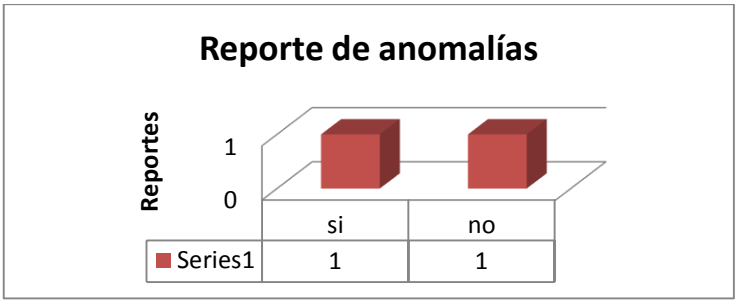


Gráfico 10. Reporte de anomalías.

10. ¿Existe un proceso formal para las autorizaciones respecto a los sistemas de información?

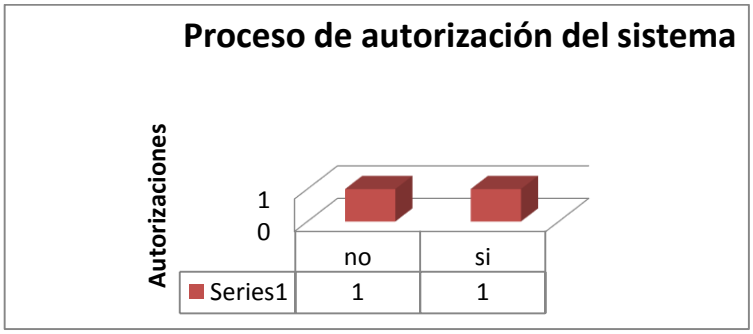


Gráfico 11. Proceso de autorización del sistema.

11. ¿Existen normativa contempla el proceso de autorización de utilización de soportes de información?

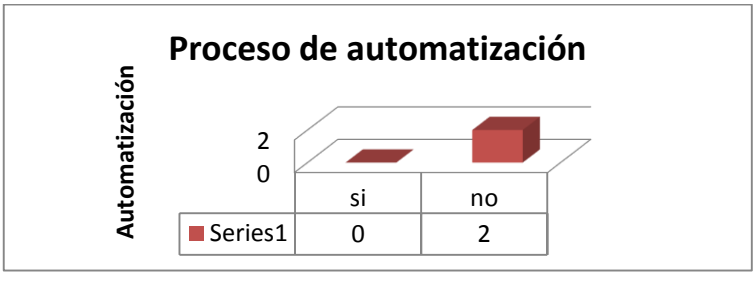


Gráfico 12. Proceso de autorización de soporte de información.

12. ¿Dispone de un análisis de riesgos, al menos, informal?

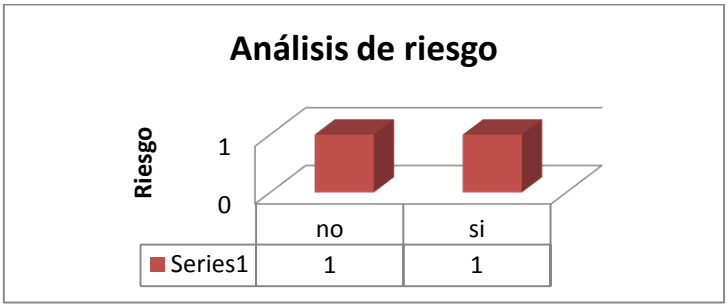


Gráfico 13. Análisis de riesgo informal.

13. ¿Dicho análisis identifica los activos más valiosos del sistema?

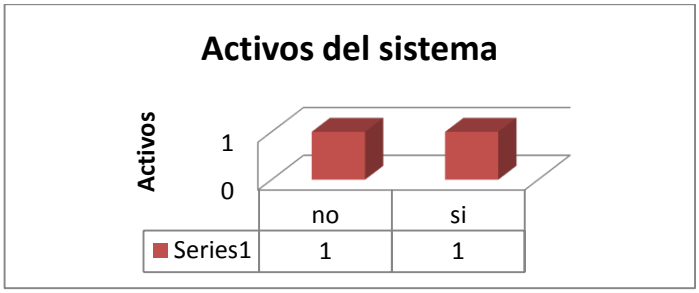


Gráfico 14. Activos valiosos del sistema.

14. ¿Identifica las amenazas más probables (incendio, robo, virus informático, ataque informático, etc.)?

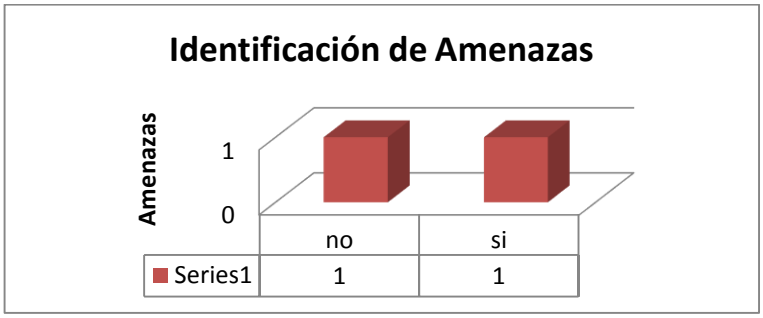


Gráfico 15. Identificación de amenazas.

15. ¿Identifica las salvaguardas que protegen de dichas amenazas (extintor, puerta con cerradura, antivirus, cortafuegos)?

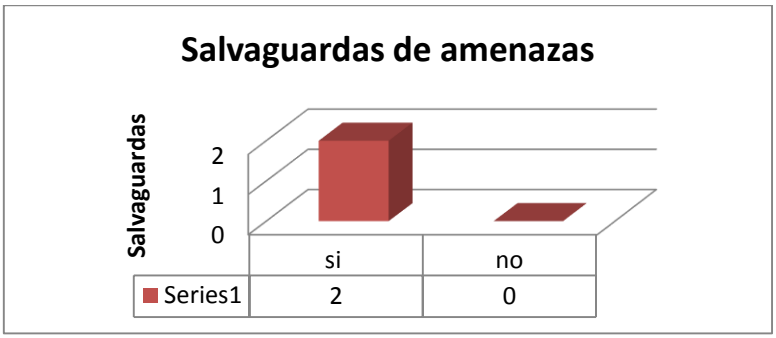


Gráfico 16. Salvaguardas para amenazas.

16. ¿Dispone de un análisis de riesgos formal (lenguaje específico y con un fundamento metodológico reconocido internacionalmente)?

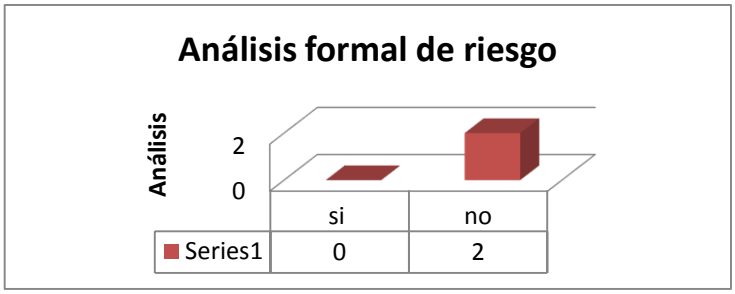


Gráfico 17. Análisis formal de riesgo.

17. ¿Este análisis formal identifica y valora cualitativamente los activos más valiosos del sistema?

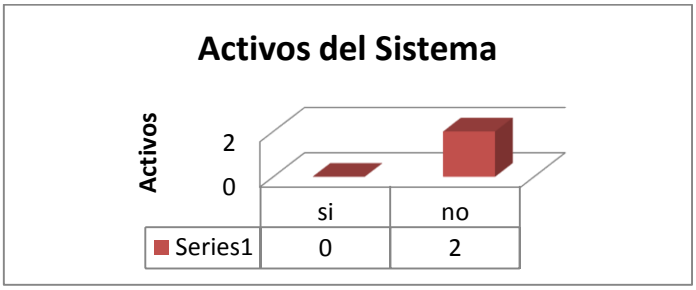


Gráfico 18. Activos valiosos del sistema.

18. ¿Identifica y cuantifica las amenazas posibles?

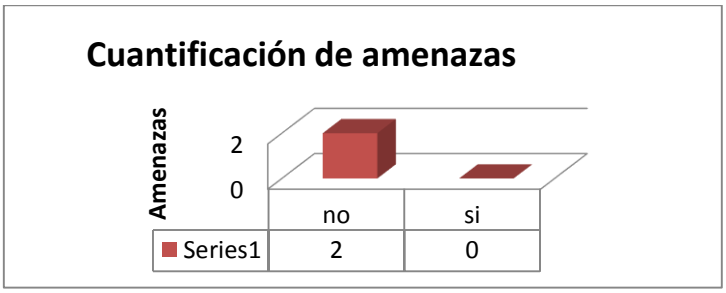


Gráfico 19. Cuantificación de amenazas.

19. ¿Identifica y valora el riesgo al que están expuestos los servicios (bajo, medio o alto)?

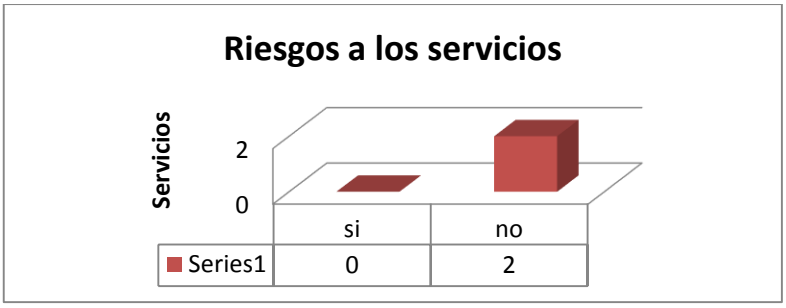


Gráfico 20. Riesgos a los servicio.

20. ¿Identifica y valora cualitativamente los activos más valiosos del sistema?

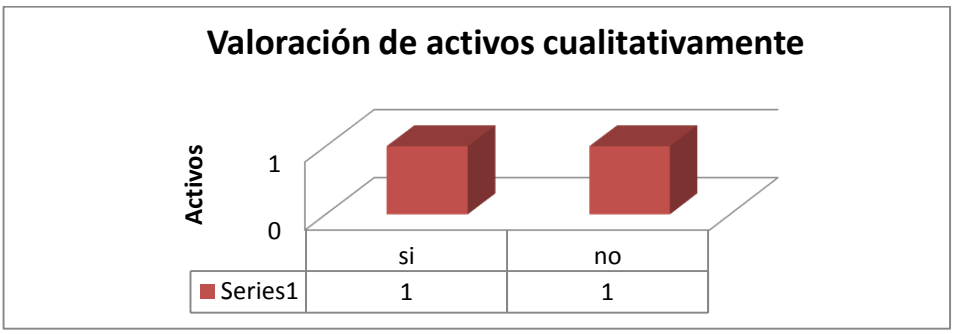


Gráfico 21. Valoración de Activos cualitativamente.

21. ¿Dispone de documentación de las instalaciones?

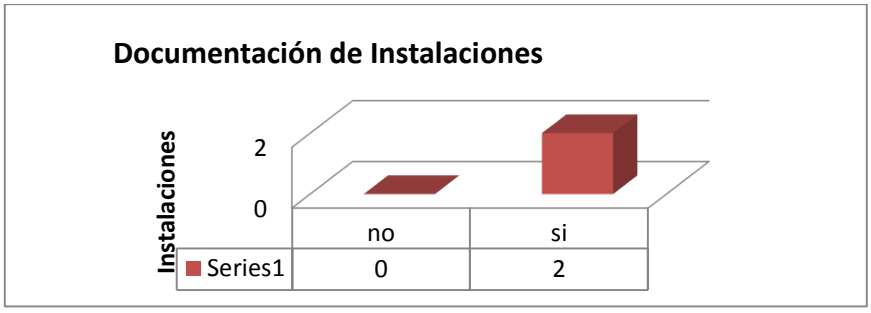


Gráfico 22. Documentación de las instalaciones.

22. ¿Dispone de un inventario de los sistemas de información?

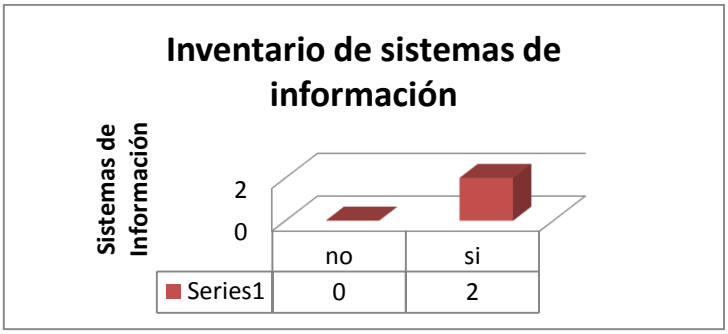


Gráfico 23. Inventario de Sistemas de Información.

23. ¿Este inventario describe los activos del sistema (ejemplo: servidor de correo, robot de backup, etc.)?

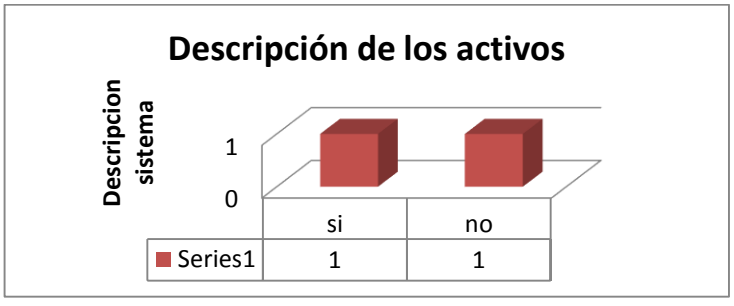


Gráfico 24. Descripción de activos del Sistema**.**

24. ¿Describe las redes existentes (ejemplo: red local con direccionamiento 192.168.0.0/24, DMZ con direccionamiento 172.16.0.0/24, etc.) y los elementos de conexión al exterior (ejemplo: la red local está separada de Internet mediante un firewall, etc.)?

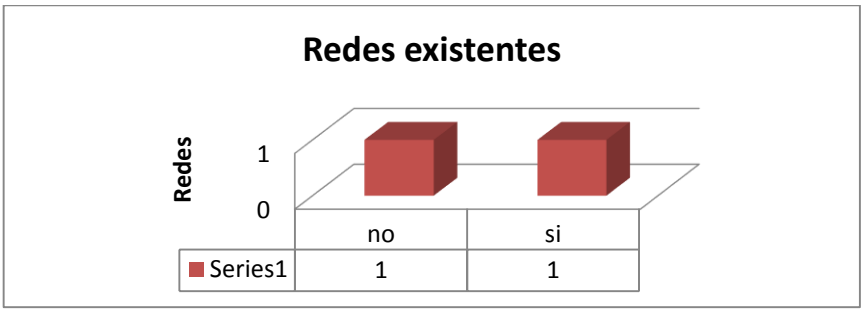


Gráfico 25. Redes existentes**.**

25. ¿Precisa los puntos de acceso al sistema?

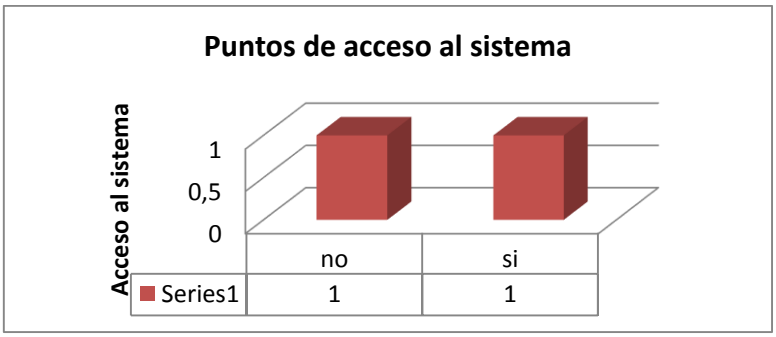


Gráfico 26. Puntos de acceso al sistema.

26. ¿Disponen de un inventario donde se describe los sistemas de seguridad de que disponen (firewalls, antivirus, antispam, antiphishing, etc)?

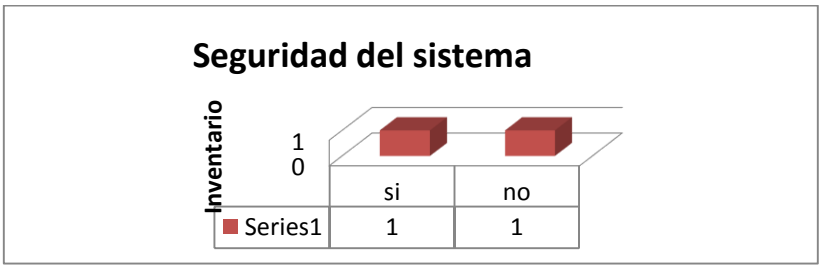


Gráfico 27. Seguridad del Sistema**.**

27. ¿Describe los elementos de defensa en las conexiones a otras redes?

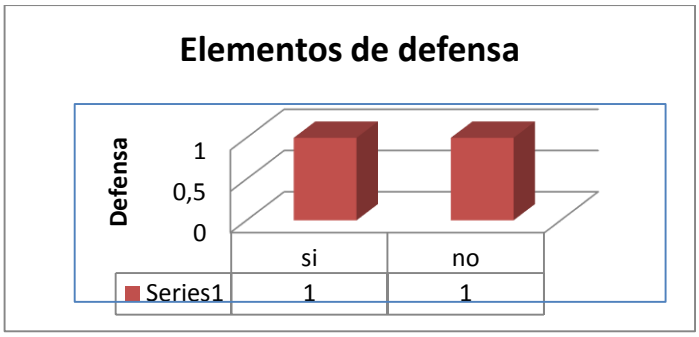


Gráfico 28**.** Elementos de defensa**.**

28. ¿Utilizan tecnologías de seguridad diferentes (el antivirus del firewall es diferente del antivirus del servidor de correo, el sistema operativo del router es diferente del sistema operativo del firewall, etc.)?

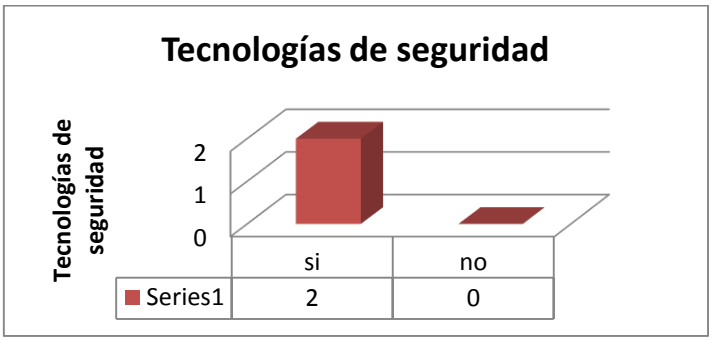


Gráfico 29. Tecnologías de seguridad.

29. ¿Dispone de un documento que detalla los sistemas de identificación y autenticación de usuarios para cada sistema o servicio?

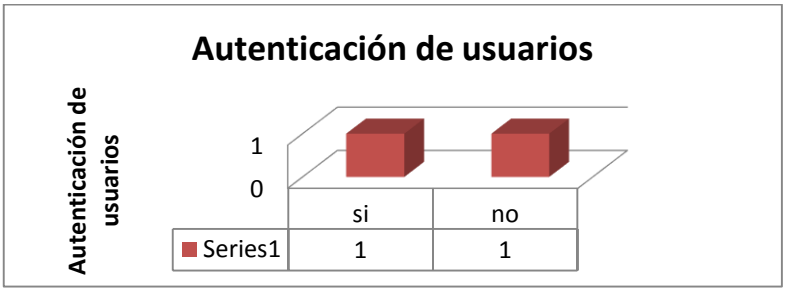


Gráfico 30. Autenticación de usuarios.

30. ¿Detalla el mecanismo de autenticación a cada sistema o servicio?

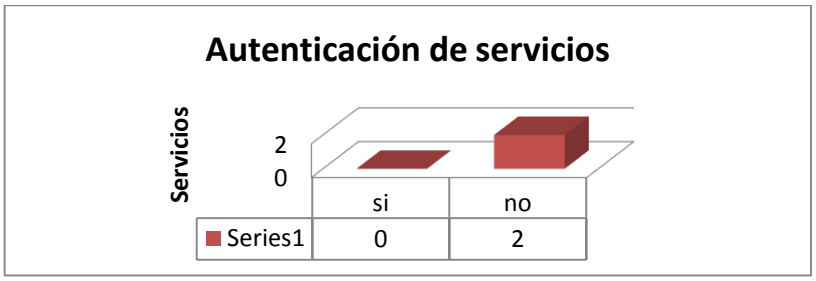


Gráfico 31. Autenticación de servicios.

31. ¿Detalla dónde se almacenan las contraseñas (las claves se almacenan cifradas en el fichero /etc/shadow en Linux, Active Directory en Windows, etc.)?

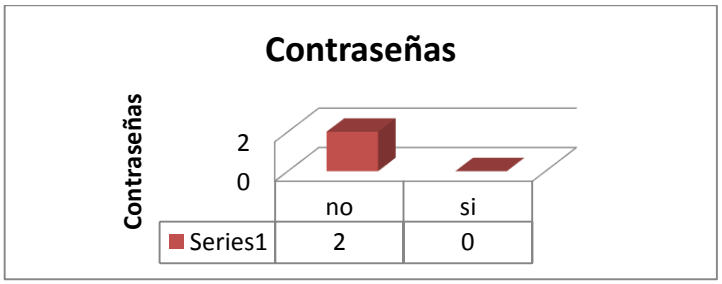


Gráfico 32. Contraseñas

32. ¿Detalla cómo se controlan los datos una vez en los sistemas?

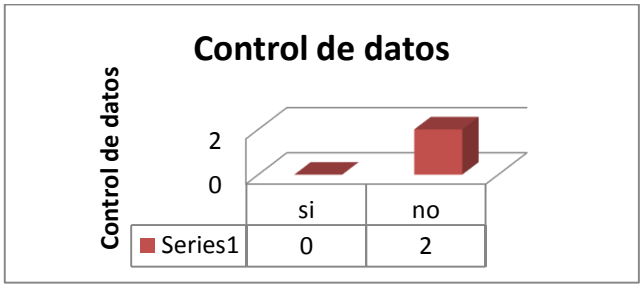


Gráfico 33. Control de datos.

33. ¿Precisa la validación de datos de entrada, salida y datos intermedios?

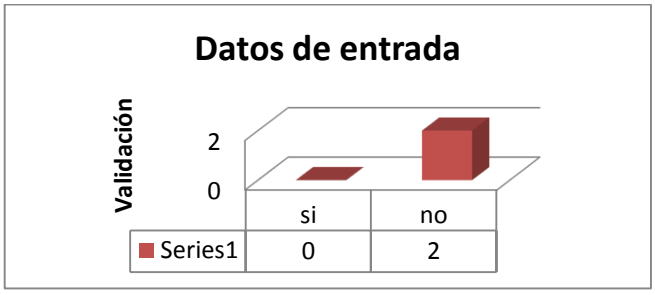


Gráfico 34. Validación de datos de entrada.

34. ¿Dicho estudio estima las necesidades de almacenamiento tanto para su funcionamiento como para el tiempo durante el que la información debe mantenerse?

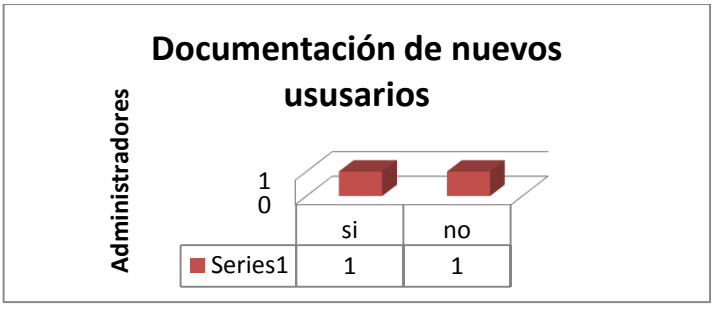


Gráfico 35. Tiempo de información.

35. ¿El Centro de Tecnología Educativa dispone de una normativa documentada que especifica que los usuarios no pueden compartir su identificador con nadie?

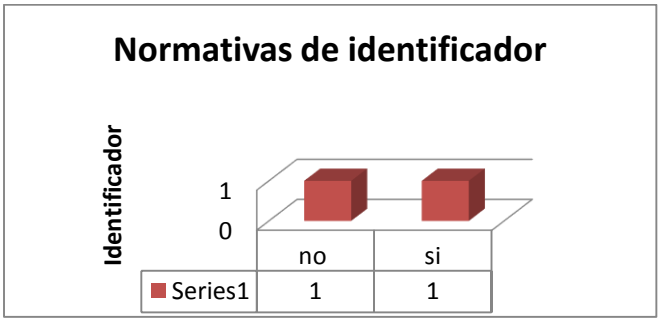


Gráfico 36. Normativas de Identificador.

36. ¿Se puede conocer un registro de las entidades responsables de cada identificador. Existe una relación de los identificadores con sus usuarios?.

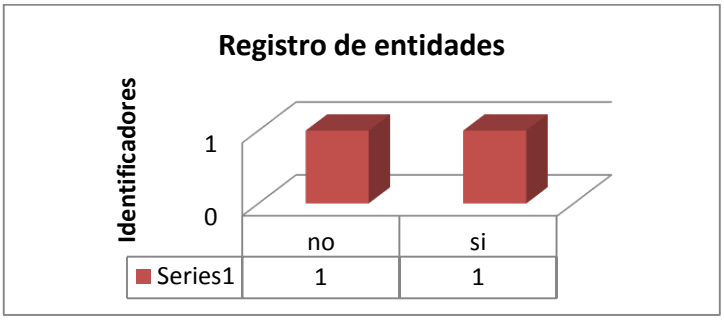


Gráfico 37. Registro de entidades responsables de los identificadores.

37. ¿Usted puede saber qué derechos tiene?

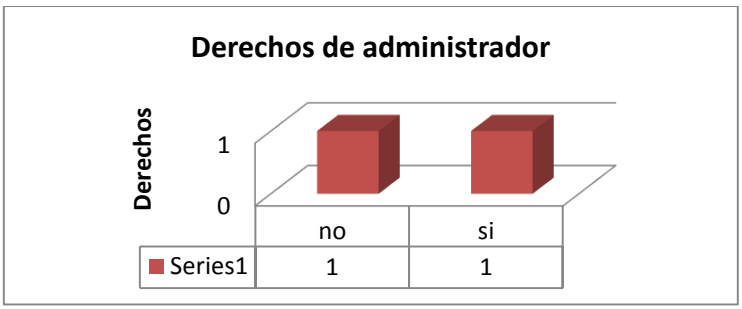


Gráfico 38. Derechos de administrador.

38. ¿Identifica el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad, procedimiento que indica que debe llevarse a cabo en los sistemas previos a su puesta en explotación?

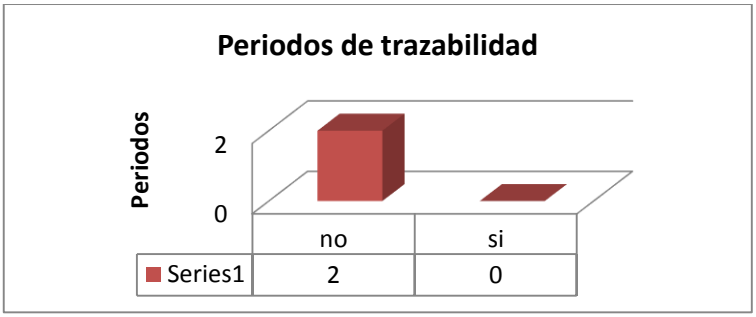


Gráfico 39. Periodos de trazabilidad.

39. ¿Se protegen los recursos del sistema con algún mecanismo que impida su utilización?

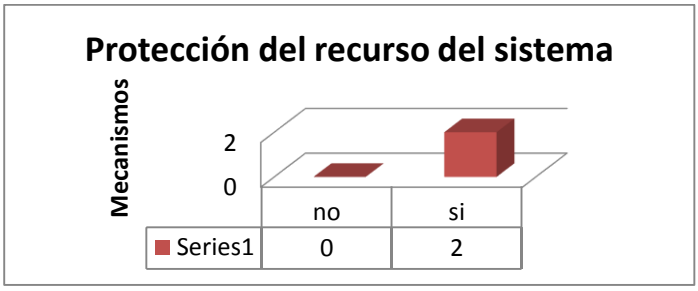


Gráfico 40. Protección del recurso del sistema

40. ¿Se dispone de evidencia documental (manual de administración, documento desarrollado internamente, etc.) donde se especifica cuáles son los componentes del sistema y sus ficheros o registros de configuración, así como los permisos de usuario que deben establecerse de forma que sólo los usuarios autorizados tengan acceso?

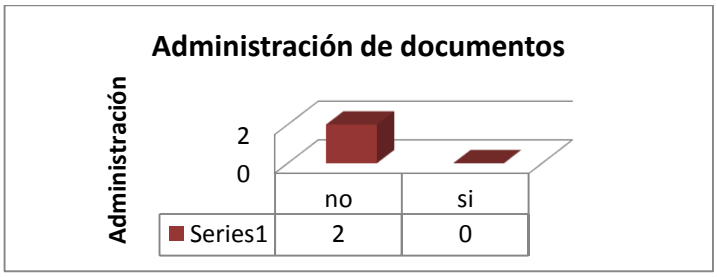


Gráfico 41. Administración de documentos.

41. La política y normativa de seguridad del sistema especifican quién es el responsable de cada recurso y, por lo tanto, es también responsable de la asignación de autorización y nivel de acceso a cada recurso.

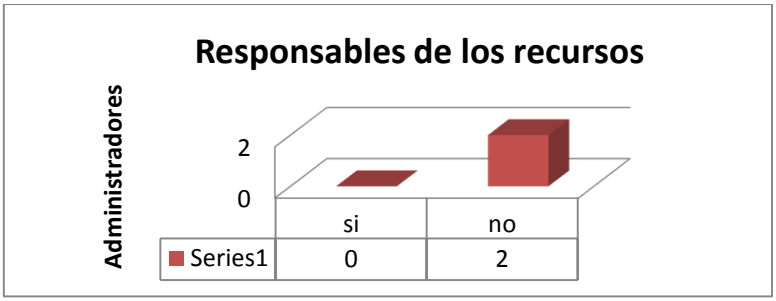


Gráfico 42. Responsabilidades de los recursos.

42. ¿Dispone de un documento en el que se detallan cuáles son las tareas críticas?

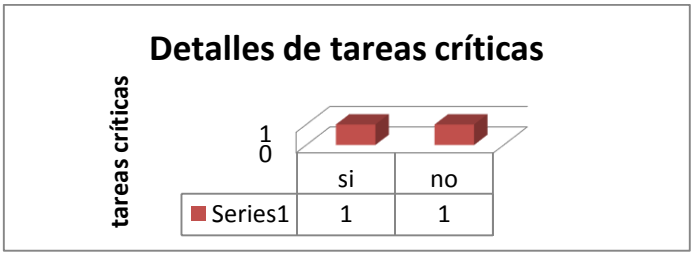


Gráfico 43. Detalle de tareas críticas.

43. ¿Dispone de un esquema de funciones y tareas en el que se contemplan las tareas críticas que son incompatibles en una misma persona?

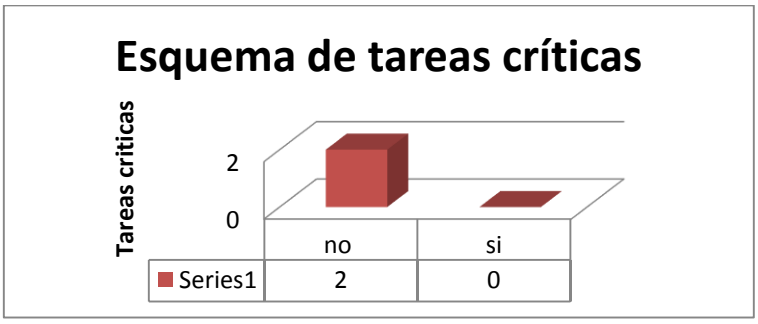


Gráfico 44. Esquema de tareas críticas.

44. ¿Contempla la incompatibilidad de tareas de auditoría o supervisión con las de cualquier otra función relacionada con el sistema?

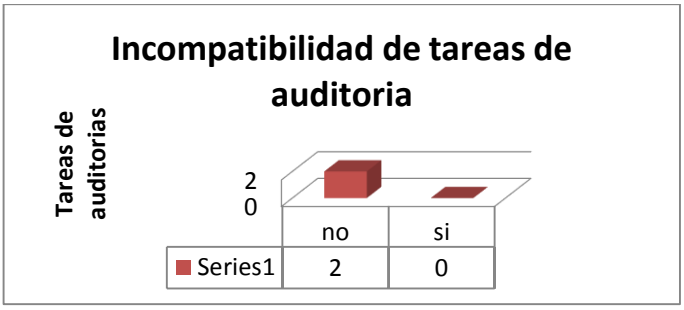


Gráfico 45. Incompatibilidad de tareas de auditoria.

45. ¿Se limitan los privilegios de cada usuario al mínimo estrictamente necesario para acceder a la información requerida y para cumplir sus obligaciones?

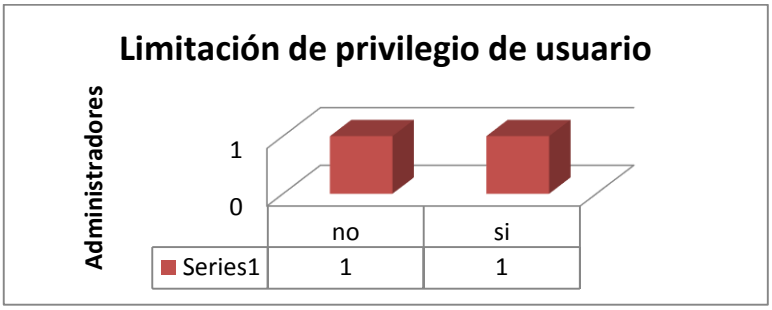


Gráfico 46. Limitación de acceso de usuario.

46. ¿Se encuentra identificado el mecanismo de autenticación en cada recurso?

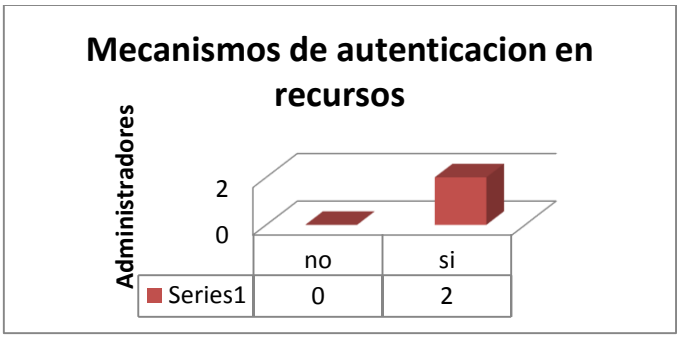


Gráfico 47. Mecanismos de autenticación en recursos.

47. Si utilizan contraseñas ¿cumplen las reglas básicas de calidad?

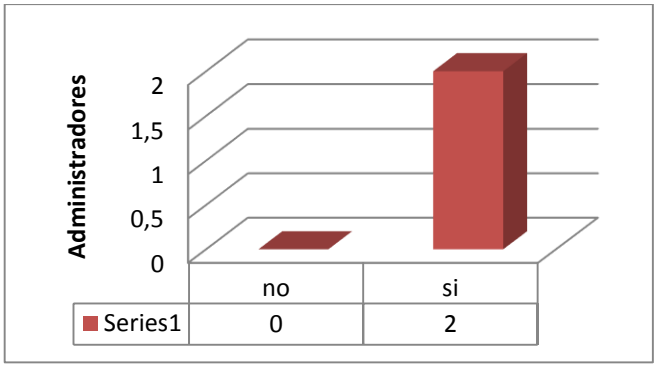


Gráfico 48. Reglas básicas de contraseñas.

48. ¿Dicha política o normativa establece que la cuenta del usuario no se habilita hasta que éste haya confirmado la recepción del autenticador?

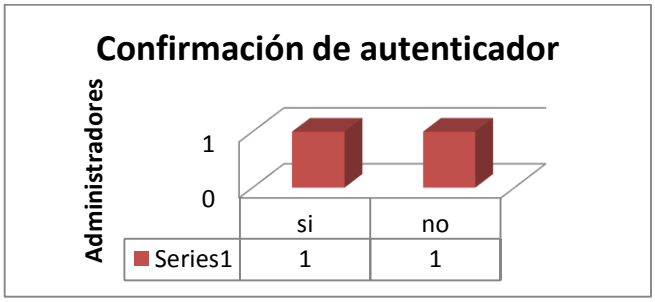


Gráfico 49. Confirmación de autenticador.

49. ¿Están los autenticadores bajo el control exclusivo del usuario?

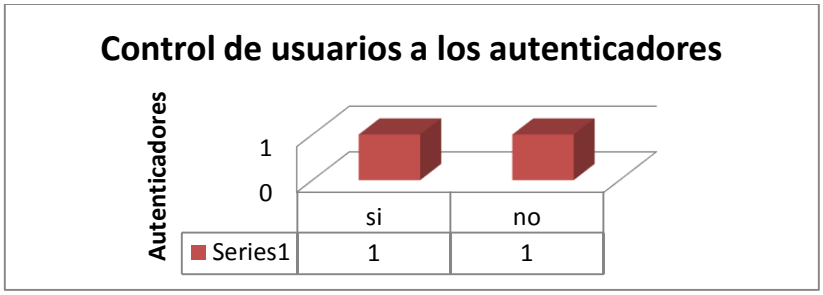


Gráfico 50. Control de usuarios a los autenticadores.

:

50. ¿Se cambian los autenticadores con la periodicidad marcada por la política de la organización (atendiendo a la categoría del sistema al que se accede)?

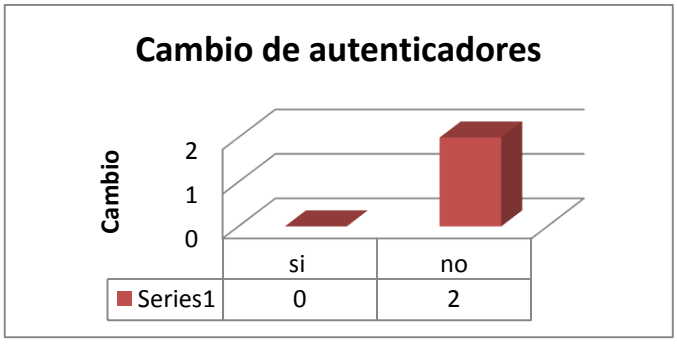


Gráfico 51. Cambio de autenticadores.

51. ¿Se utilizan claves concertadas?

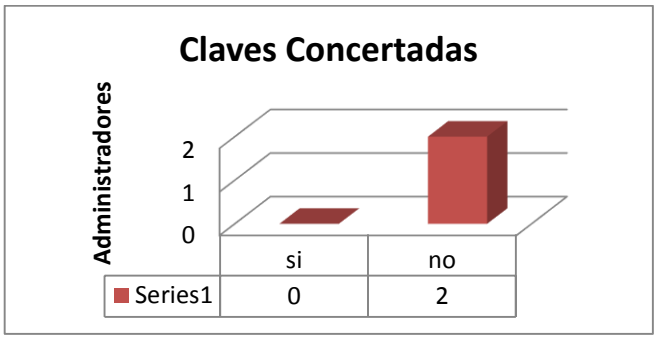


Gráfico 52. Claves Concertadas.

52. Si utilizan contraseñas ¿cumplen las políticas rigurosas de calidad y renovación?

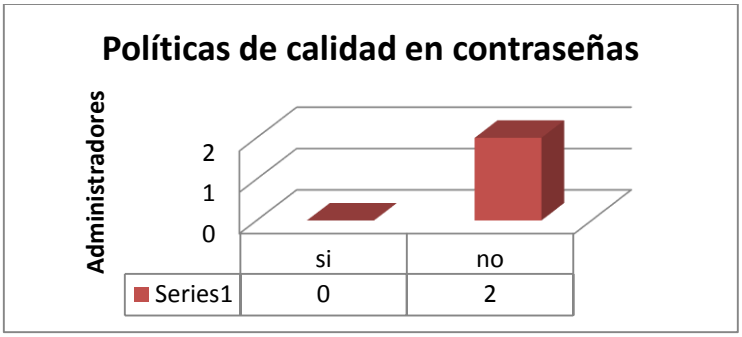


Gráfico 53. Políticas de calidad de contraseña**.**

53. ¿Dispone de una política o normativa documentada que especifica que los sistemas antes de entrar en explotación o los ya existentes son configurados de forma que no revelen información del sistema antes de un acceso autorizado?

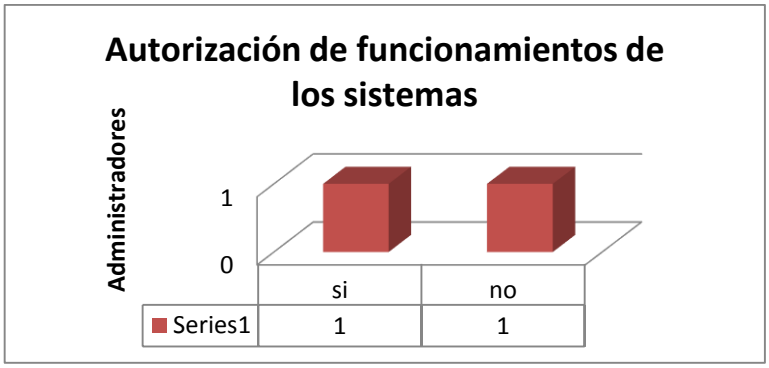


Gráfico 54. Autorización de funcionamiento de los sistemas.

54. ¿Se limita el número de intentos fallidos de acceso?

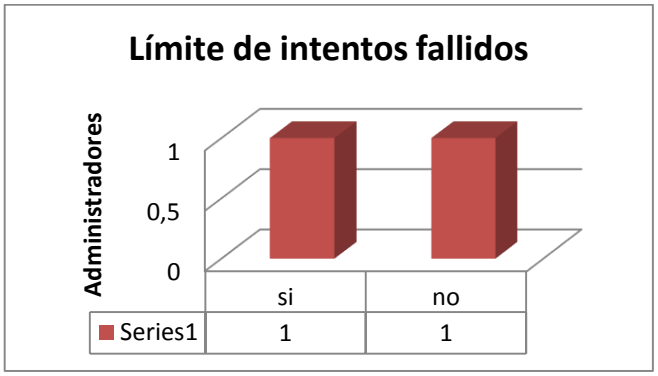


Gráfico 55. Límite de intentos fallidos.

55. ¿Se registran los accesos con éxito y los fallidos?

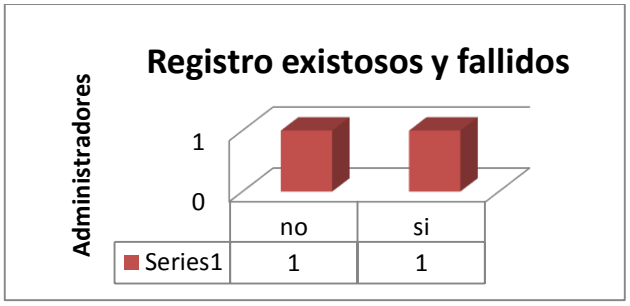


Gráfico 56. Registro de intentos exitosos y fallidos.

56. ¿Informa el sistema al usuario de sus obligaciones inmediatamente después de obtener el acceso?

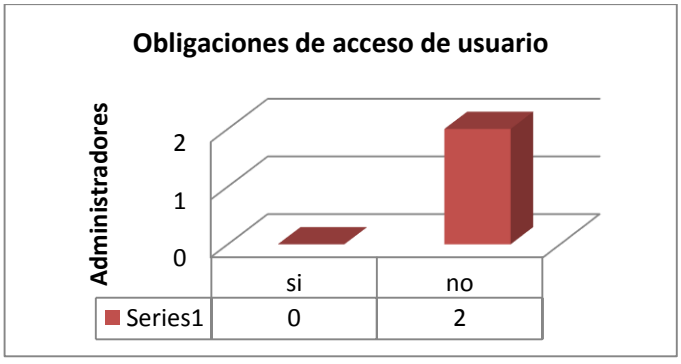


Gráfico 57. : Obligaciones de acceso de usuario.

57. ¿Informa el sistema al usuario del último acceso con su identidad con éxito?

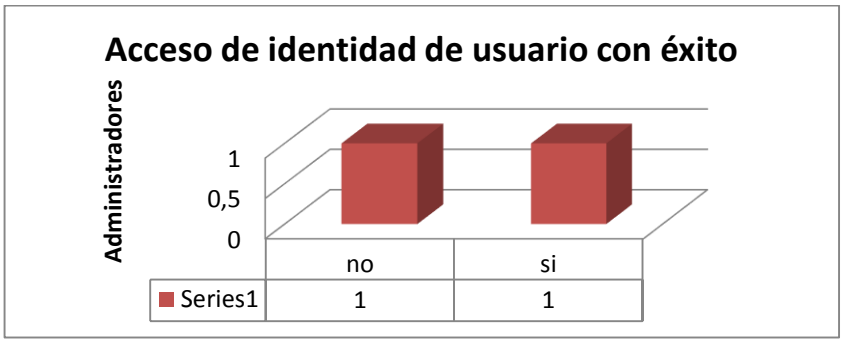


Gráfico 58. Acceso de identidad exitoso.

58. ¿Se limita el horario, fechas y lugar desde donde se accede?

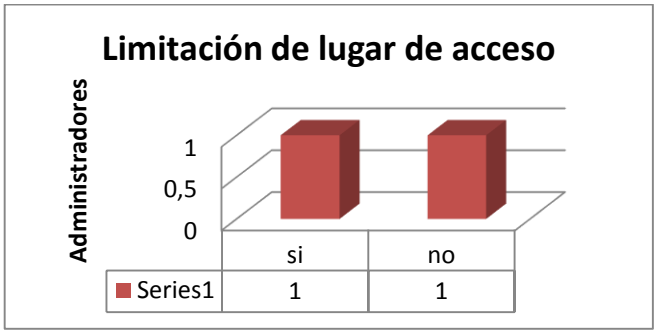


Gráfico 59. Limitación de lugar de acceso.

59. ¿Se garantiza la seguridad del sistema cuando acceden remotamente usuarios u otras entidades?

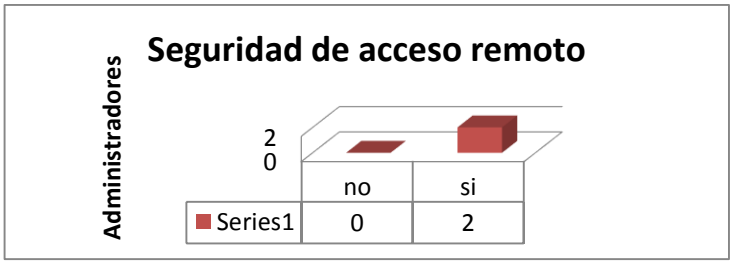


Gráfico 60. Seguridad de acceso remoto.

60. ¿Dispone de una política o normativa documentada que regula las actividades que pueden realizarse remotamente?

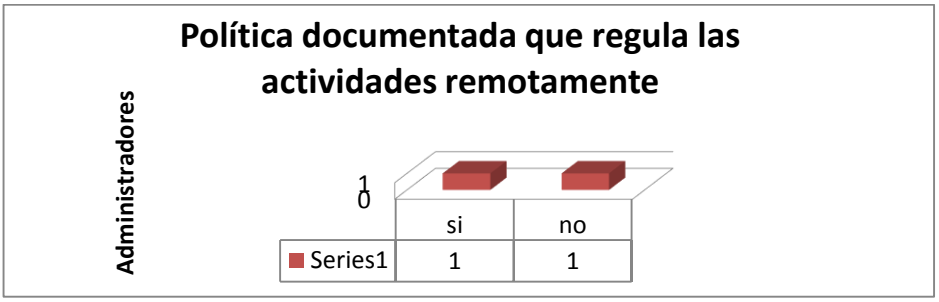


Gráfico 61. Políticas documentadas que regulan las actividades remotamente.

61. ¿Los accesos remotos deben ser autorizados previamente, indicando la persona que puede autorizar el acceso?

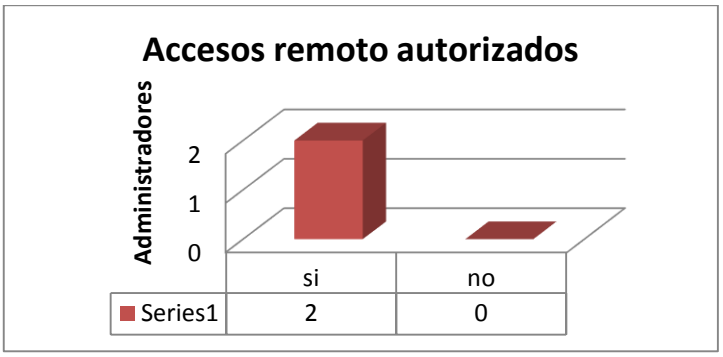


Gráfico 62. Accesos remotos autorizados.

62. ¿Dispone de un inventario del sistema?

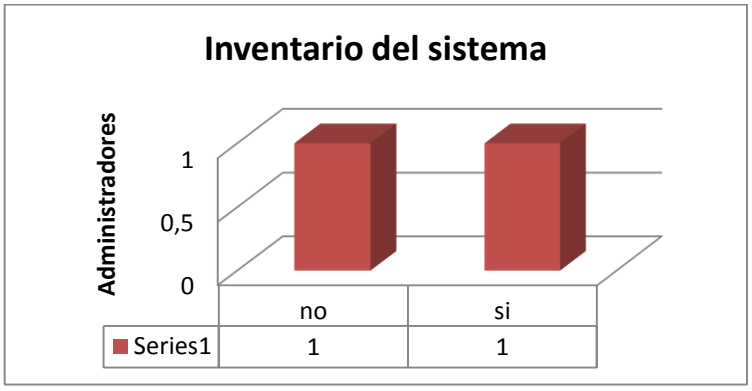


Gráfico 63. Inventario del sistema.

63. ¿Dispone de un procedimiento documentado que especifica el responsable y la frecuencia de su revisión y/o actualización?

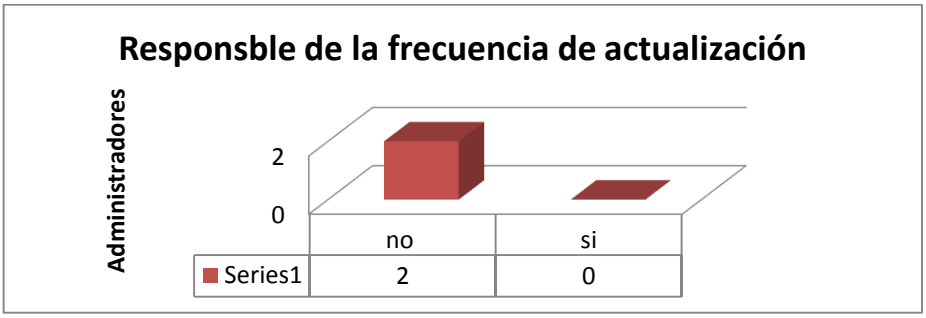


Gráfico 64. Responsable de la frecuencia de actualización.

64. ¿Dispone de un plan de mantenimiento del equipamiento físico y lógico?

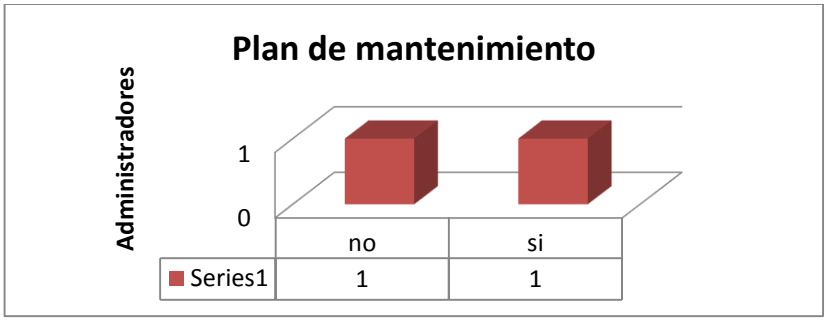


Gráfico 65. Plan de mantenimiento.

65. ¿Atiende a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas?

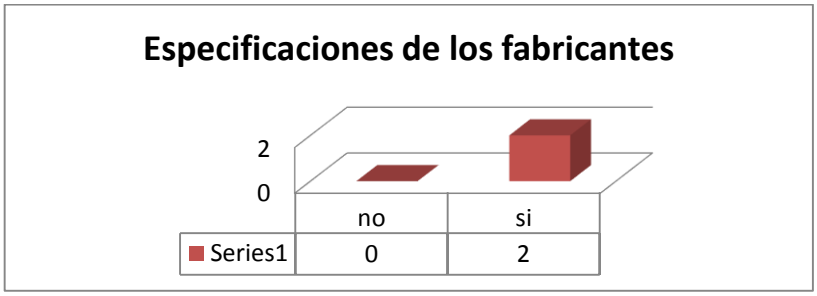


Gráfico 66. Especificaciones de los fabricantes.

66. ¿Dispone de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones, teniendo en cuenta el cambio en el riesgo de cara a su priorización?

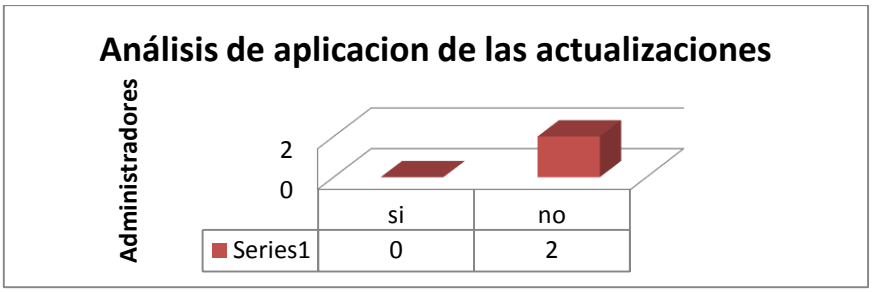


Gráfico 67. Análisis de aplicación de las actualizaciones.

67. ¿Dispone de mecanismos de prevención y reacción frente a código dañino (virus, gusanos, troyanos, programas espía y "malware" en general)?

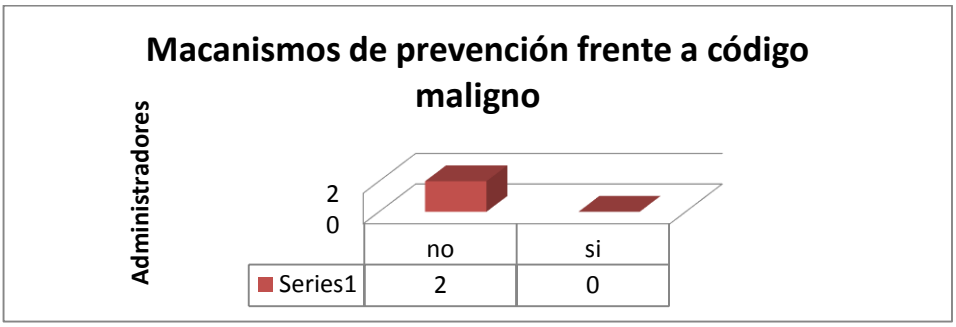


Gráfico 68. Mecanismos de prevención frente a código maligno.

68. ¿Dispone de un proceso integral para hacer frente a incidentes que puedan tener un impacto en la seguridad del sistema?

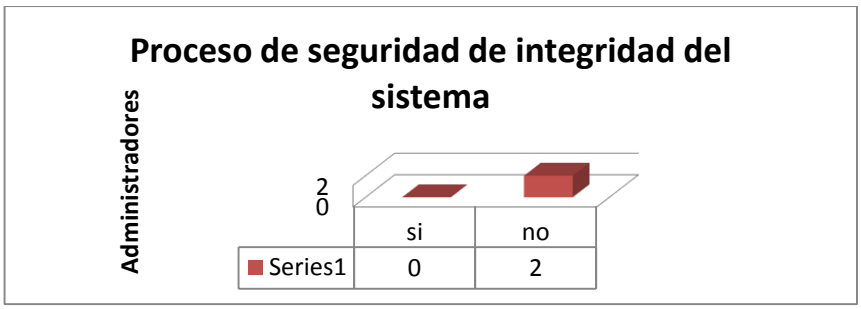


Gráfico 69. Proceso de Seguridad de integridad del sistema.

69. ¿Incluye la toma de medidas urgentes, contemplando la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros (según convenga al caso)?

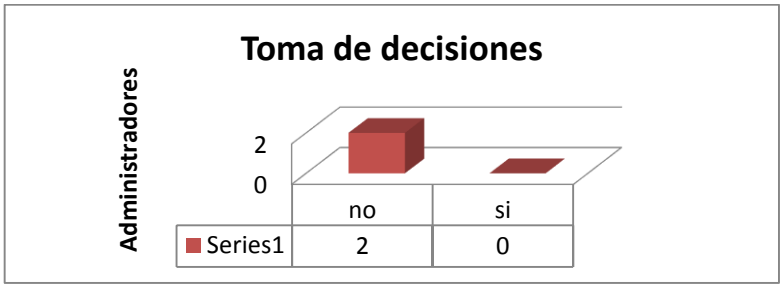


Gráfico 70. Toma de decisiones.

70. ¿Incluye la asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente?

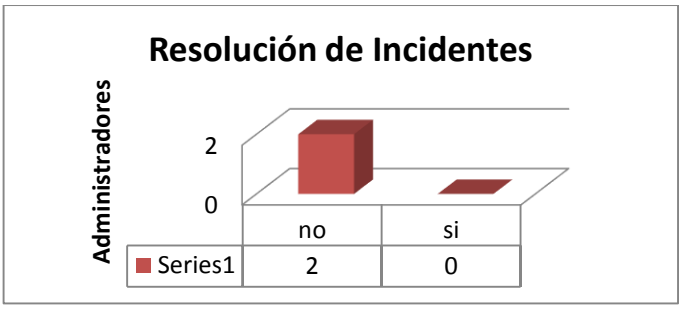


Gráfico 71. Resolución de incidentes.

71. ¿Incluye en los procedimientos de usuario la identificación y forma de tratar el incidente?

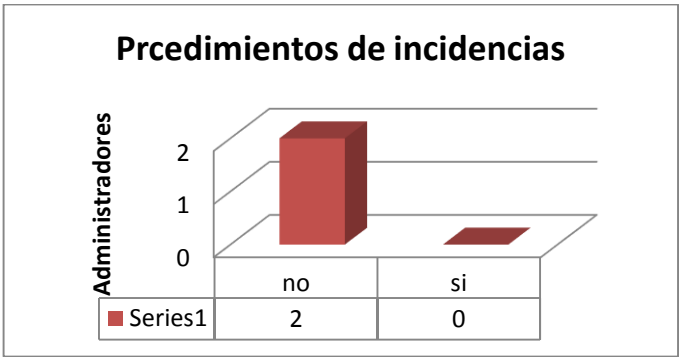


Gráfico 72. Procedimientos de incidencias.

72. ¿Dispone de mecanismos que garanticen la corrección de la hora a la que se realiza el registro?

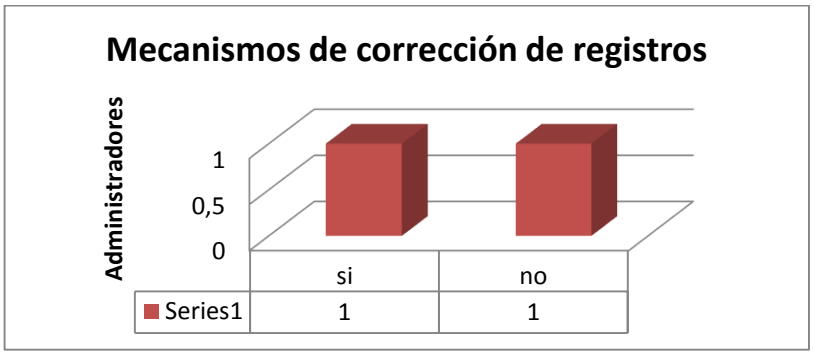


Gráfico 73. Mecanismos de corrección de registros.

73. ¿Se registran todas las actividades de los usuarios en el sistema?

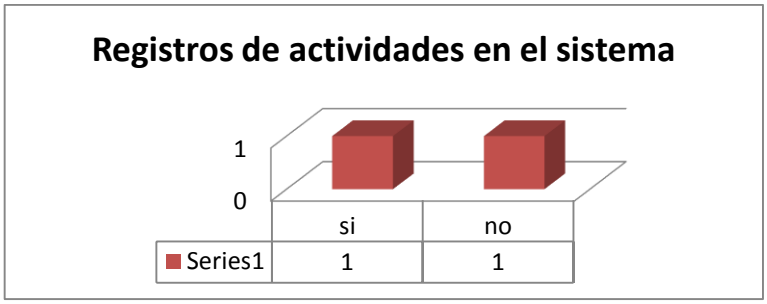


Gráfico 74. Registro de actividades en el sistema.

74. ¿Indican quién realiza la actividad, cuándo la realiza y sobre qué información, sea cual sea el usuario?

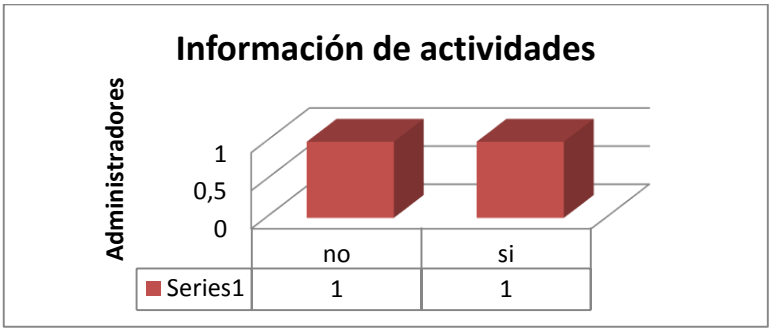


Gráfico 75. Información de actividades**.**

75. ¿Incluye la actividad de los operadores y administradores del sistema?

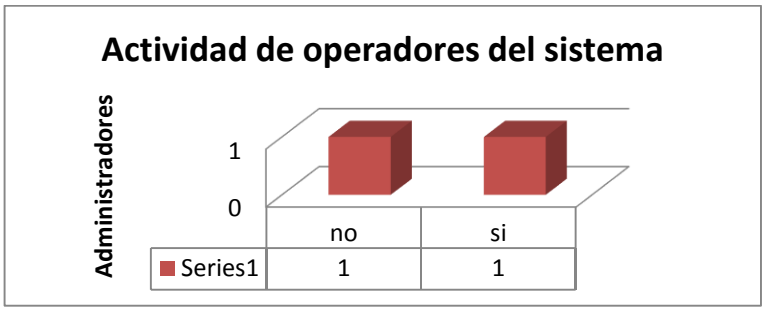


Gráfico 76. Actividad de operadores del sistema.

76. ¿La determinación de las actividades a registrar y su nivel de detalle se determinan en base al análisis de riesgos del sistema?

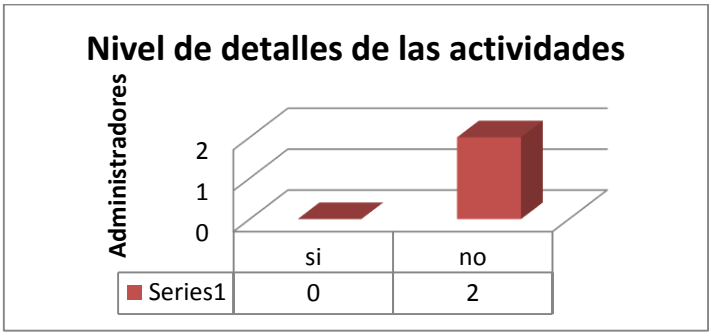


Gráfico 77. Nivel de detalles de las actividades.

77. ¿Se encuentran protegidos los registros del sistema?

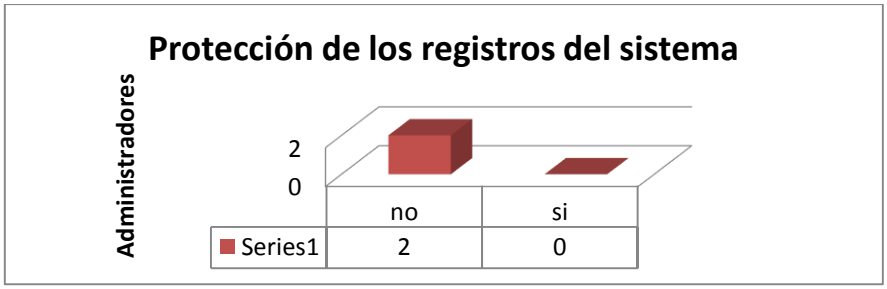


Gráfico 78. Protección de los registros del sistema.

78. ¿Se encuentran protegidos frente a su modificación o eliminación por personal no autorizado?

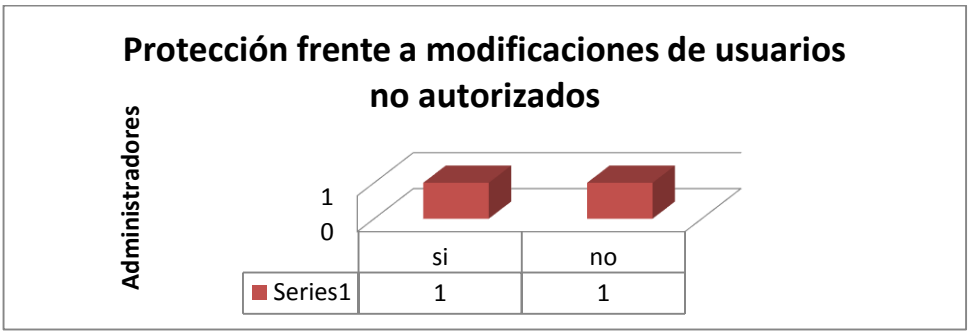


Gráfico 79. Protección frente a modificaciones de usuarios no autorizados.

79. ¿Las copias de seguridad, si existen, se ajustan a los mismos requisitos?

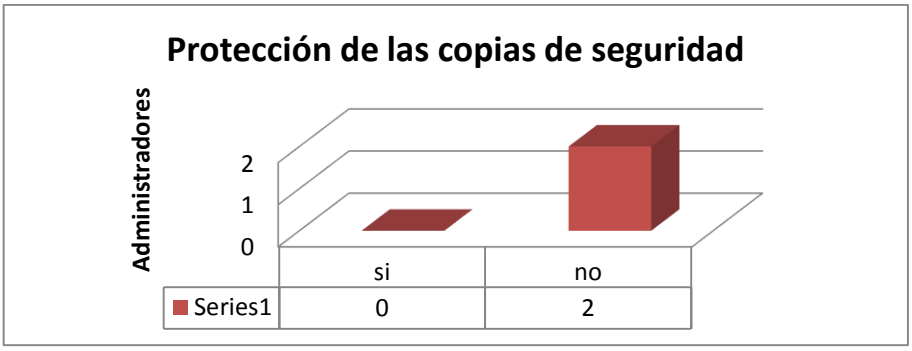


Gráfico 80. Protección de las copias de seguridad.

80. ¿Dispone de un conjunto de indicadores que midan el desempeño real del sistema en materia de seguridad?

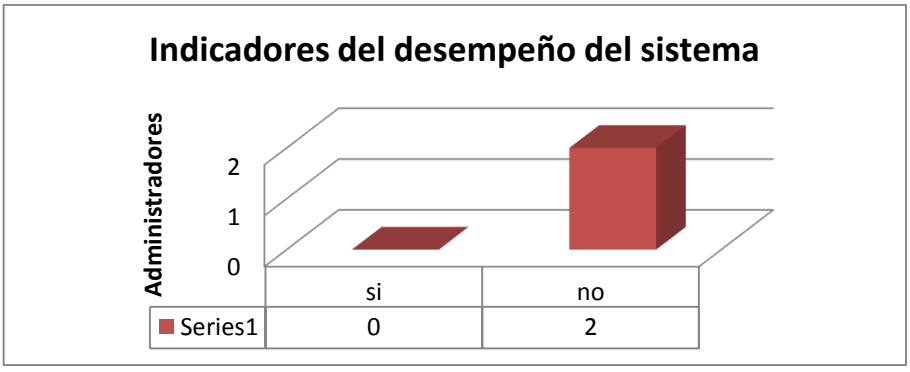


Gráfico 81. Indicadores del desempeño del sistema.

81. ¿Miden la eficacia y eficiencia de las medidas de seguridad?

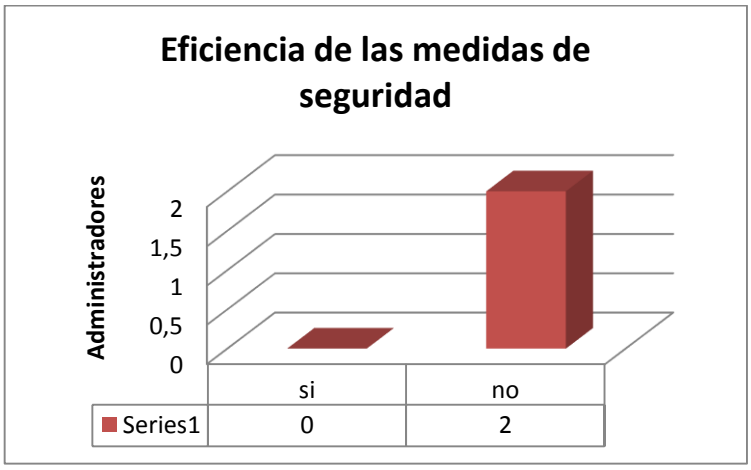


Gráfico 82. Eficiencia de las medidas de seguridad.

82. ¿Miden el impacto de los incidentes de seguridad?

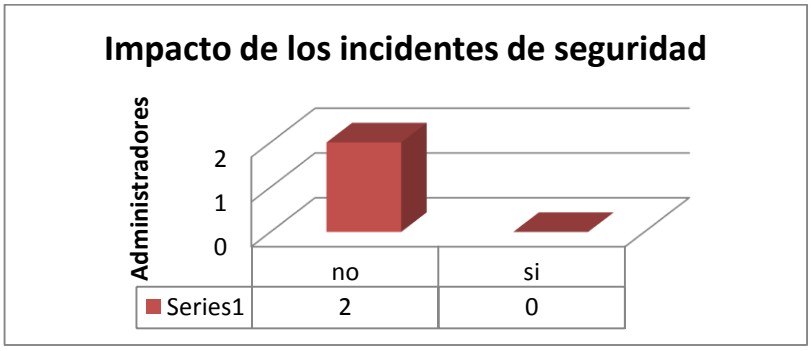


Gráfico 83. Impacto de los incidentes de seguridad.

83. ¿El equipamiento ha sido instalado en áreas separadas específicas para su función?

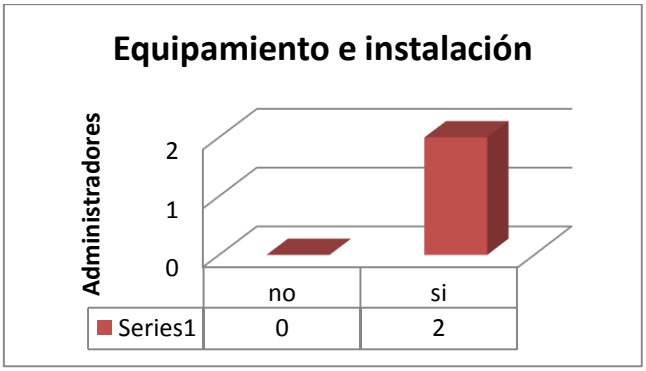


Gráfico 84. Equipamiento e instalación.

84. ¿El acceso a las áreas separadas se encuentra controlado?

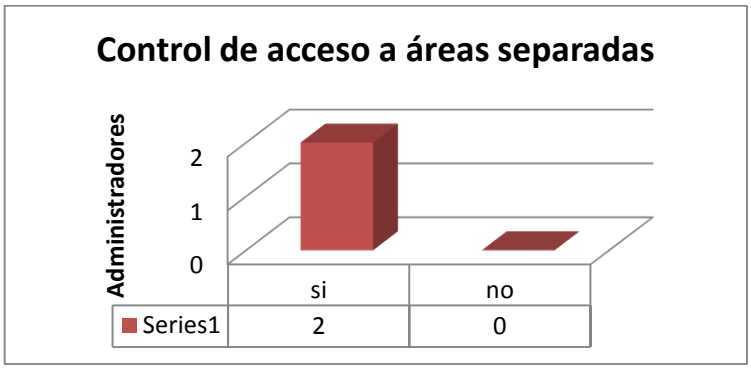


Gráfico 85. Control de acceso a áreas separadas.

85. ¿El control de acceso a los locales donde hay equipamiento que forme parte del sistema de información se encuentra gestionado?

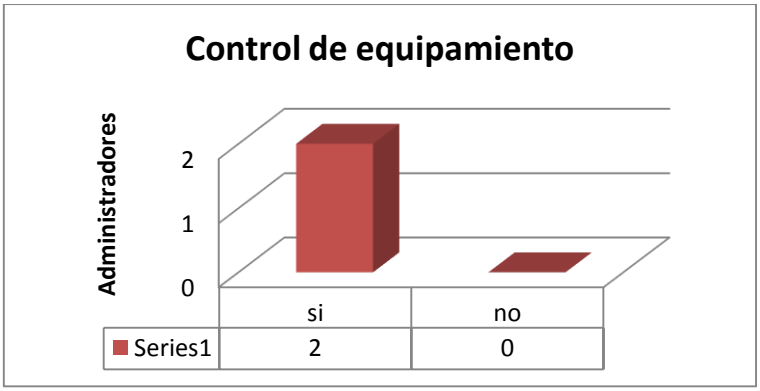


Gráfico 86. Control de equipamiento.

86. ¿Se identifican a todas las personas que accedan a estos locales?

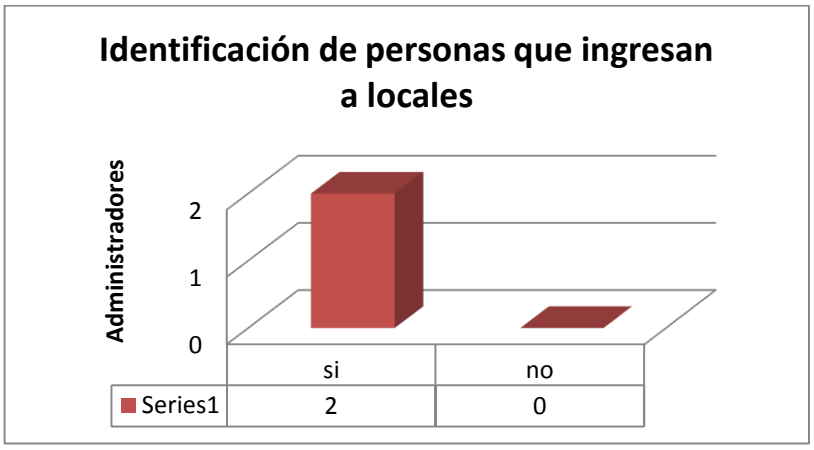


Gráfico 87. Identificadores de personas que ingresan a locales.

87. ¿Los locales donde se ubican los sistemas de información y sus componentes disponen de las adecuadas condiciones de temperatura y humedad?

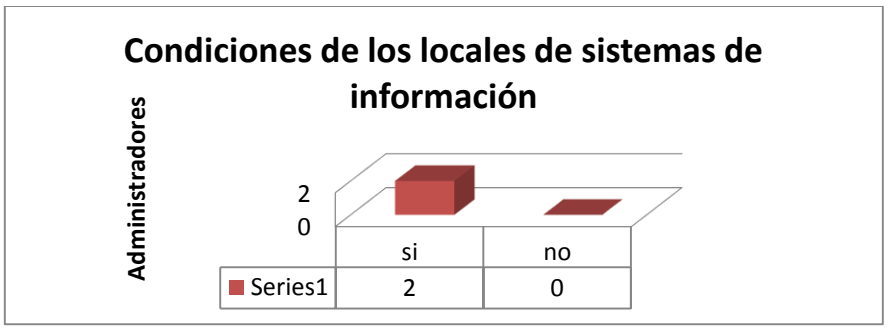


Gráfico 88. Condiciones de los locales de sistemas de información.

88. ¿Cuentan con protección del cableado frente a incidentes fortuitos o deliberados?

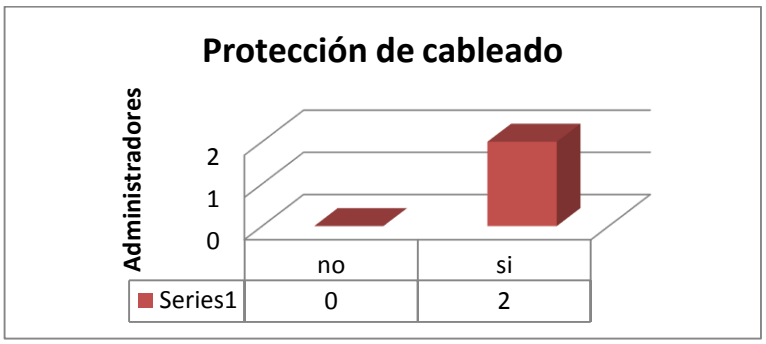


Gráfico 89. Protección de cableado.

89. ¿Existe equipamiento redundante en caso de fallo de los equipos principales de acondicionamiento?

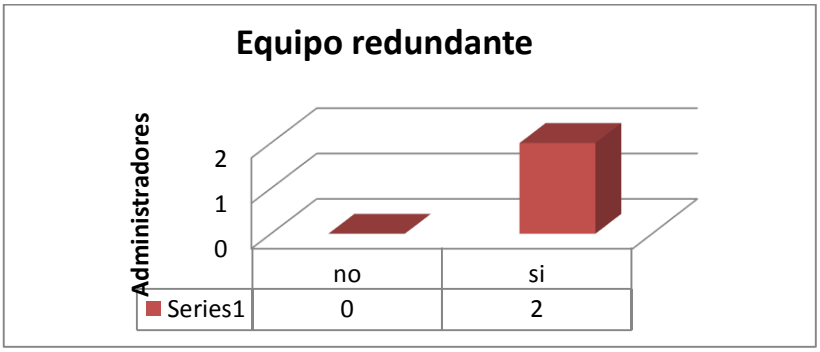


Gráfico 90. Equipos redundantes.

90. ¿Se encuentra actualizado el etiquetado de los cables?

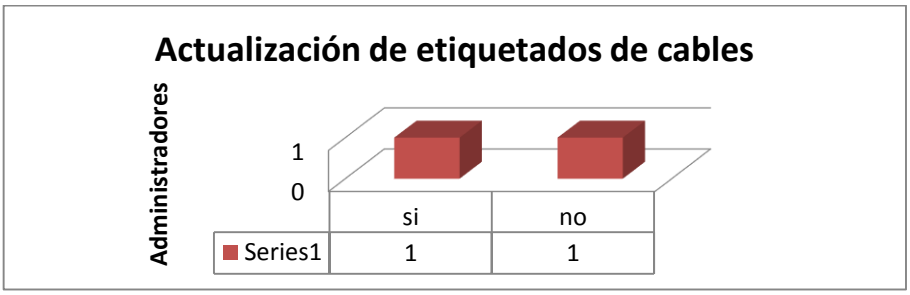


Gráfico 91. Actualización de etiquetados de cables.

91. ¿Se protegen los locales donde se ubiquen los sistemas de información y sus componentes frente a incendios fortuitos o deliberados?

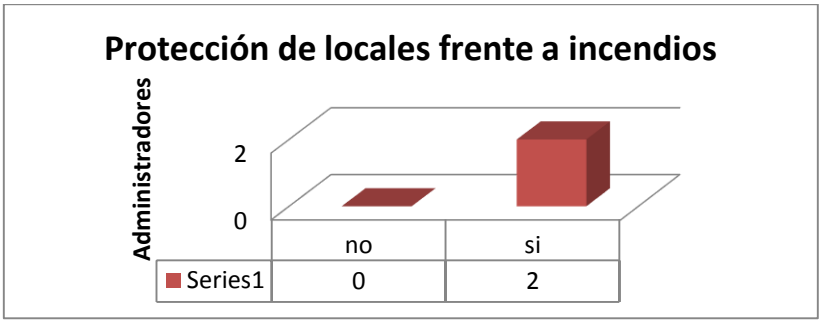


Gráfico 92. Protección de locales de ubicación de la información.

92. ¿Se protegen los locales donde se ubiquen los sistemas de información y sus componentes frente a incidentes fortuitos o deliberados causados por el agua?

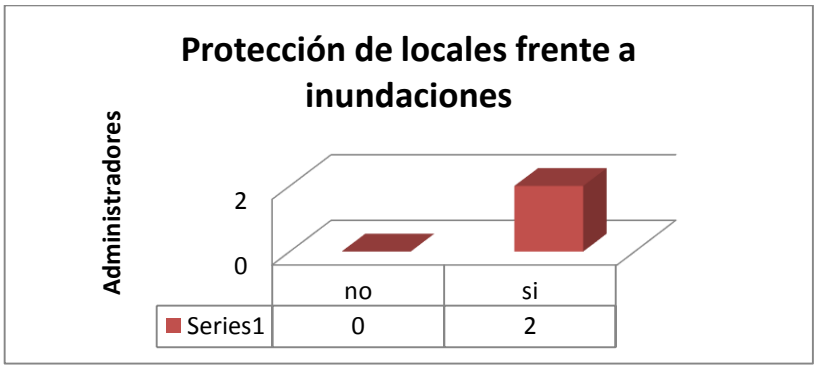


Gráfico 93. Protección de locales frente a inundaciones.

93. ¿Está garantizada la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles?

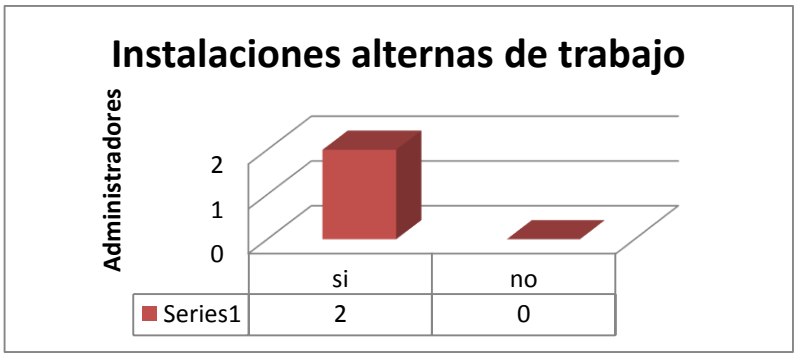


Gráfico 94. Instalaciones alternas de trabajo

.

94. ¿Dispone de cortafuegos que separe la red interna del exterior?

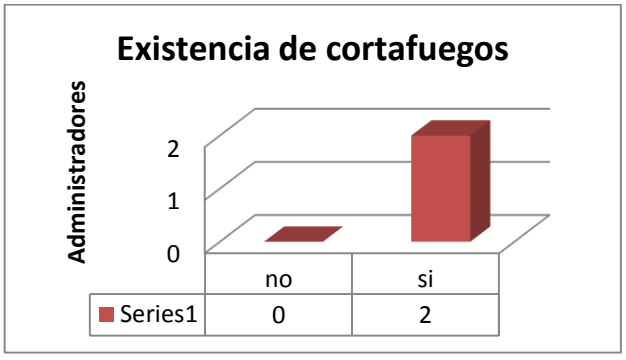


Gráfico 95. Existencia de cortafuegos.

95. Respecto a dichos cortafuegos ¿Consta de dos o más equipos de diferente fabricante dispuestos en cascada?

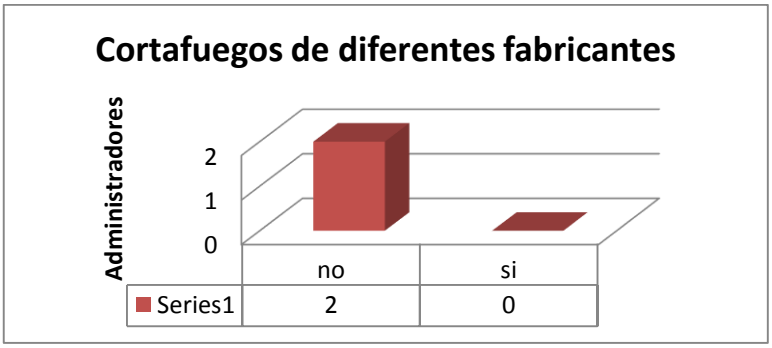


Gráfico 96. Cortafuegos de diferentes fabricantes.

96. ¿Se emplean redes privadas virtuales cuando la comunicación discurre por redes fuera del propio dominio de seguridad?

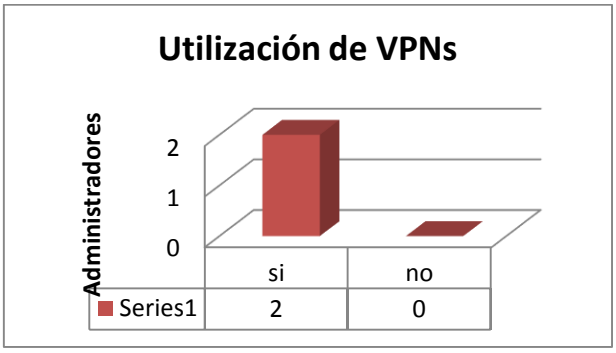


Gráfico 97. Utilización de VPNs.

.

97. ¿Se encuentra la red segmentada?

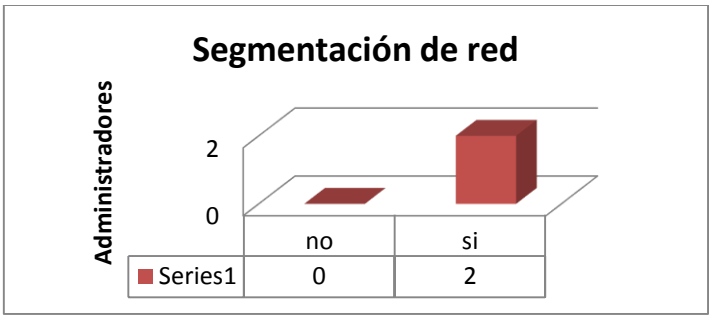


Gráfico 98. Segmentación de red.

98. ¿Existe control de entrada de los usuarios que llegan a cada segmento?

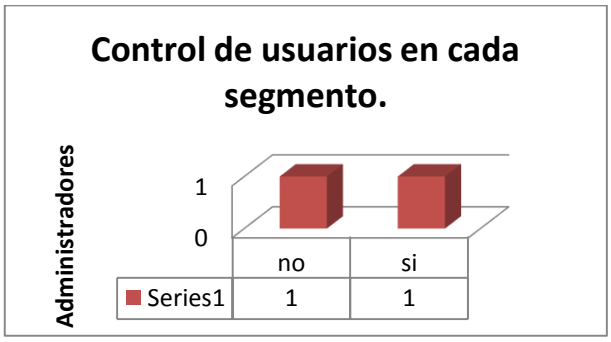


Gráfico 99. Control de usuarios en cada segmento.

99. ¿Existe control de salida de la información disponible en cada segmento?

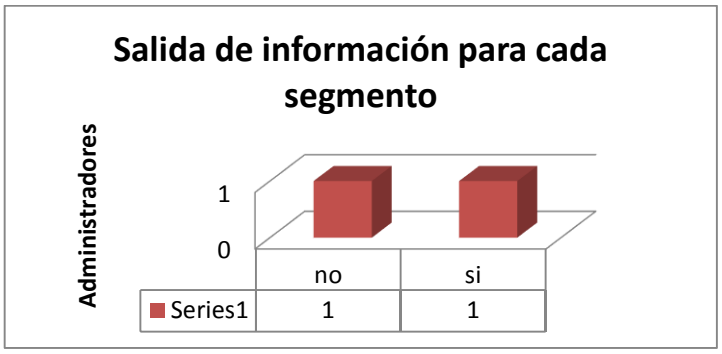


Gráfico 100. Salida de información por segmentos.

100. ¿Está el punto de interconexión particularmente asegurado, mantenido y monitorizado?

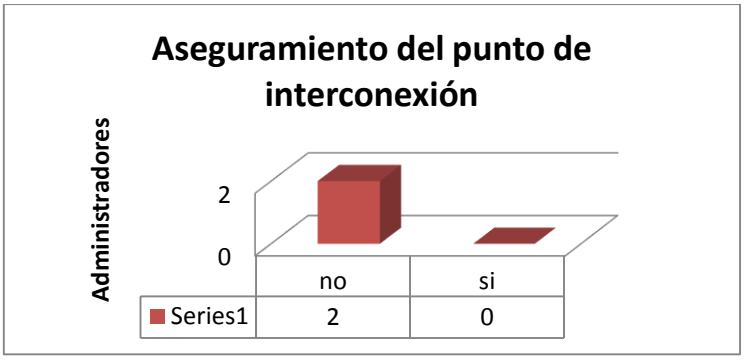


Gráfico 101. Aseguramiento del punto de interconexión.

101. ¿Se ha establecido un tiempo máximo para que los equipos alternativos entren en funcionamiento?

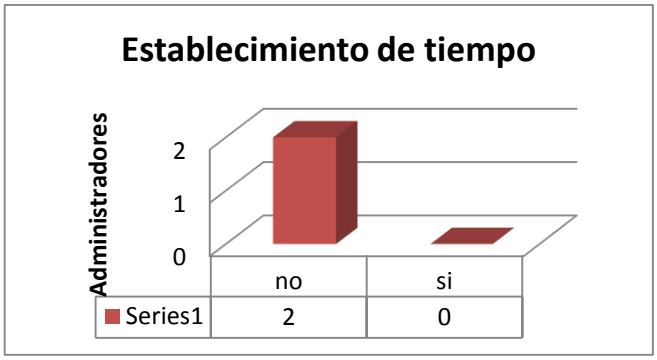


Gráfico 102. Establecimiento de tiempo para el funcionamiento de equipos alternativos.

102. ¿Realizan copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad determinada?

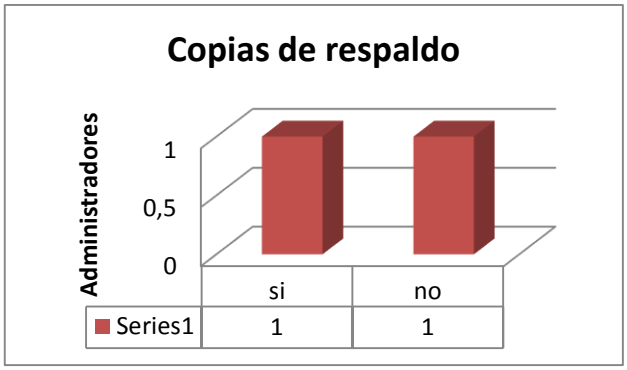


Gráfico 103. Copias de respaldo.

103. ¿Estas copias de seguridad abarcan la información de trabajo del CTE?

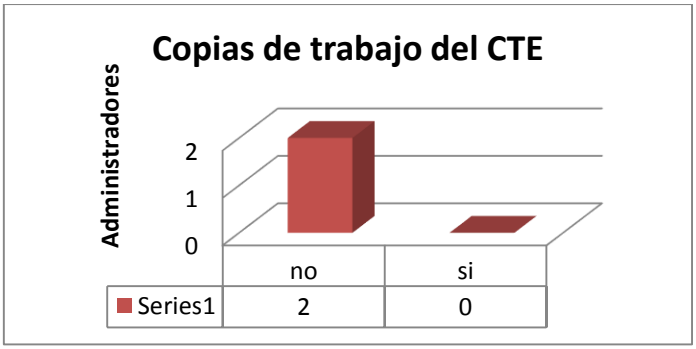


Gráfico 104. Copias de trabajo del CTE.

104. ¿Abarcan las aplicaciones en explotación, incluyendo los sistemas operativos?

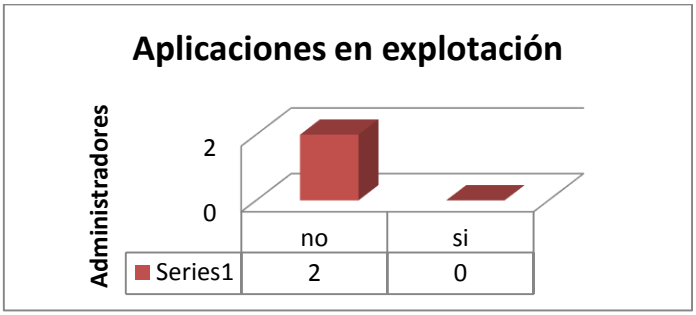


Gráfico 105. Aplicaciones en explotación.

105. ¿Existe un proceso de autorización para la recuperación de información de las copias de seguridad?

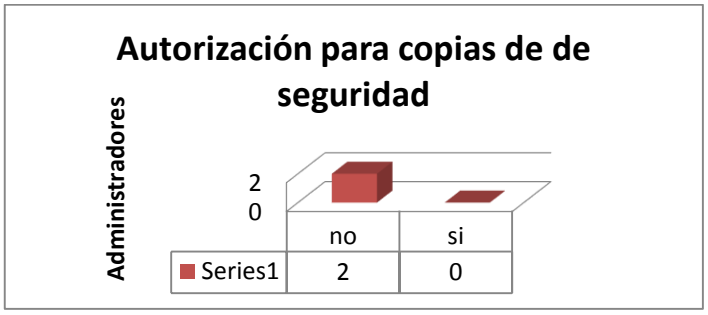


Gráfico 106. Autorización para copias de seguridad.

106. ¿Se verifica regularmente que la información respaldada está correctamente dispuesta para ser recuperada en caso de necesidad?

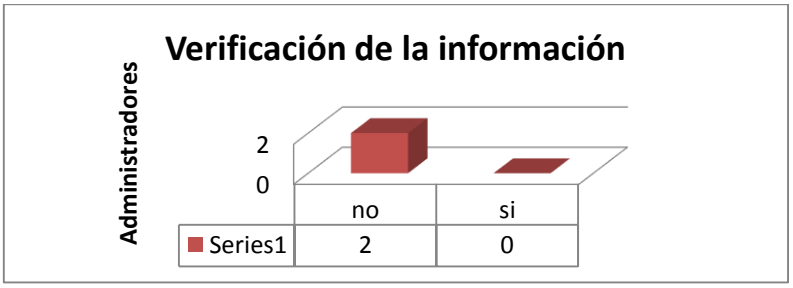


Gráfico 107. Verificación de la Información

107. ¿La información que se distribuye por medio de correo electrónico se protege, tanto en el cuerpo de los mensajes como en los anexos?

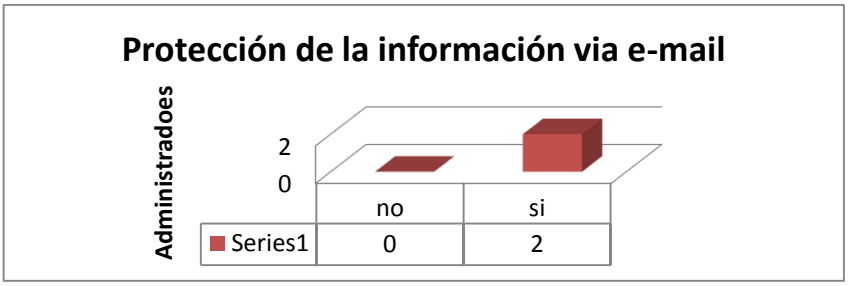


Gráfico 108. Protección de la Información vía e-mail.

108. ¿Se protege la información de encaminamiento de mensajes y establecimiento de conexiones?

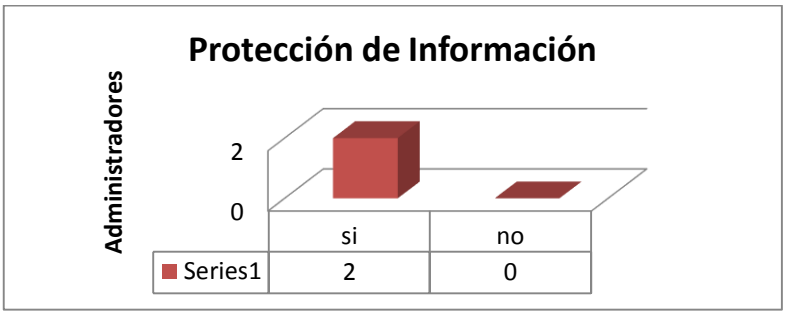


Gráfico 109. Protección de información.

109. ¿Se protege frente a programas dañinos (virus, gusanos, troyanos, espías u otros de naturaleza análoga)?

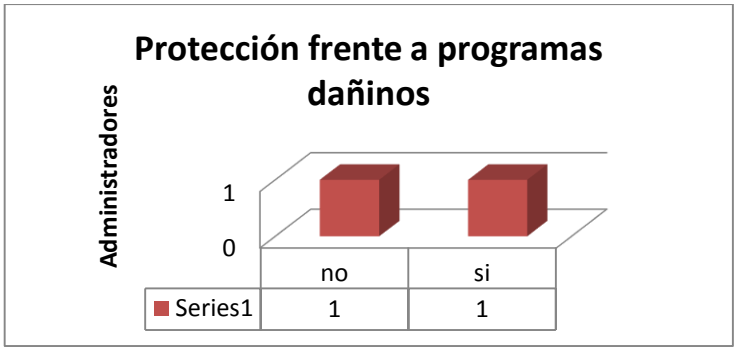


Gráfico 110. Protección frente a programas dañinos.

110. ¿Se encuentran protegidos los subsistemas dedicados a la publicación de información frente a las amenazas que les son propias?

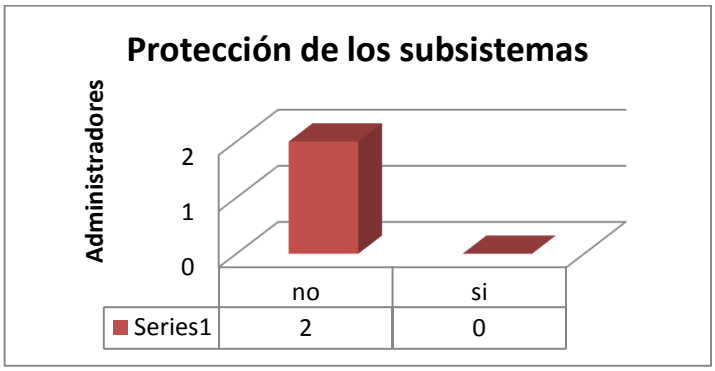


Gráfico 111. Protección de los subsistemas.

111. Cuando la información tenga algún tipo de control de acceso ¿se garantiza la imposibilidad de acceder a la información obviando la autenticación?

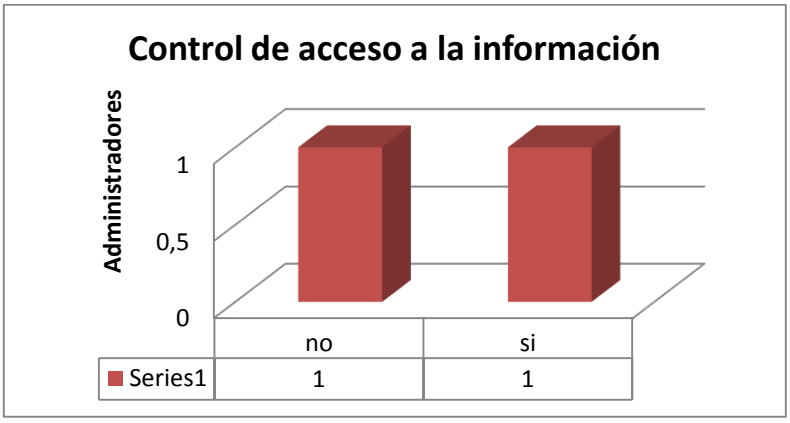


Gráfico 112. Control de acceso a la información.

112. ¿Se previenen ataques de manipulación de URL?

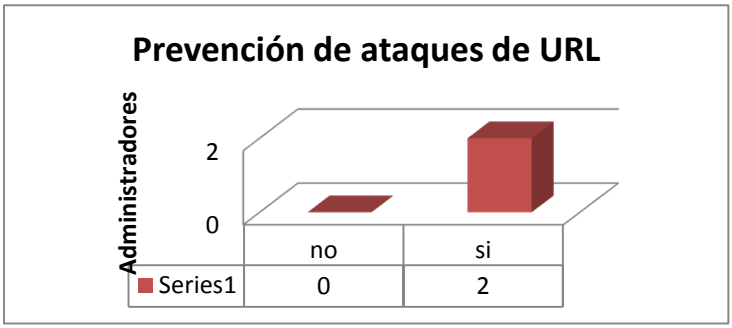


Gráfico 113. Prevención de ataques de URL.

113. ¿Se previenen ataques de manipulación de las cookies de los usuarios?

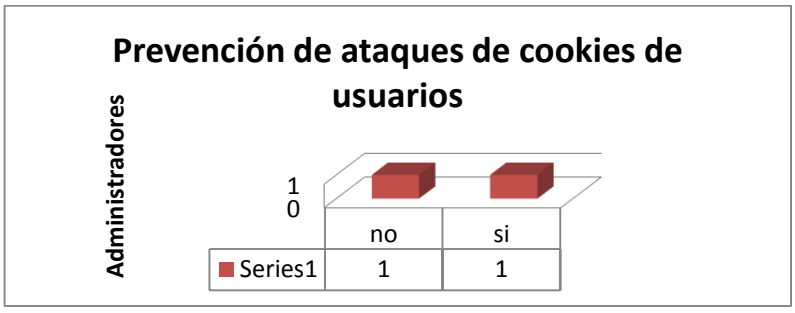


Gráfico 114. Prevención de ataques de cookies de usuarios.

114. ¿Se previenen ataques de manipulación de “proxys” o “cachés”?

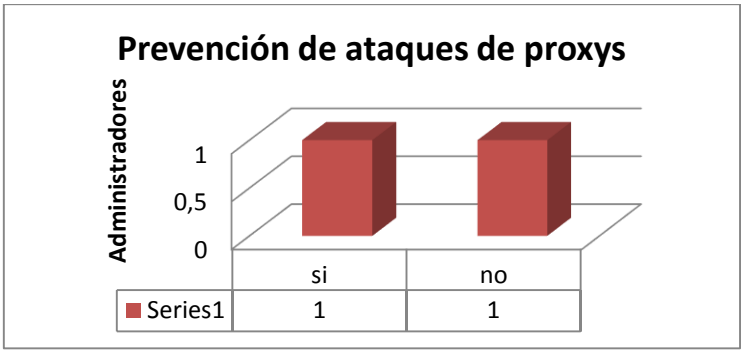


Gráfico 115. Prevención de ataques de proxys.

115. ¿Se realizan auditorías de seguridad y pruebas de penetración?

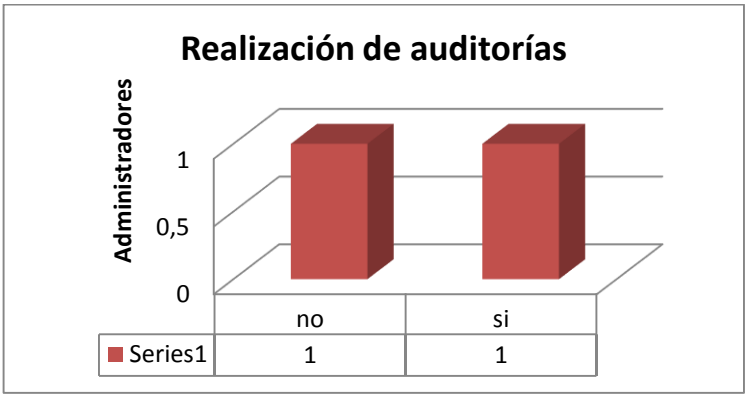


Gráfico 116. Realización de Auditorías.

ANEXO 5.- TABULACIÓN DE LAS ENCUESTAS APLICADAS A LOS ESTUDIANTES DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO.

1. ¿Ha utilizado usted antes una plataforma B-learning?

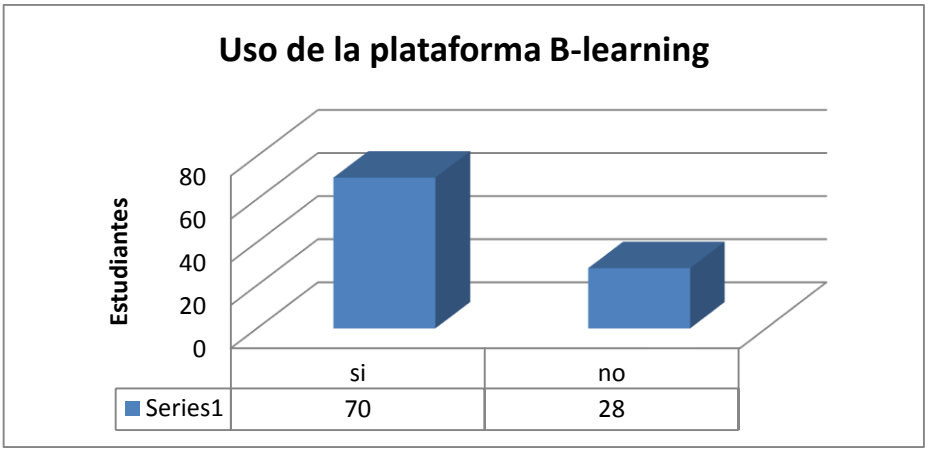


Gráfico 117. Uso de la plataforma B-learning.

En caso de ser afirmativa la repuesta indique cual es……

2. ¿Utilizas con frecuencia la plataforma B-learning?

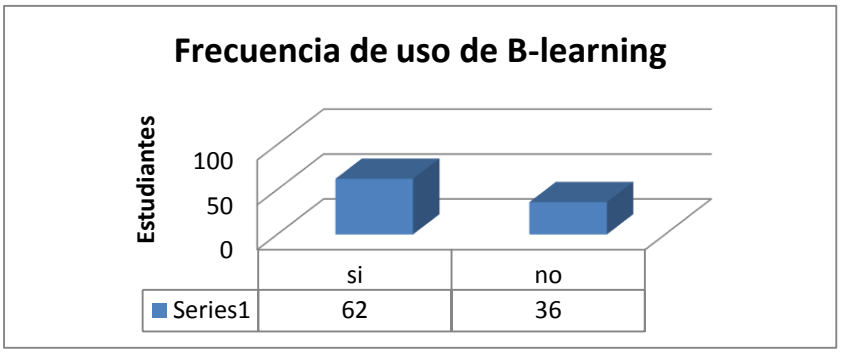


Gráfico 118. Frecuencia de uso de B-learning.

3. ¿Utilizas la plataforma B-learning como método de enseñanza?

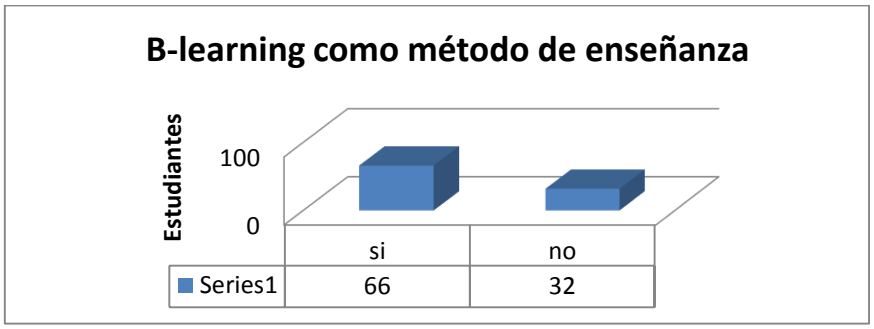


Gráfico 119. B-learning como método de enseñanza.

4. ¿La enseñanza a través de la plataforma B-learning ayuda a mejorar el desempeño del desarrollo académico?

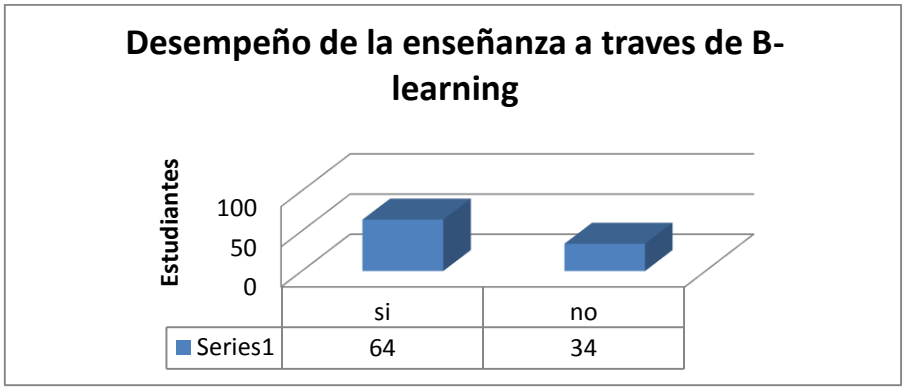


Gráfico 120. Desempeño de la enseñanza a través de B-learning

5. Recibió usted una introducción previa sobre el servicio que ofrece la plataforma B-learning.

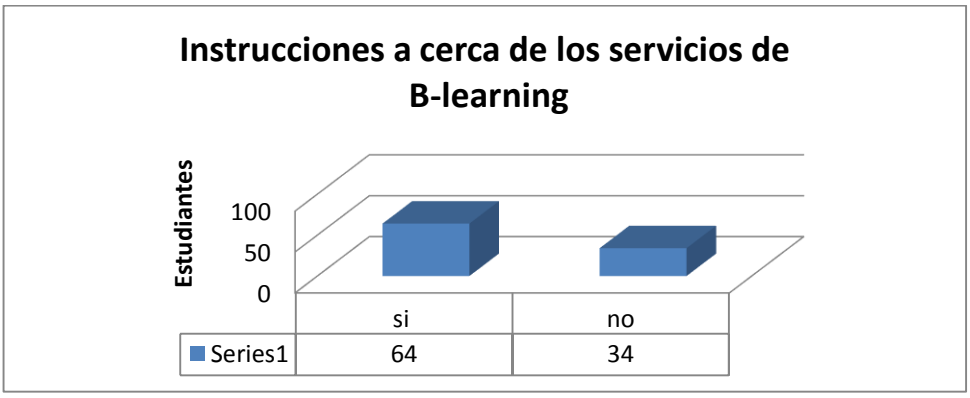


Gráfico 121. Instrucciones a cerca de los servidores de B-learning.

6. Existe documentación de ayuda sobre el funcionamiento del sistema.

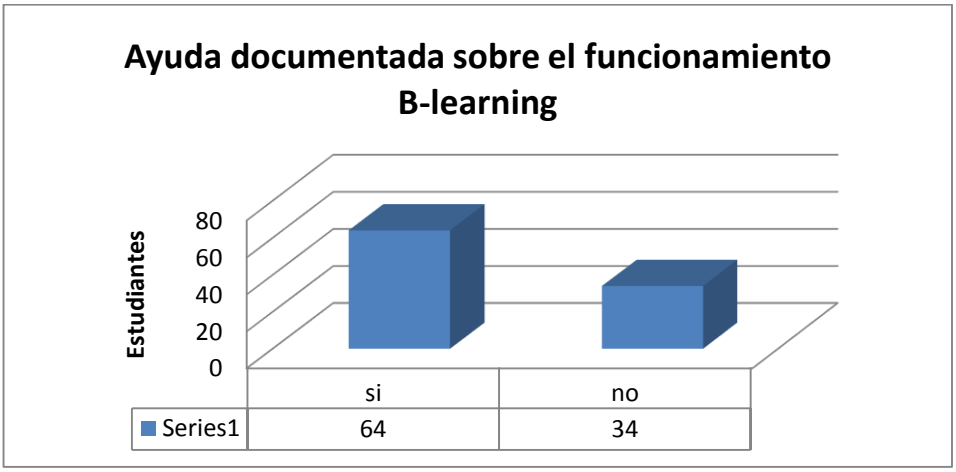


Gráfico 122. Ayuda documentada sobre el funcionamiento B-learning.

7. Ha aplicado algún examen mediante esta plataforma.

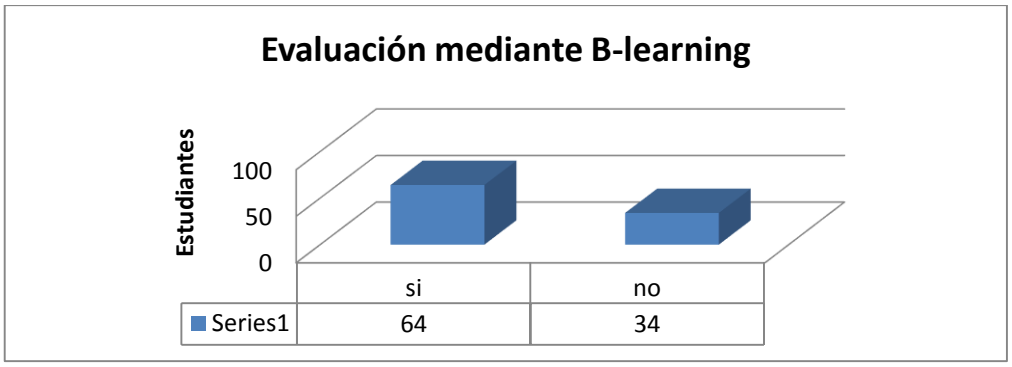


Gráfico 123. Evaluación mediante B-learning.

8. ¿Cree la plataforma B-learning cuenta con una interface de usuario amigable?

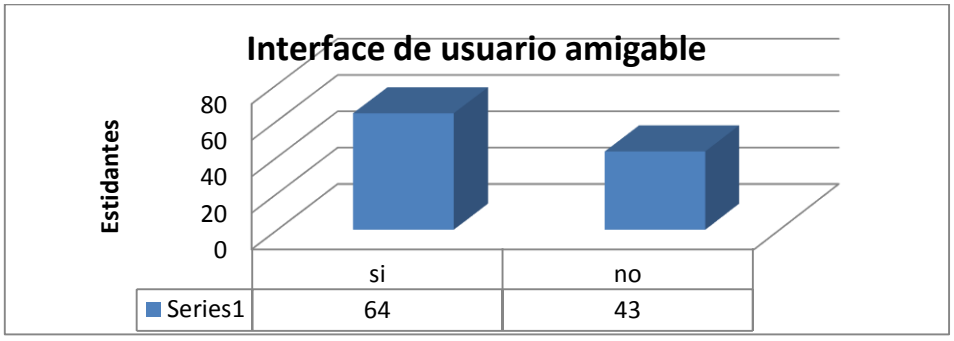


Gráfico 124. Interface de usuario plataforma B-learning

9. ¿Crees usted que la plataforma B-learning cuenta con las seguridades adecuadas como para proteger su información?

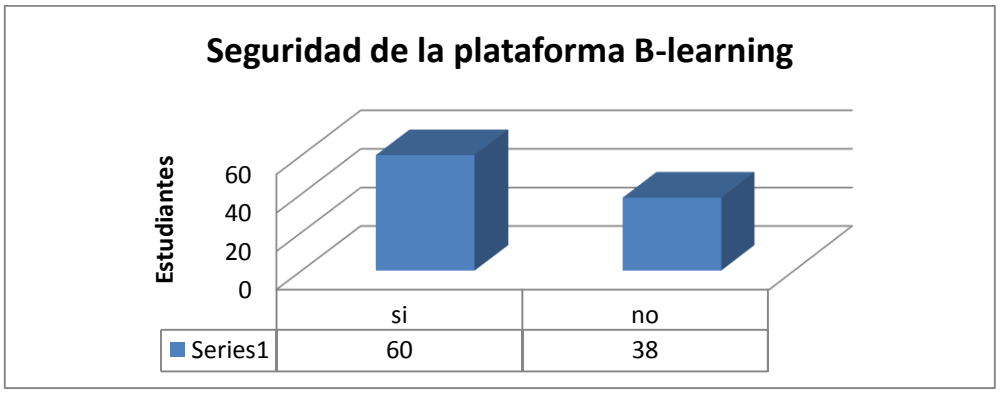


Gráfico 125. Seguridad de la plataforma B-learning

10. ¿Sabe usted si la información que proporciona al sistema es confidencial?

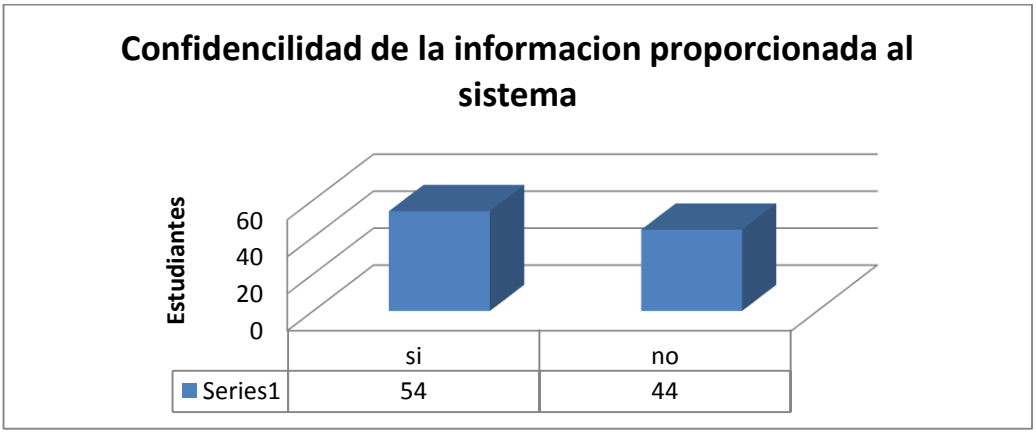
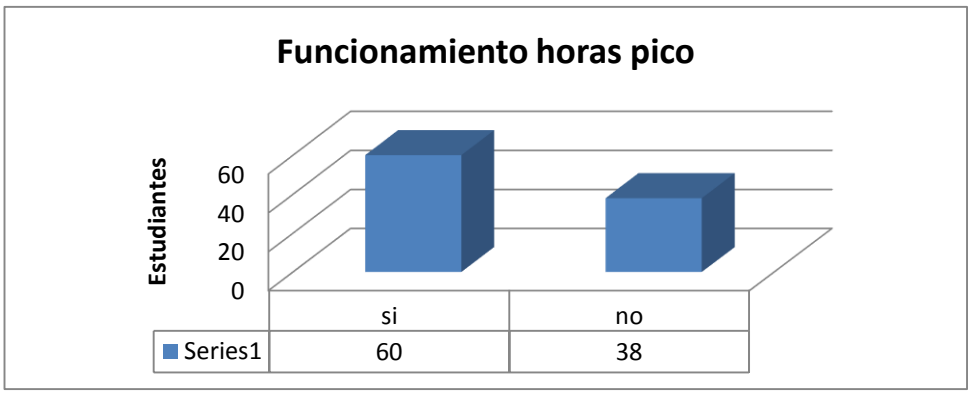


Gráfico 126. Confidencialidad de la información proporcionada al sistema.

11. ¿El funcionamiento durante las horas picos es satisfactorio?

Gráfico 127. Funcionamiento horas pico.



12. Usted accede a los servicios del B-learning desde la Universidad.

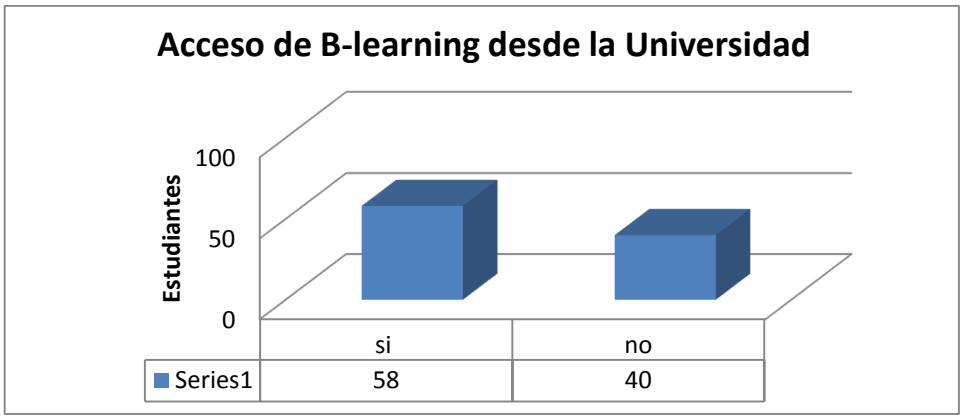


Gráfico 128. Acceso de B-learning desde la Universidad.

13. ¿Al crear su contraseña el sistema, le pide crear una contraseña segura (utilización de mayúsculas, minúsculas, números, caracteres especiales)?

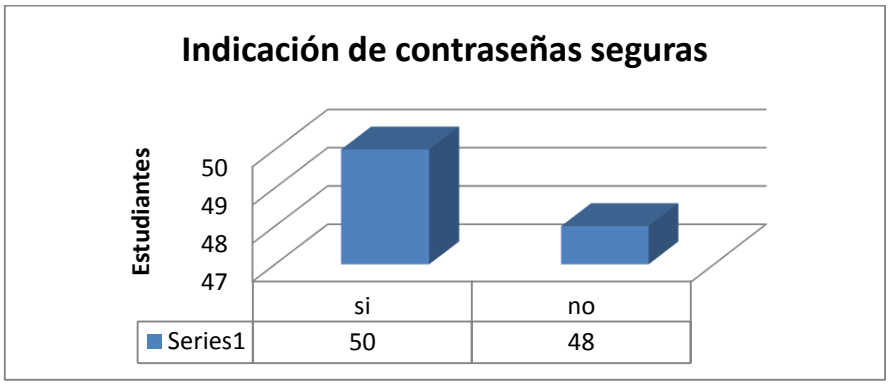


Gráfico 129. Indicación de contraseñas seguras.

14. ¿Existe un Periodo en el que el sistema le pide cambiar su contraseña?

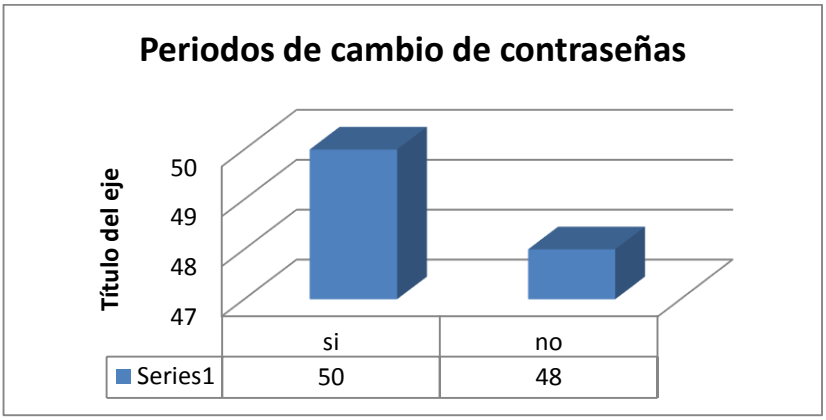


Gráfico 130. Periodos de cambio de contraseña.

ANEXO 6.- TABULACIÓN DE LAS ENCUESTAS APLICADAS A LOS USUARIOS PROFESORES DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO.

1. Ha utilizado usted antes una plataforma B-learning?

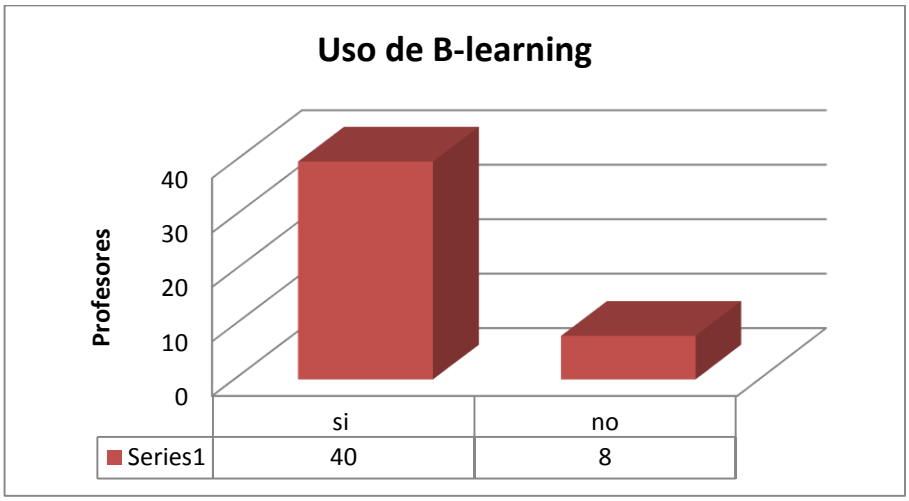


Gráfico 131. Utilización de B-learning.

En caso de ser afirmativa la repuesta indique cual es……

2. ¿Utiliza con frecuencia la plataforma B-learning?

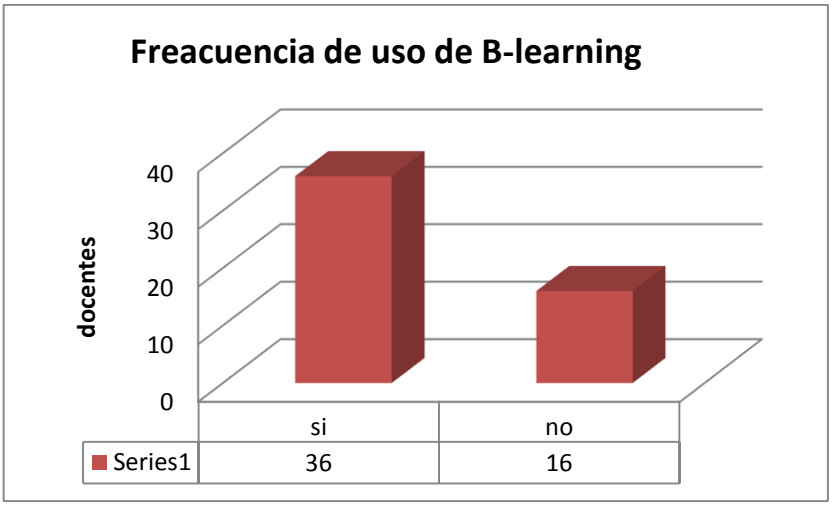


Gráfico 132. Frecuencia de uso de B-learning.

3. ¿Utilizas la plataforma B-learning como método de aprendizaje?

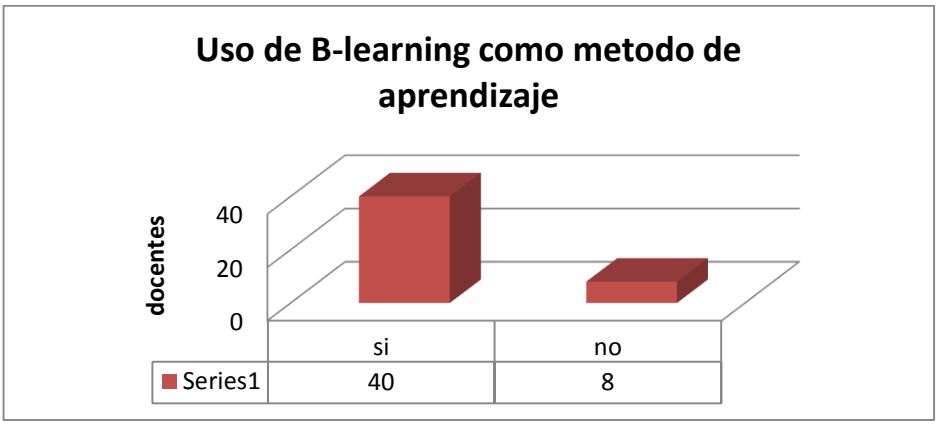


Gráfico 133. Uso de B-learning como método de aprendizaje.

4. ¿La enseñanza a través de la plataforma B-learning ayuda a mejorar el desempeño del desarrollo académico?

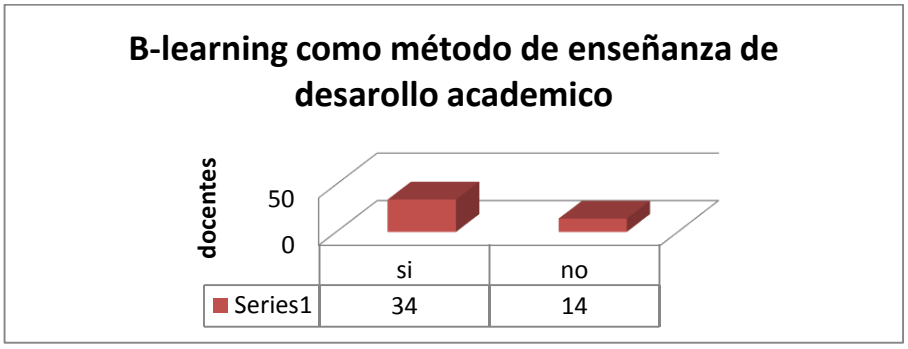


Gráfico 134. B-learning como método de desarrollo académico.

5. Recibió usted una introducción previa sobre el servicio que ofrece la plataforma B-learning.

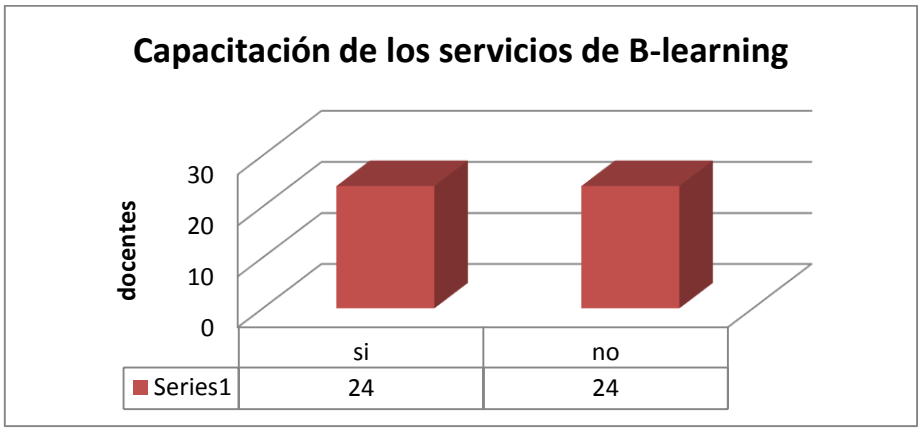


Gráfico 135. Capacitación de los servicios de B-learning.

Existe documentación de ayuda sobre el funcionamiento del sistema.

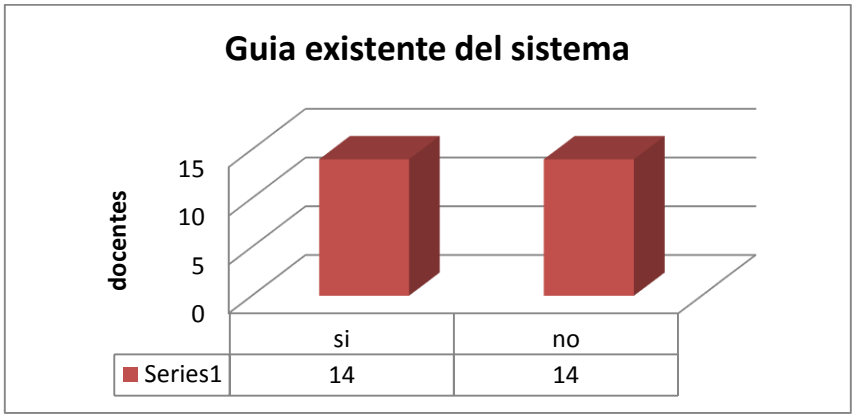


Gráfico 136. Guía existente del sistema.

6. Ha realizado algún examen mediante esta plataforma
.

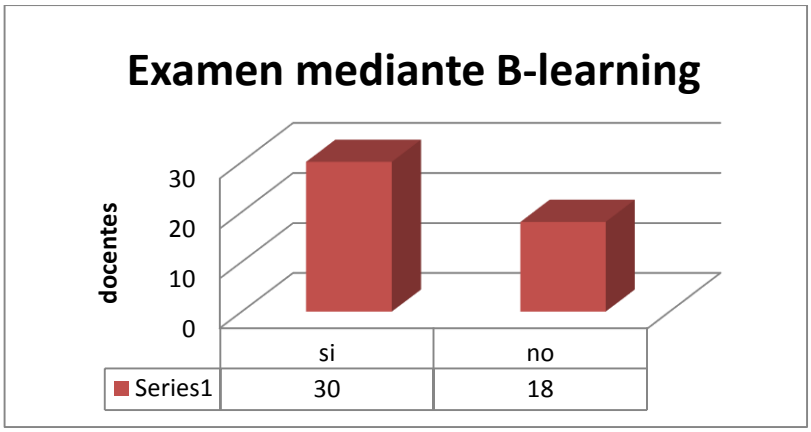


Gráfico 137. Examen mediante B-learning.

7. ¿La educación mediante la plataforma B-learning cuenta con una interface de usuario amigable?

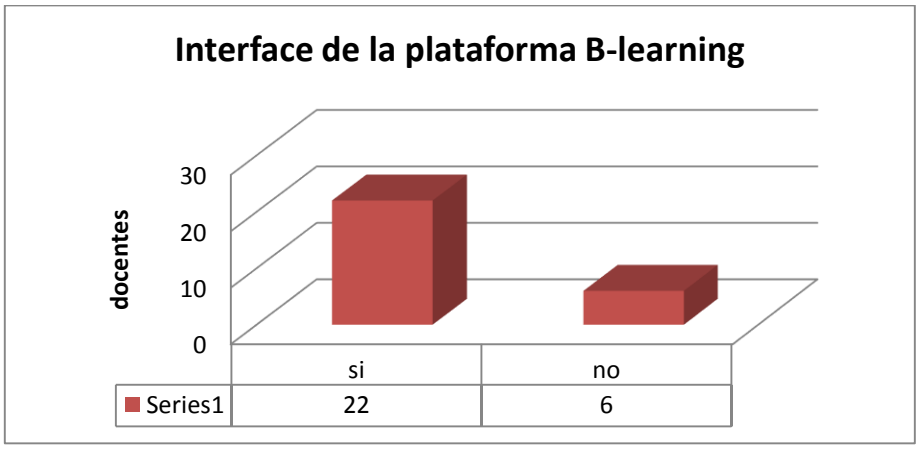


Gráfico 138. Interface de la plataforma B-learning.

8. ¿Crees usted que la plataforma B-learning cuenta con las seguridades adecuadas como para proteger su información?

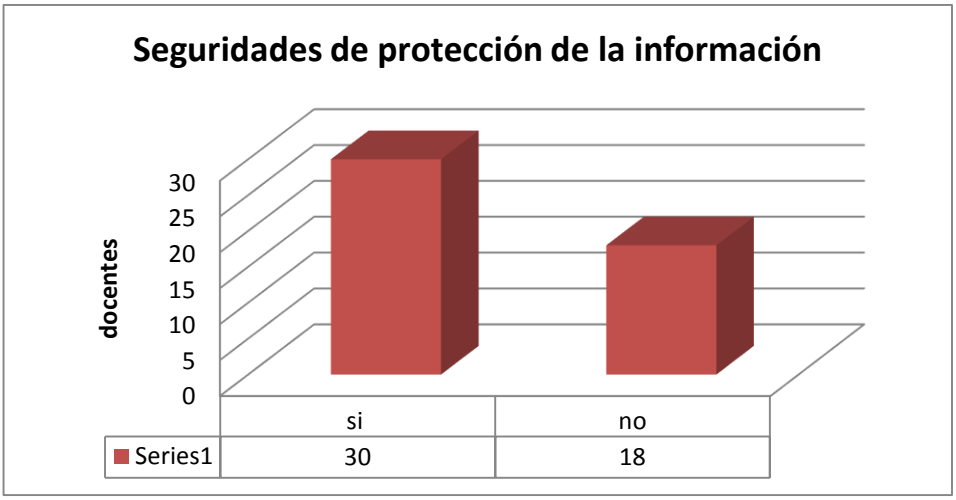


Gráfico 139. Seguridad en la protección de la información.

9. ¿Sabe usted si la información que proporciona al sistema es confidencial?

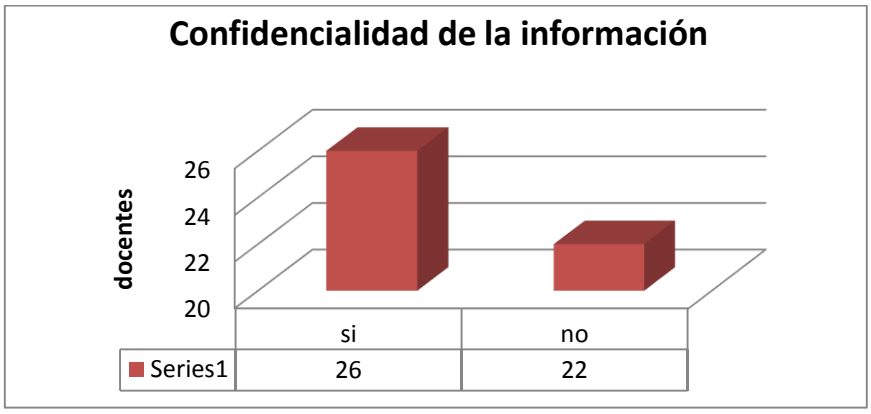


Gráfico 140. Confidencialidad de la información proporcionada al sistema.

GLOSARIO

MAGERIT

[N]: Desastres naturales: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[I]: De origen industrial: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
[E]: Errores y fallos no intencionados: Fallos no intencionales causados por las personas.
[A] Ataques intencionados: Fallos deliberados causados por las personas.

A DE ACCIDENTES

A1: Accidente físico de origen industrial: incendio, explosión, inundación por roturas, contaminación por industrias cercanas o emisiones radioeléctricas.

A2: Avería: de origen físico o lógico, debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.

A3: Accidente físico de origen natural: riada, fenómeno sísmico o volcánico, meteoro, rayo, corrimiento de tierras, avalancha, derrumbe.

A4: Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicación, fluidos y suministros diversos.

A5: Accidentes mecánicos o electromagnéticos: choque, caída, cuerpo extraño, radiación, electrostática.

E DE ERRORES

E1: Errores de utilización ocurridos durante la recogida y transmisión de datos o en su explotación por el sistema

E2: Errores de diseño existentes desde los procesos de desarrollo del software (incluidos los de dimensionamiento, por la posible saturación)

E3: Errores de ruta, secuencia o entrega de la información en tránsito

E4: Inadecuación de monitorización, trazabilidad, registro del tráfico de información.

P DE AMENAZAS INTENCIONALES PRESENCIALES

P1: Acceso físico no autorizado con inutilización por destrucción o sustracción (de equipos, accesorios o infraestructura)

P2: Acceso lógico no autorizado con intercepción pasiva simple de la información

P3: Acceso lógico no autorizado con alteración o sustracción de la información en tránsito o de configuración; es decir, reducción de la confidencialidad para obtener bienes o servicios aprovechables (programas, datos)

P4: Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración: es decir, reducción de la integridad y/o disponibilidad del sistema sin provecho directo (sabotaje inmaterial, infección vírica)

P5: Indisponibilidad de recursos, sean humanos (huelga, abandono, rotación) o técnicos (desvío del uso del sistema, bloqueo).

T DE AMENAZAS INTENCIONALES TELEACTUADAS.

T1: Acceso lógico no autorizado con intercepción pasiva (para análisis de tráfico).
T2: Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración.
T3: Acceso lógico no autorizado con modificación (Inserción, Repetición) de información en tránsito.
T4: Suplantación de Origen (del emisor o reemisor, 'man in themiddle') o de Identidad
T5: Repudio del Origen o de la Recepción de información en tránsito.

TIPOS DE ACTIVOS:

[S] Servicios: Función que satisface una necesidad de los usuarios.

[D] Datos / Información: Elementos de información que, de forma singular o agrupada de alguna forma, representan el conocimiento que se tiene de algo

[SW] Aplicaciones (software): Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) son tareas que han sido automatizadas para su desempeño por un equipo informático.

[HW] Equipos informáticos (hardware): Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos

[COM] Redes de comunicaciones: Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros

[SI] Soportes de información: Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo

[AUX] Equipamiento auxiliar: Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

[L] Instalaciones: Lugares donde se hospedan los sistemas de información y comunicaciones.

[P] Personal: Personas relacionadas con los sistemas de información.

DIMENSIONES DE VALORACIÓN DE UN ACTIVO.

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

[I] integridad de los datos: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento

[C] confidencialidad de los datos: Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

[A_S] autenticidad de los usuarios del servicio: Aseguramiento de la identidad u origen.

[A_D] autenticidad del origen de los datos: Aseguramiento de la identidad u origen.

[T_S] trazabilidad del servicio: Aseguramiento de que en todo momento se podrá determinar quién usó qué y en qué momento.

[T_D] trazabilidad de los datos: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

ENS: Esquema Nacional de Seguridad.

LMS: Learning Management System.

LDAP: (Protocolo compacto de acceso a directorios) es un protocolo estándar que permite administrar directorios, esto es, acceder a bases de información de usuarios de una red mediante protocolos TCP/IP.

IMAP: Protocolo de Internet estándar para correo electrónico que permiten a su programa de correo electrónico el acceso a las cuentas de correo electrónico de su espacio web.

Permite acceder a varios clientes al mismo buzón, facilitando el acceso posterior a los mensajes de correo disponibles en el servidor mediante correo web

POP3: Descarga los mensajes eliminándolos del servidor. Los mensajes de correo electrónico ya no se encuentran disponibles por correo web o un programa de correo

NNTP: Network News TransportProtoco, es un protocolo inicialmente creado para la lectura y publicación de artículos de noticias en Usenet. Su traducción literal al español es "protocolo para la transferencia de noticias en red

HTML: HyperTextMarkupLanguage, («lenguaje de marcado hipertextual»), hace referencia al lenguaje de marcado predominante para la elaboración de páginas web que se utiliza para describir y traducir la estructura y la información en forma de texto, así como para complementar el texto con objetos tales como imágenes.

WYSIWYG: What You See Is What You Get (en español, "lo que ves es lo que obtienes"). Se aplica a los procesadores de texto y otros editores de texto con formato (como los editores de HTML) que permiten escribir un documento viendo directamente el resultado final, frecuentemente el resultado impreso.

TTLS: transistor-transistor logic, es decir, "lógica transistor a transistor". Es una familia lógica o lo que es lo mismo, una tecnología de construcción de circuitos electrónicos digitales. En los componentes fabricados con tecnología TTL los elementos de entrada y salida del dispositivo son transistores bipolares

CSV: (comma-separatedvalues) son un tipo de documento en formato abierto sencillo para representar datos en forma de tabla, en las que las columnas se separan por comas (o punto y coma en donde la coma es el separador decimal: España, Francia, Italia...) y las filas por saltos de línea.

Rootkis: Programa que permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones. El término proviene de una concatenación de la palabra inglesa “root” que significa raíz

(nombre tradicional de la cuenta privilegiada en los sistemas operativos Unix) y de la palabra inglesa “kit” que significa conjunto de herramientas (en referencia a los componentes de software que implementan este programa). El término “rootkit” tiene connotaciones negativas ya que se lo asocia al malware.
En otras palabras, usualmente se lo asocia con malware, que se esconde a sí mismo y a otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a una amplia variedad de sistemas operativos como pueden ser GNU/Linux, Solaris o Microsoft Windows para remotamente comandar acciones o extraer información sensible.

Exploits: (del inglés toexploit, explotar o aprovechar) es una pieza de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo. Ejemplos de comportamiento erróneo: Acceso de forma no autorizada, toma de control de un sistema de cómputo, consecución privilegios no concedidos lícitamente, consecución de ataques de denegación de servicio

IIS: Internet InformationServices, es un servidor web y un conjunto de servicios para el sistema operativo Microsoft Windows. Originalmente era parte del Option Pack para Windows NT. Luego fue integrado en otros sistemas operativos de Microsoft destinados a ofrecer servicios, como Windows 2000 o Windows Server 2003. Windows XP Profesional incluye una versión limitada de IIS. Los servicios que ofrece son: FTP, SMTP,NNTP y HTTP/HTTPS. shibboleth,

LOPD: Ley Orgánica de Protección de Datos.

INTECO: Instituto Nacional de Tecnologías de Comunicación

AEPD: Agencia Española de Protección de Datos.

TICs: Tecnologías de la información y la comunicación (TIC), a veces denominadas nuevas tecnologías de la información y la comunicación (NTIC) son un concepto muy asociado al de informática. Si se entiende esta última como el conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información, esta definición se ha matizado de la mano de las TIC, pues en la actualidad no basta con hablar de una computadora cuando se hace referencia al

procesamiento de la información. Internet puede formar parte de ese procesamiento que, quizás, se realice de manera distribuida y remota

CTE: Centro de tecnologías educativas.

APÉNDICE

Nomenclatura	Significado
PAR	**Proyecto de análisis de riesgos**
PAR.1	Actividades preliminares
PAR.1 1	Estudio de oportunidad
PAR.1 2	Determinación del alcance del proyecto
PAR.1 3	Planificación del proyecto
PAR.1 4	Lanzamiento del proyecto
PAR.2	Elaboración del análisis de riesgos
PAR.3	Comunicación de resultados
PS	**Plan de Seguridad**
PS1	Identificación del proyecto de seguridad.
PS2	Plan de ejecución
PS3	Ejecución.
[arch]	**Arquitectura del sistema**
[sap]	Punto de [acceso al] servicio (1)
[ip]	Punto de interconexión (2)
[ext]	Proporcionado por terceros (3)
[D]	**Datos / Información**

[source]	Código fuente
[exe]	Código ejecutable
[test]	datos de prueba
[K]	**Claves criptográficas**
[keys]	Claves criptográficas
[info]	Protección de la información
[encrypt]	Claves de cifra
[shared_secret]	Secreto compartido (clave simétrica) (1)
[public_encryption]	Clave pública de cifra (2)
[public_decryption]	Clave privada de descifrado (2)
[shared_secret]	Secreto compartido (clave simétrica) (1)
[public_encryption]	Clave pública de cifra (2)
[sign]	Claves de firma
[shared_secret]	Secreto compartido (clave simétrica)
[public_signature]	Clave privada de firma (2)
[public_verification]	Clave pública de verificación de firma (2)
[com]	Protección de las comunicaciones
[channel]	Claves de cifrado del canal
[authentication]	Claves de autenticación
[verification]	Claves de verificación de autenticación
[disk]	Cifrado de soportes de información
[encrypt]	Claves de cifra

[x509]	Certificados de clave pública
[sign]	Claves de firma
[shared_secret]	Secreto compartido (clave simétrica)
[public_signature]	Clave privada de firma (2)
[public_verification]	Clave pública de verificación de firma (2)
[com]	Protección de las comunicaciones
[channel]	Claves de cifrado del canal
[authentication]	Claves de autenticación
[verification]	Claves de verificación de autenticación
[channel]	Claves de cifrado del canal
[authentication]	Claves de autenticación
[verification]	Claves de verificación de autenticación
[channel]	Claves de cifrado del canal
[disk]	Cifrado de soportes de información
[encrypt]	Claves de cifra
[x509]	Certificados de clave pública
[S]	**Servicios**
[anon]	Anónimo (sin requerir identificación del usuario)
[pub]	Al público en general (sin relación contractual)
[ext]	A usuarios externos (bajo una relación contractual)
[int]	Interno (a usuarios de la propia organización)

[anon]	Anónimo (sin requerir identificación del usuario)
[S]	**Servicios**
[www]	World wide web
[telnet]	Acceso remoto a cuenta local
[email]	Correo electrónico [file] almacenamiento de ficheros
[ftp]	Transferencia de ficheros
[edi]	Intercambio electrónico de datos
[dir]	Servicio de directorio (1)
[idm]	Gestión de identidades (2)
[ipm]	Gestión de privilegios
[pki]	PKI - infraestructura de clave pública (3)
[www]	World wide web
[telnet]	Acceso remoto a cuenta local
[email]	Correo electrónico [file] almacenamiento de ficheros
[ftp]	Transferencia de ficheros
[edi]	Intercambio electrónico de datos
[dir]	Servicio de directorio (1)
[idm]	Gestión de identidades (2)
[ipm]	Gestión de privilegios
[pki]	PKI - infraestructura de clave pública (3)

[www]	World wide web
[telnet]	Acceso remoto a cuenta local
[SW]	**Aplicaciones (software)**
[prp]	Desarrollo propio (in house)
[sub]	Desarrollo a medida (subcontratado)
[std]	Estándar (off the shelf).
[prp]	Desarrollo propio (in house)
[sub]	Desarrollo a medida (subcontratado)
[std]	Estándar (off the shelf).
[prp]	Desarrollo propio (in house)
[sub]	Desarrollo a medida (subcontratado)
[std]	Estándar (off the shelf).
[prp]	Desarrollo propio (in house)
[sub]	Desarrollo a medida (subcontratado)
[std]	Estándar (off the shelf).
[prp]	desarrollo propio (in house)
[sub]	Desarrollo a medida (subcontratado)
[std]	Estándar (off the shelf).
[prp]	Desarrollo propio (in house)
[browser]	Navegador web

[www]	Servidor de presentación
[app]	Servidor de aplicaciones
[email_client]	Cliente de correo electrónico
[email_server]	Servidor de correo electrónico
[file]	Servidor de ficheros
[dbms]	Sistema de gestión de bases de datos
[tm]	Monitor transaccional
[office]	Ofimática
HW]	**Equipos informáticos (hardware)**
[host]	Grandes equipos (1)
[mid]	Equipos medios (2)
[pc]	Informática personal (3)
[mobile]	Informática móvil (4)
[pda]	Agendas electrónicas
[vhost]	Equipo virtual
[backup]	Equipamiento de respaldo (5)
[peripheral]	Periféricos
[host]	Grandes equipos (1)
[mid]	Equipos medios (2)
[pc]	Informática personal (3)

[mobile]	Informática móvil (4)
[pda]	Agendas electrónicas
[vhost]	Equipo virtual
[print]	Medios de impresión (6)
[scan]	Escáneres
[crypto]	Dispositivos criptográficos
[print]	Medios de impresión (6)
[scan]	Escáneres
[crypto]	Dispositivos criptográficos
[print]	Medios de impresión (6)
[print]	Medios de impresión (6)
bp]	Dispositivo de frontera (7)
[network]	Soporte de la red (8)
bp]	Sispositivo de frontera (7)
[network]	Soporte de la red (8)
[network]	Soporte de la red (8)
[modem]	Módems
[hub]	Concentradores
[switch]	Conmutadores
[router]	Encaminadores

[modem]	Módems
[hub]	Concentradores
[switch]	Conmutadores
[router]	Encaminadores
[bridge]	pasarelas
[firewall]	cortafuegos
[wap]	punto de acceso inalámbrico
[bridge]	pasarelas
[firewall]	cortafuegos
[wap]	punto de acceso inalámbrico
[bridge]	pasarelas
[pabx]	centralita telefónica
[ipphone]	teléfono IP
[pabx]	centralita telefónica
[ipphone]	teléfono IP
[pabx]	centralita telefónica
[ipphone]	teléfono IP
[pabx]	centralita telefónica
[ipphone]	teléfono IP
[pabx]	centralita telefónica

[COM]	**Redes de comunicaciones**
[PSTN]	red telefónica
[ISDN]	rdsi (red digital)
[X25]	X25 (red de datos)
[ADSL]	ADSL [pp] punto a punto
[radio]	comunicaciones radio
[wifi]	red inalámbrica
mobile]	telefonía móvil
[sat]	por satélite
[LAN]	red local
[MAN]	red metropolitana
[Internet]	Internet
[Media]	**Soportes de información**
[electronic]	electrónicos
[ic]	tarjetas inteligentes
[vdisk]	discos virtuales
[san]	almacenamiento en red
[disk]	discos
[cd]	cederrón
[disquette]	disquetes
[usb]	memorias USB
[tape]	cinta magnética
[mc]	tarjetas de memoria
[P]	**Personal**
ue]	usuarios externos
[ui]	usuarios internos
[op]	operadores
[adm]	administradores de sistemas

[com]	administradores de comunicaciones
ue]	usuarios externos
[ui]	usuarios internos
[op]	operadores
[adm]	administradores de sistemas
[com]	administradores de comunicaciones
ue]	usuarios externos
[ui]	usuarios internos
[L]	**Instalaciones**
[site]	recinto
[building]	edificio
[local]	cuarto
[mobile]	plataformas móviles
[site]	recinto

Título del proyecto:

APLICACIÓN DE PROCESOS Y POLÍTICAS DE LA INFORMÁTICA FORENSE EN LAS SEGURIDADES DE SERVIDORES. CASO PRÁCTICO SERVIDOR B-LEARNING DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO

Autor:

Fredy Alejandro Fierro Zúñiga

Co-autor:

Lida Barba

Universidad Nacional de Chimborazo

Facultad de Ingeniería

Escuela de Ingeniería en Sistemas y Computación

RESUMEN

El presente trabajo tiene como objeto determinar la importancia que tiene la Informática Forense para identificar las fortalezas y vulnerabilidades del sistema de B-learning de la Universidad Nacional de Chimborazo, con el único fin de que se realice un seguimiento a este proceso para que se implementen y mejoren las normas de este servicio.

Durante el análisis se determinaron varios parámetros de investigación, se aplicó la metodología MAGERIT, que permite identificar los principales aspectos a tener en cuenta para la protección de los servicios informáticos que presta la Universidad Nacional de Chimborazo, poniendo énfasis en los de mayor acceso, con los cuales se ha logrado monitorearlos y detectar las diversas falencias que podrían presentarse y así evitar riesgos futuros.

Este trabajo tiene como fin el dar una pauta en cuanto a la utilización de la Informática Forense, la aplicación de normas y estándares de seguridad de la información, evaluación de métodos y la verificación de posibles riegos. El estudio conlleva a la implementación de planes de contingencia que fortalezcan al nuevo Centro de Tecnología Educativa con la visión de que éste se convierta en uno de los Centros de Datos pioneros en cuanto a seguridad y eficiencia dentro de la ciudad, provincia y el país, aportando en el posicionamiento de la Universidad Nacional de Chimborazo como una institución educativa de primer nivel.

Se puede considerar que la Informática Forense no puede ser la única herramienta para determinar falencias ocultas de los sistemas, esta debe ir acompañada de la actualización de metodologías, implementación de estándares y capacitación del personal a cargo de la administración del edificio Centro de Tecnología Educativa, la Informática Forense brinda una cantidad de posibilidades que nos permiten saber el estado del sistema que es objeto de investigación, por lo que se puede decir que se convierte en aliada para mejorar la seguridad de los sistemas informáticos.

SUMMARY

The following work aims to determine the importance that forensic informatics has to identify strengths and weakness into the B-learning system of the Chimborazo National University. Once done, it could help to make a follow up to this process in order to apply and also improve the parameters of this service.

During the analysis, some features of investigation were pointed out. After that, it was applied MAGERIT methodology, which allows identifying the mains aspects to take into consideration for protect those informatics services that the University gives to their students. A special emphasis was made into those services with more expanded use, monitoring them, so it could be detected possibilities of failures and avoiding future risks.

The objective of this work is to provide a guideline in the usage of Forensic Informatics, the application of norms and information security standards, the evaluation of methods and the evaluation of possible failures. The study entails the implementation of contingency plans that strengthens the new Educational Technology Center. The vision for this new center is to become one of the pioneer Data Center in the province and also nationwide for its security and efficiency, and in this way contributing to make the Chimborazo National University as first level education institution.

Forensic Informatics could be considered as one in many other tools to determine hidden failures in technological systems. It would be appropriate to make it work in complementation with other procedures such as methodologies update, standards implementation and also capacitation for the personal in charge of the administration of the center. Since Forensic Informatics gives a great number of possibilities to determine the current status of any studied system, we could catalogue it as a great ally to improve informatics systems security.

INTRODUCCIÓN

En los últimos años las tecnologías de la información y las comunicaciones, han tenido un crecimiento exponencial, éste crecimiento, si bien ofrece muchas posibilidades para tener nuevos servicios, también conforma el ambiente propicio, para que desaprensivos basados en el anonimato, intenten acceder a la información existente en nuestros sistemas, casi siempre con fines delictivos o destructivos.

La Seguridad Informática se puede clasificar en seguridad lógica y seguridad física y busca con la ayuda de políticas y controles mantener la seguridad de los recursos y la información manejando los riesgos, sin embargo cuando se habla de seguridad se debe tener en cuenta que no existe la seguridad total.

Este documento pretende, ser el medio de comunicación en el cual se establecen las reglas, normas, controles y procedimientos que regulen la forma en que la institución, prevenga, proteja y maneje los riesgos de seguridad en diversas circunstancias. Las normas y políticas expuestas en este documento servirán de referencia, en ningún momento pretenden ser normas absolutas, las mismas están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad.

En la Universidad Nacional de Chimborazo como parte del modelo enseñanza-aprendizaje se ha implementado la modalidad de enseñanza B-learning ya que en estos tiempos en donde la tecnología es parte de nuestra vida en todos los aspectos, también la actividad pedagógica empieza a incorporarse a esta tendencia y así empieza a sortear las diversas barreras y dificultades que existían tales como: costos, distancias, horarios, entre otros con esta modalidad.

En B-learning el docente desempeña su rol tradicional, pero usa en beneficio propio el material didáctico que la informática e internet le proporcionan, para ejercer su labor en dos frentes: como tutor on-line (tutorías a distancia) y como educador tradicional (cursos presenciales). La forma en que combine ambas estrategias depende de las necesidades específicas de ese curso, dotando así a la formación on-line de una gran flexibilidad.

FUNDAMENTACIÓN TEÓRICA

El estudio teórico se enfoca a describir que es la seguridad informática así como también conceptualizar la informática forense, describir que es el B-learning y sus características, funciones y su uso dentro de la institución, a su vez se investiga sobre MAGERIT que es una metodología de análisis y gestión de riesgos para concluir con la elaboración de una guía de seguridad aplicada a los servidores informáticos de la Universidad Nacional de Chimborazo.

Seguridad Informática: es el área de la Informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta incluyendo la información contenida. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore como un activo y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Informática Forense: La Informática Forense o Auditoria Informática, es un proceso realizado por personal experto, esta consiste en la recolección, agrupamiento y evaluación de evidencia que nos permitan determinar si el Sistema de Información que maneja una empresa, entidad o compañía protege de manera efectiva uno de sus activos más importantes que es la información.

B-learning: es la combinación de la educación presencial y a distancia y el e-learning, también llamado educación virtual o educación a distancia basada en el uso de computadoras. Los principales ingredientes de esta mezcla (blend) son la comunicación e intercambio de información cara-a-cara y mediada por tecnologías, experimentación, trabajo tele-colaborativo y la enseñanza presencial y a distancia.

En B-learning el docente desempeña su rol tradicional, pero usa en beneficio propio el material didáctico que la informática e internet le proporcionan, para ejercer su labor en dos frentes: como tutor on-line (tutorías a distancia) y como educador tradicional (cursos presenciales). La forma en que combine ambas estrategias depende de las necesidades específicas de ese curso, dotando así a la formación on-line de una gran flexibilidad.

Moodle: es una plataforma de aprendizaje a distancia (e-learning) basada en software Libre, es un sistema de gestión avanzada es decir, una aplicación diseñada para ayudar a los educadores a crear cursos de calidad en línea.

Estos tipos de sistema de aprendizaje a distancia a veces son también llamados Ambientes de Aprendizaje Virtual o Educación en Línea.

Metodologías para análisis de riesgos: El análisis de riesgo es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Metodología MAGERIT: es una metodología que se esfuerza por dividir los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier inconveniente.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

En el periodo transcurrido desde la publicación de la primera versión de MAGERIT (1997) hasta la fecha, el análisis de riesgos se ha venido consolidando como paso necesario para la gestión de la seguridad.

La Evaluación del riesgo es fundamental para llevar cabo planes de seguridad y de contingencia dentro de la organización, para poder gestionarlos y hacerse riguroso frente a posibles ataques a los datos y la información tanto de la organización, como de los servicios que presta.

El desarrollo de cada uno de los temas descritos se encuentra en la tesis titulada:
"**APLICACIÓN DE PROCESOS Y POLÍTICAS DE LA INFORMÁTICA FORENSE EN LAS SEGURIDADES DE SERVIDORES. CASO PRÁCTICO SERVIDOR B-LEARNING DE LA UNIVERSIDAD NACIONAL DE CHIMBORAZO**"

METODOLOGÍA

TIPO DE ESTUDIO

Según el objetivo de estudio

- Investigación Aplicada

Según la fuente de información

- Investigación bibliográfica

Según las variables

- Descriptiva Aplicada

POBLACIÓN MUESTRA

Al tratarse de una investigación aplicada, la población se ha considerado para el estudio fueron los usuarios de la Plataforma B-learning de la Universidad Nacional de Chimborazo donde se consideró varios aspectos sobre la seguridad informática como:

- Marco Organizativo de seguridad.
- Arquitectura de seguridad.
- Control de acceso.
- Segregación de funciones y tareas.
- Mecanismo de autenticación.
- Acceso local.
- Mantenimiento.
- Protección frente a código dañino.
- Registro de la actividad de los usuarios.
- Protección de los registros de actividad.
- Monitorización del sistema.
- Protección de las instalaciones e infraestructuras.
- Protección de las comunicaciones y confidencialidad.
- Segregación de redes.
- Copias de seguridad.
- Protección de los servicios.

Donde:

89 es la muestra total de alumnos a los que se aplicó la encuesta.

48 es el número total de docentes a los que se aplicó la encuesta.

2 es el número total de administradores a los que se aplicó la encuesta.

OPERACIONALIZACIÓN DE VARIABLES

Operacionalización de Variables.

VARIABLE	TIPO	DEFINICION CONCEPTUAL	DIMENSIONES	INDICADORES
Procesos y políticas de Seguridad Informática	Independiente	Técnicas científicas y analíticas que permiten identificar, preservar, analizar y presentar datos.	Cumplimiento Porcentual	Políticas de seguridad aplicados Normas de seguridad de software Normas de seguridad de hardware Estándares ISO Seguridad WEB Seguridad en los servicios
Seguridades en el servidor B-learning	Dependiente	La seguridad se enfoca a la protección de la infraestructura computacional existen estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad comprende software, bases de datos, metadatos, archivos y todo lo que la se valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Información privilegiada o confidencial.	Cumplimiento Porcentual Unidad	Accesos de usuarios Protección, control de acceso Niveles y categorías de usuarios Rendimiento de servidores Firewalls Físicos y Lógico Períodos Backup

Para el análisis de resultados se trabajó con las siguientes tablas de valoración de riesgos:

Valoración del Riesgo

NIVEL DE RIESGO	EQUIVALENCIA
1% – 30 %	Alto
31 % – 60 %	Medio
61 % – 100 %	Bajo

Nota: Para el análisis se consideró como 1% - 30% de cumplimiento el nivel de riesgo es alto. De 31% - 60% de cumplimiento se define el nivel de riesgo medio. De 61% - 100% de cumplimiento se define como nivel de riesgo bajo.

RESULTADOS

Los resultados se presentan en forma de porcentajes como se lo detalla a continuación:

Al aplicar las encuestas a los administradores del Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo, se obtuvieron los siguientes resultados:

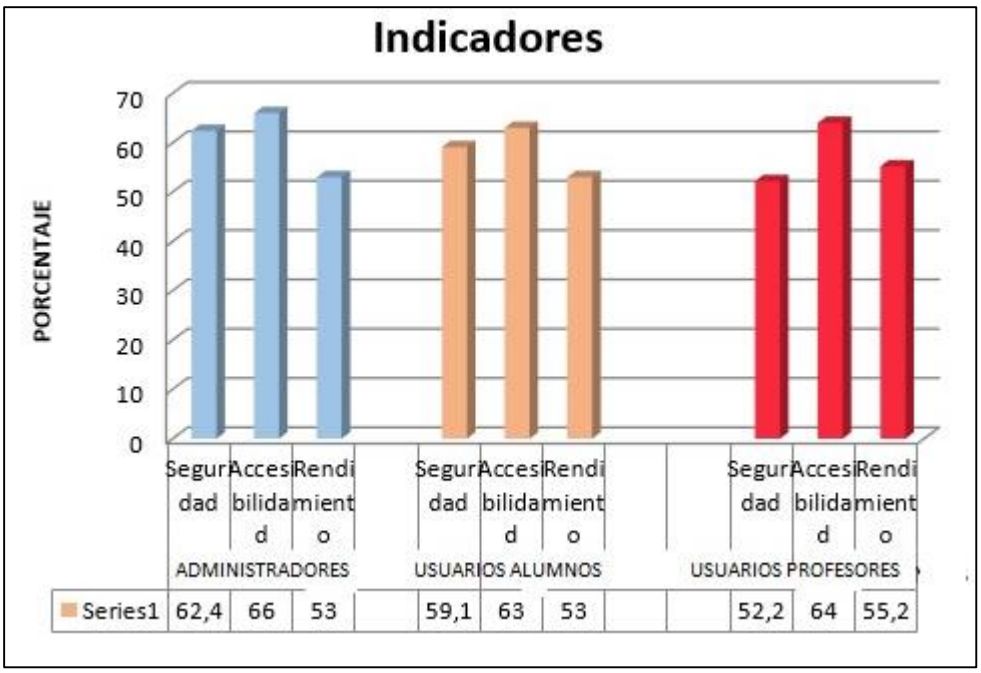
- Seguridad de 62,4% seguro.
- Accesibilidad 66% Accesible
- Rendimiento 53%

Los resultados de las encuestas aplicadas a los usuarios estudiantes determinaron los siguientes resultados.

- Seguridad de 59.1% seguro.
- Accesibilidad 63% Accesible
- Rendimiento 53%

- Resultados obtenidos por los usuarios profesores.
- Seguridad de 52,2% seguro.
- Accesibilidad 64% Accesible
- Rendimiento 55,2%

Figura: Indicadores.



CONCLUSIONES

- La Seguridad Informática permite proteger la infraestructura computacional incluyendo también la información que aquí se encuentre, por esto se la debe tratar con la mayor responsabilidad en todas las áreas del Centro de Tecnología Educativa, para que así sea uno de los factores de éxito dentro de la institución; un recurso humano organizado con Normas y Políticas establecidas y apoyado en las herramientas informáticas permite la prevención de amenazas y disminución de Riesgos en Seguridad.

- Mediante la Informática Forense se logró identificar las principales vulnerabilidades con las que cuenta el Centro de Tecnología Educativa, tanto en su seguridad física como lógica lo cual permitió elaborar una guía de seguridad que contienen normas y estándares que puede servir como un referente para la implementación de un reglamento de uso dentro de la Universidad Nacional de Chimborazo.

- Con la nueva infraestructura que posee la Universidad Nacional de Chimborazo a partir de la construcción del Edificio Inteligente en el campus MS. Edison Riera Rodríguez, en donde hoy se encuentra instalado el Centro de Tecnología Educativa, ha permitido de manera extraordinaria reforzar muchas de los estándares internacionales que se deben seguir al poseer y administrar un Centro de Datos ya que se crearon, implementaron, reforzaron muchas de las políticas de seguridad que en el anterior Centro de Cómputo no se aplicaban por diversas razones, pero gracias a la inversión en recursos tecnológicos de vanguardia por parte de la institución hoy se han logrado.

- La utilización de la plataforma B-Learning en la Universidad Nacional de Chimborazo en la actualidad permite que la educación mejore en gran medida pues el acceso y aplicación está estandarizado dentro de la institución y su aceptación por parte de los estudiantes y docentes es muy alta, esto da a entender que con el paso del tiempo se convertirá en una herramienta más de aprendizaje e implicará que se manejen elevados volúmenes de información y datos por lo que la seguridad y accesibilidad del sistema B-learning será vital en este caso.

- Con relación a la seguridad que ofrece la plataforma B-Learning a los alumnos y profesores de la Universidad Nacional de Chimborazo se detectó luego del estudio que existen aún falencias en el sistema que si se aplican normativas y estándares puntuales pueden ser resultas y así poder garantizar la confidencialidad y el buen uso de la información que se registra y almacena dentro del servidor.

- La Metodología MAGERIT ha permitido en el transcurso de esta investigación la identificación, el análisis y la gestión de riesgos que soportan los sistemas de información de la Universidad Nacional de Chimborazo; con la ayuda del software Pilar se pudo conocer y evaluar la información a través de los Pilares en Seguridad Informática como: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, esto ayuda a tener resultados más reales y que pueden ser discutidos y aplicados a la realidad del entorno de la Universidad Nacional de Chimborazo con el fin de mejorar e implementar políticas de seguridad Informática.

- La implementación de políticas de seguridad se puede efectuar conociendo e identificando los riesgos basados en la estimación del grado a que está expuesto el sistema a que una amenaza se materialice sobre uno o más activos y que causen daños o perjuicios a la institución, para que se puedan minimizar al máximo mediante la aplicación de los mecanismos de control y salvaguardas para evitar que se materialicen.

REFERENCIAS BIBLIOGRÁFICAS

LIBROS

- Delgado, M. L. (2010). *Análisis Forense Digital .* Madrid: CRIPTORED.
- Gómez., L. S. (2009). *El tratamiento de la evidencia digital.* JAIIO.
- Gutiérrez, G. Z.–J. (2010|). *Informática Forense .* Colombia: Universidad de los Andes.
- Kano, J. A.-A.-J. (2005). *Evidencia Digital.* Colombia: Universidad de los Andes.
- Kano, J. J. (2008). *Introducción a la Informática Forense.* Colombia: Universidad de los Andes.
- Keith J. Jones, R. B. (2005). *Real digital forensics.* Addison - Wesley Education Publishers inc.
- Miguel, L. D. (2007). *Análisis Forense Digital.* CRIPORED.
- Óscar López, H. A. (2009). *INFORMÁTICA FORENSE: GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS.* Buenos Aires: CRPTORED.
- P.Leonard, W. (2005). *La evaluación de la gestión: Una evaluacion de los métodos de gestión y desempeño.* Ennglewood Clifs: McGraw-Hill.
- Pino, D. S. (2011). *Introducción a la Informática Forense.* Pontifica Universidad del Ecuador.
- Venema, D. F.-W. (2005). *Forensic Discovery.*Addison - Wesley Professional.

LINKOGRAFIA

- 27001, E. I. (2009). *El portal de ISO 27001*. Obtenido de http://www.iso27000.es/iso27000.html
- España, P. d. (s.f.). *Libro de MAGERIT 2*. Obtenido de http://administracionelectronica.gob.es/: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General
- Standard, I. 2. (2009). *Estándar Internacional ISO/IEC 27002 International Standard*. Obtenido de http://www.iso27000.es/sgsi.html#section2d
- Venema, D. F.-W. (2005). *Forensic Discovery.* Addison - Wesley Professional.
- Wikipedia. (s.f.). Obtenido de http://es.wikipedia.org/wiki/Moodle

ANEXOS

Cd de instalación

ANEXO 1.- Encuesta aplicada a los administradores del Centro de Tecnología Educativa de la Universidad Nacional de Chimborazo.

ANEXO 2.- Encuestas aplicadas a los usuarios estudiantes.

ANEXO 3.- Encuesta aplicada a los usuarios profesores.

ANEXO 4.- Tabulación de las encuestas realizadas a los administradores del Centro de Tecnología Educativa.

ANEXO 5.- Tabulación de las encuestas aplicadas a los estudiantes de la Universidad Nacional de Chimborazo.

ANEXO 6.- Tabulación de las encuestas aplicadas a los usuarios profesores de la Universidad Nacional de Chimborazo.