UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

ANÁLISIS DE RIESGOS Y PLAN DE SEGURIDAD
DEL DIAGNÓSTICO Y DISTINTIVO AMBIENTAL
UNAM UTILIZANDO LA METODOLOGÍA MAGERIT

TESIS

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

Mendivil Luna Joshimar

DIRECTORA DE TESIS

M. en C. María Jaquelina López Barrientos

Ciudad Universitaria, Cd. Mx., 2017

Todo pasa, lo único permanente es el cambio.

El aleteo de las alas de una mariposa se puede sentir al otro lado del mundo.

Agradecimientos

Este trabajo está dedicado especialmente a Lucero y Francisco, mis Padres, los cuales me enseñaron y dieron todo lo necesario para ser quien soy, a mis hermanas Erika, Daniela y hermano Alexis de los cuales he aprendido infinidad de cosas útiles para la vida.

A la UNAM por todo lo que me ha dado desde hace más de diez años, entre los cuales destacan, conocer grandes personas, verdaderos amigos, infinidad de conocimientos, mi primer empleo el cual cambió mi perspectiva de ver al mundo y preocuparme más por él.

A Kari y Moni dos personas que de ser compañeras de trabajo se han convertido en dos hermanas en las cuales puedo confiar plenamente.

A Paula por muchas pláticas, consejos muy juiciosos y bacanos, espero pueda leer esto disfrutando de un buen tinto.

Tabla de contenido

Índice de figuras

Índice de Tablas

Prólogo

Prólogo

Los problemas que se tienen actualmente con relación a la contaminación del aire, agua, suelo, falta de alimentos y calentamiento global son el resultado del desarrollo por el que está pasando este mundo cada vez más globalizado; como consecuencia a todos estos problemas se tienen un gran impacto para el medio ambiente y en la calidad de vida de los seres vivos, no obstante se han iniciado diferentes programas de forma simultánea para la protección del medio ambiente y la salud en la población, así de esta forma se trata de reducir los daños que se están causando.

En México se llevan a cabo diferentes planes de acción para mitigar los distintos problemas en cuanto al daño del medio ambiente, desde las distintas Organizaciones No Gubernamentales (ONG) con un gran número de proyectos y programas, entidades educativas con investigación y desarrollo de nuevas tecnologías hasta el gobierno que trabaja por la mejora del medio ambiente en sus diferentes niveles; federal, estatal y municipal; un claro ejemplo es la Secretaría de Medio Ambiente y Recursos Naturales (SEMARNAT) y sus distintos programas y/o proyectos con los que cuenta para mejorar el medio ambiente, diferentes universidades de México son las que cuentan con proyectos que se enfocan en el cuidado del medio ambiente, sin dejar de lado la parte social y económica tratando así de crear espacio sostenibles.

Dentro de las universidades que están realizando trabajos se encuentra la Universidad Nacional Autónoma de México (UNAM), a través del Programa Universitario de Medio Ambiente (PUMA) ahora Programa Universitario de Estrategias para la Sustentabilidad (PUES); está desarrollando el proyecto denominado “Estrategia de Universidad Sustentable, ECOPUMA”, mismo que incluye la realización del Diagnóstico y Distintivo Ambiental UNAM y se está llevando a cabo en todas las dependencias de la Universidad, dependencias gubernamentales entre otras, como resultado se emiten recomendaciones para disminuir el consumo de energía eléctrica y agua, realizar el manejo adecuado en torno a los residuos sólidos urbanos y en la adquisición de

productos con un menor impacto ambiental, este proyecto tiene gran trascendencia ya que se ha realizado en 19 escuelas privadas incorporadas a la UNAM, 142 Entidades de la UNAM 111 Entidades en CU, 7 en Campus Morelos, 6 en Campus Juriquilla, 1 en Campus Morelia, 5 Colegios de Ciencias y Humanidades, 12 Entidades en la ZMVM, en 9 Escuelas del Instituto Nacional de Bellas Artes (INBA), así como en 10 Edificios sede de la Administración Pública Federal incluyendo la SEMARNAT, La Cámara de Diputados del H. Congreso de la Unión y dos edificios del Instituto Federal de Telecomunicaciones, el Instituto de Información Estadística y Geográfica del estado de Jalisco y el Instituto Nacional para la Evaluación de la Educación.

Así, el presente trabajo de tesis tiene como Objetivo General:

Diseñar y desarrollar un plan de seguridad para garantizar la Integridad, Disponibilidad y Confidencialidad de la información del Diagnóstico y Distintivo Ambiental UNAM que forma parte de la estrategia de Universidad Sustentable ECOPUMA.

Y como Objetivos Particulares:

- Realizar el análisis de riesgos que permita identificar cómo se encuentra actualmente la seguridad de la información en la dependencia.
- Garantizar el mínimo de riesgos en la información y la infraestructura informática.
- Diseñar un plan de seguridad para los diferentes niveles de seguridad del sistema utilizado.
- Proponer políticas de seguridad que mejoren el funcionamiento del sistema, y las tareas relacionadas con el diagnóstico y distintivo ambiental.

Para alcanzar los objetivos planteados, es que en el capítulo 1 se presenta la historia, entorno, ambiente y proyección dentro del programa, con lo cual es posible adentrarse en la problemática presentada y en su entorno a través de las actividades cotidianas sin interrumpir la operación.

En el capítulo 2 se describe la Metodología MAGERIT, los métodos sistemáticos para analizar los riesgos derivados del uso del uso de tecnologías de la información y comunicación, identificación de activos, amenazas y las salvaguardas correspondientes.
Dentro del capítulo 3 diseño del plan de seguridad se lleva a cabo la aplicación de la metodología MAGERIT al proceso del Diagnóstico y Distintivo ambiental UNAM donde se describen cada uno de los pasos y los resultados obtenidos de dicha implementación.
Y finalmente se dan las conclusiones las cuales mencionan los objetivos alcanzados en estre trabajo.

Capítulo 1

Marco teórico

Capítulo 1 Marco Teórico

1.1 Historia sobre sostenibilidad

En las últimas décadas, el concepto de sostenibilidad ha adquirido mayor relevancia en la definición de las políticas del desarrollo en distintas instituciones de educación superior. Sin embargo, los cambios que se han generado desde la década de los setentas a la fecha han integrado en la noción del desarrollo humano sostenible, una nueva perspectiva sobre las dimensiones de este concepto.

A principio de la década de los setenta, organizaciones como el Club de Roma expusieron en distintos informes la preocupación ambiental sobre los límites del crecimiento y consumo de recursos naturales (Brundtland, 2007)[1]. Para responder a esta necesidad en el plano internacional, en 1972, en la Conferencia de las Naciones Unidas para un Medio Ambiente Humano celebrado en Estocolmo, se definió la necesidad de contar con instituciones y un marco jurídico que atendiera el tema ambiental. Fue a partir de esta sugerencia que surgió el Programa de las Naciones Unidas para el Medio Ambiente Humano (PNUMA)

Una de las recomendaciones del PNUMA fue la creación, en 1983, de la Comisión Mundial sobre el Medio Ambiente y el Desarrollo. El objetivo de la comisión fue sugerir las formas para resolver las necesidades de la creciente población frente al deterioro ambiental. De esta forma surgió, en 1987, el documento “Informe Nuestro Futuro Común”. De donde se desprende la definición más conocida del Desarrollo Sustentable, como “el desarrollo que satisface las necesidades del presente, sin comprometer la capacidad de las generaciones futuras para satisfacer sus propias necesidades” (Brundtland, 2007)[2].

[1] Brundtland, G. H. (2007). Nuestro Futuro Común. ONU

[2] Brundtland, G. H. (2007). *Nuestro Futuro Común.* ONU

En el concepto de Desarrollo Sustentable, la vertiente del Desarrollo se enfoca en la pobreza humana y la desigualdad en la distribución de la riqueza económica. Sin embargo, el antecedente de que el crecimiento económico no representaba necesariamente una mejora en la calidad de vida de las personas, generó, como respuesta a esta disparidad, el concepto de Desarrollo Humano.

El concepto de Desarrollo Humano fue planteado en 1990, de forma conjunta, por el Programa de las Naciones Unidas para el Desarrollo (PNUD). Este concepto se centra en un desarrollo orientado hacia el individuo y la comunidad en particular y no hacia todo un país o economía nacional.

La discusión derivada de "Nuestro Futuro Común (Informe Brundtland)" fue una parte fundamental de la Conferencia de las Naciones Unidas sobre Medio Ambiente y Desarrollo (Cumbre de la tierra), celebrada en 1992 en Río de Janeiro. En esta cumbre, cerca de 180 países adoptaron un conjunto de principios, denominado Carta de la Tierra (Brundtland, 2007)[2], y se generó un programa de acciones para promover la sustentabilidad, la cual se denominó Agenda 21. Dentro de las estrategias que se definieron se planteó la importancia de contar con un sistema de indicadores de sostenibilidad que mostrara el grado de avance hacia los objetivos estratégicos del desarrollo sostenible.

En las instituciones de educación superior, la incorporación del desarrollo sostenible en las universidades se ubica en 1989, con la publicación del libro In Our Backyard: Enviromental Issues at UCLA, Proposals for Change, and the Institution´s Potencial as a Model, que hizo énfasis en la necesidad de una política ambiental institucional.

En los años siguientes, en 1990, representantes de 20 instituciones de educación superior de diferentes regiones del mundo, firmaron en Francia la declaración de Talloires (Mayer, 1990)[3] Este documento es una declaración a favor de la sostenibilidad, creada para y por directivos de institución superior; que reconoce que el rol de las

[3] Mayer, J. (1990). *Declaración de Talloires.* Talloires: University Leaders for a Sustainable Future

universidades en la educación, investigación, formación de políticas y necesidades de intercambio de información para atender “los cambios ambientales causados por los inequitativos e insostenibles patrones de consumo y producción que agravan la pobreza en muchas regiones del mundo”.

A partir de esta declaración es posible listar una serie de declaraciones y convenios entre los que se encuentran las declaraciones de: **Halifax** (1991), **Barbados** (1995). Convenciones como las: Cartas de Bologna y la Carta de Copérnico para el Desarrollo Sustentable. Todas ellas para abordar el desarrollo sostenible en universidades.

En México distintas universidades han desarrollado diferentes esquemas de administración ambiental, entre ellas la Universidad Autónoma de San Luis Potosí, la Universidad Autónoma Metropolitana, la Universidad la Salle, la Universidad Veracruzana, la Universidad Autónoma de Morelos, el Instituto Tecnológico de Estudios Superiores de Monterrey, la Universidad Iberoamericana, el Instituto Politécnico Nacional, entre otros.

La Universidad Nacional Autónoma de México ha desarrollado programas de administración ambiental tales como el Programa Universitario de Medio Ambiente (PUMA) que nace en 1991 y en 2015 cambia su nombre a Programa Universitario de Estrategias para la Sustentabilidad (PUES), el Proyecto de Ahorro de Energía que inició sus actividades en 1993 y el Programa de Manejo, Uso y Reúso del Agua (PUMAGUA) que inició sus actividades en 2005.

1.2 Programa Universitario de Estrategias para la Sustentabilidad antes Programa Universitario de Medio Ambiente

El Programa Universitario de Medio Ambiente nace el 15 de noviembre de 1991, es un espacio para la integración entre el quehacer universitario y las necesidades de la sociedad, a través del impulso y coordinación de proyectos multi e interdisciplinarios, así como multi-institucionales, que incentiven la investigación, la educación, la capacitación,

la difusión, la comunicación y la vinculación de los temas ambientales y del desarrollo sustentable (México, 2011)[4].

Las actividades que coordina el PUMA por la naturaleza compleja de la problemática que atienden, son abordadas de manera integral y requieren el concurso de diversas especialidades, por ello trabajamos con entidades académicas de las áreas científicas, sociales y humanísticas, formando así redes académicas que permiten abordar y generar respuestas a estas problemáticas (México, 2011)[4].

En el año 2009 la UNAM oficializó la puesta en marcha de la Estrategia de Universidad Sustentable Eco-PUMA (UNAM, 2009)[5]. En el marco de la Estrategia de Universidad Sustentable, EcoPuma; se ha desarrollado el Diagnóstico ambiental UNAM, herramienta que permite determinar el nivel de impacto ambiental que se genera por la operación de edificaciones académicas y administrativas, así como generar una hoja de ruta para generar mejoras con base en las tecnologías más avanzadas y factibles, con respecto a cuatro ejes: energía, agua, residuos y consumo responsable.

1.3 Diagnóstico y Distintivo ambiental UNAM

El Diagnóstico ambiental UNAM (DAUNAM) (UNAM, 2009)[5] permite la obtención de información sobre la infraestructura y la operación de las dependencias donde se realiza; a partir de este se establece una ruta de trabajo para aprovechar las principales áreas de oportunidad, mismas que se convierten en acciones que al ser implementadas se puedan evaluar y observar el beneficio ambiental.

Se emite un distintivo ambiental como reconocimiento en función al grado de cumplimiento integral en los cuatro ejes de acción (energía, agua, residuos y consumo responsable) que se evalúan, en este Distintivo ambiental se muestra el cumplimiento en

[4] *México, U. N. (11 de Septiembre de 2011). Programa Universitario de Medio Ambiente. Obtenido de Programa Universitario de Medio Ambiente: http://www.puma.unam.mx*

[5] *UNAM. (16 de 02 de 2009). Gaceta UNAM. Obtenido de http://www.dgcs.unam.mx/gacetaweb/2009/090216/gaceta.pdf página 4*

los ejes de acción y de esta manera se logra obtener uno de los tres distintos niveles que se pueden alcanzar, siendo estos el básico, azul y oro.

De esta manera se establece un plan de acción a corto y mediano plazo, así se instituye un compromiso para mejorar el desempeño ambiental, la vigencia del distintivo ambiental es de tres años, durante este periodo de tiempo se deben aplicar las recomendaciones emitidas según el plan de acción para que puedan ser evaluados nuevamente y de esta manera ver reflejados los cambios implementados y tener un avance continuo.

El diseño del Diagnóstico y distintivo Ambiental UNAM se basa en los aspectos operativos de diferentes esquemas de certificación en sustentabilidad:

1) *Sustainability Tracking Assessment Rating System* (STARS).
   Es un sistema de autoevaluación y de elaboración de informes adaptado a las peculiaridades de las entidades educativas. Este Sistema fué desarrollado por la Association for the Advancement of Sustainability in Higher Education (AASHE). (Satrs a Program of aashe, 2013)[6]

2) *Leadership in Energy and Environmental Design* (LEED). Es un programa de certificación de construcción verde que reconoce mejores estrategias y prácticas de construcción. Para recibir la certificación LEED, se necesita cumplir con requisitos previos para obtener puntos y alcanzar diferentes niveles de certificación. (LEED, 2012)[7]

   Tanto STARS como LEED se basan en una lista de comprobación de créditos organizados en diferentes categorías, incluyendo créditos de innovación que reconocen las nuevas prácticas no incluidas actualmente en la lista de comprobación.

[6] *Satrs a Program of aashe. (2013). Obtenido de www.stars.aashe.org*

[7] *LEED*. (2012). Obtenido de http://www.usgbc.org/leed#rating

3) *Construcción Sustentable del Gobierno del Distrito Federal*. Está enfocado en la transformación de edificaciones actuales y futuras bajo esquemas de sustentabilidad y eficiencia ambiental.

La realización del Diagnóstico y distintivo ambiental UNAM constituye un ciclo de mejora continua que puede esquematizarse mediante la siguiente Figura.1.1

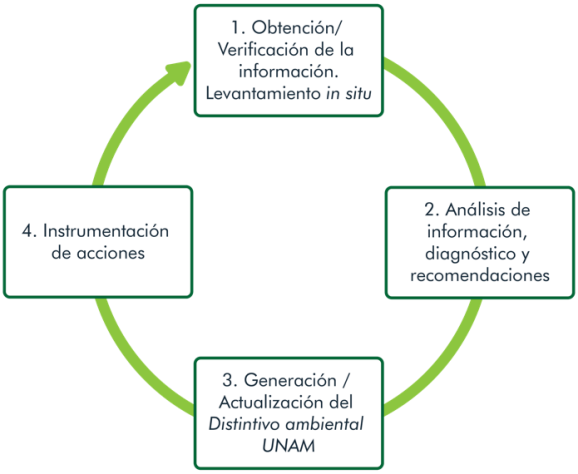


Figura1.1: Ciclo del Diagnóstico y distintivo ambiental UNAM

La información obtenida en los levantamientos es capturada y analizada a través de un sistema informático desarrollado mediante tecnologías PHP y MySQL. Este sistema analiza la información y genera un reporte sobre el estado actual de cada inmueble y sus oportunidades de mejora, genera estadísticas, criterios y determina los créditos que obtiene la organización con base en el *Diagnóstico ambiental UNAM*, mediante tablas y gráficas que describen el estado y perspectivas para cada uno de los ejes de acción.

1.4 La seguridad del Diagnóstico ambiental UNAM (DAUNAM)

El Diagnóstico ambiental UNAM (DAUNAM) se está posicionando a nivel nacional como un instrumento para medir el desempeño ambiental y emitir recomendaciones

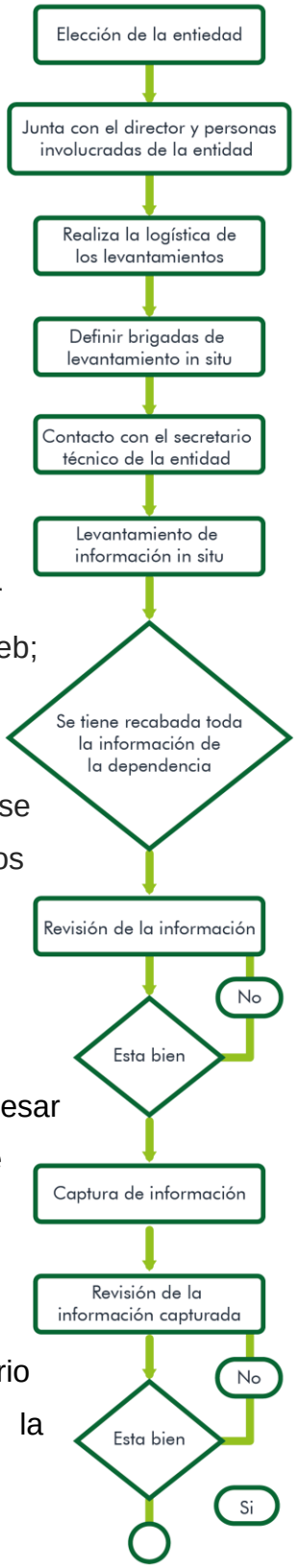
específicas de entidades administrativas y académicas, se han realizado alrededor de 150 diagnósticos en donde se incluyen dependencias de la UNAM, escuelas incorporadas a la UNAM, edificios de la Administración Pública Federal entre otras, por esta razón se cuenta con grandes volúmenes de información a la cual se les debe de dar un cuidado adecuado y evitar al mínimo cualquier riesgo que se pueda sufrir la información.

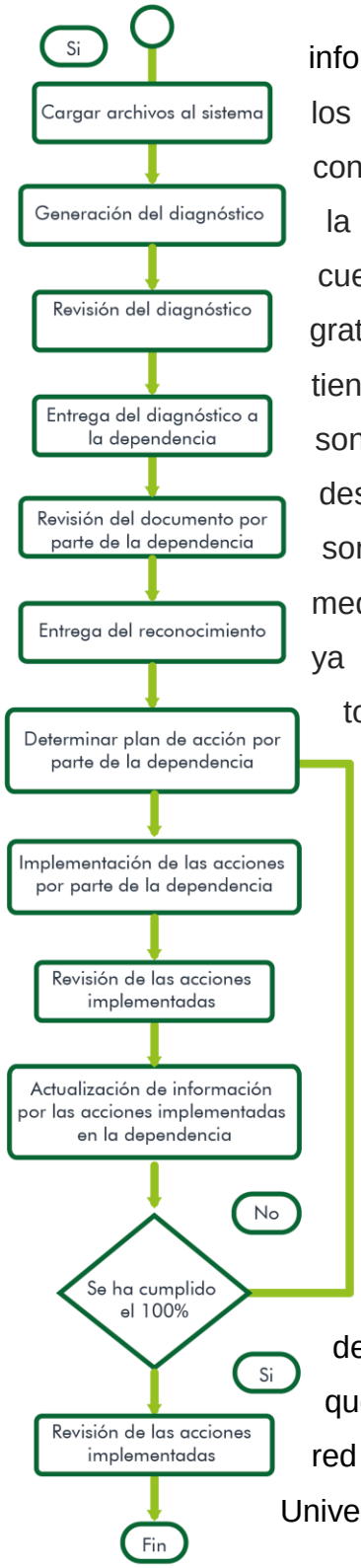
Una de las principales tareas que realiza el Programa Universitario de Estrategias para la Sustentabilidad es generar el Diagnóstico Ambiental UNAM, consta de un proceso que inicia cuando las brigadas realizan el levantamiento i*n situ* de la infraestructura de cada área en la entidad, relacionada con: eficiencia energética, gestión del agua, gestión de residuos, y consumo responsable, hasta la generación del diagnóstico y la emisión de las recomendaciones; proceso sumamente amplio, complejo y la información que genera es trascendental para las acciones que se derivan de ella (véase la Figura 1.2 Proceso)

Con base en la figura 1.2 se aprecia que las medidas de seguridad que se utilizan para el levantamiento de información, su almacenamiento, buen resguardo y procesamiento se vuelven un factor crítico en el éxito de los resultados que se esperan alcanzar en el Diagnóstico y Distintivo Ambiental UNAM.

La información que se obtiene en los levantamientos son formatos en papel los cuales se guardan en carpetas, las carpetas son colocadas en un librero que está dentro de la oficina al cual puede tener acceso cualquier persona (personal del programa, de intendencia, o incluso los visitantes) que se encuentre dentro de las instalaciones e ingrese a la oficina.

Figura 1.2 Proceso





Dicha información es capturada y los archivos se almacenan con la extensión .xls y .csv en la nube utilizando una cuenta de OwnCloud gratuita y común, a la cual solo tienen acceso las personas que son invitadas a dicha carpeta, después, los archivos .csv son cargados al sistema por medio de una plataforma web; ya que están cargados todos los archivos de la dependencia se realiza el cálculo de los indicadores del Diagnóstico y distintivo Ambiental UNAM.

Se puede ingresar al sistema a través de cualquier navegador, teniendo conocimiento de la dirección IP de la página web cualquier usuario que este conectado a la red del edificio de Programas Universitarios puede

ingresar al sitio, en el cual se pueden cargar archivos, dar de alta dependencias, editar información de las dependencias, y visualizar los resultados de los indicadores que se calculan y las puntuaciones que obtienen cada una de las dependencias.

Donde se encuentra alojado el sistema y la base de datos es un CPU que funciona como servidor; el cual se encuentra en un área común destinada a las oficinas del Programa Universitario por lo que está al alcance de cualquier persona y latente a cualquier daño intencional o accidental.

Respecto a los equipos de cómputo de los usuarios, se cuenta con 14 equipos de cómputo de usuarios que tiene una relación directa con el desarrollo del Diagnóstico ambiental UNAM y es pertinente que los usuarios cuenten con contraseñas no solamente para el acceso a los equipos, sino a la información contenida en ellos y a las aplicaciones que se requieren para su procesamiento, aspectos que son importantes para mantener la integridad, confidencialidad y disponibilidad de los datos, empezando desde los usuarios que trabajan con el sistema, el almacenamiento de la información, y las características del espacio donde se encuentra resguardado el equipo físicamente.

Dentro de todo el proceso del Diagnóstico ambiental UNAM intervienen actores que son de gran importancia para que se realice de la manera más adecuada, entre estos actores podemos encontrar:

- ***Datos recabados***

Son los obtenidos en los levantamientos de información por la brigada a través de los formatos creados para cada uno de los temas, para efectos de este análisis de riesgos, es nuestro activo de mayor importancia, necesarios para realizar la evaluación y emitir el Diagnóstico Ambiental UNAM de la dependencia correspondiente.
Los datos son el corazón que permite a una organización prestar sus servicios, la información es un activo abstracto que será almacenado en equipos, soportes de información o será transferido de un lugar a otro por los medios de transmisión de datos.

- ***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.
El Programa Universitario de Estrategias para la Sustentabilidad sigue el Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales para la Universidad Nacional Autónoma de México el cual se aprobó por el Consejo Universitario el día 26 de agosto de 2011.

- ***Archivos digitales***

Los archivos digitales se guardan en la aplicación Owncloud, a la cual solo tienen acceso algunas de las personas que se encuentran involucradas con el DAUNAM o en los equipos de cómputo de cada una de las personas que es responsable del levantamiento en la dependencia.

- ***Copias de respaldo***

Se generar copias parciales o totales del sistema para en caso de falla, siniestro, catástrofe natural o infección digital se pueda contar con un medio para disponer de los datos ya recolectados.

- ***Tipos de respaldos:***
    a) *Del sistema*: El respaldo del sistema se hace cada 15 días automáticamente y se guarda en el mismo disco donde se encuentra alojado el servidor y la base de datos con la que se trabaja en el DAUNAM. Se realiza otro respaldo del sistema y de la información en un disco duro externo el cual se lleva a cabo de manera no periódica, el disco duro externo se almacena en una de las gavetas del personal.
    b) *De la información*: Con respecto al respaldo de la información se realiza en diferentes puntos del proceso para realizar el DAUNAM, desde proteger los formatos físicos con protectores de plástico y almacenarlos

en un archivero, cuando ya están capturados los archivos se realiza una copia en una de las computadoras o en su caso en una USB, los archivos finales listos para subirse al sistema se almacenan en la nube utilizando la aplicación de OwnCloud

c) *De los usuarios:* No todos los usuarios hacen un respaldo de su información y quienes lo hacen lo realizan aperiódicamente.

- ***Seguridad***

Protección de la información y comunicaciones

La información no cuenta con la protección suficiente, se deberán generar cuentas de usuarios en la cuales se asignen actividades por nivel de usuario, así como restringir privilegios acordes a cada nivel, también tomar en cuenta la asignación de los diferentes equipos conforme a los usuarios que estén trabajando.

Además, se deberá contar con un mapeo de la red y conocer las puertas de enlace y direccionamiento ip de los equipos tanto inalámbricos como alámbricos.

- ***Servicios***

a) *Interno* (a usuarios de la propia organización) Los servicios que presta el sistema son exclusivamente para el personal del Programa Universitario de Estrategias para la Sustentabilidad que trabaja en el DAUNAM, ya que solo se puede tener acceso si se está conectado a la red de las instalaciones y se conocen las direcciones ip´s de páginas web y de las aplicaciones.

b) *Internet*: El servicio de se proporciona por cable Ethernet e inalámbrico y cuenta con la seguridad necesaria para hacer uso de él.

c) *Correo electrónico:* Una parte del personal cuenta con correo electrónico con el dominio @puma.unam.mx que se visualiza desde la cuenta de google, el resto del personal hace uso de su correo electrónico personal con el prestador del servicio que más le conviene.

d) Transferencia de archivos: Para la transferencia de archivos, muchas de las veces se utiliza una USB como medio, también se utiliza el correo electrónico

- ***Software***

a) Desarrollo propio: Se tiene un sistema llamado Sistema Estadístico de Desempeño Ambiental (SIEDA), dentro de dicho sistema se carga la información digital recabada a través de una página web la cual se autentifica a través de un usuario y contraseña, dentro del sistemas se permite hacer consultas de la información recabada, reportes y generar el entregable al cliente.

- ***Antivirus***

En la mayoría de los equipos de cómputo se tiene instalado un antivirus, algunos usuarios han instalado dos antivirus a la vez teniendo problemas con el software y el equipo.

- ***Sistema operativo***

La mayoría de los usuarios utiliza Windows en sus diferentes versiones como sistema operativo. Son muy pocos usuarios que utilizan un software libre como Linux.

- **Hardware**

a) *Computadoras de escritorio:* se cuenta con 12 equipos de escritorio, cada uno con diferentes características y programas dependiendo del usuario, la mayoría de los equipos cuenta con contraseñas para inicio de sesión y con cuentas de invitado para que puedan ser utilizadas por otros usuarios con algunas restricciones.

b) *Computadora personal:* se tienen 2 laptop, en algunas ocasiones algunos usuarios (servicios sociales) llevan su equipo de cómputo personal para poder realizar su trabajo el cual se conecta vía inalámbrica a la red.

c) *Equipos móviles:* por lo menos 12 de las personas que laboran en el área del DAUNAM cuentan con un equipo móvil (celular) que se conecta a la red inalámbrica de las instalaciones, el personal restante se conecta esporádicamente cuando va a realizar alguna actividad en las oficinas

- ***Equipo de respaldo***

Se cuenta con un disco duro externo en donde se realizan los respaldos de información del sistema SIEDA, no se realizan periódicamente, también se utiliza para guardar otro tipo de información como archivos o imágenes que son necesarias para el diagnóstico.

- ***Medios de impresión***

Se cuenta con una impresora que se conecta a la red por medio alámbrico, a esta impresora solo tiene acceso el personal que trabaja en el DAUNAM, está configurada con una ip fija y que no es conocida por el resto del personal.

- ***Soporte de la red***

Se cuenta con un par de personas que se encargan de darle soporte a la red ellos son los encargados de la seguridad empleada además de programar los mantenimientos óptimos tanto en la red y los medios que están involucrados como podría ser modem, hub, switch, router, entre otros.

- ***Equipamiento auxiliar***

Sistema de alimentación ininterrumpida: se cuenta con un UPS que proporciona energía a todo el edificio de Programas Universitarios cuando se sufre algún corte de la alimentación de energía eléctrica.

- ***Equipos de climatización***

Se cuenta con 1 aires acondicionados que se encuentran ubicados en el cuarto del UPS con 2 toneladas de refrigeración.

- ***Cableado***

Se cuenta con un cableado para proporcionar el servicio de internet en todo el edificio de Programas Universitarios.

- ***Cable eléctrico***

Se cuenta con cableado eléctrico de corriente normal y corriente regulada, en la oficina que pertenece al DAUNAM se cuenta con 2 contactos de corriente regulada los cuales no son suficientes cuando el sistema de energía es interrumpido.

- ***Fibra óptica***

Se cuenta con fibra óptica que llega solamente al site del edificio de Programas Universitarios.

- ***Mobiliario***

Dentro del mobiliario con el que se cuenta son escritorios y sillas para cada una de los usuarios, con un archivero y un librero, también se cuenta con un mueble para almacenar insumos cotidianos como papel, papel de reúso, cafetera.

- ***Instalaciones***

Las instalaciones se pueden describir que es un edificio de dos niveles (planta baja y primer nivel) el cual está ocupado por diferentes dependencias de la UNAM entre las cuales se encuentra el Programa Universitario de Estrategias para la Sustentabilidad (PUES).

- ***Usuarios externos***

Se tienen usuarios externos, la cantidad de estos pueden ser variables ya que el edificio alberga a diferentes Programas Universitarios y esto cuentan con un número de visitas indefinido dependiendo de las actividades que se realicen ya sea por reuniones, entrega de productos o mensajería.

- ***Usuarios internos***

Se cuenta con 10 personas que están de base en la oficina del DAUNAM, hay 2 personas de medio tiempo y por lo menos 3 personas realizando su servicio social,

también dependiendo de la carga de trabajo algunas personas de la brigada van a realizar la capturar información.

- ***Administradores del sistema***

Se tiene un administrador del sistema el cual se encarga de realizar las modificaciones al código fuente, administrar la base de datos y hacer los cambios necesarios a la página web con la que se cuenta.

- ***Administradores de telecomunicaciones***

Son dos los administradores de las telecomunicaciones, físicamente se encuentran en otro edificio y son los encargados de administrar los dos edificios, lo que ocasiona que su tiempo de respuesta sea muy tardado ante un problema

- ***Administradores de seguridad***

Las personas encargadas de administrar las comunicaciones también se encargan de administrar la seguridad respecto a los sistemas digitales.

La seguridad del edificio está a cargo del administrador del edificio, la cual consta de un módulo de registro para la entrada y salida de este. Se cuenta con una bitácora donde se tiene datos del nombre de quien entra, a quien visita y la hora de entrada y salida del edificio.

Respecto a la seguridad de los equipos para el DAUNAM, no se cuenta con un administrador que trate este tema, en algunas de las ocasiones el mismo usuario se encarga de su seguridad, pero no con los conocimientos necesario

Capítulo 2

Metodología MAGERIT

Capítulo 2 Metodología MAGERIT

2.1 Importancia

La información es el activo principal y más importante de toda Organización; ya que con ella se pueden integrar un sin fin de actividades para su beneficio, por lo cual es considerable que se le dé un tratamiento adecuado con las medidas necesarias de seguridad y de esta forma no se corran grandes riesgos que puedan perjudicar o hacer desaparecer la Organización.

Cuando se habla de sistemas no se puede dejar de lado uno de los aspectos más relevantes en este ámbito, el Sistema de Gestión de Seguridad de la Información (SGSI), es la piedra angular para realizar un pertinente análisis de riesgos asociado a todos los activos de la Organización. No es posible realizar una aplicación total de medidas de seguridad sin antes haber analizado los riesgos que se pueden sufrir, de esta manera implementar las medidas proporcionadas a estos riesgos, a la condición de la tecnología y a los costos por la ausencia de seguridad, como de las medidas que puedan ser implementadas para la protección.

Es importante realizar este análisis ya que es la herramienta que permite identificar las amenazas a las que se encuentran expuestos los activos dentro de la Organización, estimar la frecuencia de que se materialicen y poder valorar el o los impactos que puede conllevar.

Una parte fundamental dentro de la gestión de la seguridad, es conocer y controlar los riesgos a los cuales está expuesta la información de la Organización. Una manera de realizar este gran trabajo e implementar un sistema de gestión de seguridad, es buscar una metodología la cual brinde un marco de trabajo definido, que facilite la administración de los riesgos y permita mejorarla, una de estas metodologías con la que se puede trabajar es MAGERIT que basa su importancia en la gestión de riesgos la cual

combina dos tareas muy importantes: el análisis y el tratamiento de los riesgos como se muestra en la figura 2.1.

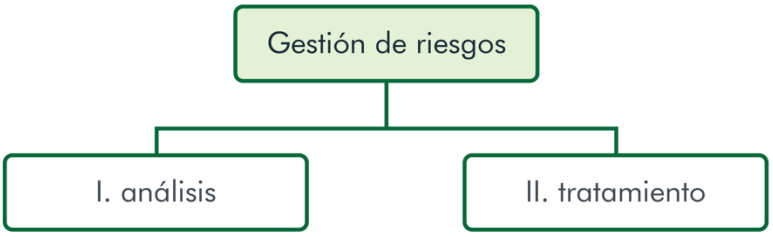


Figura 2.1 Gestión de Riesgos según MAGERIT

***Análisis**:* Se refiere al análisis de riesgos, y su tarea es determinar que tiene la organización y estimar lo que podría pasar.

Tratamiento: El tratamiento de los riesgos permite a la organización tener barreras de defensa de manera consciente y prudente, además de estar preparados en caso de un ataque para saber cómo actuar y seguir operando.

El Análisis de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Actualmente MAGERIT es una metodología de análisis y gestión de riesgo que cuenta con reconocimiento internacional, porque toman en cuenta la ISO 27005 (Gestión de Riesgos de la Seguridad Informática) e ISO 31000 (Gestión de Riesgos) que son los estándares más conocidos para realizar un análisis de riesgos, de ellos ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la

información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados.

Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos como se muestra en la figura 2.2

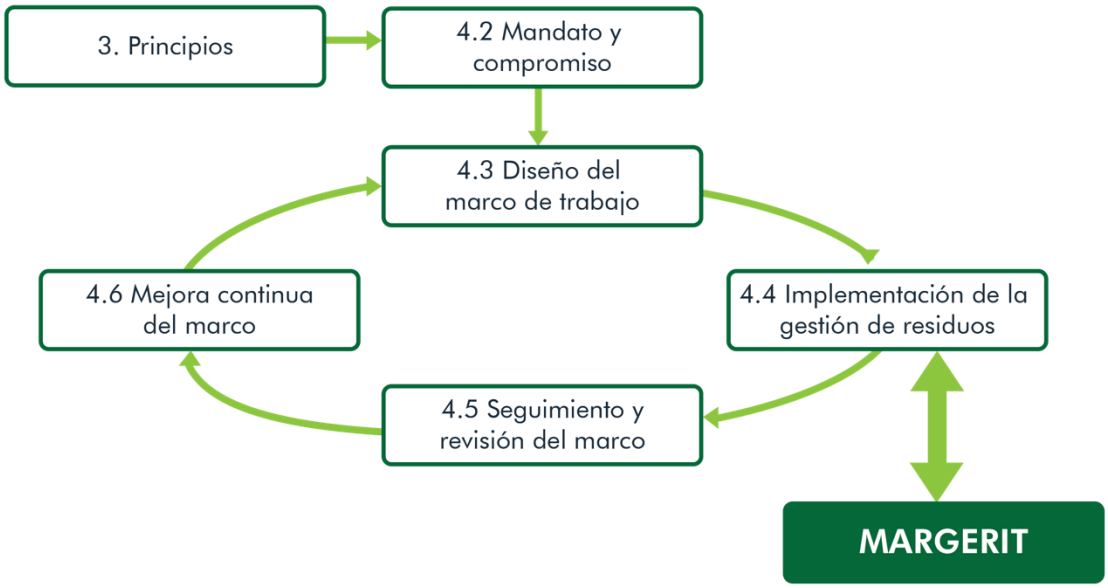


Figura 2.2 ISO 31000 - Marco de trabajo para la gestión de riesgos

Es la metodología ideal para aquellas Organizaciones que comienzan con la gestión de la seguridad de la información como es el caso del *Diagnóstico y distintivo ambiental UNAM*, debido a que permite enfocar los esfuerzos en los riesgos que resultan prioritarios, uno de los puntos más interesante es que al estar alineado con los estándares de ISO hace que su implementación se convierte en un punto de partida para la búsqueda de una certificación, para mejorar los sistemas de gestión y estar preparado para una auditoría, como se muestra en la figura 2.3.

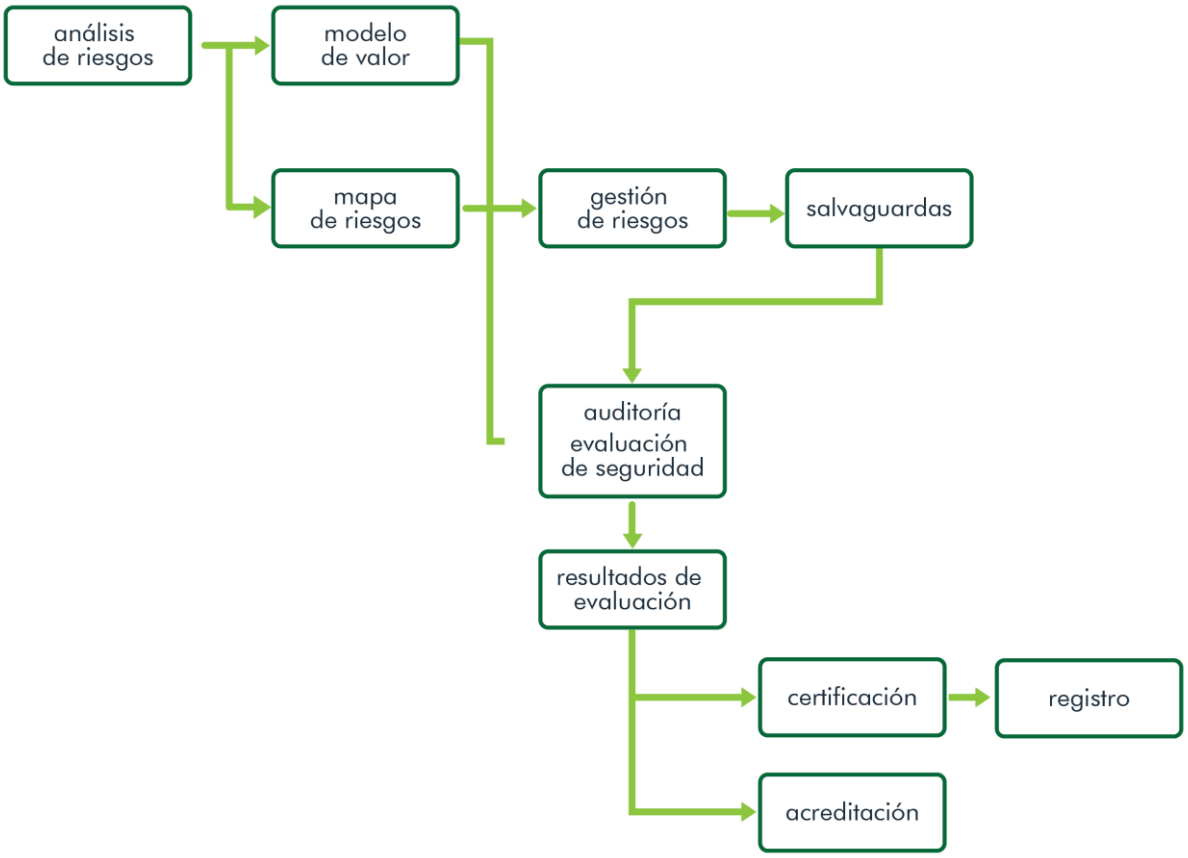


Figura 2.3 Contexto de certificación y acreditación de sistemas de información

Los puntos más importantes son:

Evaluación. Se necesita para la seguridad de los sistemas de información, tanto internamente como parte de los procesos de gestión, por medio de evaluadores independientes o externos. Las evaluaciones permiten medir el grado de confianza que merece o inspira un sistema de información.

Certificación. Si es que el punto anterior se cumple de manera debida y adecuada, el siguiente paso es una certificación, lo cual asegura responsablemente y por escrito un

comportamiento, a través de una serie de evaluaciones orientadas por un objetivo, lo cual comprueba la capacidad de protección.

Acreditación. Algunas certificaciones tienen como objetivo la acreditación del producto o sistema. La acreditación es un proceso específico cuyo objetivo es legitimar al sistema para formar parte de sistemas más amplios. Se puede ver como una certificación para un propósito específico.

Auditorías. Su objetivo es dictaminar sobre la adecuación de las medidas y controles a la ley y su desarrollo reglamentado, incluyendo datos, hechos y observaciones en que se basan dictámenes alcanzados y recomendados. Las auditorías deben repetirse regularmente tanto para seguir la evolución del análisis de riesgos (que se debe actualizar regularmente) como para seguir el desarrollo del plan de seguridad determinado por las actividades de gestión de riesgos. Otras veces requeridas por la propia Dirección de la Organización, otras veces requeridas por entidades colaboradoras que ven su propio nivel de riesgo ligado al nuestro.

2.2 Características

Descripción General

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), está reconocida por la Europan Network and Information Security Agency (ENISA) junto a otras metodologías europeas e internacionales.

Es una metodología de carácter público elaborada por el Consejo Superior de Administración Electrónica (CSAE), órgano del Ministerio de Administraciones Públicas (MAP) encargado de la preparación, elaboración, desarrollo y aplicación de la política informática del Gobierno español.

Objetivos:

MAGERIT lleva a cabo el Proceso de Gestión de Riesgos dentro de un plan que llevan las organizaciones para que puedan tomar decisiones teniendo presente los riesgos derivados por el uso de las tecnologías de la información.

MAGERIT persigue los siguientes objetivos:

Directos:

1. Concientizar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicación
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Indirectos:

4. Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación

Lo que se busca es homogeneizar los informes de los hallazgos y las conclusiones de las actividades del análisis y gestión de riesgos en los siguientes documentos:

- ***Modelo de valor****:* caracterización del valor que representan los activos para la organización, así como de las dependencias entre los diferentes activos.
- ***Mapa de riesgo:*** relación de las amenazas a que están expuestos los activos.
- ***Declaración de aplicabilidad*****:** para un conjunto de protecciones, se indica si son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.
- ***Evaluación de la protección:*** evaluación de la eficiencia de la protección existente en relación al riesgo que afrontan.

- ***Estado de riesgo:*** caracterización de los activos por su riesgo residual; es decir, por lo que puede pasar tomando en consideración las protecciones desplegadas.
- ***Informe de insuficiencias:*** Ausencia o debilidad de la protección que aparecen como oportunas para reducir los riesgos sobre el sistema. Es decir, recoge las vulnerabilidades del sistema, entendidas como puntos débilmente protegidos por los que las amenazas podrían materializarse.
- ***Cumplimiento de normativa:*** Satisfacción de unos requisitos. Declaración de que se ajusta y es conforme a la normatividad correspondiente.
- ***Plan de seguridad:*** conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos.

Estructura de la metodología

MAGERIT realiza el Proceso de Gestión de Riesgos que incluye el método de análisis de riesgos, el proyecto de análisis de riesgos y el plan de seguridad como se muestra en la figura 2.4.

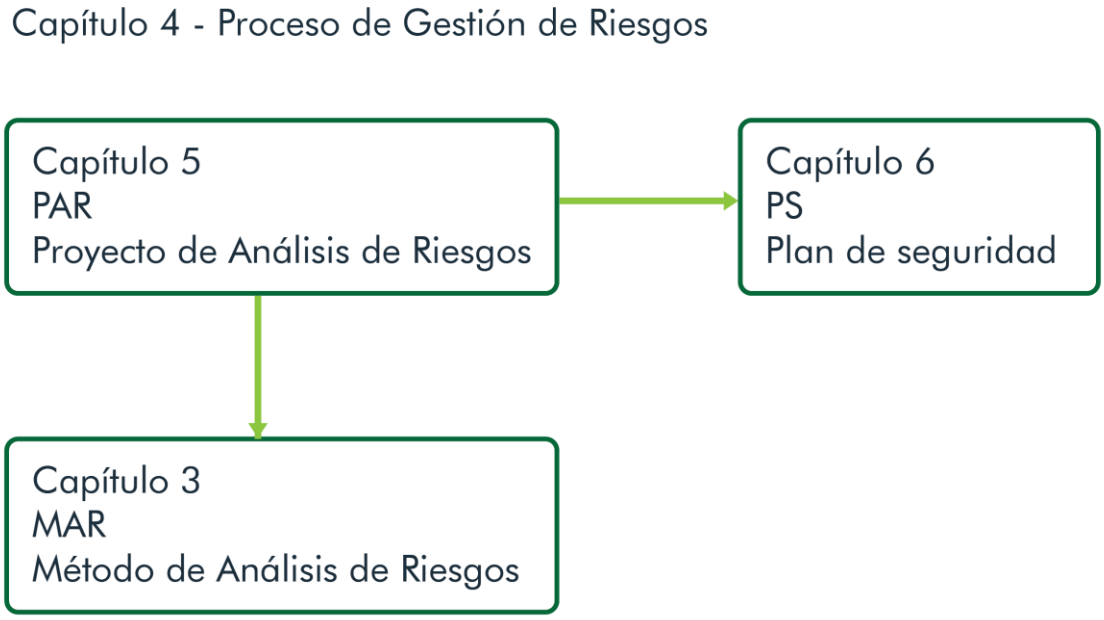


Figura 2.4 *Actividades formalizadas*

Para realizar estos análisis y el plan de seguridad, MAGERIT se ha estructurado en dos libros y una guía técnica las cuales se explican a continuación:

Libro I - Método

Presenta los conceptos, actividades y tratamiento del proceso integral de gestión de riesgos, concretando los pasos y formalizando las actividades del análisis de riesgo describiendo opciones y criterios de tratamientos para los riesgos formalizando las actividades a seguir centradas en el proyecto de análisis de riesgo, teniendo en cuenta un sistema y eventualmente cuando hay cambios sustanciales ser capaces de ampliar, modificar o rehacer el sistema.

Generar el plan estratégico con base en el sistema de información para gestionar la seguridad del producto final desde el inicio hasta su puesta en producción, para poder asegurar la protección del propio desarrollo basado en un marco legal, normativo y certificado.

Libro II - Catálogo de Elementos

Marca pautas en cuanto a:

- Tipos de activos
- Dimensiones de valoración de los activos
- Criterios de valoración de los activos
- Amenazas típicas sobre los sistemas de información
- Salvaguardas a considerar para proteger sistemas de información

Para logra el adecuado funcionamiento se persiguen dos objetivos claros:

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

Guía Técnica

Se basa en la orientación sobre algunas técnicas especificadas en el libro I para llevar a cabo proyectos de análisis y gestión de riesgos mediante técnicas específicas y generales para el análisis de riesgos las cuales se listan a continuación:

Técnicas Específicas

- Análisis Mediante Tablas
- Análisis Algorítmico
- Árboles De Ataque

Técnicas Generales

- Técnicas Gráficas
- Sesiones De Trabajo: Entrevistas, Reuniones Y Presentaciones
- Valoración Delphi

2.3 Funcionamiento

En conjunto con los objetivos, la estrategia y políticas de la Organización, las actividades del tratamiento de los riesgos permiten elaborar un plan de seguridad que, establecido y en funcionamiento, satisfagan los objetivos propuestos con el nivel de riesgos que acepta la Organización.

Dentro del proceso del análisis de riesgos, no se debe dejar de lado las dimensiones de la seguridad que para la Organización deben de ser de suma importancia, las cuales se listan a continuación:

- Disponibilidad
- Integridad
- Confidencialidad
- Autenticidad

La implementación de las medidas de seguridad, requieren de una Organización que este gestionada adecuadamente y la participación informada de todo el personal que trabaja en ella, en especial las personas involucradas con los sistemas informáticos.

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y medidas de protección, que formalizan cuatro etapas cíclicas como se muestra en la figura 2.5

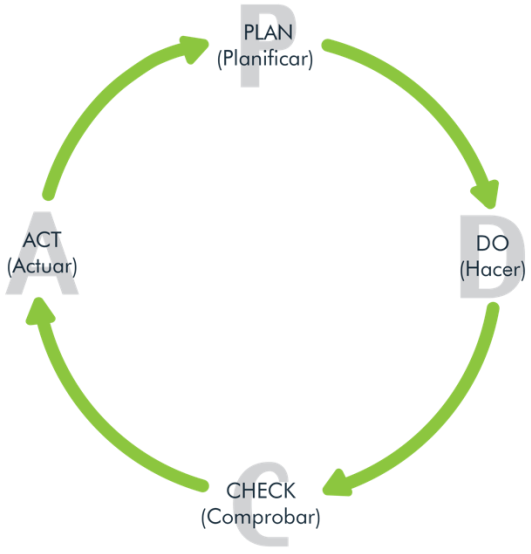


Figura 2.5 Ciclo Deming

El análisis de riesgos es parte de las actividades de *planificación*, donde se toman decisiones de tratamiento. Estas decisiones se materializan en la etapa de *hacer*, donde conviene desplegar elementos que permitan la monitorización de las medidas desplegadas para poder comprobar la efectividad de las mismas y *actuar* en consecuencia, dentro de un círculo de excelencia y mejora continua.

El método que describe MAGERIT para realizar el análisis de riesgos muestra una serie de pasos, los cuales van guiando de una manera sencilla el cómo reconocer los elementos indispensables que se necesitan para realizar el análisis completo y de gran calidad, a continuación, se muestran los pasos para realizarlo:

Identificación de los Activos

Los activos son los componentes o funcionalidades de un sistema de información susceptible a ser atacado deliberadamente o accidentalmente con consecuencias para la Organización, dentro de estos activos se pueden incluir los datos, servicios, aplicaciones, equipos físicos, redes de comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Dentro de un sistema de información se toman dos cosas esenciales, la información que se maneja y los servicios que se prestan. Estos activos son esenciales y marcan los requisitos de seguridad para todos los demás componentes que conforman el sistema.

La información y los servicios son activos de gran importancia, pero estos dependen de otros activos más prosaicos, de esta manera los activos forman grafos de dependencias donde la seguridad de los activos que se encuentran más arriba en este grafo depende de varios activos que son inferiores en la estructura del grafo. Estas estructuras reflejan de arriba hacia abajo las dependencias, mientras que de abajo hacia arriba la propagación del daño en caso de que se materialice una amenaza.

Un punto importante es la valoración que le damos a cada uno de los activos, esta valoración se puede ver desde la perspectiva de la necesidad de proteger al activo, pues cuanto más valioso sea este, mayor nivel de protección requiere en las dimensiones de seguridad que sean pertinentes. Dentro de las dimensiones que pueden interesar en los activos se encuentran la confidencialidad; ¿qué daño puede causar que conozca un activo quien no debe?, su integridad; ¿qué prejuicio puede causar que estuviera dañado o modificado el activo?, su disponibilidad; ¿qué pasaría si el activo no se puede utilizar o no se tiene?

En esta metodología se incluye la autenticidad (el saber quién hace o ha hecho) y el concepto de trazabilidad, que para efectos técnicos se puede traducir en mantener la integridad y la confidencialidad de ciertos activos del sistema.

Una vez que se establecen y determinan las dimensiones de los activos se tiene que hacer una valoración de estos, la cual consiste en saber el precio que costaría el recuperarse de un incidente que pudiera destrozar el activo parcial o totalmente.

Esta valoración puede ser cuantitativa o cualitativa, dentro de estos tipos de valoración se tienen que valora la homogeneidad que consiste en poder comparar valores, aunque sean de diferentes dimensiones a fin de poder combinar valores propios y acumulados.

Identificación de las Amenazas

Consiste en determinar las amenazas que pueden afectar a cada activo, las amenazas surgen a partir de la existencia de vulnerabilidades que pueden ser aprovechadas y con estas se puede comprometer o no la seguridad de un sistema de información, lo que interesa es que puede pasarles a los activos de la Organización y causar daño.

Dentro de la identificación de las amenazas se pueden clasificar de la siguiente forma:

- De origen natural
- Del entorno (de origen industrial)
- Defecto de las aplicaciones
- Causadas por las personas de forma accidental
- Causadas por las personas de forma deliberada

No todas las amenazas afectan a todos los activos, si no que existe una relación entre el tipo de activo y de lo que le puede ocurrir.

Cuando un activo de la organización es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma proporción, una vez que se ha determinado la amenaza que puede perjudicar al activo, hay que valorar su influencia en dos sentidos: su degradación y la probabilidad que pueda llegar a materializarse la amenaza.

La degradación mide el daño causado por un incidente, esto es, cómo un activo se ha visto totalmente degradado o solo una pequeña fracción, respecto a la probabilidad es más compleja de determinar y expresar, en ocasiones se puede modelar cualitativamente por medio de una escala nominal que puede ir desde muy alta la probabilidad de que ocurra, hasta muy baja o muy rara que ocurra, también se puede modelar numéricamente respecto a la frecuencia de ocurrencia, dándole valores de 100 cuando ocurre muy frecuente o 1/100 cuando es muy poco frecuente.
Se debe determinar el impacto potencia, el cual se refiere a la media del daño sobre el activo derivado de que se materialice la amenaza, una consideración que queda hacer es relativa a las dependencias entre activos, para enlazar unos con otros se recurre al grafo de dependencias.

Dentro de los impactos se encuentra el acumulado, se calcula este impacto teniendo en cuenta su valor acumulado y la amenaza a la que está expuesto. El impacto repercutido

es calculado sobre un activo teniendo en cuenta su propio valor y las amenazas a las que están expuestos los activos de los que depende.

Identificación de las medidas de protección

Se definen a las medidas de protección o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen un riesgo. Hay amenazas que se evitan simplemente organizándose adecuadamente, otras requieren elementos técnicos, otras de seguridad física y, por último, está la política del personal.

Dentro del gran espectro de posibles medidas de protección a considerar, es necesario realizar una discriminación inicial para considerar solo aquellas que son relevantes y necesarias para lo que hay que proteger. Dentro de esa selección discriminatoria se deben considerar los siguientes aspectos:

1. Tipo de activo a proteger
2. Dimensión o dimensiones de seguridad que requieren protección
3. Amenazas de las que se necesita proteger
4. Si existe alguna medida de protección alternativa

Además, es prudente establecer un principio de proporcionalidad y tener en cuenta:

1. El mayor o menor valor propio o acumulado sobre un activo, centrándose en la más valioso y obviando lo irrelevante
2. La mayor o menor probabilidad que una amenaza ocurra, centrándonos en los riesgos más importantes
3. La cobertura del riesgo que proporcionan salvaguardas alternativas

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

No aplica – cuando una medida de protección no se aplica por que técnicamente es inadecuada al tipo de activo que se desea proteger, no protege las dimensiones necesarias y no protege frente a la amenaza en consideración.
No se justifica – cuando la medida de protección aplica, pero no protege del riesgo en su totalidad.

Existen diferentes tipos de medidas de protección como las que se mencionan a continuación:

- Prevención
- Disuasión
- Eliminación
- Minimización del impacto/ limitación del impacto
- Corrección
- Recuperación
- Monitorización
- Detección
- Concientización
- Administración

Las medidas de protección se caracterizan por su eficiencia frente al riesgo que pretenden prevenir, la medida de protección ideal es la que es 100 porciento eficaz, la cual combina dos factores desde un punto de vista técnico:

- Es técnicamente idónea para enfrentar el riesgo que protege y
- Se emplea siempre

Desde el punto de vista de operación de la de la medida de protección:

- Está perfectamente desplegada, configurada y mantenida

- Existen procedimientos claros de uso normal y en caso de incidencias
- Los usuarios están formados y concientizados
- Existen controles que avisan de posibles fallos

2.4 Proceso de Gestión de Riesgos

Una vez identificado los pasos anteriores comienza el proceso de gestión de riesgos, en el cual se debe tener consideraciones muy importantes, ya que no solo son las políticas internas también se consideran políticas externas, por lo cual se considera:

- Las obligaciones por ley internas
- Las obligaciones por ley de acuerdo al sector
- Las obligaciones por contrato

Dicho proceso se determina impactos y riesgos, calculando la posible magnitud y efectos que podrían llegar a provocar ya que se verá reflejado en posibles daños y hasta qué grado la organización está dispuesta a permitirlos o aceptarlos

Debido al impacto que podría tener una mala decisión en la organización ya que puede repercutir tanto en imagen pública, políticas internas o externas, relaciones con otras organizaciones o nuevas ofertas de mercado, se clasifican en:

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

Para poder entender aún mejor la ruta que se toma para decisiones se observa la figura 2.6 que muestra las decisiones de tratamiento de riesgos

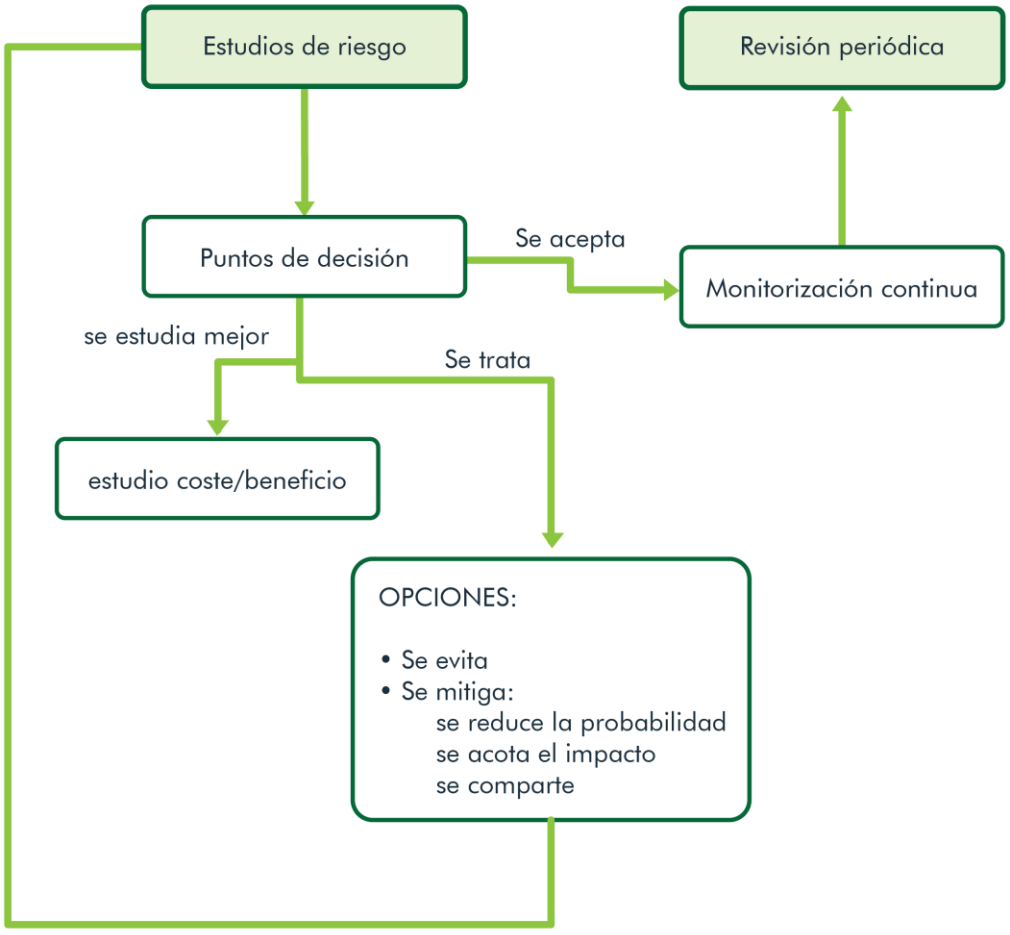


Figura 2.6 Decisiones de tratamiento de riesgos

Una vez que se tomaron las decisiones se hace una serie de cálculos para poder determinar el impacto para el cual se basa en un gráfico de zonas de riesgos como se muestra en la figura 2.7 Zonas de Riegos.

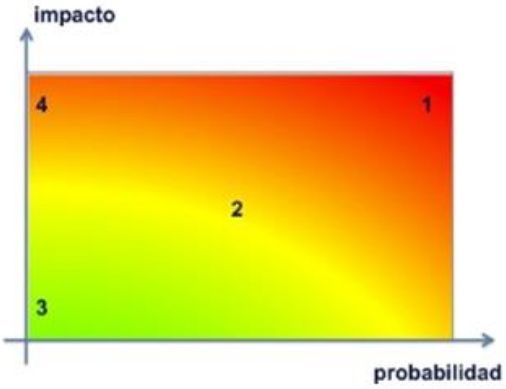


Figura 2.7 Zonas de Riegos.

De las cuales de acuerdo a su resultado se le asigna una zona lo que permite saber las características y como se podrían ver afectada:

- ***Zona 1*** – riesgos muy probables y de muy alto impacto; posiblemente nos planteemos sacar los 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.

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.

Una vez que detectamos lo anterior es importante dar opciones de tratamiento de riesgo los cuales están en 4 factores

1. Eliminación: es una opción frente a un riesgo que no es aceptable.
2. Mitigación: reducir la degradación causada por una amenaza (a veces se usa la expresión ‘acotar el impacto’) o reducir la probabilidad de que una amenaza de materializa
3. Compartición: Aceptar el riesgo, pero contratar un seguro o componentes externos porque así las consecuencias corren a cargo del tercero.
4. Financiación: Se acepta el riesgo dentro de la organización y de manera interna crear un fondo en caso de que se concrete el riesgo.

Por lo cual el proceso de gestión de riesgos queda conformado como se muestra en la Figura 2.7 para formalizar las actividades a través de roles y funciones

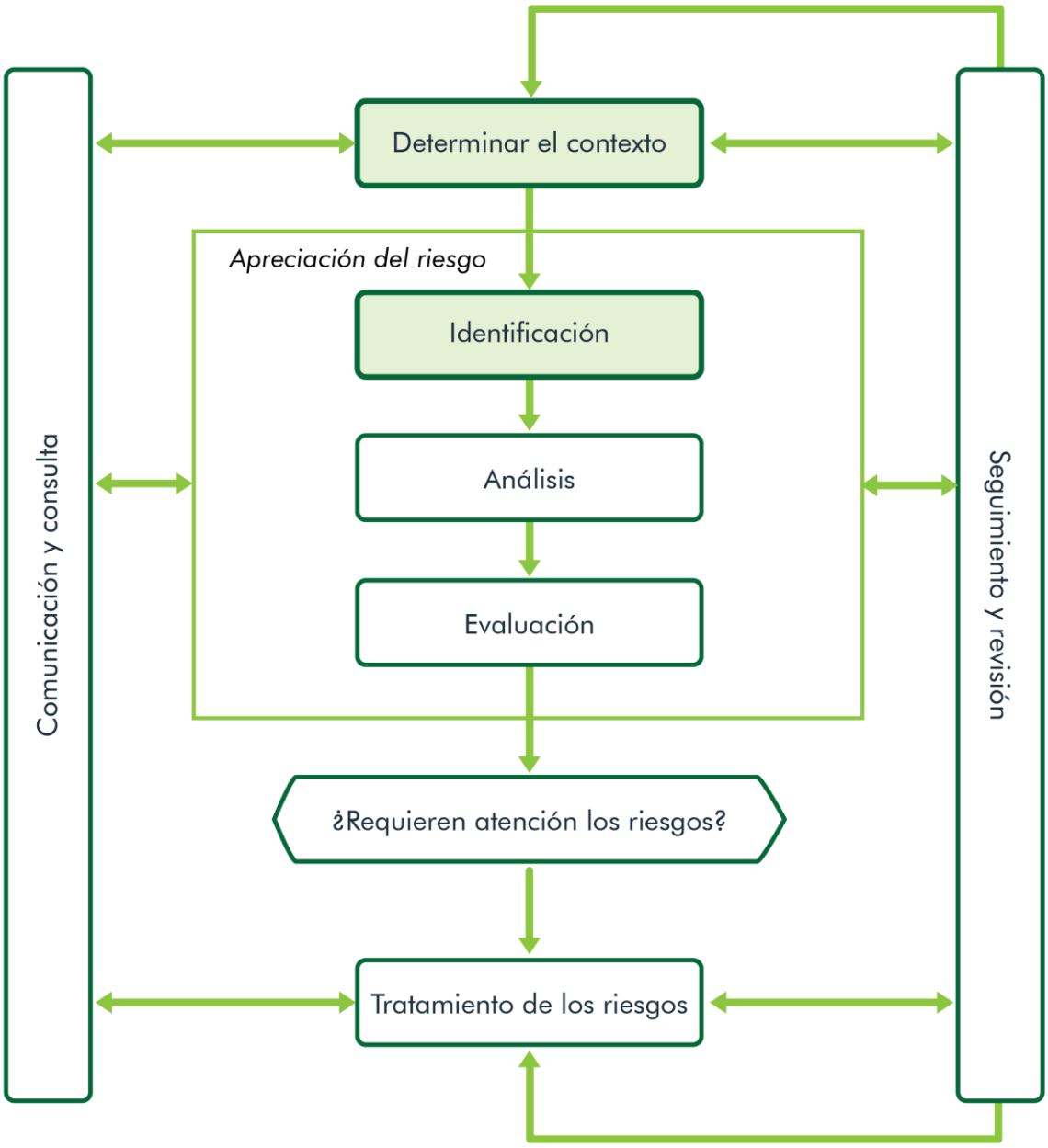


Figura 2.8 Proceso de Gestión de Riesgos

2.5 Proyecto de análisis de riesgos

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.

Por proyecto de análisis de riesgo se lleva a cabo por medio de las siguientes tareas:

- Actividades preliminares
    - Estudio de oportunidad
    - Determinación del alcance del proyecto
    - Planificación del proyecto
    - Lanzamiento del proyecto
- Elaboración del análisis de riesgos
- Comunicación de resultados

Son una serie de actividades para poder determinar el proyecto en el cual se basará para determinar un catálogo de activos, las dimensiones de seguridad a implementar además de los criterios de validación que se utilizaran.

2.6 Plan de Seguridad

El plan de seguridad es poner llevar a cabo el proyecto que hemos planteado en el punto anterior, para con esto poder materializar el objetivo principal que es resguardar los activos de la organización y disminuir en lo posible el impacto de las amenazas si es que se llegaran a efectuar.

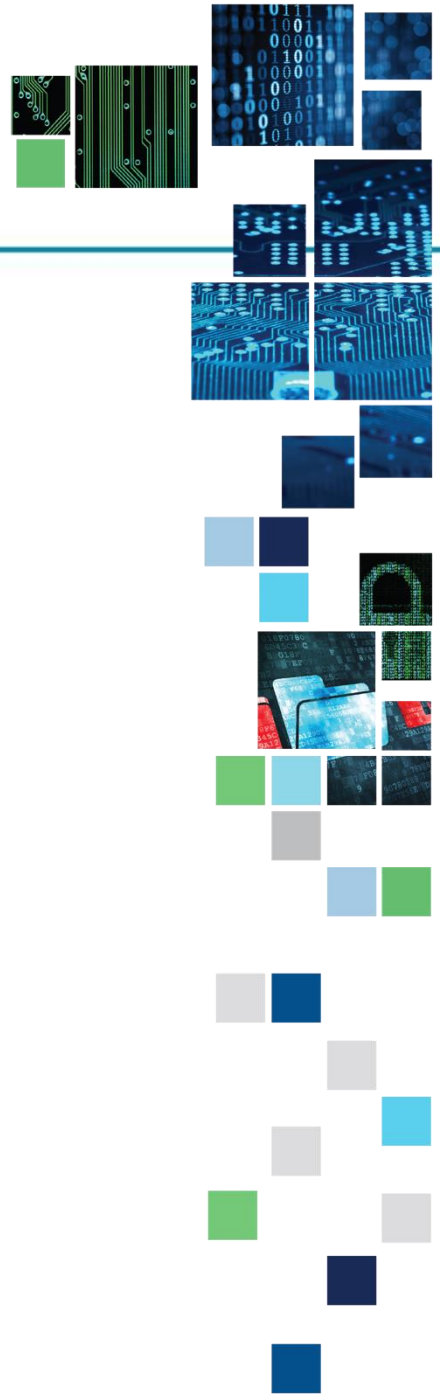
En última instancia se trata de implantar o mejorar la implantación de una serie de salvaguardas que lleven impacto y riesgo a los niveles residuales determinados por la Dirección.

Este tratamiento de las salvaguardas se materializa en una serie de tareas a llevar a cabo.

El plan de seguridad identifica tres tareas en el siguiente orden:

1. Identificación de proyectos de seguridad: Se traducen las decisiones de tratamiento de los riesgos en acciones concretas
2. Plan de ejecución: Ordenar en el tiempo los proyectos de seguridad teniendo en cuenta distintos factores.
3. Ejecución: Alcanzar los objetivos previstos en el plan de seguridad para cada proyecto planificado.

Capítulo 3
Diseño del plan de seguridad



Capítulo 3. Diseño del plan de seguridad

Para generar el plan de seguridad con base en la metodología MAGERIT, se lleva a cabo una serie de etapas las cuales se mencionan a continuación aplicándolas al problema de interés.

3.1 Análisis de riesgos

"Un análisis del riesgo de seguridad define el ambiente actual y realiza acciones correctivas recomendadas si el riesgo residual no es aceptable" (Barrientos & Reyes, 2006).

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo una serie de pasos pautados:

- Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué costo supondría su degradación, entendiendo como activo a todo aquello con valor para una Organización y que necesita de protección – datos, infraestructura, hardware, software, personal y su experiencia, información y servicios (Barrientos & Reyes, 2006).
- Determinar a qué amenazas están expuestos los activos
- Determinar qué salvaguardas existen y qué tan eficientes son frente al riesgo
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el riesgo, definido como el impacto ponderado con la taza de ocurrencia de la amenaza

La figura 3.1 muestra la relación entre los elementos de un análisis de riesgos:

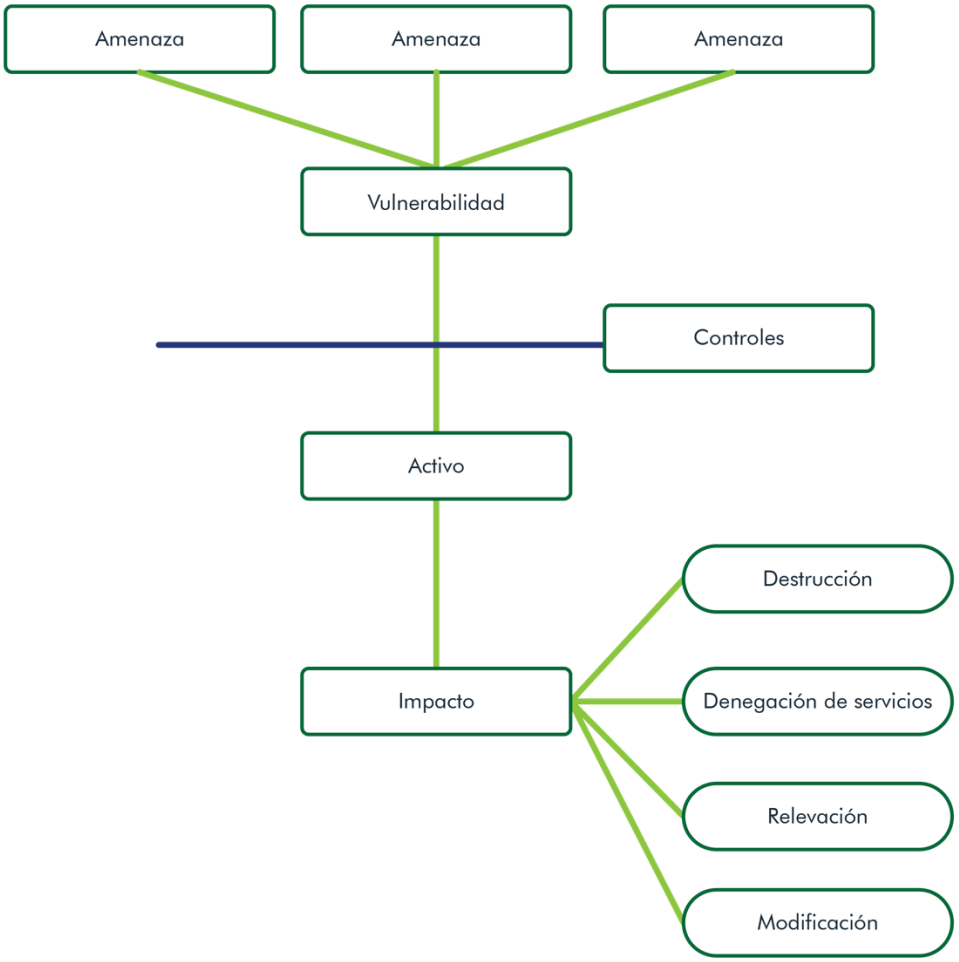


Figura 3.1 *Relación entre los elementos de un análisis del riesgo (Barrientos & Reyes, 2006)*

Las herramientas de Entorno de Análisis de Riesgos (EAR) soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT.

Los activos están expuestos a amenazas que, cuando se materializan, degradan el activo, produciendo un impacto. Si estimamos la frecuencia con que se materializan las amenazas, podemos deducir el riesgo al que está expuesto el sistema. Degradación y frecuencia califican la vulnerabilidad del sistema.

El gestor del sistema de información dispone de salvaguardas, que o bien 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.

Para propósitos de este análisis de riesgos se realizó la identificación de activos y amenazas de manera manual, revisando todo el proceso que se lleva acabo para la generación del Distintivo ambiental UNAM, de manera paralela a esta tarea se utilizó la herramienta PILAR que dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

- ISO/IEC 27002 (2005, 2013)- Código de buenas prácticas para la Gestión de la Seguridad de la Información
- Esquema Nacional de Seguridad

3.2 Identificación de Activos:

Objetivo: Identificar los activos que componen el sistema, determinando sus características, atributos y clasificación en los tipos determinados. (Metodología MAGERIT, 2012)

En la figura 1.2 se puede observar el proceso y las tareas que se llevan a cabo para realizar el Diagnóstico y Distintivo ambiental UNAM, en cada una de las etapas participan diferentes actores, para realizar la identificación de los activos se analizó el diagrama del proceso que se lleva a cabo para realizar el Diagnóstico y Distintivo ambiental UNAM (visto en el capítulo 1 pág. 13).

Dependencias entre activos:

Objetivo: 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. (MAGERIT)

Valoración de los Activos

Objetivos: Identificar en qué dimensiones es valioso el activo, valorar el coste que para la Organización supondría la destrucción del activo (Metodología MAGERIT, 2012)

- Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. (Metodología MAGERIT, 2012)
- Integridad [I]: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. (Metodología MAGERIT, 2012)
- Confidencialidad [C]: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- Autenticidad [A]: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- Trazabilidad [T]: propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

3.2.1 Tabla Identificación de activos, relación entre activos y valoración de loa activos

IDENTIFICACIÓN DE ACTIVOS							
N°	Actividad	Activos	Relación	Valoración		valoración individual	**D**imensiones: **C**onfidencialidad **I**ntegridad **D**isponibilidad **A**utenticidad **T**razabilidad
				Cuantitativa	Cualitativa		
1	Levantamiento	Usuario (brigada)	Usuarios-Información física-planos físicos	10	Alta	10	C, I, D, A, T
		Formatos físicos (información)				10	
		Planos físicos				10	
2	Traslado de Formatos	Usuario	Usuarios-Información física-planos físicos	10	Alta	10	C, I, A, T
		Formatos físicos				10	
		Planos físicos				10	
3	Revisión de levantamiento	Usuario	Usuarios-Información física-instalaciones	7	Media	7	I, D, A, T
		Formatos físicos				10	
		Instalaciones				7	

IDENTIFICACIÓN DE ACTIVOS							
N°	Actividad	Activos	Relación	Valoración		valoración individual	**D**imensiones: **C**onfidencialidad **I**ntegridad **D**isponibilidad **A**utenticidad **T**razabilidad
				Cuantitativa	Cualitativa		
4	Captura de información	Usuario (brigada)	Usuarios - Información física - Equipo de computo - Formato digital - Instalaciones	7	Media	10	I, D, A, T
		Formatos físicos	**Usuario - Equipo de computo-Instalaciones			10	
		Equipo de cómputo				7	
		Formatos Digitales				10	
		Instalaciones				7	
5	Almacenamiento de Captura	Usuario (brigada)	Usuario – información digital - Equipo de cómputo- Medio de almacenamiento - Instalaciones	7	Media	10	I, D, A, T
		Formatos digital	** Equipo de cómputo- Medio de almacenamiento- Instalaciones			10	
		Equipo de cómputo				7	
		Medio de almacenamiento				10	
		Instalaciones				7	

IDENTIFICACIÓN DE ACTIVOS							
N°	Actividad	Activos	Relación	Valoración		valoración individual	**D**imensiones: **C**onfidencialidad **I**ntegridad **D**isponibilidad **A**utenticidad **T**razabilidad
				Cuantitativa	Cualitativa		
6	Revisión de captura	Usuario	Usuario - Formato digital- Equipo de cómputo-Instalaciones	10	Alta	10	I, D, A, T
		Formatos digital	**Usuario - Equipo de cómputo-Instalaciones			10	
		Equipo de cómputo				7	
		Instalaciones				7	
7	Almacenamiento de captura revisada	Usuario	Usuario -Formato digital-Equipo de cómputo-Medio de almacenamiento-Instalaciones	10	Alta	10	I, D, A, T
		Formatos digital	** Usuario – Equipo de Computo - Medio de Almacenamiento			10	
		Equipo de cómputo				7	
		Medio de almacenamiento				10	
		Instalaciones				7	

IDENTIFICACIÓN DE ACTIVOS							
N°	Actividad	Activos	Relación	Valoración		valoración individual	**D**imensiones: **C**onfidencialidad **I**ntegridad **D**isponibilidad **A**utenticidad **T**razabilidad
				Cuantitativa	Cualitativa		
8	Búsqueda de información (potencias y equipos)	Usuario (brigada)	Usuario- Equipo de cómputo-Archivo Digital- Red inalámbrica o alámbrica - Instalaciones	7	Media	10	I, D, A, T
		Equipo de cómputo	** Usuario- Información Digital - Red inalámbrica o alámbrica			3	
		Archivo digital				10	
		Red inalámbrica o alámbrica				3	
		Instalaciones				3	
9	Completar información	Usuario	Usuario - Equipo de cómputo - Información digital - Instalaciones	3	Baja	10	I, D, A, T
		Equipo de cómputo				3	
		Archivo digital				10	
		Instalaciones				3	

IDENTIFICACIÓN DE ACTIVOS							
N°	Actividad	Activos	Relación	Valoración		valoración individual	**D**imensiones: **C**onfidencialidad **I**ntegridad **D**isponibilidad **A**utenticidad **T**razabilidad
				Cuantitativa	Cualitativa		
10	Generación de archivos (csv)	Usuario	Usuario - Equipo de cómputo - Archivo digital - Instalaciones	3	Baja	7	I, D, A, T
		Equipo de cómputo	Instalaciones			3	
		Archivo digital				7	
		Instalaciones				3	
11	Almacenamiento de información	Usuario	Usuario - Formato digital - Equipo de cómputo - Medio de almacenamiento- Instalaciones	10	Alta	10	I, D, A, T
		Formatos digital	**Usuario-Información digital - Equipo de cómputo - Medio de almacenamiento			10	
		Equipo de cómputo				3	
		Medio de almacenamiento				10	
		Instalaciones				3	

IDENTIFICACIÓN DE ACTIVOS							
N°	Actividad	Activos	Relación	Valoración		valoración individual	**D**imensiones: **C**onfidencialidad **I**ntegridad **D**isponibilidad **A**utenticidad **T**razabilidad
				Cuantitativa	Cualitativa		
12	Dar de alta a la dependencia en el sistema	Usuario	Usuario -Equipo de cómputo-Página web -Red inalámbrica o alámbrica Instalaciones	7	Media	10	C, I, D, A, T
		Equipo de cómputo	**Usuario-Equipo de cómputo-Página web -Red inalámbrica o alámbrica			7	
		Página web				10	
		Red inalámbrica o alámbrica				7	
		Instalaciones				7	
13	Cargar archivos al sistema	Usuario	Usuario -Equipo de cómputo -Red inalámbrica o alámbrica -Información digital -Servidor -Página web -Base de datos- Instalaciones	10	Alta	10	C, I. D, A, T
		Equipo de cómputo	**Equipo de cómputo -Red inalámbrica o alámbrica -Información digital -Base de datos			7	
		Red inalámbrica o alámbrica				7	
		Información digital				10	
		Servidor				10	
		Página web				10	
		Base de datos				10	
		Instalaciones				10	

IDENTIFICACIÓN DE ACTIVOS							
N°	Actividad	Activos	Relación	Valoración		valoración individual	**D**imensiones: **C**onfidencialidad **I**ntegridad **D**isponibilidad **A**utenticidad **T**razabilidad
				Cuantitativa	Cualitativa		
14	Revisar archivos en la DB	Usuario	Usuario -Equipo de cómputo -Red inalámbrica o alámbrica -Servidor -Base de datos -Instalaciones	10	Alta	10	C, I. D, A, T
		Equipo de cómputo				7	
		Red inalámbrica o alámbrica				7	
		Servidor				10	
		Base de datos				10	
		Instalaciones				7	
15	Generar diagnóstico	Usuario	Usuario - Equipo de cómputo - Red inalámbrica o alámbrica - Página web - Servidor - Base de datos – Instalaciones	10	Alta	10	C, I. D, A, T
		Equipo de cómputo	**página web -Servidor - Base de datos			7	
		Red inalámbrica o alámbrica				7	
		Página web				10	
		Servidor				10	
		Base de datos				10	
		Instalaciones				7	

IDENTIFICACIÓN DE ACTIVOS							
N°	Actividad	Activos	Relación	Valoración		valoración individual	**D**imensiones: **C**onfidencialidad **I**ntegridad **D**isponibilidad **A**utenticidad **T**razabilidad
				Cuantitativa	Cualitativa		
16	Revisión del diagnóstico	Usuario	Usuario - Equipo de cómputo - Archivo digital- Red inalámbrica o alámbrica - Página web -Instalaciones	10	Alta	10	C, I. D, A, T
		Equipo de cómputo	** Equipo de cómputo - Red inalámbrica o alámbrica - Página web			7	
		Archivo digital				10	
		Red inalámbrica o alámbrica				3	
		Página web				10	
		Instalaciones				7	

3.3 Identificación de las Amenazas

Objetivo: Determinar las amenazas que pueden afectar a cada activo, las amenazas surgen a partir de la existencia de vulnerabilidades que pueden ser aprovechadas y con estas se puede comprometer o no la seguridad de un sistema de información, lo que interesa es que puede pasarles a los activos de la Organización y causar daño.

3.3.1 Tabla Identificación de amenazas

IDENTIFICACIÓN DE AMENAZAS								
Nº	Actividad	Activos	Tipo de la amenaza: De origen natural Del entorno Defecto de las aplicaciones Personas de forma accidental Personas de forma deliberada	Amenaza	Explicación	Valoración de la amenaza (Degradación en cada dimensión)	Valoración de la amenaza (Probabilidad)	
							Cuantitativa	Cualitativa
1	Levantamiento	Usuario (brigada)	Del entorno	1. Accidente físico	Que alguna de las personas que esta realizando el levantamiento de información sufra algún tipo de accidente.	Muy malo	10	Alta
		Formatos físicos (información)	Del entorno Personas de forma accidental	1. Accidente físico 1. Inventar información 2. Modificar información 3. Falsear en la información	La persona que esta realizando el levantamiento puede falsear información respecto al levantamiento. También se puede dar el caso que al momento de entrevistar al usuario que tiene el equipo, pueda mentir en la información al sentir que esto tendrá consecuencias	Muy malo	10	Alta
		Planos físicos	Del entorno Personas de forma deliberada	1. Modificación de los planos 2. Robo de planos 3. Extravío de planos 4. Pérdida de planos	Los formatos pueden sufrir diferentes accidentes como son: pérdida, modificación, daño durante el levantamiento	Muy malo	10	Alta
2	Traslado de Formatos	Usuario	Del entorno	1. Accidente físico	El responsable de la brigada se encarga de trasladar los formatos y planos desde la dependencia hasta las oficinas del PUES durante este trayecto puede sufrir algún tipo de accidente.	Muy malo	10	Alta
		Formatos físicos	Del entorno Personas de forma accidental	1. Modificación de los formatos 2. Robo de formatos 3. Extravío de formatos 4. Pérdida de formatos	Durante el traslado los formatos pueden sufrir distintos tipos de accidentes, como pueden ser la pérdida de formatos, daño, robo o extravío.	Muy malo	10	Alta
		Planos físicos	Del entorno	1. Robo de planos 2. Extravío de planos 3. Pérdida de planos	Durante el traslado de los planos estos pueden sufrir distintos percances tales como, robo, extravío o pérdida.	Muy malo	10	Alta
3	Revisión de levantamiento	Usuario	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta
		Formatos físicos	Del entorno Persona de forma accidental Persona de forma deliberada	1. Modificación de los formatos 2. Robo de formatos 3. Extravío de formatos 4. Pérdida de formatos	Durante la revisión los formatos pueden sufrir accidentes, como pueden ser la pérdida de formatos, daño, robo o extravío.	Muy malo	10	Alta
		Instalaciones	Del entorno	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante la revisión en las instalaciones se puede sufrir algún tipo de accidente como una inundaciones, incendio o corto circuito lo que propiciaría la pérdida total o parcial de la información	Regular	3	Baja

IDENTIFICACIÓN DE AMENAZAS									
N°	Actividad	Activos	Tipo de la amenaza: De origen natural Del entorno Defecto de las aplicaciones Personas de forma accidental Personas de forma deliberada	Amenaza	Explicación	Valoración de la amenaza (Degradación en cada dimensión)	Valoración de la amenaza (Probabilidad)		
							Cuantitativa	Cualitativa	
4	Captura de información	Usuario (brigada)	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta	
		Formatos físicos	Personas de forma accidental y deliberada	1. Modificación de los formatos 2. Robo de formatos 3. Extravío de formatos 4. Pérdida de formatos 5. Daño físico y lógico	Al momento de la captura de la información el usuario puede cometer errores al momento de vaciar la información, una mala captura, omisión de registros o sólo capturar información parcial. También se puede perder, extraviar o dañar los formatos	Malo	7	Media	
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada.	Regular	3	Baja	
		Formatos Digitales	Defecto de aplicaciones Personas de forma accidental o deliberada	1. Daño de software 2. Modificación de información	"El archivo puede sufrir algún tipo de daño a consecuencia de tener aplicaciones mal configuradas o sin la seguridad necesaria. Los archivos pueden ser modificados de manera intencionada por el usuario de estar manera se pierde la integridad de los datos.	Muy malo	10	Alta	
		Instalaciones	Del entorno	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante la captura en las instalaciones se puede sufrir algún tipo de accidente como una inundaciones, incendio o corto circuito lo que propiciaría la pérdida total o parcial de la información	Regular	3	Baja	

IDENTIFICACIÓN DE AMENAZAS								
N°	Actividad	Activos	Tipo de la amenaza: De origen natural Del entorno Defecto de las aplicaciones Personas de forma accidental Personas de forma deliberada	Amenaza	Explicación	Valoración de la amenaza (Degradación en cada dimensión)	Valoración de la amenaza (Probabilidad)	
							Cuantitativa	Cualitativa
5	Almacenamiento de Captura	Usuario (brigada)	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta
		Formatos digital	Personas de forma accidental y deliberada Defecto de aplicaciones	1. Modificación de los archivos digitales 2. Robo de información 3. Pérdida de formatos 4. Daño lógico	Cambios de diseño del formato físico o digital, cambios de ubicación física o lógica de los formatos. Escribir, eliminar o modificar las ubicaciones de los archivos ya existentes o duplicar información	Malo	7	Media
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada.	Regular	3	Baja
		Medio de almacena-miento	Personas de forma accidental y deliberada	1. Daño de software o hardware	Daño lógico o físico a los medios (USB, DD, entre otros)	Muy malo	10	Alta
		Instalaciones	Del entorno De origen natural	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Daño a los archivos sufriendo modificación o borrar la información	Regular	3	Baja
6	Revisión de captura	Usuario	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta
		Formatos digital	Personas de forma accidental y deliberada Defecto de aplicaciones	1. Modificación de la información 2. Robo de archivos digitales 3. Borrado de información 4. Pérdida de formatos 5. Daño lógico	Sobrescribir, eliminar o modificar los archivos, la ubicación de los archivos ya existentes, duplicar información	Malo	7	Media
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada.	Regular	3	Baja
		Instalaciones	Del entorno De origen natural	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante la revisión de la información, las instalaciones pueden sufrir algún tipo de accidente como una inundación o incendio lo que propiciaría la pérdida total o parcial de la información	Regular	3	Baja

IDENTIFICACIÓN DE AMENAZAS								
N°	Actividad	Activos	Tipo de la amenaza: De origen natural Del entorno Defecto de las aplicaciones Personas de forma accidental Personas de forma deliberada	Amenaza	Explicación	Valoración de la amenaza (Degradación en cada dimensión)	Valoración de la amenaza (Probabilidad)	
							Cuantitativa	Cualitativa
7	Almacenamiento de captura revisada	Usuario	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta
		Formatos digital	Personas de forma accidental y deliberada Defecto de aplicaciones	1. Modificación de los archivos digitales 2. Robo de información 3. Pérdida de formatos 4. Daño lógico	Cambios de diseño del formato físico o digital, cambios de ubicación física o lógica de los formatos. Escribir, eliminar o modificar las ubicaciones de los archivos ya existentes o duplicar información	Muy malo	10	Alta
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada.	Regular	3	Baja
		Medio de almacenamiento	Personas de forma accidental y deliberada	1. Daño de software o hardware	Daño lógico o físico a los medios (USB, DD, entre otros)Daño a los archivos sufriendo modificación o borrar la información	Muy malo	10	Alta
		Instalaciones	"Del entorno De origen natural"	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante el almacenamiento de la información, las instalaciones pueden sufrir algún tipo de accidente como una inundación o incendio, lo que propiciaría la pérdida total o parcial de la información	Regular	3	Baja
8	Revisión de captura	Usuario (brigada)	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Malo	7	Media
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada. Al utilizar un navegador para realizar la búsqueda se puede dañar el equipo o archivos por los sitios visitados	Regular	3	Media
		Archivo digital	Personas de forma accidental y deliberada Defecto de aplicaciones	1. Modificación de los archivos digitales 2. Robo de información 3. pérdida de información 4. Daño lógico	Se puede modificar la información alterando la integridad de la información	Malo	7	Media
		Red inalámbrica o alámbrica	Del entorno De origen natural	1. Robo de información 2. Pérdida de información	Puede existir una intrusión a la red por parte de un tercero	Regular	3	Baja
		Instalaciones	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio.	Regular	3	Baja

IDENTIFICACIÓN DE AMENAZAS								
N°	Actividad	Activos	Tipo de la amenaza: De origen natural Del entorno Defecto de las aplicaciones Personas de forma accidental Personas de forma deliberada	Amenaza	Explicación	Valoración de la amenaza (Degradación en cada dimensión)	Valoración de la amenaza (Probabilidad)	
							Cuantitativa	Cualitativa
9	Completar información	Usuario	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada. Al utilizar un navegador para realizar la búsqueda se puede dañar el equipo o archivos por los sitios visitados	Malo	7	Media
		Archivo digital	Personas de forma accidental y deliberada Defecto de aplicaciones	1. Modificación de los archivos digitales 2. Robo de información 3. Pérdida de formatos 4. Daño lógico	"Cambios de diseño del formato físico o digital, cambios de ubicación física o lógica de los formatos. Escribir, eliminar o modificar las ubicaciones de los archivos ya existentes o duplicar información"	Malo	7	Media
		Instalaciones	Del entorno De origen natural	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante eesta tarea las instalaciones pueden sufrir algún tipo de accidente como una inundación o incendio, lo que propiciaría la pérdida total o parcial de la información	Regular	3	Baja
10	Generación de archivos (csv)	Usuario	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Regular	3	Baja
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada.	Regular	3	Baja
		Archivo digital	Personas de forma accidental y deliberada Defecto de aplicaciones	1. Modificación de los archivos digitales 2. Robo de información 3. pérdida de información 4. Daño lógico	Cambios de diseño del formato físico o digital, cambios de ubicación física o lógica de los formatos. Escribir, eliminar o modificar las ubicaciones de los archivos ya existentes o duplicar información	Malo	7	Media
		Instalaciones	Del entorno De origen natural	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante la generación de los archivos csv, las instalaciones pueden sufrir algún tipo de accidente como una inundación o incendio, lo que propiciaría la pérdida total o parcial de la información	Regular	3	Baja

IDENTIFICACIÓN DE AMENAZAS								
N°	Actividad	Activos	Tipo de la amenaza: De origen natural Del entorno Defecto de las aplicaciones Personas de forma accidental Personas de forma deliberada	Amenaza	Explicación	Valoración de la amenaza (Degradación en cada dimensión)	Valoración de la amenaza (Probabilidad)	
							Cuantitativa	Cualitativa
11	Almacenamiento de información	Usuario	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta
		Formatos digital	Personas de forma accidental y deliberada Defecto de aplicaciones	1. Modificación de los archivos digitales 2. Robo de información 3. pérdida de formatos 4. Daño lógico	Cambios de diseño del formato físico o digital, cambios de ubicación física o lógica de los formatos. Escribir, eliminar o modificar las ubicaciones de los archivos ya existentes o duplicar información	Muy malo	3	Baja
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada.	Regular	3	Baja
		Medio de almacenamiento	Del entorno Defecto de aplicaciones Personas de forma accidental y deliberada	1. Daño de software o hardware	Al utilizar un navegador para realizar la búsqueda se puede dañar el equipo o archivos por los sitios visitados	Muy malo	10	Alta
		Instalaciones	Del entorno De origen natural	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante el almacenamiento de información las instalaciones pueden sufrir algún tipo de accidente como una inundación o incendio, lo que propiciaría la pérdida total o parcial de la información	Regular	3	Baja
12	Dar de alta a la dependencia en el sistema	Usuario	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada. Al utilizar un navegador para realizar la búsqueda se puede dañar el equipo o archivos por los sitios visitados	Malo	7	Media
		Página web	Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Daño físico del equipo de manera accidental o deliberadamente que alberga la página 2.Disponibilidad del servicio	Puede que la página web no este disponible por un tiempo indeterminado, causando daño	Regular	3	Baja
		Red inalámbrica o alámbrica	Personas de forma accidental y deliberada Defecto de aplicaciones	1. Robo de información 2. Pérdida de información	Puede existir una intrusión a la red por parte de un tercero	Malo	7	Media
		Instalaciones	Del entorno De origen natural	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante esta tarea las instalaciones sufrir algún tipo de accidente como una inundación o incendio, lo que propiciaría la pérdida total o parcial de la información	Malo	7	Media

IDENTIFICACIÓN DE AMENAZAS									
N°	Actividad	Activos	Tipo de la amenaza: De origen natural Del entorno Defecto de las aplicaciones Personas de forma accidental Personas de forma deliberada	Amenaza	Explicación	Valoración de la amenaza (Degradación en cada dimensión)	Valoración de la amenaza (Probabilidad)		
							Cuantitativa	Cualitativa	
13	Cargar archivos al sistema	Usuario	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta	
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada. Al utilizar un navegador para realizar la búsqueda se puede dañar el equipo o archivos por los sitios visitados	Malo	7	Media	
		Red inalámbrica o alámbrica	Personas de forma accidental y deliberada Defecto de aplicaciones	1. Robo de información 2. Pérdida de información	Puede existir una intrusión a la red por parte de un tercero	Malo	7	Media	
		Información digital	Personas de forma accidental y deliberada Defecto de aplicaciones	1. Modificación de los archivos digitales 2. Robo de información 3. pérdida de formatos 4. Daño lógico	Cambios de diseño del formato físico o digital, cambios de ubicación física o lógica de los formatos. Escribir, eliminar o modificar las ubicaciones de los archivos ya existentes o duplicar información	Muy malo	10	Alta	
		Servidor	Del entorno De origen natural Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Modificación de los archivos digitales 2. Robo de información 3. Pérdida de formatos 4. Daño lógico 5. Negación de servicios	Puede existir modificación en los archivos de configuración del servidor, robo o pérdidas de información Puede haber negación de servicios afectando a los servicios que estén relacionados con el servidor	Muy malo	10	Alta	
		Página web	Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Daño físico del equipo de manera accidental o deliberadamente que alberga la página 2.Disponibilidad del servicio	Puede que la página web no este disponible por un tiempo indeterminado, causando daño	Muy malo	10	Alta	
		Base de datos	Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Modificación de los archivos digitales 2. Robo de información 3. Pérdida de información 4. Modificación de infamación 4. Daño lógico	Puede existir modificación, robo o pérdida de información de manera accidental o intencionada	Muy malo	10	Alta	
		Instalaciones	Del entorno De origen natural	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante la tarea de cargar los archivos al sistema, las instalaciones pueden sufrir algún tipo de accidente como una inundación o incendio, lo que propiciaria la pérdida total o parcial de la información	Muy malo	10	Alta	

IDENTIFICACIÓN DE AMENAZAS								
N°	Actividad	Activos	Tipo de la amenaza: De origen natural Del entorno Defecto de las aplicaciones Personas de forma accidental Personas de forma deliberada	Amenaza	Explicación	Valoración de la amenaza (Degradación en cada dimensión)	Valoración de la amenaza (Probabilidad)	
							Cuantitativa	Cualitativa
14	Revisar archivos en la DB	Usuario	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada. Al utilizar un navegador para realizar la búsqueda se puede dañar el equipo o archivos por los sitios visitados	Malo	7	Media
		Red inalámbrica o alámbrica	Personas de forma accidental y deliberada Defecto de aplicaciones	1. Robo de información 2. Pérdida de información	Puede existir una intrusión a la red por parte de un tercero	Malo	7	Media
		Servidor	Del entorno De origen natural Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Modificación de los archivos digitales 2. Robo de información 3. Pérdida de formatos 4. Daño lógico 5. Negación de servicios	Puede existir modificación en los archivos de configuración del servidor, robo o pérdidas de información. Puede haber negación de servicios afectando a los servicios que estén relacionados con el servidor	Muy malo	10	Alta
		Base de datos	Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Modificación de los archivos digitales 2. Robo de información 3. Pérdida de información 4. Modificación de infamación 4. Daño lógico	Puede existir modificación, robo o pérdida de información de manera accidental o intencionada	Muy malo	10	Alta
		Instalaciones	Del entorno De origen natural	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante la revisión de la información en la base de datos, las instalaciones pueden sufrir algún tipo de accidente como una inundación o incendio, lo que propiciaría la pérdida total o parcial de la información	Malo	7	Media

IDENTIFICACIÓN DE AMENAZAS									
N°	Actividad	Activos	Tipo de la amenaza: De origen natural Del entorno Defecto de las aplicaciones Personas de forma accidental Personas de forma deliberada	Amenaza	Explicación	Valoración de la amenaza (Degradación en cada dimensión)	Valoración de la amenaza (Probabilidad)		
							Cuantitativa	Cualitativa	
15	Cargar archivos al sistema	Usuario	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta	
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada. Al utilizar un navegador para realizar la búsqueda se puede dañar el equipo o archivos por los sitios visitados	Malo	7	Media	
		Red inalámbrica o alámbrica	Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Robo de información 2. Pérdida de información	Puede existir una intrusión a la red por parte de un tercero	Malo	7	Media	
		Página web	Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Daño físico del equipo de manera accidental o deliberadamente que alberga la página 2.Disponibilidad del servicio	Puede que la página web no este disponible por un tiempo indeterminado, causando daño	Muy malo	10	Alta	
		Servidor	Del entorno De origen natural Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Modificación de los archivos digitales 2. Robo de información 3. Pérdida de formatos 4. Daño lógico 5. Negación de servicios	Puede existir modificación en los archivos de configuración del servidor, robo o pérdidas de información Puede haber negación de servicios afectando a los servicios que estén relacionados con el servidor	Muy malo	10	Alta	
		Base de datos	Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Modificación de los archivos digitales 2. Robo de información 3. Pérdida de información 4. Modificación de infomación 4. Daño lógico	Puede existir modificación, robo o pérdida de información de manera accidental o intencionada	Muy malo	10	Alta	
		Instalaciones	Del entorno De origen natural	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante el almacenamiento de la información si las instalaciones sufrir algún tipo de accidente como una inundación o incendio propiciaría la pérdida total o parcial de la información	Malo	7	Media	

IDENTIFICACIÓN DE AMENAZAS								
N°	Actividad	Activos	Tipo de la amenaza: De origen natural Del entorno Defecto de las aplicaciones Personas de forma accidental Personas de forma deliberada	Amenaza	Explicación	Valoración de la amenaza (Degradación en cada dimensión)	Valoración de la amenaza (Probabilidad)	
							Cuantitativa	Cualitativa
16	Revisión del diagnóstico	Usuario	Del entorno	1. Accidente físico	Se puede sufrir de un percance por un fenómeno natural, o por un problema que se presente en las instalaciones del edificio de Programas Universitarios	Muy malo	10	Alta
		Equipo de cómputo	De origen natural Del entorno Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Fenómeno natural 2. Daño de software o hardware 3. Daño físico del equipo de manera accidental o deliberadamente	El equipo puede sufrir diferentes tipos de daños como pueden ser: algún problema con el software que se esta utilizando, daño físico al equipo como consecuencia de un accidente o que alguien lo realice de una forma deliberada. Al utilizar un navegador para realizar la búsqueda se puede dañar el equipo o archivos por los sitios visitados	Malo	7	Media
		Archivo digital	Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Modificación de los archivos digitales 2. Robo de información 3. pérdida de formatos 4. Daño lógico	Cambios de diseño del formato físico o digital, cambios de ubicación física o lógica de los formatos. Escribir, eliminar o modificar las ubicaciones de los archivos ya existentes o duplicar información	Muy malo	10	Alta
		Red inalámbrica o alámbrica	Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Robo de información 2. Pérdida de información	Puede existir una intrusión a la red por parte de un tercero	Regular	3	Baja
		Página web	Defecto de aplicaciones Personas de forma accidental Personas de forma deliberada	1. Daño físico del equipo de manera accidental o deliberadamente que alberga la página 2.Disponibilidad del servicio	Puede que la página web no este disponible por un tiempo indeterminado, causando daño	Muy malo	10	Alta
		Instalaciones	Del entorno De origen natural	1. Fenómeno natural (sismo, inundación) 2. Corto circuito, incendio	Durante la revisiión del diagnóstico las instalaciones sufrir algún tipo de accidente como una inundación o incendio, lo que propiciaría la pérdida total o parcial de la información	Malo	7	Media

3.4 Identificación de las medidas de protección

Objetivo: Definir las medidas de protección o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen un riesgo. Hay amenazas que se evitan simplemente organizándose adecuadamente, otras requieren elementos técnicos, otras de seguridad física y, por último, está la política del personal.

Al utilizar la herramienta PILAR para realizar el análisis de riesgos, se tiene como resultado una serie de medidas de protección con diferentes pesos de seguridad como se muestra en la siguiente tabla 3.1.4.

Tabla 3.4.1 Peso Relativo

Peso relativo	
Rojo	Máximo
Amarillo	Alto
Verde	Normal
Gris	Bajo

Cabe mencionar que también se tienen diferentes tipos de protecciones dependiendo del activo al que se haga referencia, las cuales pueden ser de tipo:

Tabla 3.4.2 Tipos de protecciones

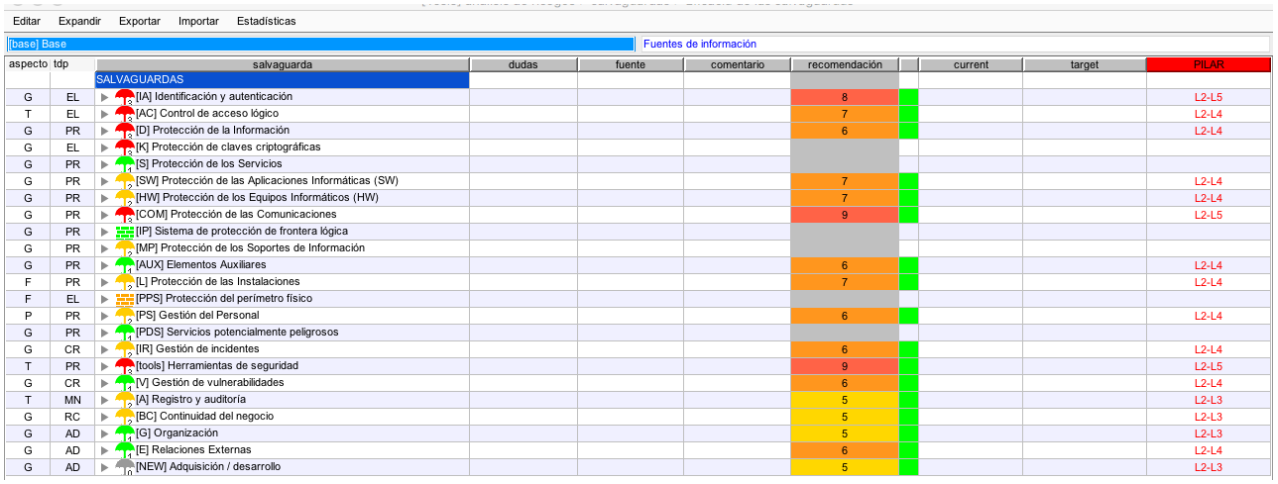
Tipo de protección	
PR	Prevención
DR	Disuasión
EL	Eliminación
IM	Minimización del impacto
CR	Corrección
RC	Recuperación
AD	Administrativa
AW	Concienciación
DC	Detección
MN	Monitorización

Para este caso en particular, las medidas de protección que se obtuvieron son las siguientes:

Tabla 3.4.3 Salvaguardas

Aspecto	Tipo de protección	Salvaguarda	Peso relativo
G	Eliminación	Identificación y autenticación	Máximo
T	Eliminación	Control de acceso lógico	Máximo
G	Protección	Protección de la información	Máximo
G	Eliminación	Protección de claves criptográficas	Máximo
G	Protección	Protección de los servicios	Normal
G	Protección	Protección de las aplicaciones informáticas(SW)	Alto
G	Protección	Protección de los equipos informáticos (HW)	Alto
G	Protección	Protección de las comunicaciones	Máximo
G	Protección	*Sistema de protección de frontera lógica	Normal
G	Protección	Protección de los soportes de la información	Alto
G	Protección	Elementos auxiliares	Normal
F	Protección	Protección de las instalaciones	Alto
F	Eliminación	*Protección del perímetro físico	Alto
P	Protección	Gestión del personal	Alto
G	Protección	Servicios potencialmente peligrosos	Normal
G	Corrección	Gestión de incidentes	Alto
T	Protección	Herramientas de seguridad	Máximo
G	Corrección	Gestión de vulnerabilidades	Normal
T	Monitorización	Registro y auditoría	Alto
G	Recuperación	Continuidad del negocio	Alto
G	Administrativa	Organización	Normal
G	Administrativa	Relaciones externas	Normal
G	Administrativa	Adquisición/desarrollo	Bajo

Cada una de estas medidas de seguridad, tiene a su vez una serie de salvaguardas a modo de árbol como se muestra en las figuras 3.4.1 y 3.4.2:



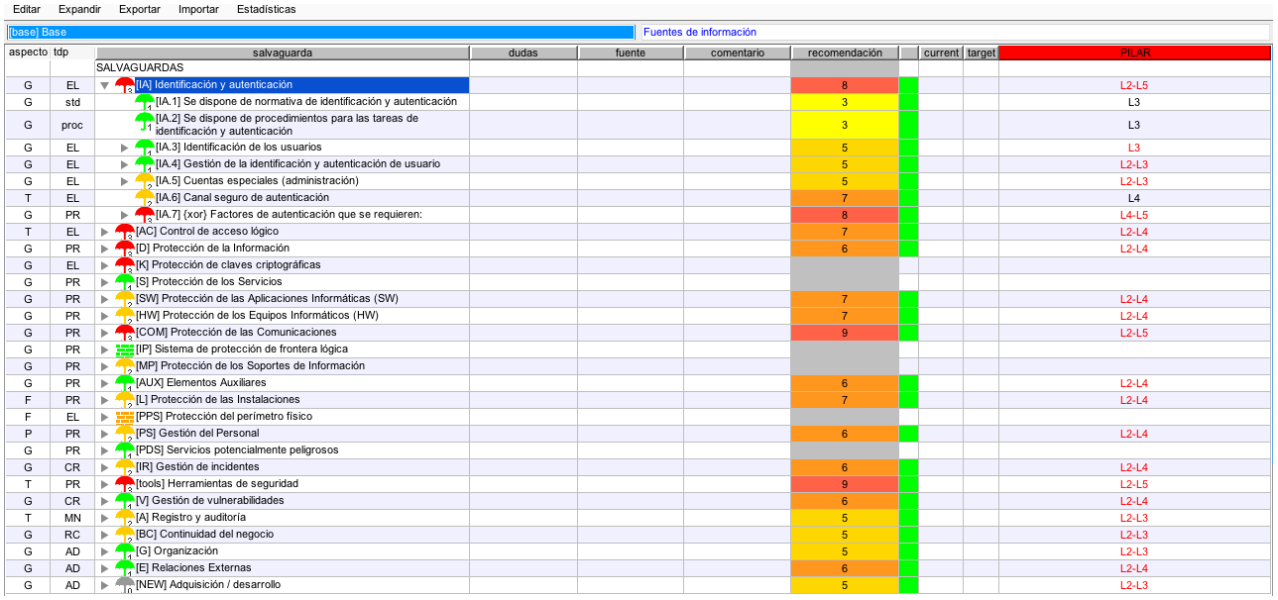
Editar Expandir Exportar Importar Estadísticas

[base] Base — Fuentes de información

aspecto	tdp	salvaguarda	dudas	fuente	comentario	recomendación		current	target	PILAR
		SALVAGUARDAS								
G	EL	[IA] Identificación y autenticación				8				L2-L5
T	EL	[AC] Control de acceso lógico				7				L2-L4
G	PR	[D] Protección de la Información				6				L2-L4
G	EL	[K] Protección de claves criptográficas								
G	PR	[S] Protección de los Servicios								
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7				L2-L4
G	PR	[HW] Protección de los Equipos Informáticos (HW)				7				L2-L4
G	PR	[COM] Protección de las Comunicaciones				9				L2-L5
G	PR	[IP] Sistema de protección de frontera lógica								
G	PR	[MP] Protección de los Soportes de Información								
G	PR	[AUX] Elementos Auxiliares				6				L2-L4
F	PR	[L] Protección de las Instalaciones				7				L2-L4
F	EL	[PPS] Protección del perímetro físico								
P	PR	[PS] Gestión del Personal				6				L2-L4
G	PR	[PDS] Servicios potencialmente peligrosos								
G	CR	[IR] Gestión de incidentes				6				L2-L4
T	PR	[tools] Herramientas de seguridad				9				L2-L5
G	CR	[V] Gestión de vulnerabilidades				6				L2-L4
T	MN	[A] Registro y auditoría				5				L2-L3
G	RC	[BC] Continuidad del negocio				5				L2-L3
G	AD	[G] Organización				5				L2-L3
G	AD	[E] Relaciones Externas				6				L2-L4
G	AD	[NEW] Adquisición / desarrollo				5				L2-L3

Figura 3.4.1 Muestra de resultados de salvaguardas PILAR

En esta imagen se muestra el resumen de todas las salvaguardas a implementar, cada una con el nombre y peso relativo a la que se encuentra asociada, la valoración de la recomendación de cada una de las salvaguardas según PILAR.

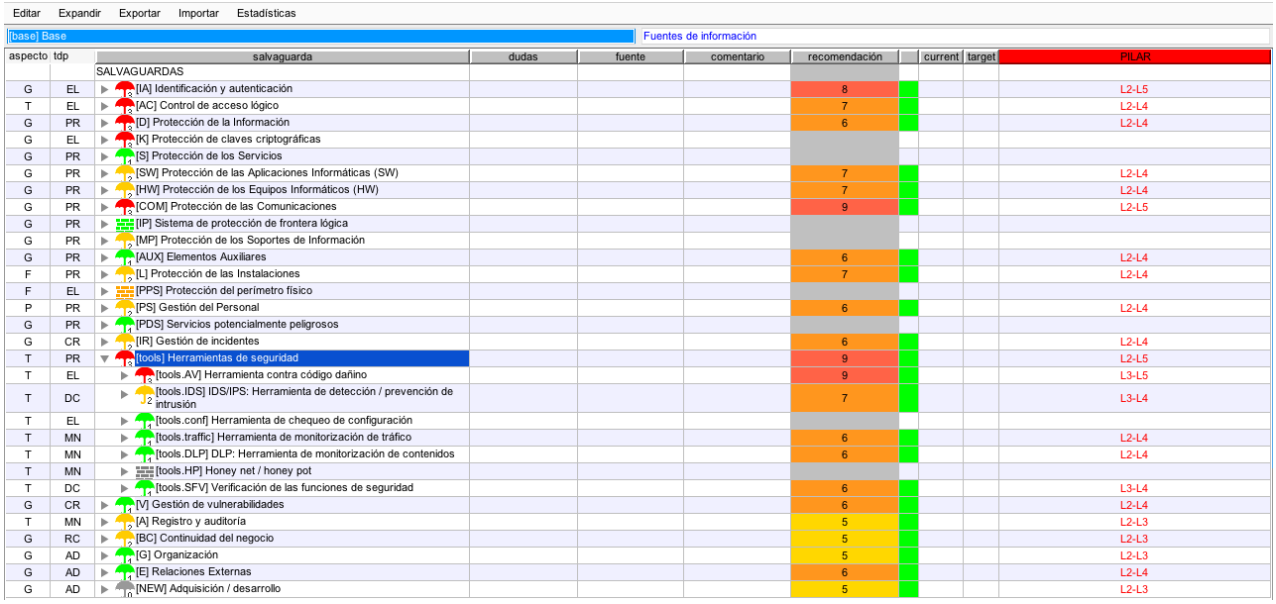


Editar Expandir Exportar Importar Estadísticas

[base] Base — Fuentes de información

aspecto	tdp	salvaguarda	dudas	fuente	comentario	recomendación		current	target	PILAR
		SALVAGUARDAS								
G	EL	[IA] Identificación y autenticación				8				L2-L5
G	std	[IA.1] Se dispone de normativa de identificación y autenticación				3				L3
G	proc	[IA.2] Se dispone de procedimientos para las tareas de identificación y autenticación				3				L3
G	EL	[IA.3] Identificación de los usuarios				5				L3
G	EL	[IA.4] Gestión de la identificación y autenticación de usuario				5				L2-L3
G	EL	[IA.5] Cuentas especiales (administración)				5				L2-L3
T	EL	[IA.6] Canal seguro de autenticación				7				L4
G	PR	[IA.7] {xor} Factores de autenticación que se requieren:				8				L4-L5
T	EL	[AC] Control de acceso lógico				7				L2-L4
G	PR	[D] Protección de la Información				6				L2-L4
G	EL	[K] Protección de claves criptográficas								
G	PR	[S] Protección de los Servicios								
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7				L2-L4
G	PR	[HW] Protección de los Equipos Informáticos (HW)				7				L2-L4
G	PR	[COM] Protección de las Comunicaciones				9				L2-L5
G	PR	[IP] Sistema de protección de frontera lógica								
G	PR	[MP] Protección de los Soportes de Información								
G	PR	[AUX] Elementos Auxiliares				6				L2-L4
F	PR	[L] Protección de las Instalaciones				7				L2-L4
F	EL	[PPS] Protección del perímetro físico								
P	PR	[PS] Gestión del Personal				6				L2-L4
G	PR	[PDS] Servicios potencialmente peligrosos								
G	CR	[IR] Gestión de incidentes				6				L2-L4
T	PR	[tools] Herramientas de seguridad				9				L2-L5
G	CR	[V] Gestión de vulnerabilidades				6				L2-L4
T	MN	[A] Registro y auditoría				5				L2-L3
G	RC	[BC] Continuidad del negocio				5				L2-L3
G	AD	[G] Organización				5				L2-L3
G	AD	[E] Relaciones Externas				6				L2-L4
G	AD	[NEW] Adquisición / desarrollo				5				L2-L3

Figura 3.4.2 Muestra de resultados de salvaguardas PILAR



aspecto	tdp	salvaguarda	dudas	fuente	comentario	recomendación		current	target	PILAR
		SALVAGUARDAS								
G	EL	[IA] Identificación y autenticación				8				L2-L5
T	EL	[AC] Control de acceso lógico				7				L2-L4
G	PR	[D] Protección de la Información				6				L2-L4
G	EL	[K] Protección de claves criptográficas								
G	PR	[S] Protección de los Servicios								
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7				L2-L4
G	PR	[HW] Protección de los Equipos Informáticos (HW)				7				L2-L4
G	PR	[COM] Protección de las Comunicaciones				9				L2-L5
G	PR	[IP] Sistema de protección de frontera lógica								
G	PR	[MP] Protección de los Soportes de Información								
G	PR	[AUX] Elementos Auxiliares				6				L2-L4
F	PR	[L] Protección de las Instalaciones				7				L2-L4
F	EL	[PPS] Protección del perímetro físico								
P	PR	[PS] Gestión del Personal				6				L2-L4
G	PR	[PDS] Servicios potencialmente peligrosos								
G	CR	[IR] Gestión de incidentes				6				L2-L4
T	PR	[tools] Herramientas de seguridad				9				L2-L5
T	EL	[tools.AV] Herramienta contra código dañino				9				L3-L5
T	DC	[tools.IDS] IDS/IPS: Herramienta de detección / prevención de intrusión				7				L3-L4
T	EL	[tools.conf] Herramienta de chequeo de configuración								
T	MN	[tools.traffic] Herramienta de monitorización de tráfico				6				L2-L4
T	MN	[tools.DLP] DLP: Herramienta de monitorización de contenidos				6				L2-L4
T	MN	[tools.HP] Honey net / honey pot								
T	DC	[tools.SFV] Verificación de las funciones de seguridad				6				L3-L4
G	CR	[V] Gestión de vulnerabilidades				6				L2-L4
T	MN	[A] Registro y auditoría				5				L2-L3
G	RC	[BC] Continuidad del negocio				5				L2-L3
G	AD	[G] Organización				5				L2-L3
G	AD	[E] Relaciones Externas				6				L2-L4
G	AD	[NEW] Adquisición / desarrollo				5				L2-L3

Figura 3.4.3 Muestra de salvaguardas PILAR

Por medidas de seguridad, las imágenes mostradas previamente sirven para ilustrar la manera en que PILAR muestra los resultados y no se muestran todas las medidas de protección, pero son consideradas en el plan de seguridad para poder mitigar los impactos negativos que pueden suceder si la amenaza llega a ocurrir.

3.5 Proceso de Gestión de Riesgos

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.

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 el riesgo ha sido modificado, desde un valor potencial a un valor residual.

Tratamiento del riesgo

El Proceso de Evaluación

Impacto y riesgo residual son una medida del estado presente, desde la inseguridad potencial (sin medida de protección alguna) y las medidas adecuadas que reducen impacto y riesgo a valores aceptables.

Si el valor residual es igual al valor potencial, el funcionamiento de las salvaguardas existentes es nulo, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin la debida atención.

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.

Aceptación de los Riesgos

El área de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable, en otras palabras, 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.

Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Dirección, para tomar una u otra decisión hay que enmarcar los riesgos soportados por el sistema de información dentro de un contexto más amplio que evalué los aspectos intangibles del negocio.

Tratamiento de los riesgos

La Dirección puede decidir aplicar algún tratamiento al sistema de seguridad desplegado para proteger el sistema de información, existen dos opciones conocidas para el tratamiento:

• reducir el riesgo residual (aceptar un menor riesgo)

• ampliar el riesgo residual (aceptar un mayor riesgo)

En condiciones de riesgo residual extremo, casi la única opción es reducir el riesgo, en condiciones de riesgo residual aceptable, se puede optar entre aceptar el nivel actual o ampliar el riesgo asumido. En cualquier caso, hay que mantener un monitoreo continuo de las circunstancias para que el riesgo formal concuerde con la experiencia real y reaccionemos ante cualquier desviación significativa.

Eliminación del Riesgo

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 poder prescindir de la información o los servicios esenciales por cuanto constituyen la misión de la Organización. Esta opción puede tomar diferentes formas:

- Eliminar cierto tipo de activos, emplear otros en su lugar. Por ejemplo: cambiar de sistema operativo, de fabricante de equipos, entre otros.
- Reordenar la arquitectura del sistema 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.

Las decisiones de eliminación de las fuentes de riesgo suponen realizar un nuevo análisis de riesgos sobre el sistema modificado.

Mitigación del Riesgo

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

- reducir la degradación causada por una amenaza (“acotar el impacto”)
- reducir la probabilidad de que una amenaza se materialice

En ambos casos lo que hay que hacer es ampliar o mejorar el conjunto de salvaguardas (subir de nivel). Algunas salvaguardas se traducen en el despliegue de más equipamiento. Estos nuevos activos estarán a su vez sujetos a amenazas que pueden perjudicar a los activos esenciales. Hay 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.

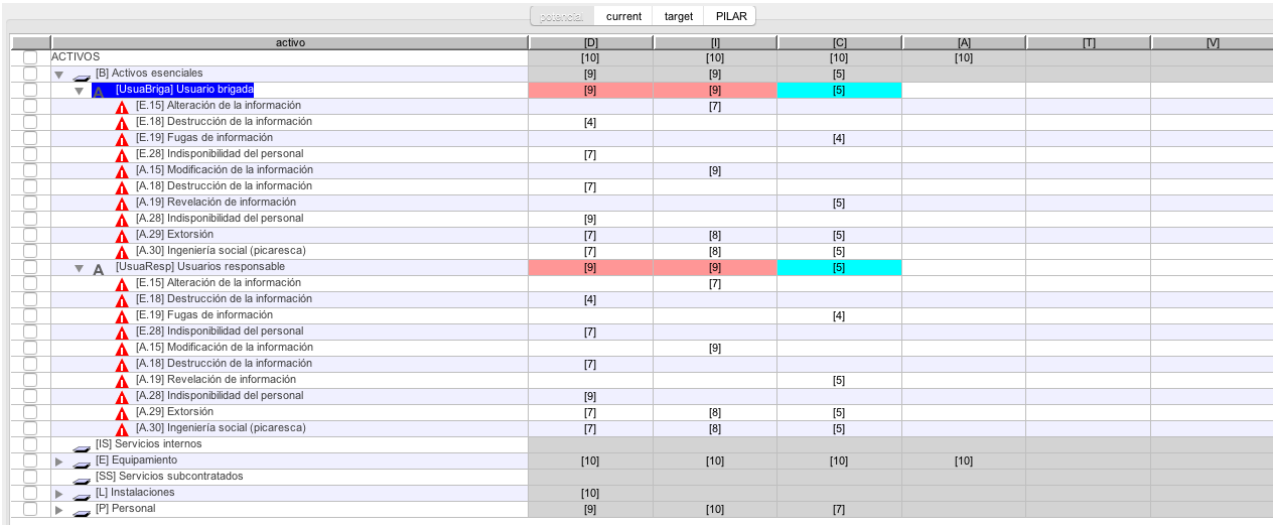
Compartición del Riesgo

Hay dos formas básicas de compartir riesgo:

a) Riesgo cualitativo: se comparte por medio de la tercerización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el componente técnico; y otras legales según el acuerdo que se establezca en la prestación del servicio.
b) Riesgo cuantitativo: se comparte por medio de la contratación de seguros, de forma
   que, a cambio de una prima, quien contrata el servicio reduce el impacto de las posibles amenazas y el asegurador corre con las consecuencias.

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

La figura 3.5.1 sirve como ilustración para ver la manera en que PILAR muestra el impacto acumulado del análisis de riesgos, en cada una de las dimensiones de seguridad evaluadas se muestra el nivel de impacto que va desde diez el cual tienen un impacto mayor, uno que muestra un nivel de impacto bajo y cero que corresponde un nivel de impacto despreciable.

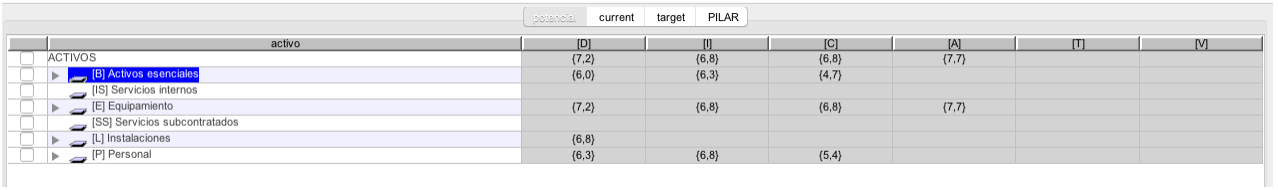


potencial current target PILAR

activo	[D]	[I]	[C]	[A]	[T]	[V]
ACTIVOS	[10]	[10]	[10]	[10]		
[B] Activos esenciales	[9]	[9]	[5]			
[UsuaBriga] Usuario brigada	[9]	[9]	[5]			
[E.15] Alteración de la información		[7]				
[E.18] Destrucción de la información	[4]					
[E.19] Fugas de información			[4]			
[E.28] Indisponibilidad del personal	[7]					
[A.15] Modificación de la información		[9]				
[A.18] Destrucción de la información	[7]					
[A.19] Revelación de información			[5]			
[A.28] Indisponibilidad del personal	[9]					
[A.29] Extorsión	[7]	[8]	[5]			
[A.30] Ingeniería social (picaresca)	[7]	[8]	[5]			
[UsuaResp] Usuarios responsable	[9]	[9]	[5]			
[E.15] Alteración de la información		[7]				
[E.18] Destrucción de la información	[4]					
[E.19] Fugas de información			[4]			
[E.28] Indisponibilidad del personal	[7]					
[A.15] Modificación de la información		[9]				
[A.18] Destrucción de la información	[7]					
[A.19] Revelación de información			[5]			
[A.28] Indisponibilidad del personal	[9]					
[A.29] Extorsión	[7]	[8]	[5]			
[A.30] Ingeniería social (picaresca)	[7]	[8]	[5]			
[IS] Servicios internos						
[E] Equipamiento	[10]	[10]	[10]	[10]		
[SS] Servicios subcontratados						
[L] Instalaciones	[10]					
[P] Personal	[9]	[10]	[7]			

Figura 3.5.1Impacto acumulado

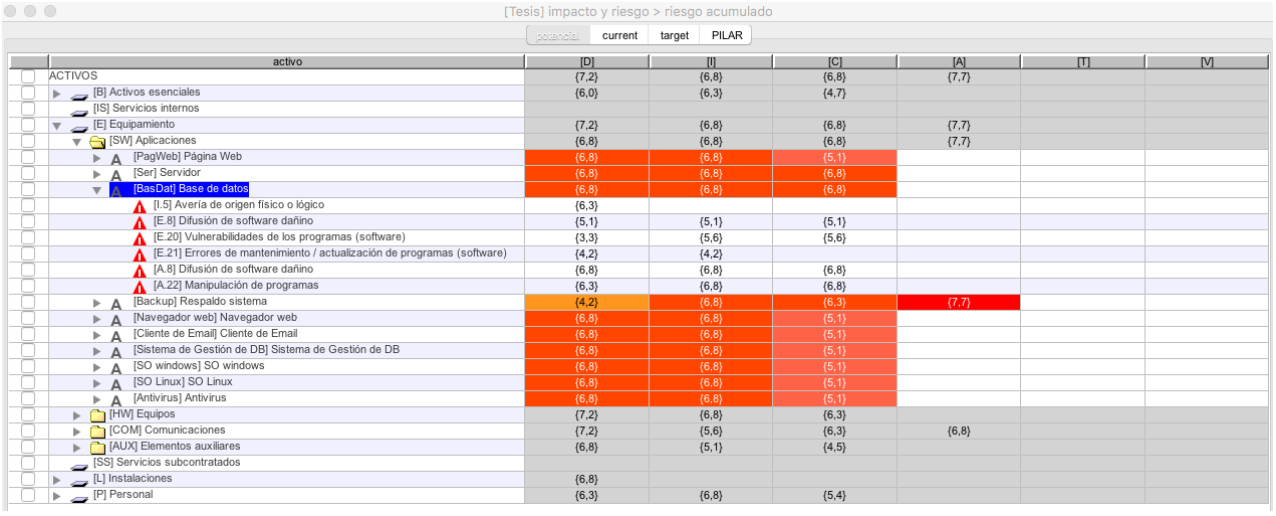
Las figuras 3.5.2 y 3.5.3 muestran el riesgo acumulado del análisis de riesgos, en cada una de las dimensiones nos muestran que tan crítico es el riesgo que va desde nueve que PILAR lo evalúa como catástrofe, cinco como crítico, uno tiene un nivel bajo de criticidad y cero como despreciable.



potencial current target PILAR

activo	[D]	[I]	[C]	[A]	[T]	[V]
ACTIVOS	{7,2}	{6,8}	{6,8}	{7,7}		
[B] Activos esenciales	{6,0}	{6,3}	{4,7}			
[IS] Servicios internos						
[E] Equipamiento	{7,2}	{6,8}	{6,8}	{7,7}		
[SS] Servicios subcontratados						
[L] Instalaciones	{6,8}					
[P] Personal	{6,3}	{6,8}	{5,4}			

Figura 3.5.2 Riesgo acumulado



activo	[D]	[I]	[C]	[A]	[T]	[V]
ACTIVOS	{7,2}	{6,8}	{6,8}	{7,7}		
[B] Activos esenciales	{6,0}	{6,3}	{4,7}			
[IS] Servicios internos						
[E] Equipamiento	{7,2}	{6,8}	{6,8}	{7,7}		
[SW] Aplicaciones	{6,8}	{6,8}	{6,8}	{7,7}		
[PagWeb] Página Web	{6,8}	{6,8}	{5,1}			
[Ser] Servidor	{6,8}	{6,8}	{6,8}			
[BasDat] Base de datos	{6,8}	{6,8}	{6,8}			
[I.5] Avería de origen físico o lógico	{6,3}					
[E.8] Difusión de software dañino	{5,1}	{5,1}	{5,1}			
[E.20] Vulnerabilidades de los programas (software)	{3,3}	{5,6}	{5,6}			
[E.21] Errores de mantenimiento / actualización de programas (software)	{4,2}	{4,2}				
[A.8] Difusión de software dañino	{6,8}	{6,8}	{6,8}			
[A.22] Manipulación de programas	{6,3}	{6,8}	{6,8}			
[Backup] Respaldo sistema	{4,2}	{6,8}	{6,3}	{7,7}		
[Navegador web] Navegador web	{6,8}	{6,8}	{5,1}			
[Cliente de Email] Cliente de Email	{6,8}	{6,8}	{5,1}			
[Sistema de Gestión de DB] Sistema de Gestión de DB	{6,8}	{6,8}	{5,1}			
[SO windows] SO windows	{6,8}	{6,8}	{5,1}			
[SO Linux] SO Linux	{6,8}	{6,8}	{5,1}			
[Antivirus] Antivirus	{6,8}	{6,8}	{5,1}			
[HW] Equipos	{7,2}	{6,8}	{6,3}			
[COM] Comunicaciones	{7,2}	{5,6}	{6,3}	{6,8}		
[AUX] Elementos auxiliares	{6,8}	{5,1}	{4,5}			
[SS] Servicios subcontratados						
[L] Instalaciones	{6,8}					
[P] Personal	{6,3}	{6,8}	{5,4}			

Figura 3.5.3 Riesgo acumulado

3.6 Plan de Seguridad

El plan de seguridad se puede definir como un conjunto de decisiones que definen cursos de acciones futuros, así como los medios que se van a utilizar para conseguirlos.

Después de haber realizado el análisis de las salvaguardas que generó PILAR, en la tabla 3.6.1 se pueden ver las salvaguardas críticas que se deben que atender de manera inmediata ya que cuentan con un peso relativo máximo.

Tabla 3.6.1 Salvaguardas específicas

#	Identificación PILAR	Descripción
1	A	Identificación y autenticación
2	A.7	Factores de autentificación que se requieren
3	A.7.1.1	Token físico- algo que se tiene
4	A.7.1.2	El mecanismo se inhabilita cuando se ve comprometido o hay sospecha de ello
5	A.7.2.1.3	Se seleccionan contraseñas fáciles de recordar, pero difíciles de conjetura
6	A.7.2.1.4	Los usuarios se responsabilizan de la confidencialidad de las contraseñas
7	A.7.2.1.a	Las contraseñas de usuarios administradores se cambian con mayor frecuencia
8	A.7.2.1.b.3	Las contraseñas iniciales tienen una duración limitada
9	A.7.2.1.c	La información de verificación está protegida

#	Identificación PILAR	Descripción
10	A.7.2.2	Las contraseñas se modifican al ser comprometidas o existir sospecha de ello
11	AC	Control de acceso lógico
12	A.C.1.2.1	Se dispone de procedimientos para las tareas de control de accesos, procedimientos para la concesión de privilegios
13	A.C.1.c	Los privilegios se anulan cuando termina la autorización
14	A.C.1.d	Los privilegios se revisan cundo el usuario cambia de responsabilidades o de función
15	A.C.1.e	Los privilegios se anulan cuando el usuario abandona la organización
16	A.C.1.f.3	Se revisan regularmente los derechos de acceso, se revisan al causar baja
17	A.C.2.4	Se restringe el acceso a la configuración de seguridad del sistema
18	H.ST.1	Segregación de tareas, SE separan las responsabilidades de administración y operación
19	D	Protección de la información
20	D.2.1	Se clasifica la información
21	D.2.1.3	El nivel de clasificación se mantiene cuando la información se transfiere
22	D.backup	Copias de seguridad
23	D.backup.2	Protección de la disponibilidad de la información
24	D.DS.6.3	Uso de firmas electrónicas, Implantación de los algoritmos, Dispositivos seguros de firma
25	K	Protección de claves criptográficas
26	K.IC	Protección de claves de cifra de información
27	K.IC.6	Distribución de claves
28	K.IC.7	Almacenamiento de claves
29	K.DS	Protección de claves de firma de información
30	K.DS.6	Distribución de claves
31	K.DS.7	Almacenamiento de claves
32	K.disk	Protección de claves para contenedores criptográficos
33	K.disk.5	Las claves se generan en un entorno separado del de explotación
34	K.disk.7	Distribución de claves
35	K.disk.8	Almacenamiento de claves
#	**Identificación PILAR**	**Descripción**
36	K.comms	Protección de claves de comunicaciones

37	K.comms.5	Las claves se generan en un entorno separado del de explotación
38	K.comms.7	Distribución de claves
39	K.comms.8	Almacenamiento de claves
40	S	Protección de los servicios
41	S.SC	Se aplican perfiles de seguridad
42	S.SC.3	Se eliminan, o modifican, las cuentas estándar de administrador
43	S.SC.4	Sólo los administradores de seguridad autorizados pueden modificar la configuración
44	S.SC.5	Los servicios activados se configuran de modo que el funcionamiento sea seguro
45	S. End. 3	Desmantelamiento, Almacenamiento seguro o destrucción de a información
46	S.dir.2	Los administradores deben autenticarse para acceder
47	S.dns.7	Protección del servidor de nombre de dominio (DNS), Software de prestación del servicio
48	S.2	Servicios subcontratados, Operación
49	S.2.3.3	Se activan los servicios de registro de actividad
50	S.2.3.7	Se definen procedimientos para notificar e investigar los incidentes y fallos de seguridad
51	S.2.5.1	Autenticación del servidor, SE autentica el servicio antes de transferir información alguna
52	S.2.6	Continuidad de operaciones
53	S.2.7.4	Desmantelamiento, Destrucción de la información del proveedor
54	SW.start	Puesta en producción, La instalación y la configuración de aplicaciones que afecta en a la seguridad del sistema, estará limitado a un número determinado de administradores de sistema y administradores de seguridad
55	SW.SC	Se aplican perfiles de seguridad
56	SW.SC.3	Se eliminan o modifican las cuentas estándar de administrador
57	SW.SC.4	Sólo los administradores de seguridad pueden modificar la configuración
58	SW.SC.5	Las funciones activadas se configuran de forma segura
59	SW.CM.5	Se priorizan las actuaciones encaminadas a corregir riesgos elevados
60	HW	Protección de los equipos informáticos (HW)
#	**Identificación PILAR**	**Descripción**
61	HW.SC	Se aplican perfiles de seguridad
62	HW.SC.1	Sólo los administradores de seguridad autorizados pueden

		modificar la configuración
63	HW.SC.3	Las funciones activadas se configuran de forma segura
64	HW.cont	Aseguramiento de la disponibilidad
65	HW.cont.1	Se dimensiona holgadamente y se planifica la adquisición de repuestos
66	HW.CM.6	Cambios (actualizaciones y mantenimiento), Se priorizan las actuaciones encaminadas a corregir riesgos elevados
67	HW.PCD.8	Informática móvil, Controles aplicables
68	COM	Protección de las comunicaciones
69	COM.SC	Se aplican perfiles de seguridad
70	COM.SC.3	Se eliminan, o modifican, las cuentas estándar de administrador
71	COM.SC.4	Sólo los administradores de seguridad autorizados pueden modificar la configuración
72	COM.SC.5	Los servicios activados se configuran de forma segura
73	COM.aut.5	Mecanismos de autenticación
74	COM.aut.5.1.1.3	Se seleccionan contraseñas fáciles de recordar, pero difíciles de conjetura
75	COM.aut.5.1.1.4	Los usuarios se responsabilizan de la confidencialidad de las contraseñas
76	COM.aut.5.1.1.a	Las contraseñas de usuarios administradores se cambian con mayor frecuencia
77	COM.wifi	Seguridad Wireless (WiFi)
78	COM.mobile.6	Telefonía móvil, Se prohíbe la conexión a ordenadores que manejan datos sensibles
79	IP.3	Sistema de protección de frontera lógica, Arquitectura de protección: red local (LAN)
80	IP.4	Dispositivos portátiles
81	IP.BS	Protección de los equipos de frontera
82	IP.BS.1	Se controla el producto
83	IP.BS.2	Se aplican perfiles de seguridad
84	IP.BS.2.2	Se eliminan, o modifican, las cuentas estándar de los usuarios
85	IP.BS.2.3	Se eliminan, o modifican, las cuentas estándar de administrador
86	IP.BS.2.6	Los administradores de seguridad autorizados, pueden modificar la configuración
87	IP.BS.2.7	Los servicios activados se configuran de forma segura
#	**Identificación PILAR**	**Descripción**
88	IP.BS.2.8	Los protocolos activados se configuran de forma segura
89	Tools	Herramientas de seguridad

90	Tools.AV.4	Herramientas contra código dañino, La base de datos de virus se actualiza regularmente
91	Tools.AV.7	Se revisan los programas y servicios de arranque del sistema
92	Tools.IDS.8	Herramientas de detención / prevención de intrusión, Disparos de alarmas en tiempo real
93	Tools.conf.3	Se revisa el sistema operativo
94	Tools.SFV.4.3	Cuando se detectan anomalías, se apaga el sistema
95	V.2.3	Gestión de vulnerabilidades, Se han previsto mecanismos para estar informado de vulnerabilidades del software base
96	tools.V	Herramienta de análisis de vulnerabilidades, se actualiza regularmente el conjunto de vulnerabilidades utilizado por el proveedor
97	V.4.1	Se analiza el impacto potencial (estimación de riesgo) Daños sobre la misión o negocio del sistema
98	V.6.1	Se disponen de procedimientos de reacción, medidas de emergencia ante riesgos elevados
99	V.7.1	Reparación de las vulnerabilidades detectadas, Se reparan urgentemente las vulnerabilidades que implican un alto riesgo
100	BC.DRP.2	Continuidad del negocio, Plan de recuperación de desastres (DRP), todas las áreas de la organización están coordinadas y los planes se prueban regularmente
101	G.1.3.3	Organización, Roles de identificación, Responsable de a seguridad de la información
102	G.3.2.3	Documentación organizativa, Políticas de seguridad de la organización, Está aprobada y respaldada por la dirección
103	RM	Gestión de riesgos
104	G.plan.5	Planificación de actividades de seguridad, Se definen responsabilidades y responsables
105	G.exam	Inspecciones de seguridad, Plan de acción Se reparan urgentemente los defectos descubiertos que implican un alto riesgo
106	G.8	Salvaguardas de los registros de la Organización, El almacenamiento se realiza de forma segura
107	E.2.3	Relaciones Externas, Se usan identificadores únicos y se controla su uso
108	E.2.6	Se garantiza el derecho para controlar (y suspender en su caso) la actividad de los usuarios

Cabe señalar que la tabla anterior se vuelve de vital importancia ya que cada área involucrada en el Distintivo ambiental UNAM se ve impactada por cada una de las salvaguardas, estableciendo el mecanismo de implementación de la seguridad la cual garantice el funcionamiento óptimo del activo o definir si asumen el riesgo que implica el no implementar ningún tipo de salvaguarda.

Conclusiones

Conclusiones

El plan de seguridad es pieza fundamental para la prevención de incidentes en el tema de seguridad informática que afectan principalmente a los activos más valiosos con los que cuenta la Organización, parte importante del plan de seguridad es el análisis de riesgos el cual funciona como un diagnóstico, muestra el estado verdadero de la Organización, ayuda a tener una idea más clara de cuáles son los activos con los que cuenta la Organización y la importancia de estos, ver cuáles son las amenazas que tiene cada uno de estos activos y poder implementar salvaguardes que eliminen el riegos o que lo hagan aceptable.

Como resultado de la implementación del análisis de riesgos se determinó cuáles son los activos que conforman al Diagnóstico ambiental UNAM, que va desde contactar a la dependencia a la cual se le va a realizar el diagnóstico hasta la reevaluación de la misma, se estableció la relación que existente entre los activos, se determinó el valor que tienen cada uno de los activos para el Programa Universitario de Estrategias para la Sustentabilidad y las dimensiones de seguridad (Integridad, Disponibilidad, Confidencialidad Autenticidad y Trazabilidad) que comparten los activos. Una vez detectados los activos se detectaron las amenazas relacionadas a cada uno de los activos y el valor que tienen cada una de estas para finalmente poder determinar las salvaguardas que hacen que el riesgo existente se minimice o desaparezca.

Se analizar las 16 actividades que se llevan a cabo para la implementación del Distintivo ambiental UNAM, se sintetizo una gran cantidad de información la cual se recabo por primera vez ya que nunca se había implementado un análisis de riesgos en la dependencia, fue un análisis exhaustivo en el cual se encontraron 108 salvaguardas críticas que se deben de atender de manera inmediata ya que cuentan con un peso relativo máximo, lo cual implica que la atención debe ser inmediata en cada área correspondiente según el proceso, para que estas puedan determinar la implementación de la salvaguarda o asuman el riesgo que existe al hacer caso omiso.

Este tipo de trabajos beneficia de manera directa al Programa Universitario de Estrategias para la Sustentabilidad con la iniciativa de promover una cultura en el ámbito de la seguridad informática y se establezcan medidas de precaución preventivas y no correctivas en los sistemas informáticos, esperando que el siguiente trabajo ayude en la mejora de las medidas de seguridad a nivel Universidad.

Referencias

Referencias

Barrientos, M. J., & Reyes, C. Q. (2006). Fundamentos de seguridad informática. En M. J. Barrientos, & C. Q. Reyes, *Fundamentos de seguridad informática* (pág. 207). México: Facultad de Ingeniería.

Brundtland, G. H. (2007). *Nuestro Futuro Común.* ONU.

Dell. (s.f.). *Medioambiente* . Recuperado el 2 de 05 de 2017, de http://www.dell.com/learn/mx/es/mxcorp1/dell-environment

LEED. (2012). Obtenido de http://www.usgbc.org/leed#rating

Mayer, J. (1990). *Declaración de Talloires.* Talloires: University Leaders for a Sustainable Future.

Metodología MAGERIT. (2012). *Metodología MAGERIT.* España.

México, U. N. (11 de Septiembre de 2011). *Programa Universitario de Medio Ambiente*. Obtenido de Programa Universitario de Medio Ambiente: http://www.puma.unam.mx

Residuos, L. G. (2015). *Camara de Diputados H. Congreso de la Unión.* Recuperado el 5 de 2 de 2017, de Camara de Diputados H. Congreso de la Unión: www.diputados.gob.mx/LeyesBiblio/pdf/263_220515.pdf

Satrs a Program of aashe. (2013). Obtenido de www.stars.aashe.org

SEDEMA. (2016). *Reciclatrón*. Recuperado el 15 de 05 de 2017, de Reciclatrón: http://data.sedema.cdmx.gob.mx/reciclatron/#.WT7jMMbmFo4

UNAM, F. I. (2017). *Ingeniería en computación*. Recuperado el 15 de 05 de 2017, de http://www.ingenieria.unam.mx/programas_academicos/licenciatura/computacion.php

UNAM. (16 de 02 de 2009). *Gaceta UNAM*. Obtenido de http://www.dgcs.unam.mx/gacetaweb/2009/090216/gaceta.pdf página 4

Glosario

Glosario

ACTIVO

Un activo es, generalmente hablando, algo que la Organización tiene o usa y que, si es perdido o dañado, causaría un daño a la Organización.

AMENAZA

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

Evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.

ANÁLISIS DE RIESGOS

El análisis de riesgos es la parte del proceso de gestión de riesgos en la que se calculan los indicadores de impacto y riesgo que se utilizarán para tomar decisiones de tratamiento.

AUTENTICIDAD

Aseguramiento de la identidad u origen.

CONFIDENCIALIDAD

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

DISPONIBILIDAD

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

GESTIÓN DE RIESGOS

Proceso para gestionar los riesgos a que está sometida la organización (incluyendo la misión, funciones, imagen o reputación), los activos de la organización, o individuos relacionados con la explotación de un sistema de información, e incluye: (i) la realización de una evaluación del riesgo, (ii) la aplicación de una estrategia de mitigación de riesgos, y (iii) el empleo de técnicas

y procedimientos para el seguimiento continuo del estado de seguridad del sistema de información.

GESTIÓN DE LA SEGURIDAD

Parte del sistema general de gestión que comprende la política, la estructura organizativa, los recursos necesarios, los procedimientos y los procesos necesarios para implantar la gestión de la seguridad de la información en una organización

IMPACTO

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

INCIDENTE DE SEGURIDAD

Es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras.

INTEGRIDAD

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

PLAN DE SEGURIDAD

Conjunto de decisiones que definen cursos de acciones futuros, así como los medios que se van a utilizar para conseguirlos.

POLÍTICA DE SEGURIDAD

Declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

RECURSOS DEL SISTEMA

Son los activos a proteger del sistema informático de la organización.

RIESGO

Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

RIESGO ACUMULADO

Es la valoración del daño para la organización, evaluado en los activos inferiores.

RIESGO REPERCUTIDO

El riesgo repercutido estima el daño a la organización, calculando el daño en los activos explícitamente valorados.

RIESGO RESIDUAL

Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.

SALVAGUARDA

Cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de la amenaza y/o el nivel de impacto en la organización.

SEGURIDAD INFORMÁTICA

Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevar a daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o boquear el acceso de usuarios autorizados al sistema.

TRAZABILIDAD

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

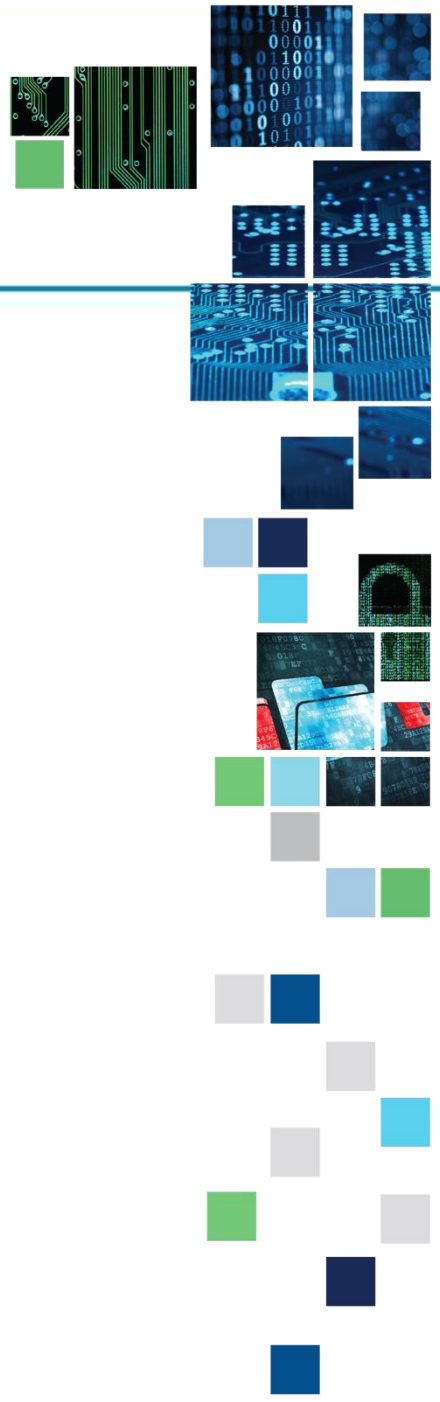
VULNERABILIDAD

Es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daño y producir pérdidas en la organización.

Abreviaturas

EcoPUMA	Estrategia de Universidad Sustentable
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
ONG	Organizaciones No Gubernamentales
PNUMA	Programa de las Naciones Unidas para el Medio Ambiente Humano
PUES	Programa Universitario de Estrategias para la Sustentabilidad
PUMA	Programa Universitario de Medio Ambiente
SEMARNAT	Secretaría de Medio Ambiente y Recursos Naturales
SIEDA	Sistema Estadístico de Desempeño Ambiental

Apéndice



Apéndice

El ingeniero en computación y los residuos electrónicos

El acelerado proceso de urbanización y la modificación en los patrones de consumo de las sociedades ha incrementado la generación de Residuos Sólidos Urbanos (RSU) y Residuos de Manejo Especial (RME), lo que disminuyó la capacidad de tratamiento en los sitios de disposición final y dio lugar a un manejo no controlado, ocasionando la contaminación de cuerpos de agua y sistemas terrestres, además de la pérdida de procesos regeneradores en los sistemas ecológicos.

En la Ciudad de México se estima que en el año 2015 se generaron cerca de 12,843 toneladas al día de residuos sólidos, lo que representa un serio problema, dado que la única alternativa para su disposición hasta hace algunos años era el confinamiento en el relleno sanitario en Bordo Poniente, el cual ha restringido la recepción de residuos porque se ha rebasado su capacidad.

Los residuos se clasifican de la siguiente forma:

- Residuos Sólidos Urbanos (RSU): son los generados en las casas habitación, que resultan de la eliminación de los materiales que utilizan en sus actividades domésticas, de los productos que consumen y de sus envases, embalajes o empaques; los residuos que provienen de cualquier actividad dentro de establecimientos o en la vía pública que genere residuos con características domiciliarias, y los resultantes de la limpieza de las vías y lugares públicos. (Residuos, 2015)
- Residuos de Manejo Especial (RME): son aquellos generados en los procesos productivos, que no reúnen las características para ser considerados como peligrosos o como residuos sólidos urbanos, o que son producidos por grandes generadores de residuos sólidos urbanos.

  Los residuos de manejo especial se clasifican en:

  - Residuos de las rocas

- Residuos de servicio de salud
- Residuos generados por las actividades pesqueras, agrícolas, silvícolas, forestales, avícolas, ganadera
- Residuos de los servicios de transporte
- Lodos provenientes del tratamiento de aguas residuales
- Residuos de tiendas departamentales o centros comerciales
- Residuos de la construcción
- ***Residuos tecnológicos de la industria de la informática***
- Pilas
- Neumáticos usados (Residuos, 2015)

- Residuos Peligrosos (RP): son aquellos que posean alguna de las características de corrosividad, reactividad, explosividad, toxicidad, inflamabilidad o que contengan agentes infecciosos que les confieran peligrosidad, así como envases, recipientes, embalajes y suelo que hayan sido contaminados cuando se transfiere a otro sitio. (Residuos, 2015)

Ante esta problemática y la tendencia generalizada del incremento de generación de residuos, se ha optado por analizar estrategias y alternativas que permitan un adecuado manejo, por lo que la reducción de origen y el aprovechamiento de los residuos generados están cobrando mayor relevancia.

Para esto es de gran importancia contar con un Programa de Gestión Integral de Residuos de Manejo Especial, el cual concierne a las personas físicas o morales que generen, almacenen, transporten, manejen, traten, dispongan, aprovechen, reciclen o reutilicen cualquier tipo de residuo sólido en la Ciudad de México(CDMX).

Asimismo, este programa es aplicable a todas las dependencias, órganos desconcentrados y entidades del Gobierno de la CDMX que, en el ámbito de su competencia, tengan relación con los residuos en esta Ciudad, así como a los fabricantes, productores, distribuidores, importadores, exportadores, comercializadores y

prestadores de servicios, que de manera directa o indirecta generen y manejen residuos sólidos urbanos o de manejo especial.
El ingeniero en computación además de cumplir con el objetivo de ser capaces de planear, diseñar, organizar, producir, operar y dar soporte técnico a los sistemas electrónicos para el procesamiento de datos, a los sistemas de programación de base y de aplicación del equipo de cómputo, así como efectuar el control digital de procesos automáticos (UNAM F. I., 2017), debe de tener un sentido ético, humanista y ecológico, para resolver problemas.

Atendiendo a estos objetivos como ingenieros en computación tendemos a dejar muy de lado el tema ecológico y para estos tiempos el término sustentable, no se tienen consideraciones en relación a diferentes aspectos de los equipos electrónicos, desde saber cuáles son los equipos con un menor consumo de energía, qué va a suceder después de que cumplan su ciclo de vida, saber cuál es su tiempo de vida ya que el avance tecnológico acelerado ha llevado a la rápida obsolescencia de los productos y mucho menos, qué recursos fueron los empleados para desarrollar el producto ni si las condiciones humanas fueron las adecuadas.

Se estima que a nivel mundial se generan alrededor de 40 millones de toneladas de residuos electrónicos al año, México no es ajeno a esta situación, de acuerdo con el Instituto Nacional de Ecología y Cambio Climático (INECC), en 2014 se generaron en nuestro país alrededor de 358 mil toneladas de este tipo de residuos, lo que proporciona un indicador de 3.2 kg per cápita. (SEDEMA, 2016)

Los aparatos electrónicos y eléctricos que se convierten en residuos y no son reciclados o dispuestos de manera adecuada son un problema de salud, contienen una gran cantidad de compuestos y sustancias peligrosas como: plomo, cadmio, mercurio, arsénico, níquel entre otros, además de contaminantes orgánicos persistentes (COP´s), por ejemplo, los bifenilos policlorados.

Algunas compañías se preocupan por este gran problema que son los residuos electrónicos, por lo que están realizando campañas de reciclaje para evitar la contaminación del medio ambiente, a continuación, se mencionan algunos de estas compañías y sus programas:

HP

Todos los cartuchos de tóner y tinta Originales HP devueltos mediante el programa HP Planet Partners son sometidos a un proceso de reciclaje de fases múltiples. Son reducidos a materias primas, las cuales pueden ser usadas para fabricar nuevos productos plásticos y metálicos, como cartuchos HP. Todo material remanente es desechado o manejado de manera responsable en un proceso con recuperación de energía.

Ningún cartucho Original HP devuelto mediante HP Planet Partners es enviado a rellenos sanitarios, y HP nunca rellena o re manufactura los cartuchos.

Solamente se tiene que ingresar a la página http://www8.hp.com/mx/es/ads/planet-partners/index.html y solicitar la recolección de los cartuchos.

DELL

Diseñamos nuestros productos pensando en el medioambiente

En Dell se tiene en cuenta el impacto ambiental que pueden causar los productos en cada una de sus etapas del ciclo de vida, se tienen en cuenta los siguientes aspectos a la hora de diseñarlos: elección inteligente de los materiales, eficiencia energética, qué hacer con ellos al final de la vida útil y estándares medioambientales.

Como empresa global, en Dell se mantiene el compromiso de minimizar el impacto que tienen sus operaciones y las de la cadena de suministros sobre el planeta.

La actividad comercial se rige por las siguientes líneas de actuación:

Compromiso de no generar residuos: los residuos significan falta de eficiencia, por lo que su estrategia se centra en eliminar los residuos de cualquier tipo.

Mitigación del cambio climático: son conscientes de que todos debemos tomar parte en la transición hacia una economía con menores emisiones de carbono. Controlan y reducen el impacto ambiental.

Ahorro energético y electricidad verde: El uso inteligente de la energía resulta beneficioso tanto para los negocios como para el planeta.

En Dell se piensa que el embalaje ecológico y el transporte de los productos constituyen una oportunidad de innovación, a través de la cual pueden ayudar a empresas y hogares a reducir los residuos que generan mediante los siguientes elementos, por otra parte, al reducir el tamaño del embalaje, se consigue transportar más cajas en el mismo espacio. Incluyendo más productos en la misma caja, como se hace al utilizar el sistema Multipack en algunos pedidos, lo cual logra reducir la cantidad total de residuos generados. (Dell, s.f.)

CISCO

Programa de devolución y reciclaje

Todos los días usamos dispositivos electrónicos para trabajar, vivir, jugar y aprender. Cuando se vuelven obsoletos, necesitamos reciclarlos. No obstante, la rápida proliferación de productos electrónicos ha llevado a su acumulación creciente en los vertederos.

Mediante programas voluntarios y obligatorios, los productores están asumiendo la responsabilidad de eliminar y reciclar los productos electrónicos como corresponde.

A través de sus programas de fin de vida útil, Cisco reduce significativamente el impacto de los productos electrónicos usados. El Programa de devolución y reciclaje está diseñado para recuperar y reutilizar los materiales incluidos en los equipos retirados. Los productos se desarman y procesan para rescatar materiales como acero, aluminio, cobre, plásticos, placas de circuito trituradas y cables.

El Programa de devolución y reciclaje de Cisco permite desechar de forma correcta los productos que alcanzaron el fin de su vida útil. El programa está abierto a todos los usuarios de equipos de Cisco y de equipos cuya marca pertenece a empresas adquiridas por Cisco.
Cada vez más son las empresas preocupadas con el medio ambiente al diseñar productos pensados para proporcionar un servicio de calidad satisfaciendo a los clientes, pero también se preocupan con el medio ambiente, desde tener consumos de energía mucho menores, políticas de logística muy bien establecidas, hasta tener corresponsabilidad con sus productos cuando estos terminan su ciclo de vida y reutilizar y manejad de manera adecuada los residuos generados.

Así como las empresas comienzan a dar grandes pasos en los temas de sustentabilidad y preocuparse por los temas ambientales, el ingeniero en computación debe sumarse a estos esfuerzos para que su trabajo genere el menor número de impactos de forma indirecta al medio ambiente, comenzar a preocuparse en que va a suceder con los equipos que utiliza cuando se vuelvan obsoletos o las necesidades requeridas ya no se cumplan, y tener muy en mente la corresponsabilidad que debemos de tener desde que se va adquirir un producto, durante el tiempo de funcionamiento y después de este.