UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN INFORMÁTICA

TEMA:	"EL ANÁLISIS DE RIESGOS INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN EN LA FACULTAD DE INGENIERÍA CIVIL Y MECÁNICA DE LA UNIVERSIDAD TÉCNICA DE AMBATO."

Trabajo de Investigación

Previa a la obtención del Grado Académico de Magíster en Informática

AUTOR: Ing. Donald Eduardo Reyes Bedoya

Director: Ing. Mg. David Guevara Aulestia.

Ambato – Ecuador

2014

Al Consejo de Posgrado de la Universidad Técnica de Ambato

El tribunal receptor de la defensa del trabajo de investigación con el tema: "EL ANÁLISIS DE RIESGOS INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN EN LA FACULTAD DE INGENIERÍA CIVIL Y MECÁNICA DE LA UNIVERSIDAD TÉCNICA DE AMBATO", presentado por: Ing. Donald Eduardo Reyes Bedoya y conformado por: Ing. Mg. Hernando Buenaño Valencia, Ing. Mg. Galo López Sevilla, Ing. Mg. Jaime Ruiz Banda, Miembros del Tribunal, Ing. Mg. David Guevara Aulestia, Director del trabajo de investigación y presidido por: Ing. Mg. Edison Álvarez Mayorga Presidente del Tribunal e Ing. Mg. Juan Garcés Chávez Director de Posgrado, una vez escuchada la defensa oral el Tribunal aprueba y remite el trabajo de investigación para uso y custodia en las bibliotecas de la UTA.

Ing. Mg. Edison Álvarez Mayorga
Presidente del Tribunal de Defensa

Ing. Mg. Juan Garcés Chávez
Director de Posgrado

Ing. Mg. David Guevara Aulestia
Director del trabajo de investigación

Ing. Mg. Hernando Buenaño Valencia
Miembro del Tribunal

Ing. Mg. Galo López Sevilla
Miembro del Tribunal

Ing. Mg. Jaime Ruiz Banda
Miembro del Tribunal

AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el trabajo de investigación con el tema: "EL ANÁLISIS DE RIESGOS INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN EN LA FACULTAD DE INGENIERÍA CIVIL Y MECÁNICA DE LA UNIVERSIDAD TÉCNICA DE AMBATO", nos corresponde exclusivamente al Ing. Donald Eduardo Reyes Bedoya, Autor y al Ing. Mg. David Guevara Aulestia, Director del trabajo de investigación; y el patrimonio del mismo a la Universidad Técnica de Ambato.

Ing. Donald Eduardo Reyes Bedoya
AUTOR

Ing. Mg. David Guevara Aulestia
DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de este trabajo de investigación o parte de él un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de esta, dentro de las regulaciones de la Universidad.

Ing. Donald Eduardo Reyes Bedoya

C.C. 1802193431

DEDICATORIA

El presente trabajo de investigación va dedicado de manera especial a mis Padres, quienes con su esfuerzo y amor fueron el motor fundamental para mi diaria superación y crecimiento profesional.

A mi esposa y mis hijos por brindarme su apoyo incondicional para hacer este trabajo realidad.

A mis hermanos y amigos que con sus palabras de aliento fueron el impulso necesario para lograr el éxito.

Al Ing. Mg. David Guevara por el apoyo incondicional, conocimientos y dirección de esta investigación encaminada a fortalecer los conocimientos y la consecución de los objetivos planteados.

Donald Eduardo Reyes Bedoya

AGRADECIMIENTO

Agradezco a Dios por brindarme la fuerza necesaria para hacer este objetivo realidad.
A la Universidad Técnica de Ambato por la oportunidad de obtener tan valiosos conocimientos en base a la calidad de sus maestros, a la Facultad de Ingeniería Civil y Mecánica que me abrieron las puertas para apoyar con este trabajo investigativo al mejoramiento en sus actividades.

Donald Eduardo Reyes Bedoya

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DE AMBATO
DIRECCIÓN DE POSGRADO
MAESTRÍA EN INFORMÁTICA

"EL ANÁLISIS DE RIESGOS INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD E INTEGRIDAD DE LA INFORMACIÓN EN LA FACULTAD DE INGENIERÍA CIVIL Y MECÁNICA DE LA UNIVERSIDAD TÉCNICA DE AMBATO."

Autor: Ing. Donald Eduardo Reyes Bedoya
Director: Ing. Mg. David Guevara Aulestia.
Fecha: 29 de noviembre de 2013

RESUMEN EJECUTIVO

La finalidad del presente trabajo investigativo es determinar de qué manera la aplicación de una metodología de análisis y gestión de riesgos informáticos aplicada a la Facultad de Ingeniería Civil y Mecánica contribuye a mejorar la seguridad de los sistemas informáticos, mediante un análisis crítico de las metodologías de gestión de riesgos, determinando con claridad las diferentes características, ventajas y desventajas de su aplicación de cada una de las metodologías analizadas.

El presente trabajo de investigación se sustenta en el estudio de algunas metodologías de análisis y gestión de riesgos informáticos que en nuestro medio son conocidas y aplicadas por un sinnúmero de organizaciones, pretendiendo analizar las características relevantes de cada una de ellas y seleccionando la más adecuada para su aplicación en el entorno de la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato.

Descriptores: Seguridad informática, integridad de la información, amenazas informáticas, riesgos informáticos, análisis de riesgos, gestión de riesgos, activos críticos, metodologías de gestión de riesgos, MAGERIT, OCTAVE.

TECHNICAL UNIVERSITY OF AMBATO
POSGRADUATE STUDIES CENTER
MASTER IN COMPUTERS

"COMPUTER ANALYSIS OF THE RISKS AND THEIR IMPACT ON THE SECURITY AND INTEGRITY OF INFORMATION IN THE FACULTY OF CIVIL AND MECHANICAL ENGINEERING OF TECHNICAL UNIVERSITY OF AMBATO."

Author: Ing. Donald Eduardo Bedoya Reyes
Directed by:Ing.Mg . David Guevara Aulestia
Date: November 29, 2013

ABSTRACT

The purpose of this research work is to determine how the application of an analysis methodology and IT risk management applied to the Faculty of Civil Engineering and Mechanics helps to improve the security of computer systems through a critical analysis of methodologies of risk management by clearly identifying the different features, advantages and disadvantages of implementing each of the analyzed methodologies.

The present research is based on the previous studies of some methodologies for analysis and the management of information technology risks in our environment. These are known and applied by countless organizations. This study will try to analyze the relevant characteristics of each one and selecting the most appropriate application for the Faculty of Civil Engineering and Mechanics at the Technical University of Ambato.

Keywords: Computer security, data integrity, security threats, IT risk, risk analysis, risk management, critical assets, risk management methodologies, MAGERIT, OCTAVE.

INTRODUCCIÓN

Los servicios informáticos en la actualidad están presentes en todos los ámbitosdonde el ser humano realiza sus actividades cotidianas, es así que con la evolucióndel internet y el desarrollo de la web 2.0, gran cantidad de empresas, industrias einstituciones en general han encaminado sus esfuerzos en ofrecer todos sus serviciosa través de este novedoso medio de comunicación que gracias a sus prestacionesse ha vuelto el más utilizado para las relaciones humanas, prestación de servicios,comercio y transacciones en general. Si bien esto ha permitido impulsar el desarrollode muchas empresas e instituciones, a la par a dado lugar a la proliferación deataques a los sistemas y datos, delitos informáticos, y otras amenazas que día trasdía van creciendo y se diversifican.

Con estos antecedentes las organizaciones buscan la manera de dar seguridada la información, datos y transacciones que se manejan a través de los sistemas deinformación vía web, estas seguridades que van ganando espacio en las organizacionesse sustentan en diferentes metodologías que cuentan con diversas características cuyaselección estará dada por las especificaciones de cada institución y el punto de vistade los directivos y asesores informáticos.

El informe final del proyecto denominado "El Análisis y Gestión de RiesgosInformáticos y su incidencia en la seguridad e integridad de la información en laFacultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato"que se presenta a continuación, está dividido en capítulos que pretenden facilitar lacomprensión del contenido de este trabajo, así:

En el Capítulo I, "PROBLEMA", como su nombre lo indica, identifica el problemaa resolver mediante una debida justificación, análisis crítico y el planteamiento delosobjetivos tanto general como específicos.

En el Capítulo II, "MARCO TEÓRICO", se establece el marco teórico sobreel cual se pretende trabajar, con los respectivos antecedentes investigativos,fundamentación legal, hipótesis y el señalamiento de las variables de la hipótesis.

En el Capítulo III, “METODOLOGÍA”, se describe la metodología de investigación a utilizar, enfoque, modalidad básica de la investigación, tipo de investigación,población y la muestra.

En el Capítulo IV, “ANÁLISIS E INTERPRETACIÓN DE RESULTADOS”, sedetalla el análisis e interpretación de resultados obtenidos en las encuestas realizadas.

En el Capítulo V, “CONCLUSIONES Y RECOMENDACIONES”, se presenta las conclusiones obtenidas después del análisis respectivo de la información recolectadaen la encuesta para luego proponer con las recomendaciones necesarias de cada unade ellas.

En el Capítulo VI, “PROPUESTA”, se presenta el estudio y selección de lametodología basándose en el marco teórico.

Finalmente se adjuntan los anexos en los cuales se colocan los documentosrecolectados en la Facultad de Ingeniería Civil y Mecánica de la UniversidadTécnica de Ambato y los demás documentos que ayudaron en el presente trabajo deinvestigación.

CAPITULO I

El Problema

1.1 Tema

"El Análisis de Riesgos Informáticos y su incidencia en la seguridad e integridad de la información en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato."

1.2 Planteamiento Del Problema

1.2.1 Contextualización

Según Eugenia Tobar (2013), “La Web 2.0 es la transición que se ha dado de aplicaciones tradicionales hacia aplicaciones que funcionan a través del web enfocadas al usuario final. Se trata de aplicaciones que generen colaboración y de servicios que reemplacen las aplicaciones de escritorio. ”

Teniendo en cuenta lo anterior podemos afirmar que la Web 2.0 trajo un sinnúmero de prestaciones para el intercambio de información más eficiente, que ha permitido que nuevos recursos puedan ser fácilmente utilizables vía internet, esto ha hecho que se creen más y mejores programas informáticos que si bien en su mayoría pretenden ayudar al usuario, también existen sofisticados programas de alto riesgo destinados al robo de información y hacer daño a los equipos, información y datos.

Esta transición se ha visto reflejada en las instituciones tanto públicas como privadas que han implementado una gran variedad de servicios a sus usuarios vía web, así tenemos pago de planillas de consumo, pago de tarjetas de crédito, consulta de saldos, formularios de solicitudes, y en el caso de las instituciones educativas consignación y reporte de notas, matriculas, pago de derechos entre otras.

Todas las actividades descritas obligan a tomar medidas de precaución para evitar el ingreso de usuarios no autorizados, hackers, manejo indebido de información por parte del personal, virus, entre otras amenazas a las que los sistemas se exponen al estar en línea.

Según ElComercio.com (2013),“Un ataque de hackers denunció este lunes 25 de febrero la Universidad de Especialidades Espíritu Santo (UEES) de Guayaquil. En un comunicado, el centro de estudios explica que intentaron violentar la seguridad del registro de calificaciones.”

Por lo indicado podemos decir que en los últimos tiempos la universidad ecuatoriana ha sido víctima de ataques informáticos que han afectado sus sistemas y se ha producido robo de información que ha causado graves daños y una alerta para todas las universidades del país que cada día dependen más de los sistemas informáticos y el intercambio de información vía web.

En la provincia de Tungurahua, las universidades privadas y en especial la universidad pública no cuentan con políticas de prevención de riesgos en sus sistemas informáticos que permitan disminuir las amenazas a las que están expuestos; con el análisis de las metodologías de gestión de riesgos informáticos se podrá implementar los procedimientos adecuados que permitan mejorar las seguridad y salvaguardar de manera adecuada la información y los datos.

Las amenazas a las que están sometidos los equipos informáticos de la Facultad de Ingeniería Civil y Mecánica, se deben al desconocimiento y por ende a la falta de aplicación de procedimientos de gestión de riesgo que permitan definir las acciones más adecuadas para minimizar la inseguridad y vulnerabilidad de los recursos de información de la mencionada facultad.

1.2.2 Análisis Crítico

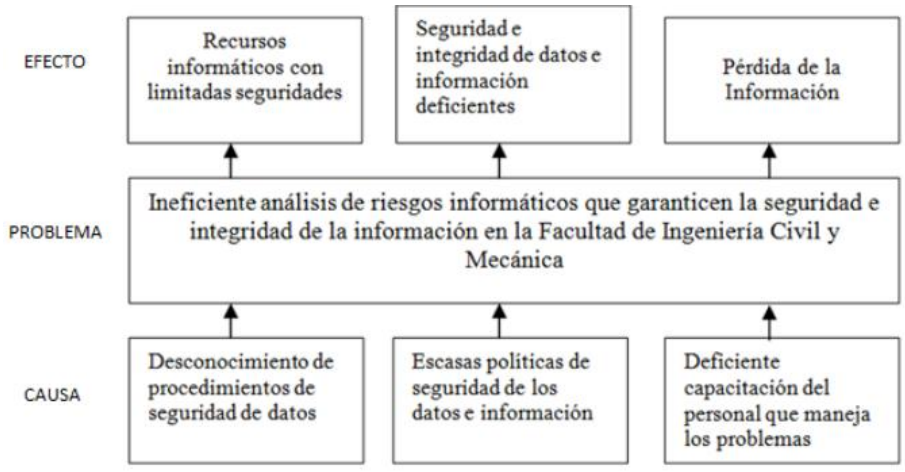

Figura1.1:Árbol de problemas(Fuente: Elaboración propia)

El desconocimiento de procedimientos de seguridad de datos ha traído como consecuencia que los recursos informáticos de la Facultad de Ingeniería Civil y Mecánica no cuenten con seguridades acordes a las exigencias actuales.

Las políticas actuales de seguridad de la información son inadecuadas ya que los riesgos y amenazas a las que están expuestos los sistemas provocan que la información y los datos tengan un alto nivel de inseguridad que los hacen fácilmente susceptibles de robo.

Con los antecedentes mencionados los datos e información que manejan los diferentes sistemas de la facultad se vuelven de fácil acceso y por consiguiente su sustracción y alteración sería una vulnerabilidad que aprovechada por personas inescrupulosas provocaría graves daños al normal desenvolvimiento de las actividades académicas que sustentan su actividad en los sistemas informáticos lo que hace que su confiabilidad sea la más alta posible.

La excesiva confianza del personal en el manejo de la información ha permitido detectar la falta de políticas adecuadas de seguridad e integridad de la información, esto se debe fundamentalmente al desconocimiento de los riesgos y vulnerabilidades a los que están sujetos tanto los sistemas como los datos que maneja el personal.

El manejo de una metodología de análisis de riesgo que se adapte a las realidades de cada institución hace posible que se minimicen las amenazas a las que están sometidos los datos por su inadecuado manejo evitando de ese modo la pérdida o alteración de la información que causaría graves problemas a la entidad.

La falta de estándares de seguridad provoca que tanto los equipos como información estén expuestos a riesgos e inseguridades que afectan directamente a la integridad de los datos.

1.2.3 Prognosis

La realización de un análisis de riesgos informáticos como es el tema de esta investigación, se hace indispensable ya que si no se realiza el mismo, no se podrá identificar las falencias y vulnerabilidades de los equipos, sistemas y datos lo que provocara que se cuente con una infraestructura poco confiable de fácil

acceso y llena de inseguridades que afectan directamente a la integridad de la información y los datos.

El desarrollo del proyecto de aplicación de una metodología de análisis de riesgos informáticos permitirá contar con una herramienta para la identificación de los recursos críticos, las amenazas a los que están expuestos los equipos y los riesgos a tener en cuenta para la seguridad e integridad de la información lo que conlleva a contar con un sistema confiable y seguro que brinde las garantías necesarias para tener datos e información con la protección requerida donde no se vea afectada su integridad.

1.2.4 Formulación Del Problema

¿En qué medida el análisis de riesgos incide en la seguridad e integridad de los datos en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato?

1.2.5 Interrogantes

- ¿La implementación de una metodología de análisis de riesgo informáticos permitirá minimizar las inseguridades y vulnerabilidades a los que está sometida la información en la facultad de Ingeniería Civil y Mecánica?
- ¿Se puede mantener la seguridad e integridad de los datos en los sistemas informáticos de la facultad de Ingeniería Civil y Mecánica?
- ¿Cuál sería el mecanismo más adecuado para controlar los sistemas informáticos de la facultad?
- ¿La implementación de medidas de control y protección evitara la pérdida, inseguridad en la integridad de los datos?

1.2.6 Delimitación del Objeto de la investigación

El presente trabajo de investigación se desarrollara bajo los siguientes parámetros:

CAMPO SEGURIDAD INFORMÁTICA

ÁREA SISTEMAS

ASPECTO ANÁLISIS DE RIESGOSINFORMÁTICOS

TIEMPO: SEMESTRE JUNIO – NOVIEMBRE 2013,

ESPACIO: FACULTAD DE INGENIERÍA CIVIL Y MECÁNICA
UNIVERSIDAD TÉCNICA DE AMBATO.

1.3 Justificación

La información es el recurso más valioso que tiene una institución sea esta pública o privada ya que en ella se sustentan todas y cada una de las actividades que se realizan, teniendo en cuenta esto tanto la información como los datos deben ser manipulados con el mayor cuidado posible entendiéndose por esto a ejecutar políticas que aseguren su integridad y eviten que caigan en manos equivocadas, por esta razón es de primordial relevancia cumplir procedimientos que garanticen la seguridad de la información.

La Universidad Técnica de Ambato mantiene varios sistemas informáticos que gestión de la información de manera adecuada para un rápido y eficaz servicio a los estudiantes, esta información es confidencial y de cuidadoso manejo, ya que son de vital importancia para el desarrollo institucional, pero al estar interconectada a través de redes y con el exterior a través de internet, está sujeta a constantes riesgos, teniendo en cuenta que estos sistemas son manejados por diversas personas lo que implica otra amenaza a tener en cuenta.

Los factores mencionados además de otros hacen necesario que cada entidad académica que conforma la universidad tenga un especial cuidado en el manejo de la información ya que las constantes amenazas a las que están sujetas requieren de políticas de análisis y control de riesgo informáticos con el propósito de salvaguardar la integridad de la misma.

La Facultad de Ingeniería Civil y Mecánica al igual que las restantes entidades académicas de la Universidad Técnica de Ambato maneja información confidencial propia de las actividades académicas que se desarrollan en ella, por esta razón se hace necesaria la utilización de procedimientos de análisis de riesgos informáticos que permitan identificar las amenazas y las acciones tendientes a minimizar o eliminar las mismas.

1.4 Objetivos

1.4.1 General

Determinar la incidencia del análisis de riesgos informáticos sobre la seguridad e integridad de la información en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato.

1.4.2 Específicos

- Realizar un análisis de riesgos sobre los sistemas informáticos de la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato.
- Establecer los niveles de seguridad e integridad de los datos e informaciónrequeridos en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato.
- Desarrollar una propuesta que mejore la seguridad e integridad de los datos y la información de los sistemas informáticos de la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato.

CAPITULO II

Marco Teórico

2.1 Antecedentes Investigativos

Debido a que la seguridad de la información se ha convertido en una necesidad creciente por las múltiples formas de ataque que se van desarrollando día tras día, muchos son los trabajos que abordan desde diferentes tópicos la salvaguarda de los datos, así tenemos diferentes trabajos de investigación que se mencionan a continuación.

Análisis y Gestión de Riesgos Informáticos para la protección de sistemas de información en el área de tecnologías informáticas del Gobierno Provincial de Tungurahua, año 2012, autor Cristina Elizabeth Padilla Pacha, unidad académica Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato

Conclusiones: Recomienda la Metodología de gestión de riesgo MAGERIT como la más adecuada para el control de la información y de los activos físicos de la organización.

Estudio e implementación de una metodología de prevención de intrusos para redes LAN, año 2010, autores Gabriela Catherine Torres Andagana y Diego Fernando Llanca Salcan, unidad académica Faculta de Informática y Electrónica de la Escuela Superior Politécnica del Chimborazo.

Conclusiones: Proporciona lineamientos de seguridad con una amplia participación del personal y fundamenta las seguridades en el liderazgo y las buenas prácticas administrativas donde sobresale el liderazgo como característica relevante.

Evaluación Técnica de la Seguridad Informática del Datacenter de la Escuela Politécnica del Ejército, autores Patricio Moscoso Montalvo, Ricardo Guagalango Vega, Walter Fuertes y RomelAldas, año 2010.

Conclusiones: Enfoca la Metodología MAGERIT con la herramienta informática PILAR para evaluar los riesgos informáticos de un Datacentrer teniendo en cuenta las recomendaciones de la norma ISO 27000.

Centro de gestión de riesgos para monitoreo de redes, en la Facultad de Ingeniería, Ciencias Físicas y Matemáticas de la Escuela Politécnica Nacional, autores Alexandra Espinosa Criollo, Freddy Roldan González y Dennis Collaguazo, año 2012

Conclusiones: Utilización de la metodología MAGERIT para el desarrollo de módulos para monitorear servidores de aplicaciones, de base de datos y dispositivos de interconexión que permiten detectar caída de servicios, ataques de intrusos para la toma de decisiones del administrador.

Análisis y gestión de riesgos para la elaboración de planes de contingencia en los sistemas de información de la ESPE-L, autores Edison Espinoza, Wellington Montes, y Eduardo Balarezo, año 2003.

Conclusiones: Describe, analiza y evalúa los principales aspectos relativos al análisis y gestión de riesgos de los Sistemas de Información, con el objetivo de elaborar un plan de contingencia como mecanismo de salvaguarda en las amenazas con mayor riesgo.

2.2 Fundamentación Filosófica

Todo derecho se fundamenta en el marco axiológico de una filosofía que define la naturaleza humana, su sentido de vida, los fines y procedimientos que articulan todo ello, uno de esos derechos fundamentales de los seres humanos es el Derecho a la Comunicación, entendida ésta como un proceso que abarca mensajes y medios, por lo que el derecho que la acompaña contiene en sí mismo al Derecho sobre los mensajes (Derecho a la Opinión, Derecho a la Información y a otros vinculados) y al Derecho sobre los Medios, indispensables estos para la transmisión de los mensajes.

El Derecho a la Comunicación, como requisito para la vigencia de todos los demás derechos, ya que en él se fundamentan los demás para coexistir.

Tan ligada la comunicación al sistema biológico y a la dimensión social, cultural y política de los seres humanos que resulta inevitable su extensión en "derecho": *"derecho a la comunicación"* para así tener derecho a la vida y ejercerla en todas sus dimensiones, expresiones y potencialidades.

A lo largo de toda su vida, las personas tienen derecho a desarrollar sus facultades innatas de comunicación, así como a desarrollar su cuerpo y sus condiciones de existencia. Podrán en ese intento y de hecho lo hacencomplementar sus potencialidades naturales de comunicación con el apoyo de tecnologías que hagan de su comunicación más eficaz y amplia.

2.3 Fundamentación Legal

La propuesta de este trabajo de investigación tiene su base legal en la Constitución de la República del Ecuador en todos los artículos referentes a la gestión de la información y las tecnologías así como también de las amenazas y riesgos, así tenemos:

Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

2. El acceso universal a las tecnologías de información y comunicación.

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existiráreserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Art. 385.- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas yla soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.

2. Recuperar, fortalecer y potenciar los saberes ancestrales.

3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

Art. 386.- El sistema comprenderá programas, políticas, recursos, acciones, e incorporará a instituciones del Estado, universidades y escuelas politécnicas, institutos de investigación públicos y particulares, instituciones públicas y

privadas, organismos no gubernamentales y personas naturales o jurídicas, en tanto realizan actividades de investigación, desarrollo tecnológico, innovación y aquellas ligadas a los saberes ancestrales.

El Estado, a través del organismo competente, coordinará el sistema, establecerá losobjetivos y políticas, de conformidad con el Plan Nacional de Desarrollo, con laparticipación de los actores que lo conforman.

Art. 387.- Será responsabilidad del Estado:

1. Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.

2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, al sumakkawsay.

3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.

4. Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales.

5. Reconocer la condición de investigador de acuerdo con la Ley.

Art. 388.- El Estado destinará los recursos necesarios para la investigación científica, el desarrollo tecnológico, la innovación, la formación científica, la recuperación y desarrollo de saberes ancestrales y la difusión del conocimiento. Un porcentaje de estos recursos se destinará a financiar proyectos mediante fondos concursables.

Las organizaciones que reciban fondos públicos estarán sujetas a la rendición de cuentas y al control estatal respectivo.

Art. 389.- El Estado protegerá a las personas, las colectividades y la naturaleza frentea los efectos negativos de los desastres de origen natural o antrópico mediante laprevención ante el riesgo, la mitigación de desastres, la recuperación y mejoramientode las condiciones sociales, económicas y ambientales, con el objetivo de minimizar la condición de vulnerabilidad.

El sistema nacional descentralizado de gestión de riesgo está compuesto por lasunidades de gestión de riesgo de todas las instituciones públicas y

privadas en losámbitos local, regional y nacional. El Estado ejercerá la rectoría a través delorganismo técnico establecido en la ley. Tendrá como funciones principales, entreotras:

1. Identificar los riesgos existentes y potenciales, internos y externos que afecten al territorio ecuatoriano.

2. Generar, democratizar el acceso y difundir información suficiente y oportuna paragestionar adecuadamente el riesgo.

3. Asegurar que todas las instituciones públicas y privadas incorporen obligatoriamente, y en forma transversal, la gestión de riesgo en su planificación y gestión.

4. Fortalecer en la ciudadanía y en las entidades públicas y privadas capacidades paraidentificar los riesgos inherentes a sus respectivos ámbitos de acción, informar sobre ellos, e incorporar acciones tendientes a reducirlos.

5. Articular las instituciones para que coordinen acciones a fin de prevenir y mitigar los riesgos, así como para enfrentarlos, recuperar y mejorar las condiciones anteriores a la ocurrencia de una emergencia o desastre.

6. Realizar y coordinar las acciones necesarias para reducir vulnerabilidades yprevenir, mitigar, atender y recuperar eventuales efectos negativos derivados de desastres o emergencias en el territorio nacional.

7. Garantizar financiamiento suficiente y oportuno para el funcionamiento del Sistema, y coordinar la cooperación internacional dirigida a la gestión de riesgo.

Art. 390.- Los riesgos se gestionarán bajo el principio de descentralización subsidiaria, que implicará la responsabilidad directa de las instituciones dentro de su ámbito geográfico. Cuando sus capacidades para la gestión del riesgo sean insuficientes, las instancias de mayor ámbito territorial y mayor capacidad técnica y

financiera brindarán el apoyo necesario con respeto a su autoridad en el territorio y sin relevarlos de su responsabilidad.

La Universidad Técnica de Ambato, creada mediante Ley No. 69-05 con fecha 18 de abril de 1969, con la visión de constituirse en “un centro de referencia académico, científico y humanístico del país”, realizadas en un “ámbito de

libertad, respeto a los derechos humanos e intelectuales, participación integrativa, equidad de género y defensa del medio ambiente, con criterios de sustentabilidad y sostenibilidad".

La Facultad de Ingeniería Civil creada mediante resolución No. 84-217-CU-P del 22 de mayo de 1984, tiene su origen en la Ex escuela de Ingeniería Civil fundada en 1974, consecuentemente la Universidad Técnica de Ambato viene formando profesionales provenientes de la zona central del país de hace 32 años, satisfaciendo las necesidades profesionales en el campo de la Ingeniería Civil.

2.4 Categorías fundamentales

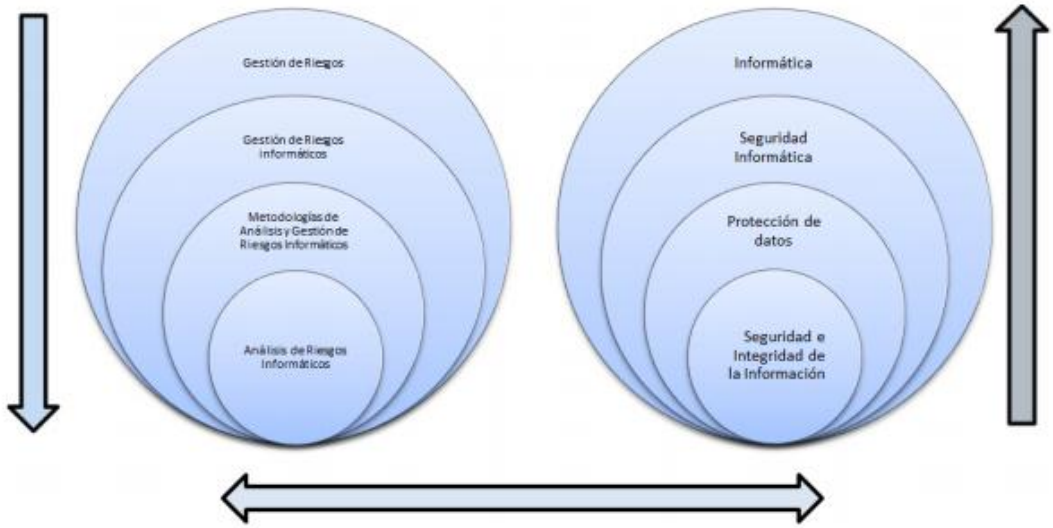

Figura 2.1: Categorias Fundamentales(Fuente: Elaboración propia)

2.4.1 Gestión de Riesgos

Según Obando, T.(2007) manifiesta que: "La gestión del riesgo es un programa de trabajo y estrategias para disminuir la vulnerabilidad y promover acciones de conservación, desarrollo, mitigación y prevención frente a desastres naturales y antrópicos".(Obando,2007)

2.4.2 Gestión de Riesgos Informáticos

En toda organización es importante contar con una herramienta, que garantice la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades del área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del entorno informático (Salvado, 2003).

La gestión de riesgos informáticos es establecer una valoración y priorización de los riesgos con base en la información ofrecida por los mapas elaborados en la etapa de identificación, con el fin de clasificar los riesgos y proveer información para establecer el nivel de riesgo y las acciones que se van a implementar. La gestión de riesgos informáticos la podemos ver de la siguiente manera:

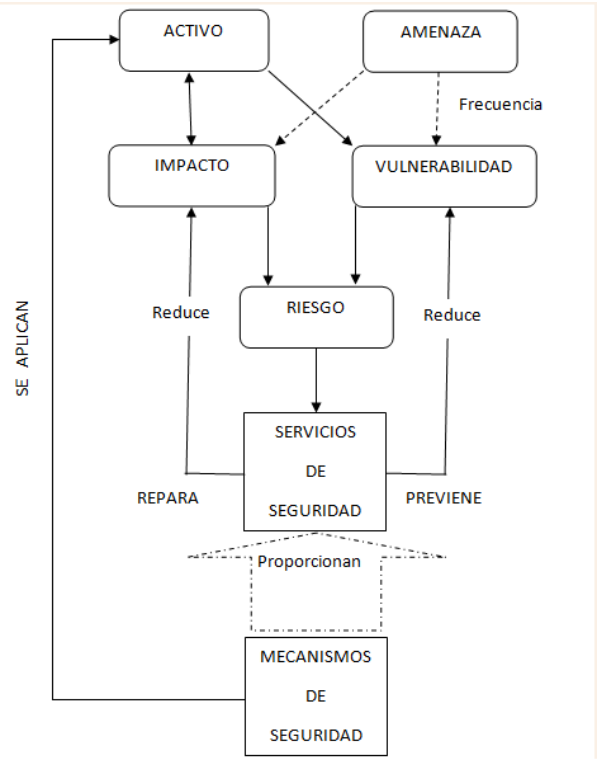

Figura 2.2: Mecanismos y servicio de seguridad (Fuente: Salvado, 2003)

Como manifiesta Salvado, J. (2003, p.81) "…se podría definir riesgo como cualquier elemento potencial que puede provocar resultados insatisfactorios en el desarrollo de un proyecto. En consecuencia, parece lógico pensar que el director de un proyecto necesitará, en todo momento, comprender y controlar el riesgo en aquellas áreas que puedan tener influencia sobre el proyecto, así como conocer los riesgos externos que puedan afectar al mismo." (Salvado, 2003).

Para De Pablos, C., López-Hermoso, J., Martín-Romo, S., Medina, S., Montero, A., Nájera, J. (2006, p.180) "La gestión de riesgos es un proceso separado que utiliza los resultados del análisis de riesgos para seleccionar e implantar las medidas de seguridad (salvaguardas) adecuadas para controlar los riesgos identificados."

Además enfatizan que "Frente a riesgos potenciales analizados se puede: Aceptar el riesgo, dada en muchos casos su baja posibilidad de ocurrencia; Transferir el riesgo, contratando los correspondientes seguros (se debe tener en cuenta que a veces la información perdida es irremplazable) o Evitar el riesgo. (De Pablos, Lopez-Hermoso, Martín-Romo, Medina, Montero, & Nájera, 2006).

2.4.3 Metodologías de Análisis y Gestión de Riesgos

Entre las metodologías más utilizadas para el análisis de riesgos informáticos podemos mencionar:

Octave.- El objetivo de Octave va direccionado a 2 aspectos diferentes: riesgos operativos y prácticas de seguridad. En este caso la tecnología es examinada en proporción a las prácticas de seguridad, esto permite a las compañías realizar la toma de decisiones de protección de información basados en los riesgos de confidencialidad, integridad y disponibilidad de los bienes afines a la información crítica.

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

Magerit Es una metodología enfocada al análisis y gestión de riesgos de los sitemas de información elaborada por el Consejo Superior de Administración Electrónica de España cuyo propósito es minimizar los riesgos de implantación y uso de Tecnologías de la Información, principalmente dirigida a las instituciones públicas. Complementa su accionar mediante la aplicación del software PILAR. Magerit persigue los siguientes Objetivos: Concientizar a los responsables de los sistemas de información de la existencia de riesgos y la necesidad de atajarlos a tiempo. Ofrecer un método sistemático para analizar tales riesgos. Ayudar a descubrir y planificar las medias oportunas para mantener los riesgos bajo control. Preparar a la organización para

procesos de evaluación, auditoria, certificación, o acreditación, según corresponda en cada caso.

2.4.4 Análisis Riesgos Informáticos

Para Capote, B., González, D., y Rodríguez, E. (2011) "La gestión de información es el proceso que se encarga de suministrar los recursos necesarios para la toma de decisiones, así como para mejorar los procesos, productos y servicios de la organización...". Teniendo en cuenta esto podemos decir que el análisis y protección de riesgo informáticos se vuelven un necesidad prioritaria ya que en la actualidad toda la información de una institución se maneja a través del computador y en constante interacción de la internet como medio de intercambio de datos entre las diferentes dependencias y departamentos que constituyen la misma.

Según Areitio, J. (2008, p. 54) manifiesta que: "Para tratar de minimizar los efectos de un problema de seguridad, se realiza el denominado análisis de riesgos, término que hace referencia al procesos necesario para responder a tres cuestiones básicas de la seguridad de una organización, que es saber qué queremos proteger, contra quién o qué se quiere proteger y cómo lo vamos a hacer."

Entre las razones que expone Areitio, J. (2008) para realizar un análisis de riesgos indica:

- Identificar los activos y controles de seguridad.
- Gestionar las alertas de los riesgos próximos.
- Identificar la necesidad de acciones correctivas.
- Proporcionar una guía de cara a los gastos de recursos.
- Relacionar el programa de control con la misión de la organización.
- Proporcionar criterios para diseñar y evaluar planes de contingencia y de continuidad de negocios.
- Mejorar la concientización global sobre la seguridad a todos los niveles.

En lo que se refiere a la gestión de riesgos Areitio, J. (2008) manifiesta: "…es el proceso total de identificar, controlar y eliminar o minimizar los eventos inciertos que puedan afectar a los recursos de una unidad de negocio. La gestión del riesgo integra las

técnicas de análisis de riesgos, análisis de beneficios, selección de mecanismos, implementación y verificación, evaluación de la seguridad de las salvaguardas y revisión de la seguridad global."

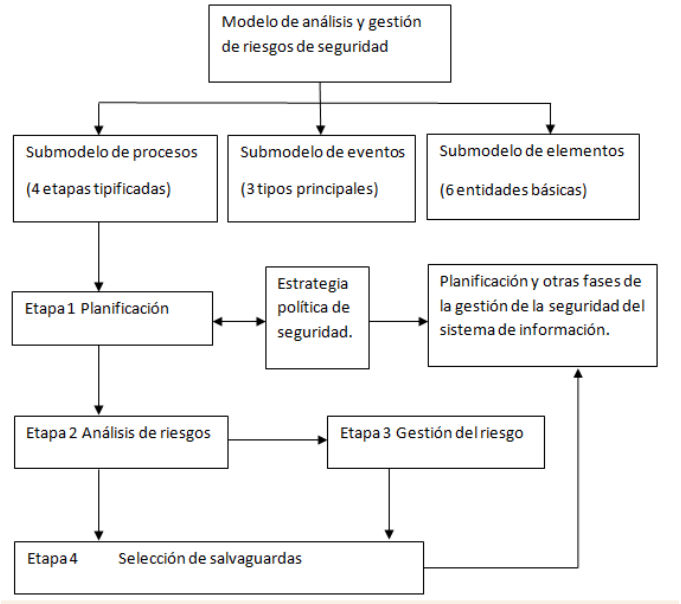

Figura 2.3: Analisis y Gestion de Riesgos (Fuente: Areitio, 2008)

Como se puede desprender de lo mencionado el análisis y la gestión de riesgos son dos etapas fundamentales en la aplicación de seguridades informáticas, la primera que va orientada a identificar: los recursos físicos y lógicos del sistema a proteger, los posibles atacantes a los que están expuestos y las acciones que se pueden ejecutar. Mientras que la gestión es la ejecución en sí de los procedimientos adecuados para minimizar y eliminar las posibles amenazas detectadas.

2.4.5 Informática

Según De Pablos, C., López-Hermoso, J., Martin-Romo, S., y Medina S. (2004, p.14) "El Diccionario de la Lengua Española de la Real Academia en su edición del año 92, define el término Informática como el "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores"." (De Pablos, López-Hermoso, Martin-Romo, & Medina, 2004).

Para Orozco, M., Chávez, M., y Chávez, J. (2006, p. 4) "La informática es la ciencia de la información. Este tecnicismo tiene su origen en la combinación de dos vocablos información y automática, y se usa para designar al conjunto de conocimientos que

permite el tratamiento automático de la información e involucra todo el proceso del manejo de datos mediante computadoras". (Orozco, Chávez, & Chávez, 2006).

Esta palabra de origen francés, es aceptada como una ciencia aplicada que abarca el estudio y aplicación del tratamiento automático de la información, utilizando como herramienta los dispositivos electrónicos y más comúnmente el computador. Este procesamiento automático, se lleva a cabo en tres etapas que son: la entrada de información, el procesamiento y la visualización de resultados.

La informática abarca un conjunto de sistemas como tal, siendo estos los equipos, la información y los usuarios, y sobre todos estos componentes se enfoca la investigación.

La informática es el tratamiento racional, automático y adecuado de la información, por medio del computador, para lo cual se diseñan y desarrollan estructuras y aplicaciones especiales buscando seguridad e integridad. Dado que para cualquier empresa o institución la información constituye un recurso de gran valor, se busca cualquier medio para mantenerla y utilizarla de la mejor manera de tal forma que se constituya en la piedra angular para la toma de decisiones más acertada posible.

2.4.6 Seguridad Informática

Para De Pablos, C., López-Hermoso, J., Martin-Romo, S., y Medina S. (2004, p.14), "La seguridad informática es la disciplina que se ocupa de diseñar normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable."

Introducción a la seguridad informática (De Pablos, López-Hermoso, Martin-Romo, & Medina, 2004)EditorialEditex Purificación Aguilera López Con respecto a la seguridad informática Royer, J. (2004, p. 4) indica que "El dominio cubierto por la seguridad informática es muy amplio. Podríamos definirla como: "La protección contra todos los daños sufridos o causados por la herramienta informática y originados por el acto voluntario y de mala fe de un individuo" (Royer, 2004)

Dado que la seguridad informática es la capacidad de mantener intacta y protegida la información de sistemas informáticos entendiéndose por estos a los equipos e información que son de vital importancia para el desarrollo de la empresa, se vuelve

necesario ejecutar políticas que permita mantener la información libre de corrupción y de intrusos no autorizados que puedan afectar la misma.

Teniendo en cuenta las definiciones anteriores podemos acotar que la seguridad informática está constituida por todas las acciones y procedimientos que permitan minimizar y de ser posible eliminar toda posible amenaza sobre la información y los equipos computacionales que una institución posee, es decir que esta seguridad no solo estará orientada a la protección de equipos, e información, sino también a la capacitación y concientización de los usuarios para un manejo adecuado y consecuente de la información y los equipos computacionales entendidos según este enfoque como el recurso más valioso de la institución y cuya seguridad es prioritaria.

2.4.7 Protección de Datos

"Todas las empresas, independientemente de su tamaño, organización y volumen de negocio, son conscientes de la importancia de tener implantadas una serie de políticas de Seguridad tendentes a garantizar la continuidad de su negocio en el caso de que se produzcan incidencias, fallos, actuaciones malintencionadas por parte de terceros, pérdidas accidentales o desastres que afecten a los datos e informaciones que son almacenados y tratados, ya sea a través de sistemas informáticos como en otro tipo de soportes, como el papel."

Según Álvarez Hernando, J. (2011, p. 51) "La protección de datos se considera un derecho fundamental que ostentan, exclusivamente, las personas físicas, que buscan proteger los datos personales que les conciernen frente a intromisiones o violaciones ilegitimas de su intimidad o privacidad." (Álvarez, 2011).

Teniendo en cuenta lo anterior la protección de la información trata de todas las acciones tendientes a garantizar que la información de un sistema informático sea accedida, manipulada y editada por cada uno de los actores del sistema respetando sus privilegios y permisos para acceder y modificar dicha información.

2.4.8 Seguridad e Integridad de la Información

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización. (ISO 27000)

Para Salvado, J. (2003, p. 101) "La seguridad de los sistemas de información está relacionada con la disponibilidad, confidencialidad e integridad de la información tratada por los ordenadores y las redes de comunicación." (Salvado, 2003)

Con estos antecedentes podemos afirmar que la seguridad de sistemas de información tienen como objetivo mantener los datos e información visible a los usuario autorizados, disponible en todo momento y libre de manipulación y alteración por parte de personal sin los privilegios establecidos para a manipulación de la misma, lo que se conseguirá mediante políticas claramente desarrolladas y documentadas teniendo en cuenta las características relevantes de la organización.

2.5 Hipótesis

El análisis de riesgos informáticos mejorará la seguridad e integridad de la información en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato.

2.6 Señalamiento de variables

Independiente

Análisis de riesgos informáticos

Dependiente

Seguridad e Integridad de la información

CAPITULO III

Metodología

3.1 Enfoque

El desarrollo del presente trabajo de investigación está enmarcado en un enfoque cuali-cuantitativo, es decir elproyectorealiza las siguientes consideraciones:

Se realizarán un estudio de los hábitos informáticos que tienen las personas, además se debe tener la calidad y cantidad de la información que se maneja, esto permitirá tener un conocimiento adecuado del entorno lo que permitirá a su vez sugerir las políticas de mejores prácticas de seguridad de la información.

Se revisarán también los activos informáticosy su utilización por parte de los usuarios administrativos, docentes y estudiantes.

3.2 Modalidad Básica de la Investigación

El presente trabajo de investigación se sustenta en las modalidades de investigación:

Investigación de Campo, ya que el investigador trabajara en el lugar y con los involucrados para recoger datos e información que permitirán el desarrollo del trabajo de investigación.

Investigación Documental, esta modalidad se hace necesaria ya que se revisaran y estudiaran trabajos de investigación, artículos, libros, revistas, papers, blogs, entre otros sobre el tema del presente trabajo.

3.3 Nivel otipo de investigación

a. Exploratorio.- Que permita observar los riesgos y amenazasmás comunes en la Facultad de Ingeniería Civil y Mecánica.
b. Descriptivo.- Detallar el uso de metodologías de análisis de riesgos informáticos a nivel universitario.

c. Correlacional.-Se busca establecer la relación de la variable independiente y la variable dependiente.

3.4 Población ymuestra

La Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato para el primer semestre del año 2013 en lo referente al recurso humano, está conformada de la siguiente forma:

Número de profesores = 69

Número de personal administrativo = 9

Número de alumnos = 1000

Total de personas = 1078

Para la determinación de la muestra se utilizó la siguiente formula:

$$n = \frac{0.25N}{\left(\frac{\alpha}{z}\right)^2 (N-1) + 0.25}$$

Como se puede observar se utilizó un nivel de confianza del 95%

N= 1078

Nivel de confianza= 95%

Z = 1.959963

n = 283

3.5 Operacionalización de las variables

Variable independiente: Análisis de Riesgos Informáticos

DEFINICIÓN CONCEPTUAL	**INDICADORES**	**ÍTEMS BÁSICOS**	**TÉCNICAS**	**INSTRUMENTOS**
Las diferentes amenazas y situaciones negativas a las que están expuestos los sistemas computacionales	Ataques de hackers Virus Usuarios maliciosos Usuarios inexpertos	¿Los procesos informáticos que se realizan poseen seguridades? ¿Los sistemas de información poseen seguridades? ¿Qué tipo de datos proporcionan los sistemas de información? ¿El hardware y software cumple con los requerimientos de los procesos realizados en la organización? ¿El personal está capacitado en el manejo del sistema de información?	Encuesta	Cuestionario dirigido a docentes, administrativos y alumnos de la Facultad de Ingeniería Civil y Mecánica.

Tabla 3.1: Variable Independiente: Análisis de Riesgos Informáticos (Fuente: Elaboración propia)

Variable dependiente: Seguridad e integridad de la información

DEFINICIÓN CONCEPTUAL	**INDICADORES**	**ÍTEMS BÁSICOS**	**TÉCNICAS**	**INSTRUMENTOS**
Característica de cualquier sistema informático, que indica que el sistema está libre de todo peligro de accesos no permitidos que puedan provocar un daño en él o la información que maneja.	Confidencialidad Integridad Disponibilidad	¿Se han producido fallas en el sistema informático? ¿Ha habido pérdida de información en los sistemas informáticos? ¿Los sistemas informáticos han sufrido algún ataque ya sea por virus, ingresos no autorizados u otro tipo de amenaza? ¿Su organización ha sufrido el robo de información por personal no autorizado? ¿Se realizan respaldos de los datos manejados por los sistemas de información?	Encuesta	Cuestionario dirigido a docentes, administrativos y alumnos de la Facultad de Ingeniería Civil y Mecánica.

Tabla 3.1: Variable dependiente: Seguridad e integridad de la información (Fuente: Elaboración propia)

3.6 Plan de recolección de información

Siendo este un proceso, por medio del cual se pasa del plano abstracto de la investigación, a un plano concreto, transformando la variable a categorías, las categorías a indicadores y los indicadores a ítems, facilitará la recolección de información por medio de un proceso de deducción lógica.

3.7 Plan de procesamiento de la información

La información recolectada se organizará, representará y analizará, presentando los resultados en porcentajes y diagramas que permitirán establecer en forma gráfica la realidad del problema planteado y la necesidad de un cambio o mejoramiento de la situación existente.

CAPITULO IV

Análisis e Interpretación de Resultados

4.1 Análisis de los resultados

En la presente investigación se utilizó como técnica de recopilación de la información la encuesta, la misma que realizada al personal administrativo, docentes y estudiantes de la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato, ha arrojado los siguientes resultados:

1. ¿Está usted capacitado para el manejo de los sistemas informáticos utilizados?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	187	66,08 %
2	Parcialmente	88	31,10 %
3	No	8	2,83 %
	TOTAL	283	100 %

Tabla 4.1: Frecuencia de la Pregunta Nro. 1 (Fuente: Elaboración propia)

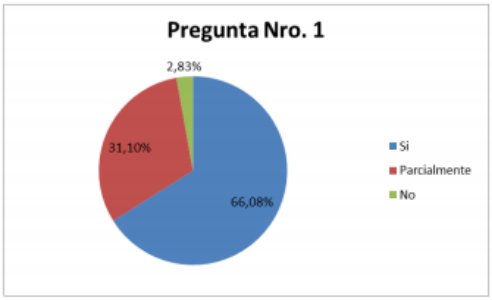

Figura 4.1: Personal Capacitado(Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 33,93% indica que no se encuentra totalmente capacitado para el manejo de los sistemas informáticos de su dependencia lo que hace pensar en mejorar la capacitación que permita un adecuado manejo de los equipos y sistemas.

Interpretación: El mayor porcentaje de los encuestados manifiesta estar total o medianamente capacitados para manejar los sistemas de información que posee la Facultad de Ingeniería Civil lo que indica que ellos tienen plena conciencia de los ataques que suelen suceder en los equipos e información y los peligros a los que se exponen los mismos.

2. ¿El hardware y software utilizado en su dependencia está acorde a las necesidades del trabajo?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	142	51,18 %
2	Parcialmente	124	42,32 %
3	No	17	6,01 %
	Total	283	100 %

Tabla 4.2: Frecuencia de la Pregunta 2 (Fuente: Elaboración propia)

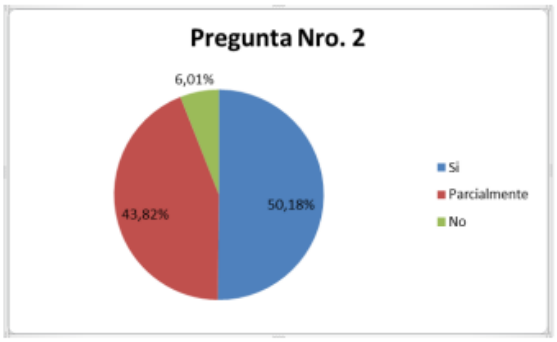

Figura 4.2: Hardware y Software utilizado (Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 48,33% indica que el hardware y software utilizados no están acordes a sus necesidades laborales lo que es un aspecto preocupante debido a que todo el trabajo se fundamenta en estas herramientas informáticas para el manejo adecuado de la información.

Interpretación: La mitad de los usuarios de los sistemas indican que los equipos utilizados no están acordes al trabajo que se realiza en los mismos, esto debe ser una alerta para la revisión y análisis de todo el entorno informático de la facultad el mismo que debe ser el adecuado para el desarrollo de las actividades y servicios que presta la unidad académica en estudio.

3. ¿Los equipos y sistemas informáticos que usted utiliza han sufrido fallas de seguridad?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	106	37,46 %
2	Parcialmene	117	41,34 %
3	No	60	21,20 %
	Total	283	100 %

Tabla 4.3: Frecuencia de la pregunta Nro. 3 (Fuente: Elaboración propia)

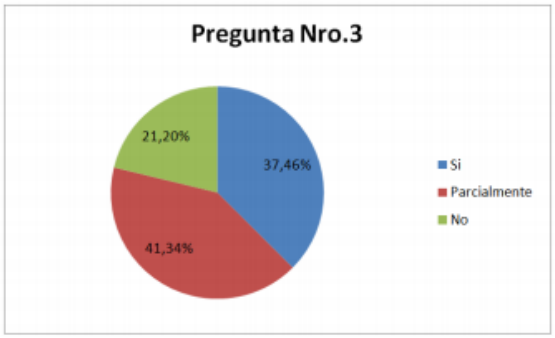

Figura 4.3: Fallas en los Sistemas Informáticos (Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 37,46% indica que los equipos no han sufrido fallas,mientras que el 41,34 manifiesta que si han sufrido fallas y el 21,20% dice que no ha sufrido falla los equipos.

Interpretación: La mayor parte de usuarios indican que han sufrido fallas ya sea graves o leves relativas a la seguridad de la información lo que indica claramente una carencia de procesos, normas y políticas que garanticen la seguridad de la información en un porcentaje alto.

4. ¿Los equipos y sistemas informáticos de la Facultad han sufrido algún ataque informático (virus, hacker, desastres naturales, otro tipo)?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	94	33,22 %
2	Parcialmente	63	22,26 %
3	No	126	44,52 %
	Total	283	100 %

Tabla 4.4: Frecuencia de la pregunta Nro. 4 (Fuente: Elaboración propia)

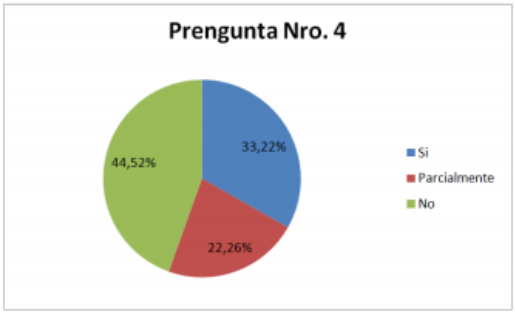

Figura 4.4: Ataques informátos (Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 66,78% manifiesta que ya sea de forma severa o leve han sufrido ataques informáticos que han comprometido en menor o mayor medida los sistemas de información a su cargo, esto ya es un indicador que requiere especial atención.

Interpretación: Los usuarios en su mayoría manifiestan que han sido víctimas de ataques ya sean leves o graves, esta aseveración permite percibir que las medidas de seguridad de los sistemas no están acordes a las necesidades y se requiere de procedimientos, normas, políticas que garanticen la integridad de la información.

5. ¿Ha sufrido robo o pérdida de información?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	51	18,02 %
2	Parcialmente	27	9,54 %
3	No	205	72,44 %
	Total	283	100 %

Tabla 4.5: Frecuencia de la pregunta Nro. 5 (Fuente: Elaboración propia)

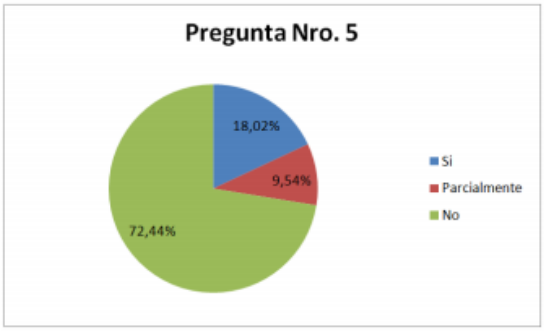

Figura 4.5: Pérdida de Información (Fuente: Elaboración propia)

Análisis: De los 283 encuestados un 27,56% manifiesta que han sufrido robo o pérdida de información ya sea parcial o total, esto hace pensar que los sistemas informaticos no se encuentran con las debidas protecciones en su totalidad que garantice la seguridad de la información.

Interpretación: Una cuarta parte de los usuarios indica que han sido víctimas de robo o pérdida de la información, que si bien aparentemente no representa un gran porcentaje no se encuentra dentro de los límites de aceptación permitidos ya que estos no deberían sobrepasar el 5%.

6. ¿Conoce el funcionamiento controles de seguridad en los sistemas de información?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	128	45,23 %
2	Parcialmente	107	37,81 %
3	No	48	16,96 %
	Total	283	100 %

Tabla 4.6: Frecuencia de la pregunta Nro. 6 (Fuente: Elaboración propia)

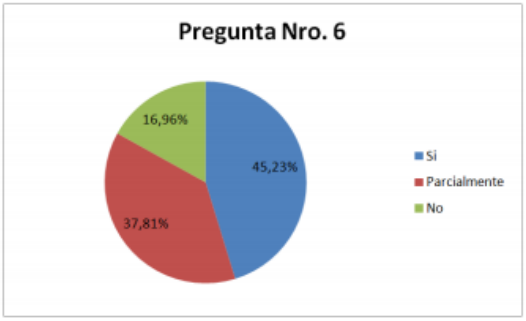

Figura 4.6: Controles de Seguridad (Fuente: Elaboración propia)

Análisis: De los 283 encuestados un 54,77% de ellos manifiesta que no existe o existen de forma parcial los controles de seguridad, lo que indica que hace falta tener un especial cuidado en este aspecto que compromete los sistemas de información y los datos.

Interpretación: La mayor cantidad de usuarios manifiesta que desconoce los procedimientos de seguridad que se aplican a los sistemas informáticos de la facultad lo que indica claramente que las políticas, normas y procedimientos no son socializados de manera correcta para conocimiento y aplicación entre los usuarios de los sistemas.

7. ¿Conoce de la existencia de un plan de seguridad de los sistemas y equipos informáticos?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	110	38,87 %
2	Parcialmente	90	31,80 %
3	No	83	29,33 %
	Total	283	100 %

Tabla 4.7: Frecuencia de la pregunta Nro.7 (Fuente: Elaboración propia)

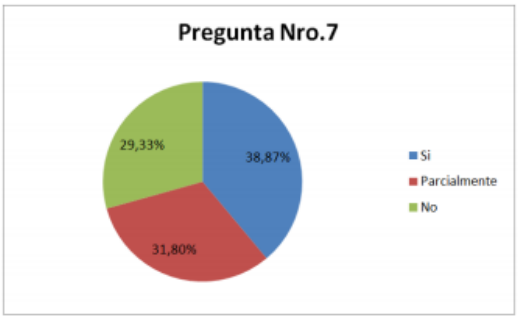

Figura 4.7: Plan de Seguridad de Sistemas y Equipos (Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 61,13% de ellos manifiesta que carecen de un plan de seguridad o se practica acciones parcialmente que no garantizan la salvaguarda de los equipos y sistemas.

Interpretación: La mayor parte de usuarios desconocen si existe un plan de seguridad de los sistemas y equipos informáticos que al igual que el ítem anterior demuestran carencia de una difusión adecuada de planes y programas de seguridad informática con que cuente la facultad.

8. ¿Conoce la existencia de un responsable que coordine las medidas de seguridad de los sistemas y equipos informáticos?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	226	79,86 %
2	No	57	20,14 %
	Total	283	100 %

Tabla 4.8: Frecuencia de la pregunta Nro. 8 (Fuente: Elaboración propia)

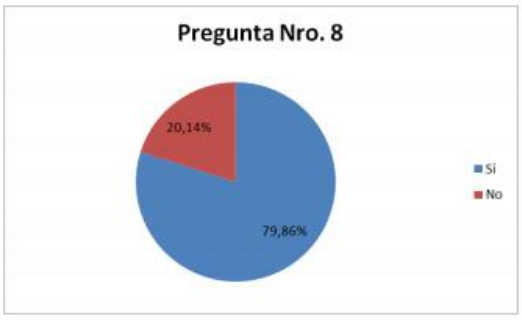

Figura 4.8: Responsable de las Medidas de Seguridad (Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 20,14% de ellos manifiesta que no conoce si existe una persona responsable de la coordinación de la seguridad de los sistemas, ya sea por no estar en contacto o no haberlo necesitado en algún momento.

Interpretación: La mayor parte de usuarios de los sistemas y equipos informáticos indican que desconocen si existe un responsable de aplicar medidas de seguridad a los sistemas informáticos de la facultad lo que refuerza la hipótesis de que no existe una buena socialización de los procedimientos, normativas y políticas de seguridad.

9. ¿Conoce usted si se hace algún tipo de revisión periódica del sistema de información?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	196	69,26 %
2	No	87	30,74 %
	Total	283	100 %

Tabla 4.9: Frecuencia de la pregunta Nro. 9 (Fuente: Elaboración propia)

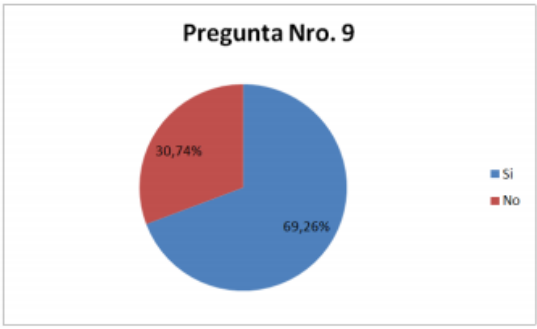

Figura 4.9: Revisión Periódica de los Sistemas (Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 30,74% de ellos indica que no se realiza ningún tipo de revisión periódica tanto de los equipos como de los sistemas de información.

Interpretación: La mayor parte de usuarios indican que si conocen que se hace una revisión periódica a los sistemas de información, esto permite ver que las revisiones las hacen diferentes personas pudiendo ser estos los ayudantes de laboratorio la que en el ítem anterior indicaban desconocer al encargado de aplicar las medidas de seguridad a los sistemas.

10. ¿Está usted capacitado en la seguridad del sistema de información?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	53	18,73 %
2	No	230	81,27 %
	Total	283	100 %

Tabla 4.10: Frecuencia de la pregunta Nro.10 (Fuente: Elaboración propia)

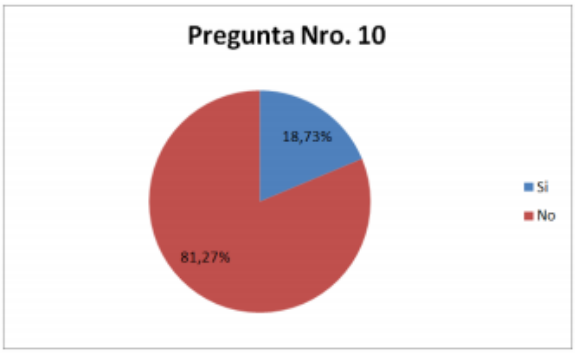

Figura 4.10: Capacitación en Seguridad (Fuente: Elaboración propia)

Análisis: De los 283 encuestados un 81,27% de ellos indica que no se encuentra capacitado en la seguridad de los sistemas de información.

Interpretación: La mayor parte de usuarios encuestados indica que no cuenta con capacitación en seguridad de los sistemas de información, esto se debe como se indicó en los ítems anteriores a la escasa o nula socialización de los procedimientos, normas y políticas por parte de los encargados de los sistemas informáticos de la facultad.

11. ¿Conoce usted si se han implementado políticas de seguridad en los sistemas y equipos informáticos?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	85	30,04 %
2	Parcialmente	132	46,64 %
3	No	66	23,32 %
	Total	283	100 %

Tabla 4.11: Frecuencia de la pregunta Nro. 11 (Fuente: Elaboración propia)

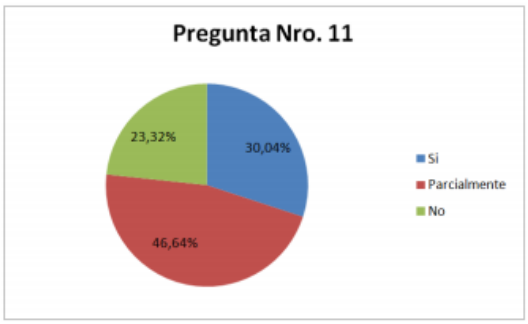

Figura 4.11: Implementación de Políticas de Seguridad (Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 76,68% de ellos, manifiesta no se han implementado o han sido escasas las implementaciones realizadas de políticas de seguridad tanto a equipos como a los sistemas de información con los que se cuenta.

Interpretación: La mayoría de encuestados indica que desconocen o parcialmente conocen que se hayan aplicado políticas de seguridad en los sistemas informáticos de la facultad y como se ha indicado esto se debe a la inexistencia de normativas o socializaciones para que los usuarios conozcan en su totalidad estas medidas si es que existen.

12. ¿Realiza usted copias de seguridad y respaldo de la información y los datos?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	33	11,66 %
2	A veces	162	57,24 %
3	No	88	31,10 %
	Total	283	100 %

Tabla 4.12: Frecuencia de la pregunta Nro. 12 (Fuente: Elaboración propia)

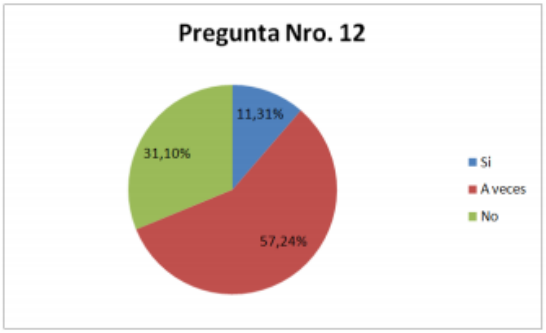

Figura 4.12: Copias de Seguridad y Respaldo (Fuente: Elaboración propia)

Análisis: De los 283 encuestados uno el 88,34% de ellos manifiesta que no se realizan copias de seguridad o si se realizan son temporales sin seguir un calendario adecuado de respaldo que permita garantizar la salvedad de la información.

Interpretación: Un alto porcentaje de usuarios encuestados manifiesta que no realiza copias de seguridad de la información que maneja, esto indica un desconocimiento de normas de seguridad y una falta de capacitación a los mismos lo que trae como consecuencia que la información se encuentre en constante peligro de perderse o ser alterada sin que los usuarios puedan garantizar la integridad de la información.

13. ¿Conoce si existe control de acceso a los sistemas y equipos informáticos (claves)?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	98	34,63 %
2	Parcialmente	60	21,20 %
3	No	125	44,17 %
	Total	283	100 %

Tabla 4.13: Frecuencia de la pregunta Nro. 13 (Fuente: Elaboración propia)

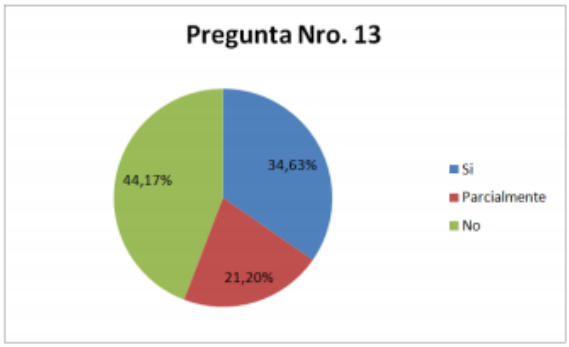

Figura 4.13: Control de Acceso a los Sistemas (Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 65,37% manifiesta que no existe control de acceso a los sistemas o si existe es en contados equipos y sistemas lo que hace pensar que la información se encuentra al alcance de usuarios inescrupulosos que pueden robar o corromper la información.

Interpretación: A pesar de ser una norma básica de seguridad los usuarios en su mayoría indican que no existe controles de acceso a los sistemas y equipos informáticos, esto demuestra claramente que la integridad de la información no está garantizada haciéndose urgente tener procedimientos y normativas formales que garanticen una mayor seguridad que la información requiere.

14. ¿Sabe si los respaldos de información se almacenan en un sitio seguro fuera de su departamento?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	43	15,19 %
2	No	46	16,25 %
3	Desconoce	194	68,55 %
	Total	283	100 %

Tabla 4.14: Frecuencia de la pregunta Nro. 14 (Fuente: Elaboración propia)

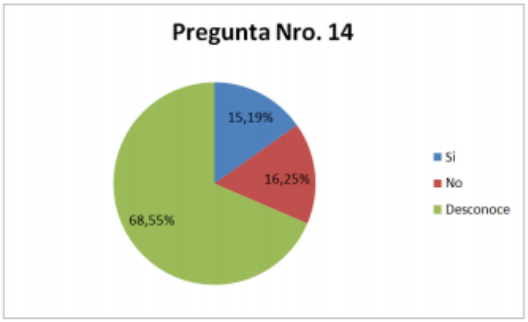

Figura 4.14: Respaldos de Información fuera del departamento (Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 84,8% indica que no se respalda o desconoce completamente si se respalda la información fuera de su departamento.

Interpretación: Los respaldos de información si se los realiza no se almacenan en un sitio seguro fuera de los diferentes departamentos lo que indica un claro desconocimiento de políticas de seguridad.

15. ¿Sabe si existen procedimientos de respaldo y recuperación de la información?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	41	14,49 %
2	No	58	20,49 %
3	Desconoce	184	65,02 %
	Total	283	100 %

Tabla 4.15: Frecuencia de la pregunta Nro.15 (Fuente: Elaboración propia)

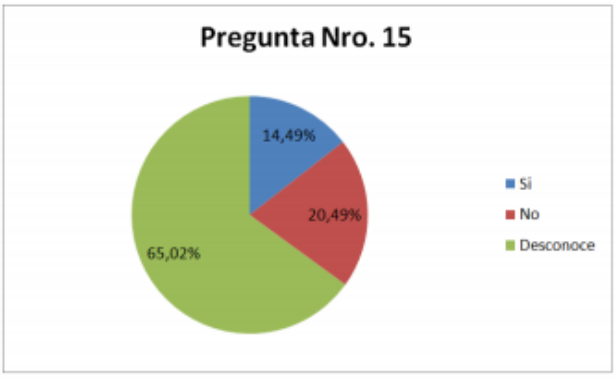

Figura 4.15: Procedimientos de Respaldo (Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 85,51% indica que no existen o desconocen completamente si existen procedimientos de respaldo y recuperación de la información manejada.

Interpretación: La gran mayoría de usuarios encuestados desconoce si existen procedimientos o indica que no existen procedimientos de respaldo y recuperación, afianzando lo indicado, las pobres o inexistentes políticas de socialización de normativas de seguridad, con ello de se puede desprender claramente que se hace necesaria la aplicación de procedimientos que aseguren y garanticen la integridad de los sistemas de información.

16. ¿Cree pertinente contar con un plan de seguridad que le permita resguardar la información de su departamento?

Nro	Ítem	Frecuencia	Porcentaje
1	Si	252	89,05 %
2	No	31	10,95 %
	Total	283	100 %

Tabla 4.16: Frecuencia de la pregunta Nro. 16 (Fuente: Elaboración propia)

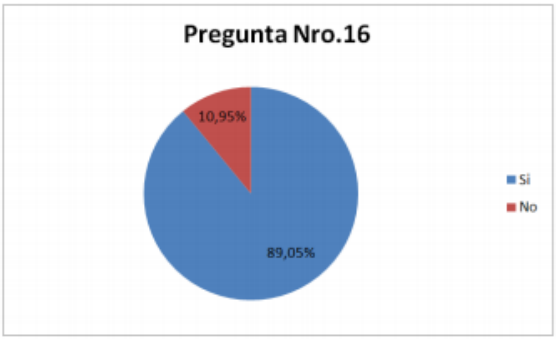

Figura 4.16: Implementación de un Plan de Seguridad (Fuente: Elaboración propia)

Análisis: De los 283 encuestados el 89,05% manifiesta que si se hace necesario contar con un plan de seguridad que permita resguardar la información de su departamento.

Interpretación: La gran mayoría concuerda que es necesario contar con un plan de seguridad formalizado para garantizar la integridad de los sistemas de información, con esto se puede desprender que se hace necesaria la aplicación de una metodología que formalmente socialice y aplique los procedimientos de seguridad necesarios que permitan contar con información integra y libre amenazas. Esta metodología permitirá la aplicación de procedimientos y normas de seguridad garantizados y probados en otros sistemas de información existentes.

4.2 Interpretación de datos

Se ha tomado en cuenta las dos preguntas discriminantes, la número 3 y número 4 de la encuesta aplicada, con los siguientes resultados arrojados.

Pregunta 3. ¿Los equipos y sistemas informáticos que usted utiliza han sufrido fallas de seguridad?

Resumen: Casi el 80% indica que han sufrido fallas de seguridad en sus sistemas informáticos con estos ataques que se han producido los sistemas se han vuelto vulnerables ocasionando pérdidas de información, esto ratifica la necesidad de salvaguardar de mejor manera la información y los servicios mediante procedimientos estandarizados.

Interpretación: según el administrador de sistemas de la facultad los sistemas de información son vulnerables a una gran variedad de ataques a pesar que poseen ciertas seguridades propias por eso se desea buscar procedimientos para evitar la pérdida de información y la funcionalidad de sus servicios sea eficaz.

Pregunta 4. ¿Los equipos y sistemas informáticos de la Facultad han sufrido algún ataque informático (virus, hacker, desastres naturales, otro tipo)?

Resumen: De igual manera más del 50% de los equipos de la facultad han sufrido algún ataque por terceras personas lo que ha provocado la manipulación de la información, reafirmando la tesis de la necesidad de contar con procedimientos adecuados y formales para la protección de la información.

4.3 Verificación de la hipótesis

La hipótesis es:

El análisis de riesgos informáticos mejorará la seguridad e integridad de la información en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato.

Las preguntas discriminantes indican que los equipos informáticos han sufrido fallas y ataques, esto debido a que no existen políticas formales de seguridad que permitan encaminar acciones tendientes a minimizar y de ser posible erradicar estas amenazas y por consiguiente la pérdida de la información, el análisis de riesgos permitirá determinar las amenazas inmediatas y los riesgos más frecuentes a los que están sometidos los equipos y la información, esto ayudará a encaminar acciones tendientes a minimizar los mismos y mediante la formalización de dichas políticas y acciones, tener continuamente la verificación y prevención de las amenazas y riesgos que puedan ocurrir.

CAPITULO V

Conclusiones y Recomendaciones

5.1 Conclusiones

Si bien los usuarios se sienten capacitados para el manejo de los sistemas de información de la facultad manifiestan que los equipos informáticos no están acordes con las necesidades y requerimientos que ellos tienen para el desarrollo adecuado de su trabajo.

Los equipos y la información han sido víctimas de ataques que en mayor o menor medida han afectado a la información que manejan llegando inclusive a la perdida por robo de la misma, esto hace ver claramente que las medidas de seguridad con que se cuentan no están acordes a las necesidades y requerimientos poniendo en peligro la integridad y veracidad de la información.

Se sabe los controles de seguridad que existen en los equipos, pero saben parcialmente o desconocen sobre un plan de seguridad sobre los sistemas, esto indica que si bien pueden identificar los programas de protección como los antivirus no tienen muy claro si existe o no planes de seguridad que se ejecuten en la entidad.

No se cuenta con capacitación en seguridades de los sistemas y además se desconoce las políticas de seguridad sobre los sistemas y equipos lo que da claramente la idea de una falta de una adecuada socialización y ejecución de políticas de seguridad.

El respaldo de la información es escaso y muchas veces inexistente, además la información respaldada no se almacena en un lugar seguro fuera de los departamentos, esto permite concluir que no existen políticas formales de seguridad de información que los usuarios ejecuten.

Existe desconocimiento de se ejecutan procedimientos de respaldo y recuperación, la carencia de esta política de seguridad hace que la integridad de la información corra riesgos de pérdida y sustracción de la misma.

Los procedimientos de seguridad de los sistemas de información que maneja la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato, son incipientes y en otros casos no existen, lo que genera la posibilidad de que los riesgos y amenazas se

ejecuten causando un gran prejuicio a la entidad, ya que tanto la información como los equipos están expuestos a desastres naturales, virus, ataque de hackes, maleware, etc.

Se hace necesario contar con una metodología que permita la salvaguarda de la información con procedimientos formales y concretos que garanticen la integridad de los equipos y la información.

5.2 Recomendaciones

Se recomienda realizar una evaluación previa de los equipos tecnológicos que manejan los sistemas de información para determinar si son los más adecuados para el desarrollo del trabajo de cada área de la dependencia en estudio, con ello se garantizará que se cuenta con la tecnología adecuada que permita un manejo óptimo de la información.

Se deben mejorar los procedimientos y en algunos casos crearlos para mejorar la seguridad de equipos e información, todo esto complementado con una buena capacitación y concientización de los usuarios de cada una de las áreas donde se mantiene la información.

Realizar capacitaciones permanentes a todos los usuarios de los sistemas de información con que cuenta la facultad para que el manejo de los equipos y recursos que formanparte de la infraestructura tecnológica tengan un uso y manejo apropiado ya que de esta manera se logrará mitigar los riesgos y amenazas a los que están expuesto los sistemas.

Implementar un antivirus corporativo en los equipos de la organización permitiendo con esto minimizar los riesgos de ataque de software malicioso garantizando la integridad de la información ante este tipo de ataques.

Se recomienda jerarquizar las amenazas de tal manera que al diseñar la metodología de análisis y gestión de riesgos se tome en cuenta esta categorización al momento de definir las acciones prioritarias a realizar para dar cumplimiento a la metodología.

Implementar los procedimientos necesarios en los equipos y sistemas de información que se sustentaran en un análisis de criticidad que permitan priorizar las salvaguardas que se implementarán con el propósito de garantizar en un alto porcentaje la integridad de los equipos e información.

Se hace necesaria la implementación de una Metodología de Análisis y Gestión de Riesgos Informáticos, que ayudará a contar con procedimientos programados, concretos

y adecuados para que tanto equipos como información tengan un alto grado de seguridad y de esta manera enfrentar los nuevas amenazas que van apareciendo día a día en el quehacer informático.

La metodología a implementar deberá tener en cuenta las características propias de la organización, los sistemas con que se cuenta, el nivel de experticia de los usuarios en el manejo del sistema, para garantizar que los procedimientos seleccionados cumplan con el cometido de garantizar la salvaguarda adecuada de todos los datos e información.

CAPITULO VI

Propuesta

6.1 Datos informativos

6.1.1 Título

"Selección de una metodología de Análisis de Riesgos Informáticos que permita tener un alto grado de seguridad e integridad de la información en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato"

6.1.2 Institución

Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato.

6.1.3 Director de Tesis

Ing. Mg. David Guevara

6.1.4 Beneficiario

Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato.

6.1.5 Ubicación

Av. Los Chasquis y Río Cutuchi

6.1.6 Tiempo Estimado

Fecha de inicio: Junio de 2013

Fecha de finalización: Noviembre de 2013

6.1.7 Responsables

Maestrante: Ing. Donald Reyes B.

Director: Ing. Mg. David Guevara

6.1.8 Costo

El costo de la propuesta es de: $ 500,00

6.2 Antecedentes de la propuesta

Según Herederos C.(2005) manifiesta que: Los sistemas de información en términos generales se diseñan para gestionar la información y el conocimiento en las organizaciones cuyo objetivo final es el permitir mejorar los procesos empresariales y de esta manera crear valor.

Para Aguilera P.(2009) la seguridad informática es "la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable." Esta definición se complementa con lo expuesto por Areitio J.,(2008) quien plantea que "la meta final de la seguridad es permitir que una organización cumpla con todos sus objetivos de negocio o misión".

La Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato, consiente de la necesidad de salvaguardar la información y datos estudiantes y de profesores deberá establecer estrategias que garanticen un adecuado manejo de los sistemas de información, estableciendo políticas tendientes a garantizar la integridad y seguridad de los datos e información.

El establecimiento de una metodología de análisis y gestión de riesgos informáticos permitirá controlar los sistemas informáticos, evaluando los riesgos existentes y detectando las amenazas en sus diferentes niveles, lo que generará un ambiente de confianza con salvaguardas de información acordes a la realidad y características institucionales.

6.3 Justificación

La disponibilidad en seguridad informática se refiere al grado en que la información esté en el lugar, momento y forma cuando es requerido por un usuario autorizado, lo cual está asociado directamente a la confiabilidad técnica de los componentes de un sistema de información, tal como lo plantea Aguilera P. (2009).

La confidencialidad se refiere al hecho de que la información está únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada, tal como lo plantea Aguilera P. (2009).

Para Mora H.,(2009) una amenaza es un conjunto de situaciones o acontecimientos que puede afectar y hacer variar la cualidad benéfica de los sistemas de información.

Mora H., (2009) determina el riesgo como la probabilidad de que un bien pueda sufrir un daño y por lo tanto se puede cuantificar como alto, medio o bajo.

Por otro lado la ISO 27002:2005 16 plantea que el riesgo es la combinación de la probabilidad de un evento y sus posibles consecuencias, esta definición es la que se tomó en cuenta para el desarrollo del presente proyecto.

Por todo lo indicado podemos decir que la ausencia de salvaguardas y cronogramas de mantenimiento a los sistemas hace que la información y los datos sean vulnerables a riesgos y amenazas que día a día se vuelven más sofisticas y peligrosas para la integridad y seguridad de los datos.

Se pretende hacer un análisis de las metodologías de análisis y gestión de riesgos MAGERIT y OCTAVE, las cuales son las más conocidas y aplicadas sin dejar de lado el mérito de otras metodologías que se aplican en diversos países del mundo.

Estas metodologías tienen permiten principalmente:

1. Identificación de activos, incluidos los sistemas de información.

2. Identificación y priorización de amenazas.

3. Estimación del impacto de cada amenaza.

4. Desarrollo de tablas descriptivas de los riesgos.

Todas estas acciones se hacen necesarias para garantizar un alto índice de seguridad de la información.

6.4 Objetivos

6.4.1 Objetivo General

Identificar una metodología de Análisis de Riesgos Informáticos que permita tener un alto grado de seguridad e integridad de la información en la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato.

6.4.2 Objetivos específicos

- Determinar las características de los sistemas informáticos de la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato y establecer los niveles de seguridad e integridad de los datos.
- Contrastar las metodologías OCTAVE y MAGERIT, para el análisis y gestión de riesgos informáticos.
- Aplicar la metodología de análisis y gestión de riesgos informáticos que mejor se ajuste a la realidad de la institución y especificar los procedimientos a llevar a cabo para minimizar las amenazas.

6.5 Análisis de factibilidad

Factibilidad Económica

El proyecto de implementación de una metodología de análisis y gestión de riesgos informáticos en la Facultad de Ingeniería Civil y Mecánica se hace factible ya que se fundamentará en metodologías libres y permitirá salvaguardar los datos de una manera más adecuada mejorando la seguridad y apoyando a una adecuada gestión de esta dependencia universitaria.

Factibilidad Socio cultural

Las buenas prácticas informáticas acompañadas de una metodología adecuada de análisis y gestión de riesgos informáticos permitirán minimizar los riesgos de pérdida y alteración de la información y los datos ya que las personas encargadas de manejar los sistemas tomarán conciencia de los peligros existentes, de esta manera habrá un ambiente más confiable en el manejo de la información.

Factibilidad Política

El desarrollo e implementación de una metodología de análisis y gestión de riesgos informáticos generará adecuadas políticas de uso y manejo tanto de equipos e información que serán conocidas y acatadas por todo el personal que labora en las diferentes dependencias de la facultad.

Factibilidad Medio Ambiental

La metodología propende a la salvaguarda de los datos, el uso y protección de computadores y demás aparatos tecnológicos aplicando acciones de manera tal que no representen un peligro para el medio ambiente que rodea a los mismos y a las personas encargadas de su manipulación.

Factibilidad Tecnológica

La metodología a desarrollar tendrá en cuenta la tecnología necesaria para el desarrollo de habilidades informáticas de seguridad que comprometa a directivos, personal administrativo, docentes y estudiantes, así como también un adecuado manejo de los datos y la información por parte de la comunidad universitaria de la Facultad de Ingeniería Civil y Mecánica.

Factibilidad Legal

El desarrollo de la metodología, el manejo y uso tanto de datos, información y sistemas de gestión de la información se lo realiza bajo normas, procedimientos y leyes que rigen los aspectos informáticos de nuestro país en general y de la Universidad ecuatoriana en particular.

Factibilidad Operativa

Las características de los sistemas y la predisposición de las personas para proteger de mejor manera la información y los datos, hace que la aplicación de una metodología de análisis y gestión de riesgos en la Facultad de Ingeniería Civil y Mecánica sea factible y su operatividad inmediata mejorará las seguridades de los sistemas informáticos.

6.6 Fundamentación

La necesidad de salvaguardar los datos e integridad de la información hace necesaria la aplicación de una metodología de análisis y gestión de riesgos informáticos por lo cual se procedió a contrastar dos Metodologías de Análisis y Gestión de Riesgos Informáticos así, se analizó la Metodología de Análisis y Gestión de Riesgos de tecnologías de la información (MAGERIT) y la OperationallyCriticalThreat, Asset, and VulnerabilityEvaluation (OCTAVE), las dos metodologías presentan un conjunto de pasos, procedimientos y acciones bien formuladas y fundamentadas que permiten la salvaguarda adecuada de los datos de organizaciones cuyo activo fundamental es la

información que maneja para una toma de decisiones adecuada y a tiempo. Estas características han hecho que su tratamiento y análisis permitan la selección de una de ellas para ser aplicada en la Facultad de Ingeniería Civil y Mecánica d la Universidad Técnica de Ambato, teniendo en cuenta todos los aspectos relevantes de los sistemas informáticos de la misma.

6.6.1 Metodología OCTAVE

La metodología OCTAVE, acrónimo de OperationallyCriticalThreat, Asset, and VulnerabilityEvaluation creada por la organización CERT

Según la guía de OCTAVE proporcionada por el CERT, OCTAVE es una valoración estratégica de los activos basada en riesgos y una técnica de planificación para la seguridad, es auto-dirigida, lo que hace que las personas de una organización asuman responsabilidades para establecer las estrategias de seguridad organizacionales.

La técnica hace hincapié en el conocimiento que tienen las personas de una organización de sus prácticas y procesos organizacionales relacionados a la seguridad, para de este modo capturar su estado actual dentro de la organización.

Los riesgos a los activos más críticos son utilizados para priorizar áreas de mejoramiento y establecer la estrategia de seguridad para la organización.

Por el contrario, la valoración del enfoque tecnológico, apuntada al riesgo tecnológico en problemas tácticos.

La metodología OCTAVE es designada al riesgo organizacional y enfocada en problemas relacionados con la práctica. Es una evaluación flexible que puede ser personalizada para la mayoría de las organizaciones.

Cuando se aplica OCTAVE, un pequeño equipo de personas de la unidad operacional o de negocios y del departamento de TI, trabajan juntos para dirigir las necesidades de seguridad de la organización, balanceando los tres aspectos fundamentales: Riesgo operacional, Prácticas de seguridad y Tecnología, como lo muestra la figura 6.1.

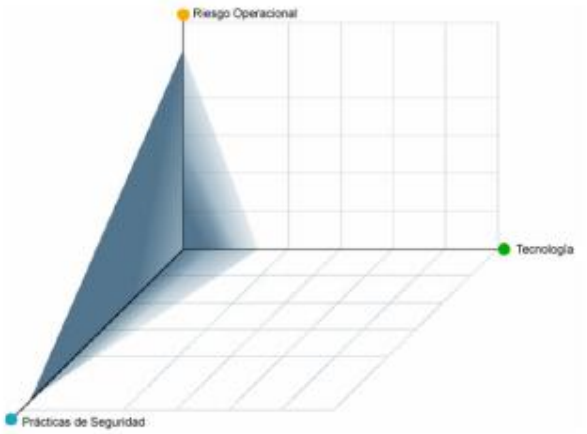

Figura 6.1: Balance de la Metodología OCTAVE (Fuente:Introduction to the OCTAVE® Approach)

OCTAVE está enfocada en dos de aspectos:

• Riesgo Operacional y

• Prácticas de Seguridad.

La Tecnología es examinada solo en relación a las prácticas de seguridad, permitiendo a la organización refinar las prácticas de seguridad actuales. OCTAVE facilita a la organización realizar decisiones de protección de la información basadas sobre riesgos a la confidencialidad, integridad y disponibilidad de activos críticos relacionados a la información.

Todos los aspectos del riesgo (activos, amenazas, vulnerabilidades e impacto organizacional) son factorizados dentro de la toma de decisiones.

6.6.1.1 Fases de la metodología OCTAVE

La metodología OCTAVE utiliza un enfoque en 3 fases para examinar las cuestiones y aspectos de la organización, su tecnología y necesidades de seguridad de la información, estas fases son:

FASE I.- Está orientada a la identificación de los elementos críticos de la organización y las amenazas sobre los activos.

FASE II.- Trata de identificar todas y cada una de las vulnerabilidades tecnológicas y organizativas, que son aquellas que exponen las amenazas creando un riesgo para la organización.

FASE III. Se desarrolla una mitigación y estrategia contra los riesgos.

Todas las actividades se apoyan en un catálogo de buenas prácticas, encuestas, hojas de trabajo que permiten captar información relevante.

La metodología ofrece una guía de implementación donde se especifica las cuestiones necesarias para la evaluación de la organización. Además se incluyen procesos detallados, hojas de trabajo y las instrucciones para realizar cada paso en el método, también material de apoyo y orientaciones para la adaptación.

Como una variante de la metodología OCTAVE se presenta la metodología OCTAVE-S que es un enfoque particular desarrollado para organizaciones pequeñas, en esta se deben tener en cuenta dos aspectos principales:

1. Se requiere de un equipo de 3 a 5 personas, que entiendan el alcance y la profundidad de la empresa u organización

2. Una exploración limitada de la infraestructura informática.

Las características de esta metodología las podemos resumir en las siguientes:

Es auto dirigida, y cuenta con pequeños equipos de personal de la organización que pueden realizar taller para analizar problemas y riesgos de las tecnologías de la información, para hacer frente a las necesidades de seguridad de la información.

6.6.2 Metodología OCTAVE-S

OperationallyCriticalThreat, Asset, and VulnerabilityEvaluationfor Small Organizations (OCTAVE-S) fue desarrollado en respuesta a las necesidades de organizaciones pequeñas. Sigue el mismo criterio que se describe en la metodología OCTAVE, siendo adaptado a las características únicas de organizaciones pequeñas. OCTAVE-S utiliza procesos más dinámicos y hojas de trabajo diferentes, pero produce la misma clase de efectos.

Se tienen las siguientes diferencias principales en relación a la metodología OCTAVE:

1. OCTAVE-S requiere de un grupo pequeño de 3 a 5 personas quienes entienden la amplitud y profundidad de la organización.

2. No incluye talleres de conocimiento formales al inicio para conseguir información sobre los activos importantes, requerimientos de seguridad, amenazas y prácticas de seguridad.

3. OCTAVE-S incluye solo una exploración limitada de la infraestructura computacional.

Esta metodología consta fundamentalmente de dos partes:

1. Identificar el perfil de riesgo, con las amenazas y vulnerabilidades que se relacionan directamente con los activos críticos desde el punto de vista organizacional y tecnológico.

2. Análisis del riesgo identificado como resultado del proceso anterior para un posterior desarrollo de estrategias y un plan de mitigación.

El proceso como tal comienza con una fase de preparación para constituir un equipo de análisis y comenzar con las entrevistas iniciales. Una vez constituido este grupo de personas, se ejecutan varios talleres de trabajo para identificar el perfil de amenaza de los activos críticos desde los puntos de vista organizacional (fase 1) y tecnológico (fase 2). Luego el equipo desarrolla las estrategias y planes de mitigación (fase 3) basándose en el análisis de riesgos que quedó como producto del proceso anterior.

6.6.2.1 Fases de la metodología

Al igual que la metodología OCTAVE, la metodología OCTAVE-S consta de tres fases que son:

Figura 6.2: Proceso de OCTAVE-S (Fuente: Alberts, 2003)

Fase 1: Construcción del perfil de amenaza basado en los activos,

Esta fase realiza una evaluación de los aspectos organizacionales, el equipo de análisis define el criterio de evaluación de impacto que será utilizado más adelante para evaluar los riesgos. También identifica los activos organizacionales importantes y evalúa las prácticas de seguridad actuales de la organización. El equipo completa todas las tareas por sí mismo, recolectando información adicional cuando es necesaria. Entonces se seleccionan de tres a cinco activos críticos para analizar en profundidad, basándose en la importancia relativa de estos para la organización. Finalmente el equipo define requerimientos de seguridad y define un perfil de amenaza para cada activo crítico. Como se muestra en la tabla 6.1

Fase	Proceso	Actividad
F1: Construcción de un perfil de amenazas bassado en los activos	P1: Identificar la información organiacional	A1.1: Establecer el criterio de evaluación de impacto
		A1.2: Identificar activos organizacionles
		A1.3: Evaluar las prácticas de seguridad organizacionales
	P2: Crear perfiles de amenaza	A2.1: Seleccionar activos críticos
		A2.2: Identificar requerimientos de seguridad para activos
		A2.3: Analizar los procesos relacionados con la tecnología

Tabla 6.1: Procesos y actividades de la fase 1.(Fuente: OCTAVE®-S Implementation Guide)

Fase 2: Identificar vulnerabilidades de infraestructura

En esta fase, se realiza una revisión de alto nivel de la infraestructura computacional, enfocándose sobre la magnitud de la seguridad considerada por el personal responsable de la infraestructura. El equipo primero analiza cómo la gente utiliza la infraestructura computacional para acceder a los activos críticos, produciendo clases de componentes clave, así como quién es responsable de configurar y dar mantenimiento a tales componentes.

El equipo de análisis examina hasta qué punto cada parte responsable incluye seguridad en sus prácticas y procesos de TI. (Ver Cuadro 6.2)

Fase	Proceso	Actividad
F2: Identificar vulnerabilidades de infraestructura	P3: Examinar infraestructura computacional en relación con los activos críticos	A3.1:Examinar rutas de acceso
		A3.2:Analizar procesos relacionados con tecnología.

Tabla 6.2: Procesos y actividades fase 2.(Fuente: OCTAVE®-S Implementation Guide)

Fase 3: Desarrollo de planes y estrategias de seguridad En esta fase,

Se identifican los riesgos a los que están expuestos los activos críticos de la organización y decide qué hacer con ellos. Basados en un análisis de la información recogida, el equipo crea una estrategia de protección para la organización y planes de mitigación para enfrentar los riesgos a los activos críticos. Las hojas de trabajo de la metodología OCTAVE-S utilizadas durante la fase 3 son altamente estructuradas y firmemente enlazadas al catálogo de prácticas de OCTAVE, permitiendo al equipo relacionar sus recomendaciones para el mejoramiento a una referencia aceptada de prácticas de seguridad. Como se muestra en la tabla 6.3

Fase	Proceso	Actividad
F3: Desarrollo de planes y estrategias de seguridad	P4: Identificar y analizar los riesgos	A4.1: Dvaluar impactos de amenazas
		A4.2: Establecer criterios de evaluación probabilística
		A4.3: Evaluar probabilidades de amenazas.
	P5: Desarrollo de estrategías de protección y planes de mitigación	A5.1: Describir las estrategías de protección actuales
		A5.2: Seleccionar aproximaciones de mitigación
		A5.3: Desarrollo de planes de mitigación de riesgo
		A5.4: Identificar cambios para las estrategias de protección
		A5.5: Identificar los siguientes pasos a seguir

Tabla 6.3: Procesos y actividades fase 3.(Fuente: OCTAVE®-S Implementation Guide)

6.6.2.2 Resultados de la metodología OCTAVE-S

La administración de los riesgos asociados a las TI requiere de un balance entre actividades reactivas y proactivas. Durante una evaluación con OCTAVE-S, el equipo de análisis mira la seguridad desde diferentes perspectivas, asegurando que las recomendaciones alcanzan el balance apropiado sobre las necesidades de la organización.

Cuando se formulan recomendaciones para mejorar las prácticas de seguridades organizacionales, el equipo asume un punto de vista proactivo, analizando los problemas desde las perspectivas organizacionales y específicas de cada activo.

En cualquier momento durante la evaluación, el equipo podría también tomar una posición más reactiva identificando elementos de acción pensados para enfrentar debilidades específicas. Estos elementos de acción, son considerados para ser más reactivos en carácter porque a menudo llenan un vacío en lugar de mejorar las prácticas de seguridad organizacionales.

Los resultados de la metodología OCTAVE-S incluyen:

1. Una estrategia de protección para toda la organización – La estrategia de protección perfila la dirección de la organización con respecto a sus prácticas de seguridad de la información

2. Planes de mitigación de riesgos – Estos planes están pensados para mitigar los riesgos a los activos críticos por el mejoramiento de prácticas de seguridad seleccionadas.

3. Listas de acción – Estas incluyen elementos de acción de corto plazo necesitados para enfrentar debilidades específicas.

4. Un listado de activos de información importantes que soportan los objetivos organizacionales y las metas.

5. Un panorama de los resultados mostrando la magnitud para la cual la organización está siguiendo buenas prácticas de seguridad.

6. Un perfil de riesgo para cada activo crítico describiendo un rango de riesgos para tal activo.

Cada fase de la metodología OCTAVE-S produce resultados utilizables, incluso una evaluación parcial producirá información útil para mejorar la postura organizacional de seguridad.

6.6.3 Metodología MAGERIT

Acrónimo de Metodología de Análisis y Gestión de Riesgos de Sistemas de la información, que según el Consejo Superior de Administración Electrónica España (CSAE) indica que ha elaborado y promueve MAGERIT como respuesta a la percepción de que la Administración (y en general toda la sociedad) depende de forma creciente de las tecnologías de la información para la consecución de sus objetivos. El uso de tecnologías de la información y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios. (Ver figura 6.3)

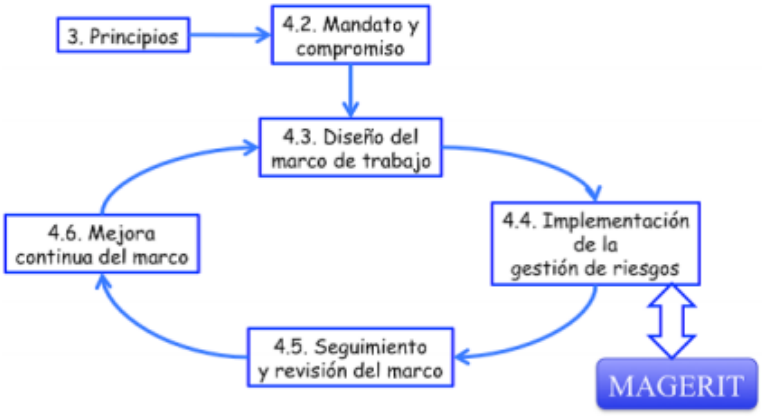

Figura 6.3: ISO 31000 - Marco de trabajo para la gestión de riesgos

En forma general MAGERIT cubre las siguientes actividades:

1. Determinar los activos relevantes para la organización, su interrelación y su valor.

2. Determinar las amenazas que están expuestos los activos.

3. Determinar las salvaguardas posibles y su eficacia.

4. Estimar el impacto

5. Estimar el riesgo

6. Selección de salvaguardas

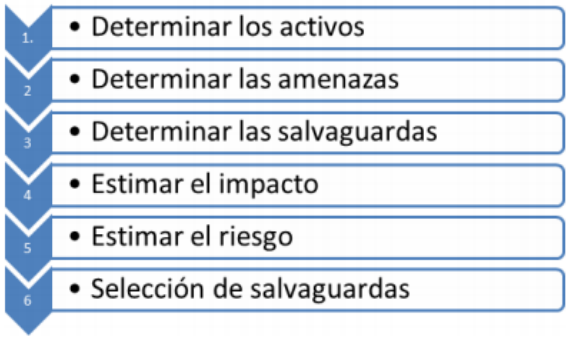

Figura 6.4: Actividades de la metodología MAGERIT (Fuente: Elaboración propia)

Todas estas actividades MEGARIT las divide en etapas que son:

1. Método de análisis de riesgos

2. Proyecto de análisis de riesgos

3. Plan de seguridad

Figura 6.5: Etapas de la Metodología MEGARIT (Fuente: Elaboración propia)

La metodología recoge lo de las Guías de la OCDE para la seguridad de los sistemas de información y redes que, en su principio 6 dice:

6) Evaluación del riesgo. Los participantes deben llevar a cabo evaluaciones de riesgo.

La metodología es relevante para todos aquellos que trabajan con información automatizada y los sistemas informáticos que la tratan. Si dicha información o los servicios que se prestan gracias a ella son valiosos, esta metodología les permitirá saber cuánto de este valor está en juego y les ayudará a protegerlo.

Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos, esta es la razón por la que han aparecido un sinnúmero de guías para la gestión del riesgo, manuales y metodologías tanto libres como de paga que buscan mitigar y controlar todas las amenazas que van apareciendo.

Objetivos de la metodología MAGERIT

MAGERIT persigue los siguientes objetivos:

Directos:

1. Concienciar 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 comunicaciones (TIC).

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, auditoría, certificación o acreditación, según corresponda en cada caso.

Se busca además la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos, estos son:

Modelo de valor

Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

Mapa de riesgos

Relación de las amenazas a que están expuestos los activos.

Declaración de aplicabilidad

Para un conjunto de salvaguardas, se indica si son de aplicación en el sistema de información bajo estudio o si, por el contrario, carecen de sentido.

Evaluación de salvaguardas

Evaluación de la eficacia de las salvaguardas existentes 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 salvaguardas desplegadas.

Informe de insuficiencias

Ausencia o debilidad de las salvaguardas 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 normativa correspondiente.

Plan de seguridad

Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos.

Análisis y gestión de riesgos en MAGERIT

El objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

Disponibilidad:

Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Integridad:

Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad:

Que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos. A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que nos acerquen a la percepción de los usuarios de los sistemas de información:

Autenticidad:

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

Trazabilidad:

Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad. Todas estas características pueden ser requeridas o no dependiendo de cada caso. Cuando se requieren, no es evidente que se disfruten sin más. Lo habitual que haya que poner medios y esfuerzo para conseguirlas. A racionalizar este esfuerzo se dedican las metodologías de análisis y gestión de riesgos que comienzan con una definición:

Riesgo:

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es im-portante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema:

Tratamiento de los riesgos

Proceso destinado a modificar el riesgo.

Es por ello que se requiere la creación de una "cultura de seguridad" que, emanando de la alta dirección, conciencie a todos los involucrados de su necesidad y pertinencia.

Contexto del análisis y gestión de riesgos

Las tareas de análisis y gestión de riesgos no son un fin en sí mismas sino que se encajan en la actividad continua de gestión de la seguridad.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que se acepta la Dirección.

La implantación de las medidas de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con el sistema de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y

de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

Este esquema de trabajo debe ser repetitivo pues los sistemas de información rara vez son inmutables; más bien se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto.

Aquí se deben abarcar dos aspectos fundamentales que son:

A1. Concienciación y formación

A2. Incidencias y recuperación

A1. Concienciación y formación

El mejor plan de seguridad se vería seriamente hipotecado sin una colaboración activa de las personas involucradas en el sistema de información, especialmente si la actitud es negativa, contraria a las medidas o pasarse luchando contra medidas que consideran absurdas. Por esta razón se requiere la creación de una "CULTURA DE SEGURIDAD" que, emanando de la alta dirección, conciencie a todos los involucrados de su necesidad y pertinencia.

Son dos los pilares fundamentales para la creación de esta cultura:

1. Una política de seguridad corporativa que se entienda (escrita para los que no son expertos en la materia), que se difunda y que se actualice continuamente.

2. Una normativa de seguridad que, entrando en áreas específicas de actividad, aclare la postura de la Organización; es decir, defina lo que es uso correcto y lo que es incumplimiento.

3. Una formación continua a todos los niveles, recordando las cautelas rutinarias y las actividades especializadas, según la responsabilidad adscrita a cada puesto de trabajo

A fin de que estas actividades cuajen en la organización, es imprescindible que la seguridad sea:

1. Mínimamente intrusiva: que no dificulte innecesariamente la actividad diaria ni hipoteque alcanzar los objetivos de productividad propuestos,

2. Sea “natural”: que no dé pie a errores gratuitos, que facilite el cumplimiento de las buenas prácticas propuestas y

3. Practicada por la Dirección que de ejemplo en la actividad diaria y reaccione con presteza a los cambios e incidencias.

A2. Incidencias y recuperación

Las personas involucradas en la utilización y operación deben ser conscientes de su papel y relevancia continua para prevenir problemas y reaccionar cuando se produzcan. Es importante crear una “CULTURA DE RESPONSABILIDAD” donde los potenciales problemas, detectados por los que están cercanos a los activos afectados, puedan ser canalizados hacia los puntos de decisión. De esta forma el sistema de seguridad responderá con presteza a cada circunstancia.

Cuando se produce una incidencia, el tiempo empieza a correr en contra del sistema: su supervivencia depende de la agilidad y corrección de las actividades de reporte y reacción. Cualquier error, imprecisión o ambigüedad en estos momentos críticos, se ve amplificado convirtiendo lo que podía ser un mero incidente en un desastre.

Conviene aprender continuamente tanto de los éxitos como de los fracasos e incorporar estos aprendizajes al proceso de gestión de riesgos. La madurez de una organización se refleja en la pulcritud y realismo de su modelo de valor y, consecuentemente, en la idoneidad de las salvaguardas de todo tipo, desde medidas técnicas hasta una óptima organización.

Realización del análisis y gestión de riesgos

El análisis y gestión de riesgos basa su accionar en dos grandes tareas a realizar que son:

I. Análisis de riesgos

Permite determinar qué tiene la Organización y estimar lo que podría pasar.

Los elementos involucrados son:

1. Activos, que no son sino los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización.

2. Amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización.

3. Salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

1. El impacto: lo que podría pasar

2. El riesgo: lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento.

II. Tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

La gestión de riesgos involucra tanto el análisis así como el tratamiento de los riesgos.

A. Método de análisis de riesgos

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

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.

2. Determinar a qué amenazas están expuestos aquellos activos.

3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectación de materialización) de la amenaza.

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

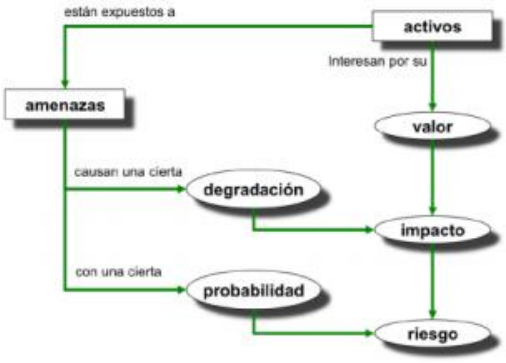

Figura 6.6: Elementos del análisis de riesgos potenciales Fuente: MAGERIT, 2012

Paso 1: Activos

Se pueden definir como los componentes o funcionalidades de un sistema de información susceptible de ser atacado deliberada o accidentalmente.

Dentro de un sistema de información tenemos dos cosas esenciales: la información que maneja y los servicios que presta.

En este paso se debe determinar los activos por dependencias y realizar una codificación de los mismos ubicándolos en dos categorías activos informáticos y no informáticos.

Subordinados a estos se pueden identificar otros activos relevantes:

- Los datos que materializan la información
- Los servicios auxiliares que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.
- Como no todos los activos son de la misma especie tanto las amenazas como las salvaguardas son diferentes.

Dependencias

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

De aquí se desprende el concepto de "dependencias entre activos" o la medida en que un activo superior se vería afectado por un incidente de seguridad del activo del que depende.

Aquí se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. Dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior.

De aquí que podemos colegir que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

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

- Capa 1: el ambiente o entorno
- Capa 2: el sistema de información
- Capa 3: la información y servicios
- Capa 4: Misión y visión de la Organización
- Capa 5: Otros activos (escalafón a nivel de carreras)

Valoración

En la valoración se debe tomar en cuenta los activos desde el punto de vista de utilidad para el sistema, es decir el valor viene dado por el aporte hacia la organización no por su costo monetario.

Si algo no vale para nada, debe prescíndase de ello. Si no se puede prescindir de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger. El valor puede ser propio, o puede ser acumulado. Se dice que los activos

inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

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

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

Dimensiones

La valoración de los activos debe tener en cuenta:

- Confidencialidad: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
- Autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
- Integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
- Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.
- Trazabilidad: (acceso a servicios) ¿qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?
- Trazabilidad: (acceso a los datos) ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Como se puede observar en la metodología se ha introducido el concepto de trazabilidad (accountability) tanto de datos como de servicios, que en conjunto con la autenticidad a efectos técnicos se traduce en mantener la integridad y confidencialidad de ciertos activos del sistema como ficheros que contengan información de carácter personal.

La valoración debe iniciar por los activos superiores, los que son importantes por si mismos. Por el árbol de dependencias automáticamente el valor se acumulará a los activos inferiores, que adicionalmente tendrán su propia valoración posterior.

Dimensiones de interés

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

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

La valoración puede ser cuantitativa o cualitativa. Los criterios más importantes son:

- La homogeneidad: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra
- La relatividad: es importante poder relativizar el valor de un activo en comparación con otros activos

Todos estos criterios se satisfacen con valoraciones económicas (requerido para “curar” el activo) y es frecuente la tentación de ponerle precio a todo.

Incluso se puede ponerle precio a los aspectos más tangibles (equipamiento, horas de trabajo, etc.); pero al entrar en valoraciones más abstractas (intangibles como la

credibilidad de la Organización) la valoración económica exacta puede ser escurridiza y motivo de agrias disputas entre expertos.

Paso 2: Amenazas

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

Las amenazas a considerar son:

- Naturales.- Dentro de estas tenemos erupciones volcánicas, terremotos, inundaciones, etc.
- Industriales.- Desastres industriales como contaminaciones, fallos eléctricos, etc.

Ante estos los sistemas de información son víctimas pasivas; pero no por ser pasivos hay que permanecer indefensos.

- Defecto de las aplicaciones.- Ya sea por su diseño o por su implementación, se denominan vulnerabilidades técnicas.
- Personales.- ya sea errores, o bien ataques intencionados.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

Valoración de las amenazas

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

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

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

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

La degradación se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto "totalmente degradado", o

“degradado en una pequeña fracción”. Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La frecuencia de ocurrencia se puede cuantificar numéricamente, utilizando como medida de tiempo un año como referencia, como se puede observar en el cuadro 6.4

Valor	Ocurrencia	Tiempo
100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco Frecuente	Cada varios años

Tabla 6.4: Probabilidad de ocurrencia Fuente: MAGERIT, 2012

Paso 3: Determinación del impacto

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

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema de información se centre en la información que maneja y los servicios que presta, pero las amenazas suelen materializarse en los medios.

Impacto acumulado

Es el calculado sobre un activo teniendo en cuenta:

- Su valor acumulado (el propio más el acumulado de los activos que dependen de él)
- Las amenazas a que está expuesto

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada, teniendo en cuenta 2 aspectos:

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

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

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

Impacto repercutido

Es el calculado sobre un activo teniendo en cuenta

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

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

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

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

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

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

Agregación de valores de impacto

Los párrafos anteriores determinan el impacto que sobre un activo tendría una amenaza en una cierta dimensión. Estos impactos singulares pueden agregarse bajo ciertas condiciones:

- Puede agregarse el impacto repercutido sobre diferentes activos,
- Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún activo superior común,

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

Paso 4: Salvaguardas

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

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

Al diseñar las salvaguardas se debe tener en cuenta:

1. tipo de activos a proteger, pues cada tipo se protege de una forma específica

2. dimensión o dimensiones de seguridad que requieren protección

3. amenazas de las que necesitamos protegernos

4. si existen salvaguardas alternativas

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

Reduciendo la frecuencia de las amenazas. Se llaman salvaguardas preventivas.

Las ideales llegan a impedir completamente que la amenaza se materialice.

Limitando el daño causado. Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta

recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

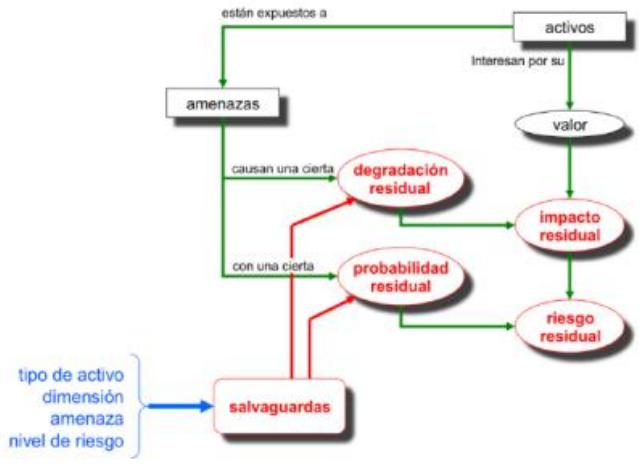

Figura 6.7: Elementos de análisis del riesgo residual. Fuente: MAGERIT, 2012

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar.

Revisión del paso 4: impacto residual

Si se han hecho todos los deberes a la perfección, el impacto residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un impacto residual.

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

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

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

Paso 5: Determinación del riesgo

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia.

El riesgo crece con el impacto y con la frecuencia.

Riesgo acumulado

Es el calculado sobre un activo teniendo en cuenta:

- El impacto acumulado sobre un activo debido a una amenaza y
- La frecuencia de la amenaza

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

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

Riesgo repercutido

Es el calculado sobre un activo teniendo en cuenta

- El impacto repercutido sobre un activo debido a una amenaza y
- La frecuencia de la amenaza

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

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

Agregación de riesgos

Los párrafos anteriores determinan el riesgo que sobre un activo tendría una amenaza en una cierta dimensión.

Estos riesgos singulares pueden agregarse bajo ciertas condiciones:

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

Revisión del paso 5: Riesgo residual

Si se han hecho todos los deberes a la perfección, el riesgo residual debe ser despreciable.

Si hay deberes a medio hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no controlan) entonces se dice que el sistema permanece sometido a un riesgo residual.

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

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

La magnitud de la frecuencia tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real. El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

B. Gestión de Riesgos

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

Si el impacto y el riesgo residuales son despreciables, se ha terminado. Si no, hay que hacer algo.

Paso 1: La interpretación de los valores de impacto y riesgo residuales

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores despreciables. Son pues una métrica de carencias.

Los párrafos siguientes se refieren conjuntamente a impacto y riesgo.

Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer.

Si el valor residual es despreciable, ya está. Esto no quiere decir descuidar la guardia; pero si afrontar el día con cierta confianza.

Mientras el valor residual sea más que despreciable, hay una cierta exposición.

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. Los responsables de la toma de decisiones deberán prestar cuidadosa atención a esta relación de tareas pendientes, que se denomina Informe de Insuficiencias.

Paso 2: Selección de salvaguardas

Las amenazas hay que conjurarlas, por principio y mientras no se justifique lo contrario.

Hay que planificar el conjunto de salvaguardas pertinentes para atajar tanto el impacto como el riesgo, reduciendo bien la degradación del activo (minimizando el daño), bien reduciendo la frecuencia de la amenaza (minimizando sus oportunidades).

Toda amenaza debe ser conjurada profesionalmente, lo que quiere decir que hay que:

1. Establecer una política de la Organización al respecto; o sea, unas directrices generales de quién es responsable de cada cosa

2. Establecer una norma; o sea, unos objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada

3. Establecer unos procedimientos; o sea, instrucciones paso a paso de qué hay que hacer

4. Desplegar salvaguardas técnicas que efectivamente se enfrenten a las amenazas con capacidad para conjurarlas

5. Desplegar controles que permitan saber que todo lo anterior está funcionando según lo previsto

A este conjunto de elementos se le encasilla habitualmente bajo el nombre de Sistema de Gestión de la Seguridad de la Información (SGSI), aunque se está gestionando tanto como actuando.

En la práctica lo dicho se traduce en desarrollar una política, unas normas y unos procedimientos junto con el despliegue de una serie de salvaguardas y controles y, ahora sí, verificar que todas y cada una de las amenazas tienen una respuesta adecuada.

De los puntos anteriores, el más "abierto" es el de determinación de las salvaguardas apropiadas.

Es realmente un arte que requiere personal especializado aunque en la práctica las situaciones más habituales están perfectamente documentadas en la literatura y basta elegir de entre un catálogo en función de la magnitud del riesgo.

Tipos de salvaguardas

Un sistema debe considerar prioritariamente las salvaguardas de tipo preventivo que buscan que la amenaza no ocurra o su daño sea despreciable. Es decir, impedir incidentes o ataques.

En la práctica, no todo es previsible, ni todo lo previsible es económicamente razonable atajarlo en sus orígenes. Tanto para enfrentar lo desconocido como para protegerse de aquello a lo que se permanece expuesto, es necesario disponer de elementos que detecten el inicio de un incidente y permitan reaccionar con presteza impidiendo que se convierta en un desastre.

Tanto las medidas preventivas como las de emergencia admiten una cierta degradación de los activos por lo que habrá que disponer por último de medidas de recuperación que devuelvan el valor perdido por los activos.

Es de sentido común intentar actuar de forma preventiva para que las cosas no puedan ocurrir o no puedan causar mucho daño; pero no siempre es posible y hay que estar preparados para que ocurran. Lo que no debe ser de ninguna manera es que un ataque pase inadvertido: hay que detectarlo, registrarlo y reaccionar primero con un plan de emergencia (que pare y limite el incidente) y después con un plan de continuidad y recuperación para regresar a donde se debe estar.

Por último, hay que recordar que conviene llegar a un cierto equilibrio entre:

- Salvaguardas técnicas: en aplicaciones, equipos y comunicaciones
- Salvaguardas físicas: protegiendo el entorno de trabajo de las personas y los equipos
- Medidas de organización: de prevención y gestión de las incidencias
- Política de personal: que, a fin de cuentas, es el eslabón imprescindible y más delicado, política de contratación, formación permanente, Organización de reporte de incidencias, plan de reacción y medidas disciplinarias.

Fases de un análisis y gestión de riesgos

Las fases donde se sustenta el análisis y gestión de riesgos son:

F1: Planificación

La tabla 6.5 enumera los procesos y actividades a tener en cuenta en la fase de planificación.

Fase	Proceso	Actividad
Fase 1: Planificación	P1.1: Estudio preliminar de oportunidad	A1.1.1: Estudio de oportunidad
		A1.1.2: Fundamentación de la realización.
		A1.1.3: Elaboración del informe preliminar
	P1.2: Determinación del alcance del proyecto	A1.2.1: Definición de objetivos generales
		A1.2.2: Determinación del dominio y límites
		A1.2.3: Elaboración del perfil del proyecto.
	P1.3: Planificación del proyecto	A1.3.1: Evaluar cargas de trabajo
		A1.3.2: Determinar los actores, involucrados y grupos de trabajo
		A1.3.2: Planificar entrevistas
		A1.3.3: Planificar y organizar el trabajo por grupos
	P1.4: Lanzamiento del proyecto	A1.4.1: Adaptar los cuestionarios
		A1.4.2: Elaboración del plan de entrevistas
		A1.4.3: Elaboración del catálogo de activos
		A1.4.4: Socialización de la sensibilización del plan
		A1.4.5: Elaboración de los criterios de valoración
El objetivo principal de esta fase es establecer el marco general de referencia para todo el proyecto.		

Tabla 6.5: Fase de Planificación. Fuente: Elaboración propia

F2: Análisis de riesgos

La tabla 6.6 indica los procesos y actividades que involucra el análisis de riesgos.

Fase	Proceso	Actividad
Fase 2: Análisis de riesgos	P2.1: Caracterización de los activos	A2.1.1: Identificación de los activos
		A2.2.2: Dependencias entre activos
		A2.3.3: Valoración de los activos
	P2.2: Caracterización de las amenazas	A2.2.1: Identificación de las amenazas
		A2.2.2: Valoración de las amenazas
	P2.3: Caracterización de las salvaguardas	A2.3.1: Identificación de las salvaguardas existentes
		A2.3.2: Valoración de las salvaguardas existentes
	P2.4: Estimación del estado del riesgo	A2.4.1: Estimación del impacto
		A2.4.2: Estimación del riesgo
		A2.4.3: Interpretación de los resultados
Documentación final · Modelo de valor.- Informe que detalla los activos · Mapa de riesgos.- Informe que detalla las amenazas significativas. · Evaluación de salvaguardas.- Informe que detalla las salvaguardas · Estado de riesgo.- Informe que detalla para cada activo el impacto y el riesgo. · Informe de insuficiencias.-Informe que detalla las salvaguardas necesarias.		

Tabla 6.6: Fase de Análisis de Riesgos. Fuente: Elaboración propia

F3: Gestión de riesgos

En la tabla 6.7 se puede apreciar los procesos y actividades inmersos en la gestión de los riesgos.

Fase	Proceso	Actividad
Fase 3: Gestión de Riesgos	P3.1: Toma de decisiones	A3.1.1: Calificación de los riesgos
	P3.2: Plan de seguridad de la información	A3.2.1: Programas de seguridad
		A3.2.2: Plan de ejecución
	P3.3: Ejecución del plan	A3.3.1: Ejecución de cada programa de seguridad
	P3.1.1: Toma de decisiones	A3.1.1: Calificación de los riesgos
	P3.2.1: Elaboración del plan seguridad de la información	A3.2.1: Programas de seguridad
		A3.2.2: Plan de ejecución
	P3.3.1: Ejecución del plan	A3.3.1: Ejecución de cada programa de seguridad
Resultados: Documentación por procesos,Calificación de los escenarios de impacto y riesgo, Documentación final, Plan de Seguridad		

Tabla 6.7: Fase de Gestión de Riesgos. Fuente: Elaboración propia

Estas fases no son secuenciales necesariamente, ya que puede haber una retroalimentación entre ellas.

Herramientas de soporte

Según ccn-cert(2011) dice: " Las herramientas 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 de cada activo 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.

PILAR 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 - Código de buenas prácticas para la Gestión de la Seguridad de la Información

· ENS - Esquema Nacional de Seguridad

Herramienta PILAR

El Ministerio de Administraciones Públicas (2005, Pág.130) dice:" PILAR, acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología MAGERIT.

La herramienta está completamente desarrollada en Java, pudiendo emplearse sobre cualquier plataforma que soporte este entorno de programación, sin depender de licencias de productos de terceras partes. El resultado es una aplicación gráfica mono puesto.

La herramienta soporta todas las fases del método MAGERIT:

- Caracterización de los activos: identificación, clasificación, dependencias y valoración
- Caracterización de las amenazas
- Evaluación de las salvaguardas

La herramienta incorpora los catálogos del "Catálogo de Elementos" permitiendo una homogeneidad en los resultados del análisis:

• Tipos de activos

• Dimensiones de valoración

• Criterios de valoración

• Catálogo de amenazas

Para incorporar este catálogo, PILAR diferencia entre el motor de cálculo de riesgos y la biblioteca de elementos, que puede ser reemplazada para seguir el paso de la evolución en el tiempo de los catálogos de elementos.

La herramienta evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de por qué se da cierto impacto o cierto riesgo.

Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Típicamente se puede incorporar el resultado de los diferentes programas de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema.

Los resultados se presentan en varios formatos: informes RTF, gráficas y tablas para incorporar a hojas de cálculo. De esta forma es posible elaborar diferentes tipos de informes y presentaciones de los resultados.

Finalmente podemos indicar que PILAR cuenta con modelos cualitativos y cuantitativos, que se pueden alternar de acuerdo a las necesidades del investigador lo que mejora el análisis del sistema.

7.7 Selección de la mejor metodología

Teniendo en cuenta las características propias de la organización como tamaño, servidores de información con que cuenta la facultad, equipos informáticos, cantidad de personal, entre los más relevantes, podemos hacer la selección de la metodología más adecuada a nuestra organización.

Se han definido los siguientes puntajes:

1. No adecuado

2. Poco adecuado

3. Adecuado

4. Muy adecuado

Criterio	MAGERIT	OCTAVE-S
Tamaño de la organización	2	4
Metodología Auto-dirigida	1	4
Activos d ela organización	2	4
Intervención de expertos	2	2
Medidas adaptables y flexibles	3	4
Enfoque de pocos puntos críticos	3	4
Trabajo en equipos	1	4
Total	14	26

Tabla 6.8: Selección de la metodología. Fuente: Elaboración propia

Como se puede observar si bien MAGERIT puede ser aplicada en la facultad, la que mejor se adapta de acuerdo a las peculiaridades de la organización es la metodología OCTAVE-S.

Por lo indicado se ha escogido la metodología OCTAVE –S por las razones que justifican su aplicación en la Facultad de Ingenieria Civil y Mecánica como son:

- OCTAVE-S fue desarrollado para organizaciones pequeñas con alrededor de 100 personas o menos, se enmarca en la estructura administrativa de la facultad
- Resume la mayoría de las normas y regulaciones sobre seguridad de la información, internacionales como las ISO para seguridad.
- Es auto dirigido ya que recurre al personal de la organización, quienes conocen los problemas que tiene la misma, y puede enfocar el análisis en los puntos más críticos con el fin de no desperdiciar recursos ni tiempo en estudios innecesarios y costosos.
- Es una metodología de evaluación integral que considera el mayor número posible de factores que intervienen en la seguridad.
- OCTAVE-S toma en cuenta los elementos tecnológicos de la seguridad, en relación con la organización, y los puntos más débiles o vulnerables se evalúan en relación con los demás factores que afectan la seguridad de la información.
- OCTAVE permite un acoplamiento mejor dentro de la problemática de las instituciones a las cuales se les aplica la metodología para el análisis de riesgos. En este punto se tiene especial cuidado en el desarrollo de las estrategias y planes de mitigación de riesgos ya que estos se elaboran tomando en cuenta la realidad de la institución y sobre todo se utilizan las habilidades y perspectivas de los integrantes del grupo para solventar y enfrentar las amenazas identificadas a los activos críticos.
- La aplicación de la metodología OCTAVE, al igual que otras metodologías, puede sufrir algunos inconvenientes que radican principalmente en el criterio de las autoridades máximas de la facultad, el mismo que puede no considerar válido el proceso para la aplicación dentro de la institución. Sin embargo, al tener en cuenta criterios diversos, esto se puede solucionar.

Dado que además, uno de los principios sobre los cuales se basa la metodología OCTAVE-S, es que se cuente con el apoyo de todas las instancias de la organización, donde los niveles jerárquicos tienen mucho protagonismo en el éxito de su aplicación.

6.7.1 Implementación de la metodología

La Universidad Técnica de Ambato, creada mediante Ley No. 69-05 con fecha 18 de abril de 1969, con la visión de constituirse en "un centro de referencia académico, científico y humanístico del país", realizadas en un "ámbito de libertad, respeto a los derechos humanos e intelectuales, participación integrativa, equidad de género y defensa del medio ambiente, con criterios de sustentabilidad y sostenibilidad".

La Facultad de Ingeniería Civil creada mediante resolución No. 84-217-CU-P del 22 de mayo de 1984, tiene su origen en la Ex escuela de Ingeniería Civil fundada en 1974, consecuentemente la Universidad Técnica de Ambato viene formando profesionales provenientes de la zona central del país de hace 32 años, satisfaciendo las necesidades profesionales en el campo de la Ingeniería Civil.

En la Facultad de Ingeniería Civil y mecánica se cuenta con dos servidores que gestionan tanto las redes internas como la información propia de la facultad, además se cuenta con tres laboratorios de 20 máquinas cada uno, las estaciones de trabajo de las secretarias que manejan toda la información referente a los estudiantes de la facultad, la estación de biblioteca que maneja la información bibliográfica de la facultad, las estaciones de control docente y los restantes equipos de profesores y autoridades que se encuentran dentro de la red de la facultad.

6.7.2 Fases a aplicar

FASE PREPARATORIA: Conformación del equipo de análisis, entrevistas previas.		
FASE UNO	**PROCESO**	**ACTIVIDAD**
Construir Perfiles de Amenaza de Activos de Información	P1: Identificar la Información Organizacional	A1.1: Establecer los Criterios de Evaluación del Impacto
		A1.2: Identificar Activos de Información de la Organización
		A1.3: Evaluar Prácticas de Seguridad Organizacional
	P2: Crear Perfiles de Amenaza	A2.1: Seleccionar los Activos Críticos.
		A2.2: Identificar los Requerimientos de Seguridad para Activos Críticos
		A2.3: Identificar las Amenazas a los Activos Críticos
FASE DOS	**PROCESO**	**ACTIVIDAD**
Identificar Vulnerabilidades en la Infraestructura	P3: Examinar Infraestructura Computacional en relación con los Activos Críticos	A3.1: Examinar Rutas de Acceso
		A3.2: Analizar Procesos relacionados con la Tecnología
FASE TRES	**PROCESO**	**ACTIVIDAD**
Desarrollar Estrategias y Planes de Seguridad.	P4: Identificar y Analizar Riesgos	A4.1: Evaluar Impacto de las Amenazas
		A4.2: Establecer Criterio de Evaluación de la Probabilidad
		A4.3: Evaluar Probabilidad de Amenaza
	P5: Desarrollar Estrategias de Protección y Planes de Mitigación	A5.1: Describir Estrategia de Protección Actual
		A5.2: Seleccionar Enfoques de Mitigación
		A5.3: Desarrollar Planes de Mitigación del riesgo
		A5.4: Identificar Cambios de Estrategia de Protección
		A5.5: Identificar los Pasos Siguientes
DESPUÉS DE LA EVALUACIÓN: Aprobación, implementación, puesta en marcha.		

Tabla 6.9: Fases de la Metodología OCTAVE-S(Fuente: ANDRADE, M 2006)

Fase preparatoria

Aquí se seleccionara al equipo de análisis de acuerdo a los perfiles y conocimientos de los integrantes de la facultad, ellos a su vez una vez notificados, se reunirán y elaborarán las entrevistas previas.

Definición del equipo de análisis

Para realizar la evaluación OCTAVE-S dentro de la Facultad de Ingeniería Civil y Mecánica, es necesario contar con personal que esté netamente ligado al funcionamiento y operación de la infraestructura de TI con que cuenta la institución.

Para tal fin, se ha diseñado el siguiente perfil que lista en detalle los conocimientos que cada posible integrante del equipo de evaluación debería saber.

Altos mandos:

Se necesita de un miembro que pertenezca a los altos mando (Nivel Ejecutivo) de la facultad

Puede ser este del Decano o el Subdecano de la facultad institución cuyo perfil será:

- Conocimiento de las plataformas e infraestructuras informáticas que se mantienen en la facultad.
- Conocimiento de los procesos clave que maneja la facultad para la normal ejecución de sus actividades y tareas.
- Conocimiento de infraestructuras computacionales dentro de la facultad
- Conocimiento de riesgos y amenazas asociadas a las tecnologías de información
- Tiempo de estadía en el cargo: Mínimo un año.

Mandos medios:

Aquí, se nombrará directamente a 2 personas para conformar la comisión: al Administrador de sistemas ya que se encuentra ligado y conoce a fondo los activos críticos que se pretenden evaluar. Siendo su perfil

- Conocimiento profundo y conciso de temas asociados al riesgo e impacto hacia los activos críticos de las tecnologías de información.
- Conocimiento de estándares para la mitigación, medición y controles de riesgo asociados a las TI.
- Conocimiento de posibles fallas, debilidades y vulnerabilidades a nivel operacional de temas relacionados con TI.
- Tiempo de estadía mínima dentro del cargo: 3 años.

Nivel de usuarios:

Se nombrará al profesor de tecnologías de la información que esta de cierta manera al tanto de la realidad informática de la facultad. Dentro de este grupo el perfil a manejar será:

- Conocimiento profundo y conciso de temas asociados al riesgo e impacto hacia los activos críticos de las tecnologías de información.

- Conocimiento de estándares para la mitigación, medición y controles de riesgo asociados a las TI.
- Conocimiento de posibles fallas, debilidades y vulnerabilidades a nivel operacional de temas relacionados con TI.
- Tiempo de estadía mínima dentro del cargo: 3 años.

De acuerdo a la naturaleza y complejidad del proyecto se hace necesario indicar que el equipo de trabajo estará formado por los tres miembros antes indicados.

Roles y responsabilidades del equipo de análisis

El equipo de análisis ayuda a:

- Establecer el alcance de la evaluación,
- Lidera la selección de los participantes de la evaluación,
- Facilita es establecimiento inicial de los talleres de obtención del conocimiento y
- Recoge y analiza información.

Los roles y responsabilidades del equipo de análisis son:

- Trabajar con administradores para establecer el alcance de la evaluación, seleccionar los participantes y planificar las actividades de la metodología
- Coordinar con los altos mandos y personal de TI para conducir la evaluación de las vulnerabilidades de la infraestructura de la organización.
- Obtener, analizar y mantener la información de la evaluación durante la evaluación
- Permitir las actividades de evaluación, particularmente asegurando que el personal designado atienda sus talleres específicos.
- Coordinar la logística para la evaluación.

Habilidades necesarias para conducir la metodología

Las habilidades específicas necesarias para cada proceso deberían ser las siguientes:

- Habilidades de facilitación

- Buenas habilidades de comunicación
- Buenas habilidades analíticas
- Habilidad para presentarse y trabajar con los altos mandos y personal en general
- Conocimiento del ambiente del negocio de la organización
- Conocimiento del ambiente de TI de la organización y de cómo el personal utiliza legítimamente las tecnologías de información dentro de la organización

Fase 1: Construir perfiles de amenazas de activos de información

Esta fase forma parte de la visión organizacional o de gestión. Entonces se realizan los procesos de: Identificar la información organizacional, y crear los perfiles de amenazas.

Información Organizacional

En este proceso se desarrollarán las actividades de: Establecer los criterios de evaluación del impacto, Identificar los activos de información de la organización, y Evaluar prácticas de seguridad organizacional.

Establecer los criterios de evaluación del impacto

Una vez conformado y reunido el equipo de análisis procederá a establecer los criterios con los que se realizará la evaluación de amenazas, vulnerabilidades y riesgos. Para ello se debe solicitar al equipo de trabajo estudie y prepare criterios que se presentan en la metodología OCTAVE-S seleccionada. Estos serán usados luego para hacer un grado de gravedad de la amenaza (alta, media o baja), estas tendrán una repercusión sobre las áreas:

- Confianza de los usuarios
- Financieras
- Seguridad de las personas
- Productividad
- Multas o sanciones legales.

Identificar los activos de información de la organización

Se identificaránlos activos de información de mayor relevancia de la organización.

En la actualidad en la Facultad de Ingeniería Civil y Mecánica se tienen los activos de información que son: Sistemas de información, Base de datos, equipos informáticos como servidores, computadores de los diferentes departamentos y componentes de los sistemas de redes como reouters, switchs, cableado,etc.

La información se trasmite utilizando canales físicos (impresiones) como electrónicos (correo electrónico). Es importante que la disponibilidad, confidencialidad, integridad y autentificación sea completa, de modo que la información pueda fluir sin dificultad por todas las dependencias de la facultad y se logre difundir la información para el óptimo desempeño de las actividades académicas y administrativas.

Evaluar prácticas de seguridad organizacional

De los activos identificados se seleccionarán los activos críticos relevantes y se evalúan el cómo las 15 áreas de práctica de seguridad de datos (OCTAVE-S) están siendo actualmente observadas dentro de la organización.

Identificación de amenazas al activo por áreas de preocupación, de esta forma se tendrá un primer contacto con las prácticas que presentan mayores falencias o que están actualmente más descuidadas.

Se marca el grado de seguridad que tienen las diferentes áreas de la organización y se identifica lo que la organización está haciendo respecto de la seguridad de esa área.

Se procede a etiquetar en rojo el área donde la seguridad es muy deficiente, en amarillo cuando el problema no es tan grave y verde si la seguridad es aceptable en esa área.

Crear perfiles de amenazas

Para caracterizar las amenazas procedemos a realizar las siguientes actividades: Seleccionar los activos críticos, identificar los requerimientos de seguridad para activos críticos y identificar las amenazas alos activos críticos.

Seleccionar los activos críticos

Se selecciona de entre los activos de información, basados en la importancia relativa para la organización, los tres o cinco activos considerados como críticos los cuales se analizan a profundidad, a continuación se identifica el sistema crítico y la razón para ser considerado como tal, se identifica quien usa y quien es responsable de dicho sistema y que activos están relacionados con él.

Identificar los requerimientos de seguridad para activos críticos

El equipo identifica los requerimientos de seguridad para cada activo crítico, sea este la disponibilidad, la confidencialidad o la integridad y se determina cuál de estos es el más importante.

Identificar las amenazas a los activos críticos

Se escribe en una casilla el nombre del activo crítico a analizar y se lo ubica en una matriz que interseca a un árbol de amenazas. Las ramas describen las características de su actor de amenaza. Pudiendo el actor tener acceso físico, interno o externo, y su motivo puede ser deliberado o accidental. Para cada amenaza, se identifica un autor como causa de ella y una consecuencia de su ataque, que puede ser revelación, modificación, pérdida o interrupción del flujo de información.

El contexto de la amenaza, se determina en base a cuales actores son de mayor consideración para el sistema en cada rama, se determina la fuerza motivo del ataque y que confianza se tiene en la estimación.

Finalmente se identifica el historial de ocurrencias de ataques en el pasado, y una estimación de cuan precisos son esos datos.

En las áreas de interés se ejemplifica como el actor ha atacado de acuerdo a cada rama.

Fase 2: Identificar vulnerabilidades en la estructura

La segunda fase para la identificación de vulnerabilidades, el equipo de trabajo realizará el siguiente proceso: Examinar la infraestructura computacional en relación con los activos críticos.

Examinar la infraestructura computacional en relación con los activos críticos.

En esta fase el equipo de análisis con un enfoque tecnológico conduce una revisión a nivel general de la infraestructura computacional de la organización y la relaciona con los encargados del mantenimiento. Así se evalúa cómo ha sido considerada la seguridad de la infraestructura computacional.

Aquí se realizan las siguientes actividades: Examinar rutas de acceso y analizar procesos relacionados con la tecnología.

Examinar rutas de acceso

El equipo de análisis primero identifica los sistemas más cercanamente relacionados con el activo crítico considerado principal (sistema de interés), a continuación se identifican los componentes clave de la red que son parte o están relacionados con el sistema de interés. Aquí se determinan puntos de acceso intermedio, es decir, los componentes de red utilizados para transmitir información desde el sistema de interés hacia los diferentes usuarios. Se consideran además desde que componentes de red se puede acceder al sistema de interés.

Se determina la localización del almacenamiento de información y se identifican en que clases de componentes esta almacenada la información con el proposito de respaldo.

Finalmente en esta actividad se identifican que otros sistemas, aplicaciones u otros componentes pueden ser utilizados para acceder al sistema de interés.

Analizar procesos relacionados con la tecnología

Se marca el camino para cada componente clave y para cada punto de acceso intermedio, para identificar qué clase de componentes de red están relacionados con uno o más activos críticos. Se relacionan los activos con cada componente y punto de acceso.

Se determina responsables de mantener y asegurar cada componente.

Finalmente se identifica el grado de protección cuando se configura y mantiene cada componente y si se conoce este hecho por medios formales o no.

Fase 3: Desarrollar estrategias y planes de seguridad

Esta fase se desarrolla siempre y cuando las fases uno y dos hayan sido completadas.

En esta fase se deben desarrollar las siguientes actividades: Evaluar el impacto de las amenazas, establecer criterios de evaluación de la probabilidad, evaluar la probabilidad de amenaza, describir la estrategia de protección actual, seleccionar enfoques de mitigación, desarrollar planes de mitigación del riesgo, identificar cambios en la estrategia de protección e identificar los pasos siguientes.

Evaluar el impacto de las amenazas

Con el registro de los criterios de evaluación del impacto ya obtenidos en la primera actividad e identificar el potencial daño a la seguridad en las áreas ya indicadas en los

diferentes árboles de amenaza, en los correspondientes cuadros de las hojas de trabajo del perfil de riesgo de cada activo crítico.

Establecer criterios de evaluación de la probabilidad

El equipo determina la probabilidad de un evento de amenaza como alta, media o baja de acuerdo con el número de ocurrencias registradas en el historial, respecto a un período de tiempo.

Evaluar la probabilidad de amenaza

Se llenan con esta probabilidad las casillas correspondientes en las matrices de perfil de riesgo para cada activo crítico. La más alta probabilidad de ocurrencia de una amenaza servirá para considerar un área de práctica de seguridad para un activo crítico como candidata para mitigación.

Describir la estrategia de protección actual

Se analizan las estrategias actuales de protección en aquellas áreas de práctica consideradas más críticas y de acuerdo con la realidad de las actividades de mitigación propuestas en grados de mayor a menor seguimiento.

Seleccionar enfoques de mitigación

Se transfieren los estados de alerta (rojo, amarillo, verde) de las áreas de práctica de seguridad en las hojas de perfil de riesgo y con la intersección de la matriz, amenazas, probabilidad, se marcan con un círculo aquellas áreas de práctica que se las considere para mitigación. No importa si se marcan dos o más actividades para una misma rama de amenaza, pues se trata de un primer indicador a ser utilizado en seguida.

Se definen criterios para determinar si una determinada práctica es candidata para mitigación, caso contrario se marcará la casilla definir la mitigación o aceptar como está siendo llevada actualmente.

Desarrollar planes de mitigación del riesgo

Se proponen las actividades de mitigación para las áreas de práctica de seguridad seleccionadas, se explica la razón de haberlas seleccionado, quien es asignado como responsable de llevarlas a cabo y qué soporte adicional se necesita para implementarlas.

Identificar cambios en la estrategia de protección

Se identifican y transfieren aquellos cambios en la estrategia de protección que se anotan como actividades en el plan de mitigación. Este plan se orienta hacia aquellas estrategias de protección que necesitan ser creadas o mejoradas, que se transforman en actividades de mitigación para las áreas de práctica de seguridad que se hallen más vulnerables.

Identificar los pasos siguientes

Se elabora una hoja de trabajo de los pasos siguientes y ésta incluye recomendaciones de qué acciones son inmediatas y cuándo se sugiere realizar la siguiente evaluación.

En cualquier fase el equipo puede elaborar sus recomendaciones de mejora y marcar los puntos importantes de práctica de seguridad en relación con las actividades de evaluación realizadas.

Un cuadro resumen de le mejor selección

Una explicación y argumentación de por qué esa es la mejor

6.8 Administración

Las personas que intervienen en la administración y aplicación de la metodología de análisis y gestión de riesgos estará conformada por:

- Decano
- Subdecano
- Directores de carrera
- Administrador de Sistemas
- Ayudantes
- Personal Administrativo
- Personal Docente
- Alumnos

6.9 Previsión de la evaluación

El realizar una previsión de la evaluación bajo una estricta vigilancia durante el proceso de su desarrollo, permitirá verificar si con la implementación de una metodología de análisis y gestión de riesgos se ha logrado mejorar la seguridad del acceso a la información, datos y recursos informáticos de la Facultad de Ingeniería Civil y Mecánica de la Universidad Técnica de Ambato, para que las autoridades puedan ejecutar sus actividades de mejor manera se ha diseñado una matriz de evaluación.

MATRIZ DE ANALISIS DE EVALUACION	
Aspectos para el plan de evaluación	**Elementos o recursos técnicos en el proceso de evaluación**
¿Quién solicita evaluar?	Decano, Subdecano, Administración,
¿Por qué evaluar?	Es necesario conocer y comprobar si la propuesta diseñada está contribuyendo al logro de los objetivos y brindando los resultados esperados
¿Para qué evaluar?	Para identificar posibles fallas en la metodología y prevenir desajustes en su implementación
¿Que evaluar?	La aplicación de la metodología, y los resultados arrojados
¿Quién evalúa?	El Decano conjuntamente con el Administrador de Sistemas.
¿Cuándo evaluar?	Cuando la propuesta se haya puesto en ejecución.
¿Cómo evaluar?	Identificando los aspectos críticos en la metodología.
¿Con que evaluar?	Se evaluara a través del criterio del profesional, y mediante la aplicación de la metodología.

Tabla 6.10: Previsión de la evaluación.(Fuente: Elaboración propia)

Bibliografía

[AGU09] Purificación AGUILERA. Seguridad informática. Editex, 2009.

[Agu10] P. Aguilera. Seguridad informática. Editex, 2010.

[ALB03] Audrey y STEVENS James y WOODY Carol ALBERTS, Christopher y DOROFEE. Visión general de OCTAVE. Software Ingineering Institute, 2003.

[ARE08] Javier AREITO. Seguridad De La información. Redes, Informática y Sistemas de Información. PARANINFO, 2008.

[Cap11] D. y Rodriguez E. Capote, B. y González. Visibilidad internacional de las ciencias médicas cubanas. 2011.

[CER11a] CERT. Metodología OCTAVE Allegro. en línea, 2011.

[CER11b] CERT. The Octave® criteria. en línea, 2011.

[CER11c] CERT. The Octave® methods. en línea, 2011.

[CER11d] CERT. The Octave-S implementation guide. en línea, 2011.

[Des06] E. y Garzón M. y Sampalo M. y Martos F. Desongles, J. y Ponce. Técnicos de Soporte Informático Grupo III de la Comunidad Autónoma de Castilla y León. 2006.

[dMAyPeIdlAE12] Dirección General de Modernización Administrativa y Procedimientos e Impulso de la Administración Electrónica. MAGERIT Metodología de Análisis y Gestión de Riesgos de Sistemas de Información. Centro de Publicaciones, 2012.

[DP04] J. y Martin-Romo S. y Medina S. De Pablos, C. y LópezHermoso. Informática y comunicaciones para la empresa. ESIC,2004.

[DP06] J. y Martín-Romo S. y Medina S. y Montero A. y Nájera J. De Pablos, C. y López-Hermoso. Dirección y gestión de los sistemas de información en la empresa. ESIC, 2006.

[Her08] J. y Romo-S. Heredero, C. y Lopez-Hermoso Agius. Dirección y gestión de los sistemas de información en la empresa. ESIC, 2008.

[Álv11] J. Álvarez. Guía práctica sobre Protección de Datos. Lex Nova, 2011.

[Meh11] Olivier Mehani. Contributions to MechanismsforAdaptive Use of Mobile Network Resources. PhD thesis, Mines ParisTech / University of New South Wales, Paris, France / Sydney, Australia, December 2011.

[MOR09] Héctor MORA. Manual del Vigilante de seguridad. Tomo 1. Club Universitario, 2009.

[Oro06] M. y Chávez J. Orozco, M. y Chávez. Informática I. ENI, 2006.

[Sal03] J. Salvado. Ingeniería de proyectos informáticos: actividades y procedimientos. Universitas, 2003.

[TR04] J. Thomson Royer. Seguridad en la informática de la empresa. ENI, 2004.

ANEXOS

Anexo A

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA CIVIL Y MECÁNICA

LUGAR A ENCUESTAR

OBJETIVO DE LA ENCUESTA:

Señores, su veracidad en las respuestas permitirá al grupo investigador desarrollar un trabajo real y efectivo.

Agradecemos su colaboración y garantizamos absoluta reversa de su información

CUESTIONARIO

INSTRUCCIONES:

Marque con una X o escriba la respuesta que UD. considere conveniente.

1. ¿El hardware y software utilizado en su dependenciaestá acorde a las necesidades del trabajo en su departamento?

( ) Si ( ) Parcialmente () No

2. ¿Está usted o el personal de su dependencia capacitado para el manejo de los sistemas informáticos utilizados?

( ) Si ( ) Parcialmente ( ) No

3. ¿Los equipos y sistemas informáticos que usted utiliza han sufrido fallas?

( ) Si ( ) Parcialmente ( ) No

4. ¿Los equipos y sistemas informáticos de su departamento han sufrido algún ataque informático (virus, hacker, desastres naturales, otro tipo)?

( ) Si ( ) Parcialmente ( ) No

5. ¿Ha sufrido robo o pérdida de información?

( ) Si ( ) Parcialmente ( ) No

6. ¿Existen controles de seguridad en los sistemas de información?

( ) Si ( ) Parcialmente ( ) No

7. ¿Existe un plan de seguridad de los sistemas y equipos informáticos?

( ) Si ( ) Parcialmente ( ) No

8. ¿Existe un responsable que coordine las medidas de seguridad de los sistemas y equipos informáticos?

( ) Si ( ) No

9. ¿Se hace algún tipo de revisión periódica del sistema de información?

( ) Si ( ) No

10. ¿Está usted capacitado en la seguridad del sistema de información?

( ) Si ( ) No

11. ¿Se han implementado políticas de seguridad en los sistemas y equipos informáticos?

( ) Si ( ) Parcialmente ( ) No

12. ¿Se realizan copias de seguridad y respaldo de la información y los datos?

( ) Siempre ( ) A veces ( ) Nunca

13. ¿Existe control de acceso a los sistemas y equipos informáticos (claves)?

( ) Si ( ) Parcialmente ( ) No

14. ¿Los respaldos de información se almacenan en un sitio seguro fuera de su departamento?

( ) Si ( ) No ( ) Desconoce

14. ¿Existen procedimientos de respaldo y recuperación de la información?

( ) Si ( ) No

15. ¿Cree pertinente contar con un plan de seguridad que le permita resguardar la información de su departamento?

( ) Si ( ) No

GRACIAS POR SU COLABORACIÓN

Anexo B

Hojas de trabajo

Guía de implementación de OCTAVE-S

El presente documento contiene la información y las tablas necesarias para el desarrollo de cada una de las fases y procesos necesarios para la aplicación de la metodología OCTAVE, estas fases son:

1. Fase 1: Construir perfiles de amenazas basadas en los activos
2. Fase 2: Identificación de vulnerabilidades en la infraestructura
3. Fase 3: Desarrollo de planes y estrategias de seguridad

Fase 1: Construir perfiles de amenazas basadas en los activos

Es una evaluación de los aspectos organizativos. Durante esta fase, el equipo de análisis define los criterios de evaluación que se utilizarán más adelante para evaluar los riesgos. También identifica importantes activos de la organización y evalúa la práctica actual de la seguridad de la organización. El equipo completa todas las tareas por sí mismo, la recopilación de información adicional sólo cuando sea necesario. A continuación, selecciona de tres a cinco activos críticos para analizar en profundidad sobre la base de la importancia relativa de la organización.
Finalmente, el equipo define los requisitos de seguridad y un perfil de amenaza para cada activo crítico.
Tabla 1: Procesos y actividades de la Fase 1.

Fase	Proceso	Actividad
Determinación de activos basados en perfiles de amenazas	S1: Identificar información organizacional	S1.1: Establecer criterios de evaluación del impacto
		S1.2: Identificación de activos de la organización
		S1.3: Evaluar prácticas de seguridad de la organización
	S2: Creación de perfiles de amenazas	S2.1: Seleccionar activos críticos
		S2.2: Identificar requerimientos de seguridad para activos críticos.
		S2.3: Identificar las amenazas de los activos críticos.

Documento para todas las fases y actividades

LISTA DE ACIONES

Actividad Hojas de trabajo (Lista de acciones)	Hojas de Referencia

Definiciones

(Lista de elementos de acción a corto plazo identificados durante las actividades OCTAVE-S)

Un elemento de acción es algo que una organización tiene la intención de completar en el corto plazo. Los elementos de acción generalmente no requieren:

• Formación especializada

• Cambios en las políticas

• Cambios en las funciones y responsabilidades

Instrucciones

Durante la evaluación, es probable que usted identifica que las acciones a corto plazo que necesitan ser completadas. Al identificar un elemento de acción, en el documento de acción de la hoja de trabajo: Lista de acciones. Incluya la siguiente información para cada elemento de acción:

• Una descripción de la acción

• La responsabilidad de completar la acción

• Una fecha para la finalización de la acción

• Las acciones de gestión que podrían ayudar a facilitar la finalización de la acción

Documento de recomendaciones y notas

Hoja de trabajo de actividades Recomendaciones y notas	Hoja de trabajo de referencia

Definiciones

Notas: Información de fondo que usted cree que es relevante para registro (es decir, la información que usted podría querer referirse durante una actividad más adelante)

Recomendaciones: Ideas que usted desea tener en cuenta al crear planes de mitigación o actualización de su estrategia de protección durante el proceso 5

Instrucciones

1. Durante la evaluación, lo más probable es pensar en las notas o recomendaciones que desee considerar en un momento posterior. Documentar cada nota o recomendación sobre los Bonos y Recomendaciones de la Hoja de Trabajo.

2. Antes de empezar cada proceso, revise las notas y recomendaciones para restablecer contexto.

S1.1 ESTABLECER LOS CRITERIOS DE EVALUACIÓN DEL IMPACTO

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Criterios de evaluación del impacto	

Definiciones

Impacto: el efecto de una amenaza sobre la misión de la organización y los objetivos de negocio

Valor del impacto: medida cualitativa del impacto de un riesgo específico para la organización (alto, medio, o bajo)

Criterios de evaluación del impacto: conjunto de medidas cualitativas contra el cual el efecto de cada riesgo sobre la misión de la organización y los objetivos de negocio son evaluados. Los criterios de evaluación de impacto definen rangos de impactos alto, medio y bajo para una organización.

Instrucciones

1. Definir un conjunto de medidas cualitativas (criterios de evaluación de impacto) contra e cual podrá para evaluar el efecto de un riesgo sobre la misión de su organización y los objetivos de negocio. Documentar sus criterios en la hoja de Criterios de Evaluación de Impacto. Como mínimo, considerar las siguientes áreas de impacto:

• Reputación / confianza de los clientes

• Vida / salud de los clientes

• Multas / sanciones legales

• Financiera

• Productividad

• otros (por ejemplo, las acciones administrativas , tales como auditorías y decrecimiento)

Rellene los espacios en blanco con los criterios que sean significativos para su organización. También puede cambiar las palabras proporcionadas o añadir palabras adicionales como sea necesario.

Nota: Dentro de cada área de impacto, hay una opción titulada "otro" para insertar un conjunto único de criterios. También hay una zona de impacto, titulado "otro" disponible para las áreas de impacto nuevas o únicas.

2. Tache las áreas de impacto que no se aplican a su organización sobre la Evaluación de Impacto de la Hoja de Trabajo: Criterios.

S1.2 IDENTIFICAR ACTIVOS DE INFORMACIÓN DE LA ORGANIZACIÓN

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Identificación de activos	

Definiciones

Activos: algo de valor para la empresa. Activos de tecnología de la información son la combinación de activos lógicos y físicos se agrupan en clases específicas (información, sistemas, servicios y aplicaciones, personas).

Categorías de activos

• Información: datos documentados (en papel o electrónicos) o propiedad intelectual usada para alcanzar la misión de una organización.

• Sistemas: una combinación de la información, software y los activos de hardware que procesan y almacenan información. Cualquier cliente o servidor puede ser considerado un sistema.

• Servicios y aplicaciones - aplicaciones y servicios de software (sistemas operativos, bases de datos aplicaciones, software de red, aplicaciones de oficina, aplicaciones personalizadas, etc) que procesan, almacenan o transmiten información.

• Personas - las personas en una organización que posean habilidades únicas, conocimientos y experiencia, esas son difíciles de reemplazar.

En una evaluación de riesgos de seguridad de la información, los activos deben estar vinculados a la información de alguna manera.

Instrucciones

1. La primera página de la Hoja de trabajo de identificación de activos se centra en los sistemas de información, servicios y aplicaciones. Considere las siguientes preguntas:

• ¿Qué necesita la gente de sistemas de la organización para realizar su trabajo?

• ¿Qué información necesita el personal de su organización para realizar su trabajo?

• ¿Qué aplicaciones y servicios necesita la gente de la organización para realizar su trabajo?

• ¿Qué otros activos están estrechamente relacionados con estos activos?

Identificar los activos de su organización, y documentarlos en la primera página de la hoja de trabajo.

Nota: Cada fila de la hoja de trabajo contiene los activos que están relacionados. Además, es posible grabar un activo en más de una fila.

S1.2 IDENTIFICAR ACTIVOS DE INFORMACIÓN DE LA ORGANIZACIÓN (continuación)

Hoja de Trabajo de Actividades Identificación de activos	Hoja de Trabajo de referencia

Instrucciones

2. La tercera página de la hoja de trabajo de identificación de activos se centra en las personas. Considere el siguientes preguntas:

• ¿Qué personas tienen una habilidad especial o conocimiento de que es vital para su organización y sería difícil de reemplazar?

• ¿Cuáles son sus habilidades o conocimientos especiales?

• ¿Qué sistemas utilizan estas personas?

• ¿Qué otros activos utilizan estas personas (información, servicios, o aplicaciones)?

Identificar los activos gente en su organización, y documentarlos en la tercera página de la hoja de trabajo.

Nota: Usted puede encontrar por usted mismo la iteración entre estas páginas. Asegúrese de que tiene lo más completo posible y documente todas relaciones relevantes entre activos.

S1.3 EVALUAR PRÁCTICAS DE SEGURIDAD ORGANIZACIONAL

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Prácticas de seguridad	

Definiciones

Una encuesta de la práctica de seguridad permite al equipo de análisis evaluar el grado en que las prácticas de seguridad reflejan la forma en que su organización gestiona la seguridad.

Prácticas de Seguridad: acciones que ayudan a iniciar , implementar y mantener la seguridad dentro de una empresa

Vulnerabilidades organizacionales: las deficiencias en la política de la organización o práctica que puede resultar en acciones no autorizadas

Catálogo de las prácticas: una colección de buenas estratégicas y prácticas operativas de seguridad que una organización puede utilizar para gestionar su seguridad

Prácticas estratégicas: prácticas de seguridad que se centran en cuestiones de organización a nivel de políticas. Ellas incluyen temas relacionados con la empresa, así como cuestiones que requieren planes y participación de toda la organización.

Prácticas operacionales: prácticas de seguridad que se centran en cuestiones relacionadas con la tecnología. Incluyen cuestiones relacionadas con cómo utiliza la gente, interactúa con, y protege la tecnología sobre la base del día a día.

Semáforo de estado: lo bien que una organización está llevando a cabo en un área de prácticas de seguridad. Los siguiente colores son asignados a un área basada en el rendimiento percibido en esa zona:

• Verde: La organización está llevando a cabo las prácticas de seguridad en el área muy bien, no hay una necesidad real de mejora.

• Amarillo: La organización está llevando a cabo las prácticas de seguridad, hasta cierto punto, no hay espacio para la mejora.

• Rojo: La organización no se está realizando las prácticas de seguridad del área; existe amplio margen de mejora.

Las siguientes áreas de práctica de seguridad se evalúan en OCTAVE-S:

Áreas Estratégicas de Práctica	Áreas de Práctica operacionales
1. Conciencia de Seguridad y Formación	7. Control de Acceso Físico
2. Estrategia de Seguridad	8. Monitoreo y Auditoría Física de seguridad
3. Gestión de la Seguridad	9. Sistema y administración de Red
4. Políticas y Reglamentos de Seguridad	10. Monitoreo y Auditoría de Seguridad Informática
5. Gestión de la Seguridad de Colaboración	11. Autenticación y autorización
6. Planes de Contingencia / Recuperación de Desastres.	12. Gestión de vulnerabilidades
	13. Encriptación
	14. Arquitectura de Seguridad y Diseño
	15. Gestión de Incidentes

S1.3 EVALUAR PRÁCTICAS DE SEGURIDAD ORGANIZACIONAL (continuación)

Hoja de Trabajo de Actividades Prácticas de seguridad	Hoja de Trabajo de referencia

Instrucciones

Revise las declaraciones de cada área de práctica de seguridad en la Hoja de Trabajo prácticas de seguridad y responda la siguiente pregunta:

• ¿Hasta qué punto esta declaración se refleja en su organización?

Encierra en un círculo la mejor respuesta de las siguientes opciones:

• Mucho: La declaración representa la práctica actual de la organización.

• Algo: La declaración representa parcialmente la práctica actual en la organización.

Algunos aspectos de la declaración no representan la práctica actual en la organización.

• No, en absoluto: La declaración no representa la práctica actual de la organización en absoluto.

Si usted no sabe si una declaración refleja la práctica de la seguridad en su organización, no haga un círculo en ninguna de las respuestas.

A medida que complete las preguntas de la encuesta , considere las siguientes preguntas:

• ¿Qué su organización actualmente está haciendo bien en esta área?

• ¿Qué su organización actualmente no está haciendo bien en esta área?

La primera cuestión se centra en las prácticas de seguridad actuales utilizadas por la organización, mientras que el segundo se centra en las vulnerabilidades de organización presentes en su organización.

Ejemplos de registros de prácticas de seguridad y vulnerabilidades de la organización relevantes para cada área de prácticas de seguridad.

Después de completar los pasos anteriores, asignar un estado de semáforo para cada área de práctica de seguridad. El estado del semáforo debe reflejar lo bien que usted cree que su organización está llevando a cabo en cada área.

Utilice las siguientes definiciones de semáforo como guía:

• Verde: La organización está llevando a cabo las prácticas de seguridad en el área muy bien, no hay necesidad real de mejora.

• Amarillo: La organización está llevando a cabo las prácticas de seguridad, en cierta medida, hay espacio para la mejora.

• Rojo: La organización no está realizando las prácticas de seguridad en el área; existe amplio margen de mejora.

S1.3 EVALUAR PRÁCTICAS DE SEGURIDAD ORGANIZACIONAL (continuación)

Hoja de Trabajo de Actividades Prácticas de seguridad	Hoja de Trabajo de referencia

Instrucciones (continuación)

Elementos de acción, Notas y Recomendaciones

1. Documentar todos los puntos de acción que ha identificado durante el proceso de S1 en la Hoja de Trabajo: Lista de Acción.

Incluya la siguiente información para cada elemento de acción:

• una descripción de la acción

• la responsabilidad de completar la acción

• una fecha para la finalización de la acción

• las acciones de gestión que podrían ayudar a facilitar la finalización de la acción

2. Documento de notas relevantes de las actividades en el proceso S1 sobre la Hoja de Trabajo: Notas y Recomendaciones.

3. Documentar todas las recomendaciones del proceso S1 que desee tener en cuenta durante el proceso de S5 de la Hoja de Trabajo: Indicaciones y Recomendaciones.

S2.1 SELECCIONAR LOS ACTIVOS CRÍTICOS

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Selección de activos críticos Información de activos críticos en un apropiado libro de trabajo: Activos críticos	

Definiciones

Activos críticos: de los activos más importantes para una organización. La organización va a sufrir una gran impacto adverso si:

- Un activo crítico se da a conocer a las personas no autorizadas
- Un activo crítico es modificado sin autorización
- Un activo crítico se pierde o destruye
- Acceso a un activo crítico se interrumpe

Instrucciones

Nota: Antes de comenzar Proceso S2, revise las notas y recomendaciones que registró en la Hoja de Trabajo: Notas y Recomendaciones durante el proceso S1. Estas notas y recomendaciones podrían ser relevantes para las actividades que se llevarán a cabo durante el proceso de S2.

Examinar los activos que registró en la hoja de trabajo de identificación de activos y considerar las siguientes preguntas:

• Qué activos tendrían un gran impacto negativo en la organización si una o más de las siguientes situaciones ocurren:

- El activo o activos fueron revelados a personas no autorizadas.
- El activo o activos fueron modificados sin autorización.
- El activo o activos se perdieron o fueron destruidos.
- El acceso al activo o los activos se interrumpió.

Al considerar las preguntas, piense en los pocos activos relacionados con la información que son más esenciales para cumplir la misión de la organización o la consecución de sus metas y objetivos.
Graba hasta cinco activos críticos en la hoja de trabajo de Selección de Activos Críticos.
También registre cualquier nota relevante acerca de cada activo.
Nota: Completar la columna " Notas" es opcional. También, los números en la hoja de cálculo no están destinados para indicar el orden de prioridad.

S2.1 SELECCIONAR LOS ACTIVOS CRÍTICOS (continuación)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Selección de activos críticos Información de activos críticos en un apropiado libro de trabajo: Activos críticos	

Instrucciones (continuación)

Iniciar Libro de trabajo: Activo Crítico para cada activo crítico.

Nota: Cada categoría de activos críticos (sistemas, información, aplicaciones, personas) tiene un único Libro de Trabajo: Activos Críticos. Los contenidos son similares para cada libro de trabajo activo crítico, pero las preguntas están redactadas de forma ligeramente diferente dependiendo de la categoría de activos. Asegúrese de que selecciona el volumen adecuado para cada activo crítico.

Anote el nombre de cada activo crítico en su Hoja de trabajo: Información de Activos Críticos ubicado en el Libro de trabajo: Activo crítico apropiado.

Documente su justificación de la selección de cada activo crítico sobre la información de la Hoja de Trabajo: Activos Críticos de dicho activo.

Considere la siguiente pregunta:

• ¿Por qué es este activo fundamental para la organización?

Anote una descripción para cada activo crítico en la Hoja de trabajo: Información de Activos Críticos de dicho activo.

Considere las siguientes preguntas:

• ¿Quién utiliza el activo?

• ¿Quién es responsable de que el activo?

Los activos de Registros que están relacionados con cada activo crítico en la Hoja de Trabajo información de activos críticos de dicho activo. Remítase a la Hoja de trabajo: Información de activos para determinar que activos están relacionados con cada activo crítico.

Considere la siguiente pregunta:

• ¿Qué activos están relacionados con este activo?

S2.2 IDENTIFICAR LOS REQUERIMIENTOS DE SEGURIDAD PARA ACTIVOS CRÍTICOS

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
La información de Activos Críticos en el correspondiente libro de trabajo: Activos Críticos	

Definiciones

Requisitos de seguridad: declaraciones que describen las cualidades de los activos relacionados con la información que es importante para una organización. Requisitos de seguridad típicos son la confidencialidad, integridad y disponibilidad. Confidencialidad: la necesidad de mantener información confidencial, sensible o personal privada e inaccesible a cualquier persona que no esté autorizada a verla. Integridad: la autenticidad, precisión y exhaustividad de un activo. Disponibilidad: cuándo o con qué frecuencia debe estar presente o listo para su uso un activo.
Nota: Los requisitos de seguridad dentro de OCTAVE-S se centran en que requisitos deben ser para un activo, no en que son ellos actualmente.

Instrucciones

1. Registre los requisitos de seguridad para cada activo crítico sobre la Hoja de Trabajo: información de activos críticos de dicho activo.

Nota: Los requisitos de seguridad se centran en lo que los requisitos deben ser para un bien, no lo que actualmente son.

Considere la siguiente pregunta:

• ¿Cuáles son los requisitos de seguridad para este activo?

Una declaración para cada categoría de los requisitos de seguridad se presenta en la Hoja de Trabajo: Información de activo crítico. Si una categoría es aplicable para un activo crítico, marque con una "X" en la casilla junto a esa categoría.

2. Completar los requisitos de seguridad para cada categoría aplicable para un activo crítico. En una como mínimo, llene los espacios proporcionados.

Usted puede cambiar las palabras proporcionadas o añadir palabras adicionales como sea necesario.
Nota: Una categoría titulada "otro" se proporciona para los requisitos de seguridad adicionales que no entran en las categorías de la confidencialidad, integridad y disponibilidad.

Para cada activo crítico , registre el requisito de seguridad más importante en la Hoja de Trabajo: Información de activo crítico de dicho activo (Vol. 5-8) marcando con una "X" en la casilla que aparece junto a la categoría de seguridad de requisitos que es más importante para ese activo .

Considere la siguiente pregunta:

• ¿Qué requisitos de seguridad es más importante para este activo?

S2.3 IDENTIFICAR LAS AMENAZAS A LOS ACTIVOS CRÍTICOS

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo en el apropiado Libro de Trabajo: Activo Crítico.	Guía de traducción de Amenaza en el apropiado Libro de Trabajo: Activos Críticos.

Definiciones

Amenaza: una indicación de un posible evento indeseable. Una amenaza se refiere a una situación en la que una persona podría hacer algo no deseable (un atacante iniciar un ataque de denegación de servicio contra un servidor de correo electrónico de la organización) o un fenómeno natural podría causar un resultado no deseado (un incendio dañar la información del hardware de tecnología de la organización).
Perfil Amenaza: una forma estructurada de presentación de una serie de amenazas a un activo crítico. Amenazas en el perfil se agrupan de acuerdo a la fuente de la amenaza.
Perfil genérico de la amenaza: un catálogo de amenazas que contiene una variedad de todas las amenazas potenciales bajo consideración. El perfil genérico amenaza es un punto de partida para crear un perfil de amenaza única para cada activo crítico.
Las amenazas se representan mediante las siguientes propiedades:
• Activos: algo de valor para la empresa
• El acceso: cómo se accede al mismo por un actor (acceso a la red, el acceso físico). Los accesos sólo se aplican a los actores humanos.
• Actor: quien o que puede violar los requisitos de seguridad (confidencialidad , integridad, disponibilidad) de un activo
• Motivo: la intención del actor (por ejemplo, deliberada o accidental). Motivo aplica sólo a actores humanos.
• Resultado: el resultado inmediato (divulgación, modificación, destrucción, pérdida, interrupción) la violación de los requisitos de seguridad de un activo
En OCTAVE-S, las amenazas se representan visualmente en una estructura de árbol, a menudo referido como un árbol amenaza.

Hay un árbol de amenaza para cada una de las siguientes categorías de fuente de la amenaza:

Categoría	Definición
Actores humanos usando acceso a la red.	Las amenazas de esta categoría son las amenazas basadas en la red de una organización de activos críticos. Requieren la acción directa de una persona y pueden ser de naturaleza deliberadas o accidentales.
Actores humanos usando acceso físico.	Las amenazas de esta categoría son las amenazas físicas a una organización de críticos activos. Requieren la acción directa de una persona y puede ser deliberada o accidental en la naturaleza.
Problemas del sistema	Las amenazas de esta categoría son los problemas con los sistemas de tecnología de información de la organización. Algunos ejemplos son los defectos de hardware, defectos de Software, código malicioso (por ejemplo, virus), y otros problemas relacionados con el sistema.
Otros problemas	Las amenazas de esta categoría son los problemas o situaciones que están fuera del control de una organización. Esta categoría de amenazas incluye desastres naturales (por ejm. Inundaciones terremotos) y los riesgos de interdependencia. Los riesgos de interdependencia incluyen ir la falta de disponibilidad de las infraestructuras críticas (por ejm, la fuente de alimentación).

S2.3 IDENTIFICAR LAS AMENAZAS A LOS ACTIVOS CRÍTICOS (continuación)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo en el apropiado Libro de Trabajo: Activo Crítico	Guía de traducción de Amenaza en el apropiado Libro de Trabajo: Activos Críticos

Instrucciones

Nota: Cada categoría de activos críticos (sistemas, información, aplicaciones, personas) tiene una única Hoja de trabajo: Perfil de riesgo. Lo encontrarás en el Libro de Trabajo: Activos Críticos para esa categoría de activos.
Nota: Usted completará sólo partes seleccionadas de la Hoja de trabajo: Perfil de riesgo durante esta actividad. Va a completar las partes restantes más adelante en la evaluación.

Nota: Si tiene dificultades para interpretar una amenaza sobre algún árbol amenaza, revise la descripción y ejemplos de esa amenaza en la Guía de traducción de amenazas.
1. Seleccione la hoja de trabajo apropiada para cada activo crítico.
Nota: Los siguientes cuatro árboles se aplican a los sistemas, la información, servicios y aplicaciones:
• Actores humanos utilizando acceso a la red
• Actores humanos usando el acceso físico
• Problemas del sistema
• Otros problemas
Nota: Sólo un árbol se aplica a las personas: otros problemas.
2. Complete todos los árboles de amenazas apropiados para cada activo crítico. Cuando marque un árbol de amenaza, considere las siguientes preguntas:
• Por qué ramas hay una posibilidad no despreciable de una amenaza para el activo? marca
estas ramas en el árbol.
• ¿Por cuál de las ramas restantes existe una posibilidad insignificante o ninguna posibilidad
de una amenaza para el activo? No marque estas ramas.
Nota: Asegúrese de marcar una amenaza si hay incluso una posibilidad remota de que pudiera producirse una amenaza.
Usted tendrá la oportunidad de aceptar la amenaza más adelante en la evaluación. En este momento, usted debe mirar a la más amplia gama de posibles amenazas.

S2.3 IDENTIFICAR LAS AMENAZAS A LOS ACTIVOS CRÍTICOS (continuación)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo en el apropiado Libro de Trabajo: Activo Crítico	Guía de traducción de Amenaza en el apropiado Libro de Trabajo: Activos Críticos

Instrucciones (continuación)

Nota: Este paso sólo es para las siguientes categorías de amenaza:
• Los actores humanos utilizando acceso a la red
• Los actores humanos usando el acceso físico
En este paso, usted proporciona detalles adicionales acerca de las siguientes combinaciones de actor y motivos:
• Adentro actuando accidentalmente
• Adentro actuando deliberadamente
• forasteros actuando accidentalmente
• forasteros que actúan deliberadamente

1. Como usted completa los árboles de amenazas para los actores humanos utilizando el acceso de red, tenga en cuenta la siguiente pregunta:
• ¿Qué actores plantean las mayores amenazas para este activo a través de la red?
Ejemplos específicos de Registros de actores de amenaza en la Hoja de Trabajo: perfil de riesgo para cada combinación aplicable actor – motivo.

2. Como usted completa los árboles de amenaza para los actores humanos usando el acceso físico, considere la siguiente pregunta:
• ¿Qué actores plantean las mayores amenazas para este activo a través de medios físicos?
Ejemplos específicos de Registros de actores de amenaza en la Hoja de Trabajo: perfil de riesgo para cada combinación aplicable actor – motivo.

S2.3 IDENTIFICAR LAS AMENAZAS A LOS ACTIVOS CRÍTICOS (continuación)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo en el apropiado Libro de Trabajo: Activo Crítico	Guía de traducción de Amenaza en el apropiado Libro de Trabajo: Activos Críticos

Instrucciones (continuación)

Nota: Este paso sólo es para las siguientes categorías de amenaza:
• Los actores humanos utilizando acceso a la red
• Los actores humanos usando el acceso físico
En este paso, usted proporciona detalles adicionales acerca de las siguientes combinaciones de actor – motivo:
• Adentro actuando deliberadamente
• foráneos que actúan deliberadamente
1. Considere la siguiente pregunta para ambas combinaciones actor – motivo:

• ¿Qué tan fuerte es el motivo del actor?
Usted está estimando alta intensidad del motivo basado en los actores específicos que ha identificado.
Marque con una "X" en la casilla junto a la mejor respuesta de las siguientes opciones:
• Alta: El actor se centra en atacar a su organización, tiene muy bien definido el objetivo, está dirigido específicamente a los activos críticos, se aplicarán medidas extraordinarias para atacar el activo crítico, y se destinará a medidas extraordinarias para asegurar el éxito.
• Medio: El actor se centra en atacar a su organización, tiene objetivos generales, están dirigidos a un rango de activos en su organización, tiene límites en los medios que serán aplicado a atacar el activo crítico, y tiene una estrategia de salida que define explícita o implícitamente cuando abandone el ataque.
• Bajo: El actor se centra en atacar a una organización (no necesariamente la suya), no tiene objetivos específicos, se dirige a cualquier activo que puede ser atacado fácilmente, se aplicará medios limitados para el ataque, y abandonarán rápidamente el ataque si el éxito no llega a ser fácil.

S2.3 IDENTIFICAR LAS AMENAZAS A LOS ACTIVOS CRÍTICOS (continuación)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo en el apropiado Libro de Trabajo: Activo Crítico	Guía de traducción de Amenaza en el apropiado Libro de Trabajo: Activos Críticos

Instrucciones (continuación)

2. Considere la siguiente pregunta para cada estimación de la intensidad del motivo:
• ¿Cuánta confianza tiene usted en esta estimación?
Marque con una "X" en la casilla junto a la mejor respuesta de las siguientes opciones:
• Mucho: Usted tiene una cantidad considerable de datos objetivos relacionados con su estimación. Cualquier persona razonable revisando los datos objetivos podría llegar a la misma conclusión.
• Algo: Usted tiene una cantidad limitada de datos objetivos relacionados con su estimación. La persona razonable tendría que hacer inferencias y suposiciones clave para llegar a la misma conclusión. Sin embargo, es probable que una persona razonable llegar a la misma conclusión.
• No, en absoluto - Usted tiene datos objetivos poco o nada relacionados con su estimación. Una persona razonable podría llegar a una conclusión diferente, porque hay poco o nada de datos objetivos sobre lo cual basar la estimación.

Nota: Realice este paso para todas las categorías de amenaza.
1. Considere la siguiente pregunta para cada amenaza activa:
• ¿Con qué frecuencia ha ocurrido esta amenaza en el pasado?
Revise algún dato objetivo que pueda tener (por ejm. , registros, datos de incidentes) y datos subjetivos (lo que la gente en el equipo de análisis o personas de su organización de revisan).
Llene los espacios en blanco en la siguiente declaración para cada amenaza:
• _____ veces en años _____.

S2.3 IDENTIFICAR LAS AMENAZAS A LOS ACTIVOS CRÍTICOS (continuación)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo en el apropiado Libro de Trabajo: Activo Crítico	Guía de traducción de Amenaza en el apropiado Libro de Trabajo: Activos Críticos

Instrucciones (continuación)

2. Considere la siguiente pregunta para cada estimación de la historia de la amenaza:
• ¿Qué tan exactos son los datos?

Marque con una "X" en la casilla junto a la mejor respuesta de las siguientes opciones:
• Mucho: Usted tiene una cantidad considerable de datos objetivos relacionados con su estimación. Cualquier persona razonable revisando los datos objetivos llegaría a la misma conclusión.
• Algo: Usted tiene una cantidad limitada de datos objetivos relacionados con su estimación. La persona razonable tendría que hacer inferencias y suposiciones clave para llegar a la misma conclusión. Sin embargo, es probable que una persona razonable llegara la misma conclusión.
• No, en absoluto - Usted tiene datos objetivos poco o nada relacionados con su estimación. Una persona razonable podría llegar a una conclusión diferente, porque hay poco o nada de datos objetivos sobre la cual basar la estimación.

Este paso proporciona un contexto adicional, en su caso. Dar ejemplos, o escenarios, de cómo amenazas específicas podría afectar el activo crítico. Registre el contexto adicional y áreas de preocupación para cada fuente de amenaza.

Elementos de acción, Notas y Recomendaciones

1. Documentar todos los puntos de acción que ha identificado durante el proceso de S2 en la Hoja de trabajo: Lista de Acción.

Incluya la siguiente información para cada elemento de acción:
• una descripción de la acción
• la responsabilidad de completar la acción
• una fecha para la finalización de la acción
• las acciones de gestión que podrían ayudar a facilitar la finalización de la acción

2. Documentar notas relevantes de las actividades en proceso S2 en la Hoja de Trabajo: Notas y Recomendaciones.

3. Documentar todas las recomendaciones del Proceso S2 que desee tener en cuenta durante el proceso S5 en la Hoja de Trabajo: indicaciones y recomendaciones.

Fase 2: Identificación Vulnerabilidades en la Infraestructura

Durante esta fase, el equipo de análisis lleva a cabo una revisión de alto nivel de la infraestructura informática de la organización, enfocándose en la medida en que la seguridad es considerada por los mantenedores de la infraestructura. El equipo de análisis primero analiza cómo la gente usa la infraestructura informática para acceso activos críticos, clases de rendimiento clave de componentes, así como quién es responsable de configuración y mantenimiento de esos componentes.

Posteriormente, el equipo examina el grado en que cada una de ellas incluye la seguridad en sus prácticas y procesos de tecnología de la información. Los procesos y actividades de la Fase 2 son se muestra en la Tabla 2.

Tabla 2: Procesos y Actividades de la Fase 2

Fase	Procesos	Actividades
Identificar vulnerabilidades de la infraestructura	S3: Examinar infraestructura computacional en relación con los activos críticos	S3.1: Examinar caminos de acceso
		S3.2: Analizar tecnologías y procesos relacionados

S3.1: Examinar rutas de acceso

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Rutas de acceso a redes en el apropiado Libro de Trabajo: Activo Crítico	Información de activo crítico en el apropiado Libro de Trabajo: Activos Críticos

Definiciones/fondo

Rutas de acceso de red: formas en que se puede acceder a los sistemas, dispositivos, información o servicios a través de la red de una organización.

Sistema de intereses: el sistema o sistemas que están más estrechamente ligada a un activo crítico, por ejemplo :

• El sistema en el que el activo " vive "
• El sistema donde va a ir para obtener una copia "oficial" del activo.
• El sistema que ofrece a los usuarios legítimos el acceso a un activo crítico.
• El sistema que le da al actor de amenaza acceso a un activo crítico.

Clases principales de componentes: Categorías de dispositivos y redes que se utilizan para acceder a un sistema de interés. Estos dispositivos y redes son parte de o se relacionan con un sistema de interés. Cuando legitiman los usuarios acceden a un activo crítico, acceden a los componentes de estas clases. Los actores de la amenaza también el acceden a los componentes de estas clases cuando se dirigen deliberadamente un activo crítico.

Los puntos de acceso: Interfaces de que, directa o indirectamente, permiten el acceso a un sistema de interés. Estas interfaces se agrupan de acuerdo a las siguientes categorías:

• Los componentes del sistema de interés
• El acceso al sistema por parte de personas
• Puntos de acceso intermedio
• Otras interfaces y los lugares de almacenamiento de datos
• Otros sistemas

Acceso al sistema por parte de personas: los tipos de componentes que la gente (por ejemplo, los usuarios, los atacantes) utilizan para acceder a un sistema de interés. Estos componentes constituyen puntos de acceso que pueden originarse internamente o externamente a los sistemas y redes de una organización.
Puntos de acceso Intermedio: redes que se utilizan para transmitir la información y las aplicaciones del sistema de interés a las personas.

Lugares de almacenamiento de datos - otros tipos de componentes que se utilizan para almacenar información crítica o proporcionar servicios de apoyo a los datos relacionados con un sistema de interés (por ejemplo, dispositivos de almacenamiento que se utilizan para realizar copias de seguridad de la información almacenada en un sistema de interés).

Otros sistemas y componentes - Sistemas que acceden a la información crítica o servicios de un sistema de interés , también , otras clases de componentes que se pueden utilizar para acceder a información crítica o aplicaciones del sistema de interés

S3.1: Examinar rutas de acceso

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Rutas de acceso a redes en el apropiado Libro de Trabajo: Activo Crítico	Información de activo crítico en el apropiado Libro de Trabajo: Activos Críticos

Definiciones

Las clases estándar de los componentes considerados en OCTAVE-S se describen en la siguiente tabla:

Clases Componentes	Descripción
Servidores	Host con la información de la infraestructura tecnológica que provee la información tecnológica de servicios de su organización.
Redes Internas	Interconectividad de la organización
Estaciones de Trabajo	Servidores utilizados por los funcionarios
Laptops	PCs portables de los miembros de la organización
Componentes inalámbricos	Otros dispositivos que acceden a las redes como teléfonos celulares, tabletas, etc.
Otros sistemas	Sistemas, procesos o aplicaciones que acceden a información
Medios de almacenamiento	Medios de almacenamiento de información como discos duros externos
Otros	Cualquier otro tipo de dispositivo que se conecte a la red

Instrucciones

S3.2: Analizar procesos tecnológicos relacionados

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Revisión de infraestructura	Rutas de acceso a redes Libro de Trabajo: Activos Críticos

Definiciones

El foco de análisis se desplaza durante la actividad S3.2. Durante la actividad S2.3, que ha realizado un análisis de actividades desde el punto de vista activo, siempre que ha identificado las amenazas a los activos críticos. Del mismo modo, durante Actividad S3.1, ha realizado actividades de análisis desde una perspectiva de activos cuando usted examinó caminos de acceso en relación con los activos críticos.

Sin embargo, durante la actividad S3.2, en lugar de llevar a cabo actividades de análisis desde la perspectiva de los activos, que ahora asume el punto de vista de la infraestructura. Durante esta actividad, se analiza el relato tecnológico de los procesos utilizados durante la configuración y el mantenimiento de la infraestructura informática.

Durante la actividad S3.2, se compila la información para cada clase de componente que ha identificado durante la actividad anterior. La información de cada clase incluye

- Los activos críticos que están relacionadas con cada clase
- La parte (o partes) responsable de mantener y asegurar cada clase de componentes
- La medida en que la seguridad se considera la hora de configurar y mantener cada clase de componentes (mucho, poco, nada, no saben)
- Cómo determinó el grado en el que la seguridad se considera la hora de configurar y mantenimiento de cada clase de componentes (técnicas formales , medios informales , otros)
- Cualquier información adicional, notas, y las cuestiones que desea grabar para cada clase

Fase 3: Desarrollo de la Estrategia de Seguridad y Planes

Durante la Fase 3, el equipo de análisis identifica los riesgos a los activos críticos de la organización y decide qué hacer con ellos. Sobre la base de un análisis de la información recopilada, el equipo crea un estrategia de protección para la organización y planes de mitigación para hacer frente a los riesgos a la crítica activos. Las hojas de trabajo OCTAVE-S usados durante la Fase 3 son muy estructurados y estrechamente vinculado a el catálogo de la octava de las prácticas, lo que permite al equipo de relacionar sus recomendaciones para mejora a un punto de referencia aceptado de práctica de seguridad. Tabla 3 representa los procesos y las actividades de la Fase 3.

Tabla 3: Procesos y Actividades de la Fase 3

Fase	Proceso	Actividad
Desarrollo de planes y estrategias de seguridad	S4: Identificar y analizar riesgos	S4.1: Evaluar impactos de amenazas
		S4.2: Establecer criterios de evaluación de la probabilidad
		S4.3: Evaluar probabilidades de amenazas
	S5: Desarrollo de estrategias de protección y planes de mitigación	S5.1: Describir la Estrategia de Protección actual
		S5.2: Seleccione enfoques de mitigación
		S5.3: Desarrollar Planes de Mitigación de Riesgo
		S5.4: Identificar cambios en la protección estratégica
		S5.5: Identificar los siguientes pasos

S4.1: Evaluar los impactos de las amenazas

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo en su caso activo crítico libro de trabajo	- Criterios de Evaluación de Impacto - Información críticas Activos en su caso libro de trabajo activo crítico

Definiciones

Riesgo - la posibilidad de sufrir daños o pérdidas. El riesgo se refiere a una situación en la que una persona puede hacer algo indeseable o una ocurrencia natural podría causar un resultado no deseado, lo que resulta en un impacto o consecuencia negativa.
Un riesgo se compone de
• un evento
• incertidumbre
• una consecuencia
En seguridad de la información, el evento básico es una amenaza.
La incertidumbre se manifiesta en gran parte de la información recopilada durante la evaluación OCTAVE - S.
Hay incertidumbre en torno a si se producirá una amenaza y si la organización es suficientemente protegidos contra el actor amenaza. La incertidumbre se representa a menudo el uso de la probabilidad de ocurrencia o probabilidad.
La consecuencia que importa en última instancia, en el riesgo de seguridad de la información es el impacto resultante en el organización debido a una amenaza. Impacto describe cómo una organización puede verse afectada según el siguiente amenaza resultados:
• divulgación de un activo crítico
• Modificación de un activo crítico
• Pérdida / destrucción de un activo crítico
• Interrupción de un activo crítico
Los resultados mencionados anteriormente están directamente relacionados con los activos, sino que describen el efecto de las amenazas sobre los activos.
El impacto se centró en la organización, sino que es el enlace directo de nuevo a la misión de la organización y los objetivos de negocio.
En la Actividad S1.1 , se crearon los criterios de evaluación de impacto para las siguientes áreas de impacto :
• Reputación / confianza de los clientes
• La vida / salud de los clientes
• Las multas / sanciones legales
• financiera
• Productividad
• otros

S4.1: Evaluar los impactos de las amenazas (cont.)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo en su caso activo crítico libro de trabajo	- Criterios de Evaluación de Impacto - Información críticas Activos en su caso libro de trabajo activo crítico

Instrucciones

Nota : Antes de comenzar Proceso S4 , revise las notas y recomendaciones que ha anotado en los procesos anteriores. Estas notas y recomendaciones podrían ser relevantes para las actividades que se llevarán a cabo durante el proceso de S4.

Nota: Antes de evaluar los impactos potenciales sobre la organización como resultado de las amenazas a los activos críticos, usted debe revisar la información de activos y la amenaza fundamental que habían documentado previamente en la evaluación.

1. Revise la información sobre la amenaza que ha grabado en la hoja de perfil de riesgos para cada activo crítico. Centrarse en los siguientes artículos:
• amenazas a los activos críticos
• Contexto amenaza (actores de amenaza , el motivo, la historia)
• Contexto amenaza adicional

2. Revise la información que ha grabado en cada hoja de trabajo de Activos Críticos (Vol. 5-8). Se centran en el siguientes artículos:
• justificación de la selección de activos relacionados
• Requisitos de seguridad
• más importante requisito de seguridad

3. Revise la información que ha grabado en la Hoja de Criterios de Evaluación de Impacto.

Enfóquese en cómo se definió alto, medio y bajo impacto para su organización.

Utilice los criterios de evaluación de impacto para evaluar el impacto de cada amenaza en su organización misión y objetivos de negocio. Asegúrese de revisar los criterios que ha grabado para la siguiente áreas:
• Reputación / confianza de los clientes
• La vida / salud de los clientes
• Las multas / sanciones legales
• financiera
• Productividad
• otros

S4.1: Evaluar los impactos de las amenazas (cont.)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo en su caso activo crítico libro de trabajo	- Criterios de Evaluación de Impacto - Información críticas Activos en su caso libro de trabajo activo crítico

Instrucciones

4. Para cada activo crítico , considere las siguientes preguntas para cada amenaza para ese activo :
• ¿Cuál es el impacto potencial a la reputación de la organización?
• ¿Cuál es el impacto potencial sobre la confianza de los clientes?
• ¿Cuál es el impacto potencial de salud o de seguridad a los clientes?
• ¿Cuál es el impacto potencial para el personal de la salud o la seguridad de los miembros?
• ¿Qué multas o sanciones legales podían imponerse a la organización?
• ¿Cuál es el potencial impacto financiero para la organización?
• ¿Cuál es el impacto potencial de la productividad de la organización o de los clientes?
• ¿Qué otros impactos podría ocurrir?
A medida que revisa las preguntas, piensa en el impacto potencial sobre su organización debido a cada amenaza activa.
Nota: Cada una de las preguntas anteriores está vinculada a un área de impacto.
5. Después de revisar las preguntas anteriores, comparar los impactos potenciales que discutieron por cada área de impacto frente a los criterios de evaluación de impacto para esa área.
El uso de los criterios de evaluación de impacto como una guía, asignar una medida de impacto (alto, medio, o bajo) para cada amenaza activa.
Documentar cada impacto en el perfil de riesgo mediante el registro
• " H" para cada uno de alto impacto
• " M " para cada impacto medio
• " L" para cada uno de bajo impacto
Nota: Es posible identificar múltiples impactos de dicha amenaza, que podría llevar a más de una valor de impacto para una zona de impacto dado. Si esto sucede, registrar el valor más alto para que el impacto área en el perfil de riesgos.

S4.2: Establecer criterios de evaluación de probabilidad

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Criterios de evaluación de la probabilidad	Perfil de riesgo en su caso activo crítico

Definiciones

Probabilidad - la probabilidad de que un evento ocurra.

Valor de probabilidad - una medida cualitativa de la probabilidad de una amenaza (alta, media o baja)

Criterios de evaluación de la probabilidad - un conjunto de medidas cualitativas utilizadas para estimar la probabilidad de una ocurrencia de la amenaza. Criterios de evaluación de la probabilidad definen los rangos de frecuencia de alta, media y bajas probabilidades, que indican con qué frecuencia se producen amenazas durante un período de tiempo común.

El tiempo entre eventos - una estimación de la frecuencia se puede producir un evento (por ejemplo , semanalmente , una vez cada dos años)

Frecuencia anualizada - la probabilidad proyectada de ocurrencia de una amenaza en un año determinado.

Probabilidades amenaza a la seguridad de la información se estimaron utilizando una combinación de datos objetivos, experiencia subjetiva, y la experiencia. Si está utilizando OCTAVE - S por primera vez, lo más probable es la falta datos objetivos relacionados con amenazas. También puede ser que carecen de experiencia y conocimientos en la información seguridad y / o gestión de riesgos. Por esta razón, la probabilidad se considera que es opcional en OCTAVE - S. Cada equipo tiene que decidir si va a utilizar la probabilidad, así como la forma de utilizarlo.

En OCTAVE -S, los valores de probabilidad se definen por un conjunto de criterios de evaluación que se clasifica según su frecuencia de aparición. Criterios de evaluación de la probabilidad definen un conjunto estándar de definiciones de valores de probabilidad. Estos criterios definen las medidas de alto, medio y bajo de amenaza probabilidades.

Medidas de probabilidad se definen considerando un rango de frecuencias (es decir , la probabilidad de un de amenaza ocurrencia en un determinado año):

- diario
- semanal
- mensual
- 4 veces al año
- 2 veces al año
- una vez al año
- una vez cada 2 años
- una vez cada 5 años
- una vez cada 10 años
- una vez cada 20 años
- una vez cada 50 años

S4.2: Establecer criterios de evaluación de probabilidad

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Criterios de evaluación de la probabilidad	Perfil de riesgo en su caso activo crítico

Instrucciones

1. Su objetivo es definir medidas de probabilidad sobre la base de la frecuencia es probable que ocurran amenazas.

Revise la siguiente información de la Hoja de Perfil de Riesgo:

- los tipos de amenazas a los activos críticos
- con qué frecuencia ha ocurrido cada amenaza en el pasado (la historia)
- cualquier información adicional relevante que ha grabado

2. Considere las siguientes preguntas :

- ¿Qué define a una "alta " probabilidad de ocurrencia? ¿Con qué frecuencia debe una amenaza ocurrió ser considerado una amenaza de alta probabilidad?
- ¿Qué define una probabilidad "media" de que se produzca? ¿Con qué frecuencia debe producirse una amenaza a ser considerado una amenaza media - la probabilidad?
- ¿Qué define una probabilidad " baja" de que se produzca? ¿Con qué frecuencia debe una amenaza ocurrió ser considerado una amenaza de baja probabilidad?

3. En la evaluación de la probabilidad Criterios, dibujar líneas verticales que separan alto de probabilidades medio y medio de bajas probabilidades.

Asegúrese de sincronizar los límites entre los niveles de probabilidad. Por ejemplo , cuando establecer la distinción entre las probabilidades altas y medias , es posible trazar una línea vertical entre los acontecimientos y sucesos que se producen cuatro veces al año mensuales.

S4.3 Evaluar Probabilidades de Amenazas

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo en su caso activo crítico	Criterios de evaluación de la probabilidad

Definiciones

Un riesgo se compone de:

• un evento • incertidumbre • una consecuencia

La incertidumbre se manifiesta en gran parte de la información recopilada durante la evaluación. Hay incertidumbre en torno a si una amenaza se producirá y si la organización es suficientemente protegida contra el actor amenaza. La incertidumbre se representa a menudo el uso de la probabilidad de ocurrencia, o probabilidad.

En la Actividad S4.2, se crearon los criterios de evaluación de probabilidad de alto, medio y bajo amenaza probabilidades.

Instrucciones

1. La siguiente tabla muestra la información de cada amenaza activa que usted puede grabar en Perfil de riesgo de cada activo crítico.

Tipo de información

La información contextual acerca de los actores de amenaza

El motivo de acciones deliberadas por parte de actores humanos

La historia de cada amenaza activa

Las áreas de preocupación

Para cada amenaza activa, revise toda la información que ha grabado para esa amenaza.

Nota: Al estimar la probabilidad, que va a utilizar la historia de una amenaza como base.

Considere la siguiente pregunta para cada amenaza :

• ¿Qué tan probable es la amenaza que se produzca en el futuro?

Revise la historia de la amenaza y asignar esa amenaza un valor de probabilidad cualitativa (alta, media o baja) en base a los criterios de evaluación de probabilidad que ha creado en la Actividad S4.2 y la historia de esa amenaza . Criterios de evaluación de la probabilidad se documentan en el Criterios de Evaluación Probabilidad Hoja de trabajo.

Nota: Haga valores de probabilidad no grabar en el Perfil de Riesgo en este momento.

Usted no debe registrar las probabilidades hasta más tarde.

2. Considere la siguiente pregunta para cada amenaza :

• ¿Cambia cualquiera de los otros datos que ha grabado para la amenaza de la estimación basado en la historia?

Considere la siguiente información que recodificado en el perfil de riesgo :

• motivo de acciones deliberadas por parte de actores humanos

• resumen de vulnerabilidades de la infraestructura informática de las amenazas de red y maliciosa código (si se ha estimado)

• resumen de vulnerabilidades de la infraestructura física para las amenazas físicas (si ha sido estimado)

• Información contextual sobre los actores de amenaza

• Ejemplos concretos de amenazas

3. Ajuste su estimación de cualquier probabilidad de amenaza si usted cree que la información que lo amerite.

Consulte los criterios de probabilidad al ajustar las estimaciones de probabilidad.

Documento cada probabilidad en el Perfil de Riesgo mediante el registro

• " H " para cada alta probabilidad • " M " para cada probabilidad media • " L " para cada baja probabilidad

Nota: Debido a que cada rama en el árbol de la amenaza que representa múltiples amenazas específicas , es posible identificar múltiples probabilidades de una amenaza determinada , lo que podría dar lugar a más de una probabilidad valor para una rama determinada . Si esto sucede, registrar el valor más alto para esa área de impacto en el Perfil de riesgo

S4.3 Evaluar Probabilidades de Amenazas

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo en su caso activo crítico	Criterios de evaluación de la probabilidad

Instrucciones

4. Considere la siguiente pregunta para cada amenaza :

• ¿Cuánta confianza tiene usted en su estimación de la probabilidad de que esta amenaza?

Considere lo siguiente:

• exactitud de los datos del historial
• confianza en su estimación de la intensidad del motivo (en su caso)
• exhaustividad de la evaluación de las vulnerabilidades de la infraestructura informática (en su caso)
• exhaustividad de la evaluación de las vulnerabilidades de la infraestructura física (en su caso)

Al lado de cada valor de probabilidad de amenaza en la Hoja de Perfil de Riesgo es una escala para confianza con los siguientes puntos definidos: mucho, algo, y no en todos. Basado en su respuesta a la pregunta anterior, marque con una "X" en la escala en el punto que indica su la confianza en el valor de la probabilidad de esa amenaza. Los puntos siguientes se proporcionan como referencias en la escala:

• Muy - Usted tiene una cantidad considerable de datos objetivos relacionados con su estimación. Cualquier persona razonable revisar los datos objetivos sería llegar a la misma conclusión.
• Algo - Usted tiene una cantidad limitada de datos objetivos relacionados con su estimación. La persona razonable tendría que hacer inferencias y suposiciones clave para llegar a la misma conclusión. Sin embargo, es probable que una persona razonable llegar a la misma conclusión.
• No, en absoluto - Usted tiene datos objetivos poco o nada relacionados con su estimación. Una razonable persona podría llegar a una conclusión diferente, porque hay poco o nada de datos objetivos sobre la cual basar la estimación.

Elementos de acción, Notas y Recomendaciones

1. Documentar todos los puntos de acción que ha identificado durante el proceso S4 en la Lista de Acción.

Recuerde que debe incluir la siguiente información para cada elemento de acción:

• una descripción de la acción
• la responsabilidad de completar la acción
• una fecha para la finalización de la acción
• las acciones de gestión que podrían ayudar a facilitar la finalización de la acción

2. El documento señala pertinentes para las actividades en proceso S4 en las Notas y Recomendaciones.
3. Documentar todas las recomendaciones de S4 Proceso que desee considerar durante Proceso S5 en la Hoja de Notas y Recomendaciones

S5.1: Describir Estrategia de protección actual

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Estrategia de Protección	Procedimientos de seguridad

Definiciones

Estrategia de Protección - define la estrategia general empleada por una organización para permitir, iniciar, implementar y mantener su seguridad interna. Se estructura en función de las áreas de práctica de seguridad.

Característica - una cualidad o atributo de una zona de prácticas de seguridad. Cada área de práctica de seguridad comprende múltiples características.

Enfoque - la manera en que una organización se ocupa de una característica de una zona de prácticas de seguridad.

Tarea - una actividad que debe ser completado como parte de una zona de prácticas de seguridad operacional

Áreas de Práctica de Seguridad - grupos de prácticas que son ya sea estratégico u operativo. Áreas de práctica de seguridad estratégica suelen ser amplias y tienden a afectar a todos los riesgos a todos los activos críticos por igual (por ejemplo, la documentación de un conjunto de políticas de seguridad para la organización). Áreas de práctica de seguridad operacional centrarse en las tareas del día a día y se pueden orientar hacia la mitigación de los riesgos específicos a los activos específicos (por ejemplo, comprobación de un sistema específico para cuentas por defecto).

Una estrategia de protección se define como una organización tiene la intención de aumentar o mantener el nivel actual de seguridad. Su objetivo es proporcionar una orientación para los futuros esfuerzos de seguridad de la información en lugar de encontrar una solución inmediata a todas las vulnerabilidades de seguridad y preocupación.

Desde una estrategia de protección proporciona la dirección de la organización con respecto a la seguridad de la información actividades, se estructura de acuerdo a las áreas de práctica de seguridad. Las áreas de práctica de seguridad son se ilustra en la tabla de abajo.

Áreas de Práctica Estratégica

1. Conciencia de Seguridad y Formación
2. Estrategia de Seguridad
3. Gestión de la Seguridad
4. Políticas y Reglamentos de Seguridad
5. Gestión de la Seguridad de Colaboración
6. Planes de Contingencia / Recuperación de Desastres

Áreas de Práctica Operacional

7. Control de Acceso Físico
8. Monitoreo y Auditoría Física seguridad
9. Sistema y Red de Gestión
10. Monitoreo y Auditoría de Seguridad Informática
11. Autenticación y autorización
12. Gestión de vulnerabilidades
13. Encriptación
14. Arquitectura de Seguridad y Diseño
15. Gestión de Incidentes

S5.1: Describir Estrategia de protección actual

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Estrategia de Protección	Procedimientos de seguridad

Instrucciones

Nota : Antes de comenzar Proceso S5 , revise las notas y recomendaciones que ha anotado en el Notas y Recomendaciones Planilla (Vol. 9) durante los procesos anteriores. Estas notas y recomendaciones podrían ser relevantes para las actividades que se llevarán a cabo durante el proceso de S5.

También revisar todos los puntos de acción que registró en la Lista de la hoja de trabajo de Acción durante el anterior proceso. Estos puntos de acción podrían ser relevantes para las actividades que se llevarán a cabo durante el proceso de S5.

Nota: Las características de una zona estratégica práctica de seguridad son diferentes a las de un área de práctica de la seguridad operacional. Las instrucciones de examinar la manera de abordar cada tipo de valor practicar área por separado.

1. Revise la información contenida en la Hoja de Trabajo Prácticas de Seguridad. Preste atención a la siguiente información para cada área de práctica de seguridad :
• El estado de semáforo
• el grado en que cada medida de seguridad para una zona se refleja en la organización
• lo que la organización está haciendo actualmente bien en un área
• lo que la organización no está haciendo bien en un área
2. Transferir el estado de la luz de parada para cada área de práctica de seguridad (por tanto estratégicos como operativos
áreas de práctica de seguridad) de la Prácticas de Seguridad Hoja de Trabajo (Vol. 4) a la zona designada en la hoja de trabajo de la Estrategia de Protección antes de definir la estrategia para esa zona.
3. Desarrollar la estrategia de protección para cada área estratégica práctica de seguridad. En la siguiente lista incluye todas las áreas de práctica de seguridad estratégicos :
Áreas Estratégicas de Práctica
1. Conciencia de Seguridad y Formación
2. Estrategia de Seguridad
3. Gestión de la Seguridad
4. Políticas y Reglamentos de Seguridad
5. Gestión de la Seguridad de Colaboración
6. Planes de Contingencia / Recuperación de Desastres
4. Cada área estratégica práctica de seguridad comprende varias características únicas. Por ejemplo, Políticas de Seguridad y Regulaciones se desglosa en las siguientes características:
• Políticas Documentados
• Gestión de Políticas
• Aplicación de la Política
• Sensibilización del personal
• Política y Cumplimiento Normativo
• Otros

S5.1: Describir Estrategia de protección actual (cont.)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Estrategia de Protección	Procedimientos de seguridad

Instrucciones

5. Para cada característica en una zona de prácticas de seguridad estratégica dada , considere lo siguiente pregunta:

• ¿Cuál es el enfoque de la organización para hacer frente a esta característica?

La Estrategia de Protección Hoja de Trabajo ofrece varias posibles respuestas a la pregunta para cada característica. Si una de las opciones coincide con la situación actual de la organización, marque con una "X" en el cuadro titulado "Actual " junto a esa opción.

Asegúrese de que usted llene los espacios en blanco proporcionados por la opción que seleccione. Puede cambiar las palabras proporcionadas o añadir palabras adicionales como sea necesario.

Nota: Se le proporcionará con líneas en blanco al final de cada característica. Si usted tiene una única respuesta por la forma en que su organización se ocupa de esa característica, registre el enfoque en los espacios en blanco siempre y marcar una "X" en el cuadro titulado "Actual" al lado de los espacios en blanco.

También se proporcionan una característica en blanco para cada área estratégica práctica de seguridad. Si usted tiene una característica única para un área, registre el enfoque de la organización en esa característica y marque con una "X" en el cuadro titulado "Actual " al lado de la aproximación.

No marque una "X" en el cuadro titulado " Cambio" en este momento. Se tendrá en cuenta los cambios en su estrategia de protección de la organización.

Complete la Hoja de Trabajo de Protección de Estrategia para todas las áreas de práctica de seguridad estratégicos.

Asegúrese de que la dirección todas las características aplicables a cada área estratégica práctica de seguridad.

6. Desarrollar la estrategia para cada área de práctica de la seguridad operacional. La siguiente lista incluye todas las áreas de práctica de seguridad operacional:

Áreas de Práctica operacionales

1. Control de Acceso Físico
2. Monitoreo y Auditoría de Seguridad Física
3. Sistema y Red de Gestión
4. Monitoreo y Auditoría de Seguridad Informática
5. Autenticación y autorización
6. Gestión de vulnerabilidades
7. Encriptación
8. Arquitectura de Seguridad y Diseño
9. Gestión de Incidentes

S5.1: Describir Estrategia de protección actual (cont.)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Estrategia de Protección	Procedimientos de seguridad

Instrucciones

7. Cada área de la práctica operativa comprende varias características. El formato de todas las medidas de las áreas de práctica operativas es bastante consistente. La siguiente tabla describe cada característica y cuando usted necesita para hacer frente a esa característica.

Característica	Descripción
Responsabilidad	Esta característica define quién tiene la responsabilidad de completar un conjunto de tareas específicas para un área práctica de seguridad operacional. La Responsabilidad característica incluye múltiples tareas para las que se ha asignado la responsabilidad. Esta característica define si la rendición de cuentas para cada tarea recae en personas de su organización, con terceros o con una combinación de personas de su organización, así como de terceros.
Procedimientos	Si las personas de su organización tienen la responsabilidad de algunas o todas las tareas de un área de práctica de la seguridad operacional, se debe abordar esta característica. La característica Procedimientos define la medida en que los procedimientos de un área de práctica de la seguridad operacional se definen formalmente.
Entrenamiento	Si las personas de su organización tienen la responsabilidad de algunas o todas las tareas de un área de práctica de la seguridad operacional, se debe abordar esta característica. La característica de Formación define el enfoque para la construcción de los miembros del personal habilidades en un área de práctica.
Cuestiones de colaboración	Si la gente de la tercera parte son responsables de algunas o todas las tareas de un área de práctica de la seguridad operacional, se debe abordar esta característica. La Problemas Colaborativos característica define el grado en que los requisitos para un área de práctica de la seguridad operacional se comunican formalmente a terceros.
Verificación	Si la gente de la tercera parte son responsables de algunas o todas las tareas de un área de práctica de la seguridad operacional, se debe abordar esta característica. La verificación característica define el grado en que cada tercero cumple con los requisitos de una zona de prácticas de seguridad operacional.

Nota: Si la gente en su organización tienen la responsabilidad exclusiva de todas las tareas en un área de práctica operativa de seguridad, no complete una estrategia para los problemas de colaboración y verificación características. Si un tercero es el único responsable de todas las tareas en un área de seguridad operativa práctica, no complete una estrategia para los procedimientos y características de formación.

S5.1: Describir Estrategia de protección actual (cont.)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Estrategia de Protección	Procedimientos de seguridad

Instrucciones

8. La Estrategia de Protección enumera varias tareas bajo la responsabilidad característica para cada área de práctica de la seguridad operacional. Inicialmente determina quién tiene responsabilidad de cada tarea para un área práctica de la seguridad operacional. En primer lugar, marque con una "X" en el cuadro titulado "actual".

Para cada área de práctica de la seguridad operacional , considere las siguientes preguntas:

• ¿Quién es actualmente responsable de completar cada tarea en esta Área de Práctica de seguridad operacional? ¿La gente en su organización? ¿Un tercero? ¿Una combinación de personas en su organización y una o más terceras partes?

La Estrategia de Protección enumera tres opciones en la columna actual para cada tarea:

• Interna - La gente en su organización son responsables de completar la tarea.

• Externo - Uno o más terceras partes son responsables de completar la tarea.

• Combinado - Una combinación de personas de su organización y uno o varios terceros las partes son responsables de completar la tarea.

Marque con una "X" en la casilla correspondiente para cada tarea. Usted puede cambiar las palabras previstas para una tarea o añadir palabras adicionales según sea necesario.

Nota: La característica de Responsabilidad para cada área de práctica de la seguridad operacional proporciona varios espacios en blanco. Si tiene tareas que no figuran en la estrategia de protección para una operativa área de práctica de seguridad, grabar esas tareas en los espacios proporcionados y marque una "X" en la designación casilla correspondiente que es responsable de cada tarea.

No marque una "X" en el cuadro titulado " Cambio" en este momento. Se tendrá en cuenta los cambios en su estrategia de protección de la organización.

9. Si las personas de su organización tienen la responsabilidad de algunas o todas las tareas de un área de práctica operativa de seguridad, se debe designar un enfoque para las características de

Procedimientos y Entrenamiento

Nota: El área de práctica rompe la formación en seguridad de cifrado en Tecnología de la Información Formación y Capacitación del Personal. Esta es la única excepción en las áreas de práctica operacional de la seguridad.

Para los procedimientos y características de formación en un área de práctica de seguridad operacional dada, considerar la siguiente pregunta:

• ¿Cuál es el enfoque de la organización para hacer frente a esta característica?

La Estrategia de Protección Hoja de Trabajo ofrece varias posibles respuestas a la pregunta para cada característica. Si una de las opciones coincide con la situación actual de la organización, marque con una "X" en el cuadro titulado "Actual " junto a esa opción.

Asegúrese de que usted llene los espacios en blanco proporcionados por la opción que seleccione. Puede cambiar las palabras proporcionadas o añadir palabras adicionales como sea necesario.

Nota: Se le proporcionará con líneas en blanco al final de los procedimientos y las características de formación.

Si usted tiene un enfoque único para la forma en que su organización se ocupa de una de esas características, grabar este enfoque en los espacios provistos y marque una "X" en el cuadro titulado "Actual" junto a los espacios en blanco.

No marque una "X" en el cuadro titulado " Cambio" en este momento. Se tendrá en cuenta los cambios en su estrategia de protección de la organización.

S5.1: Describir Estrategia de protección actual (cont.)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Estrategia de Protección	Procedimientos de seguridad

Instrucciones

10. Si la gente de la tercera parte son responsables de algunas o todas las tareas de un área de práctica operativa de seguridad, debe designar un enfoque para las Cuestiones de colaboración y verificación características. Anote el nombre de la tercera parte en el espacio proporcionado.

Nota: Es posible que tenga más de una tercera parte que proporciona servicios de seguridad de la información en un área de práctica de la seguridad operacional. Temas y verificación completa de colaboración características de cada tercero que presta sus servicios en esa área.

Para cada una de esas características en una zona de prácticas de seguridad operacional determinado , considere lo siguiente pregunta:

• ¿Cuál es el enfoque de la organización para hacer frente a esta característica?

La Estrategia de Protección Hoja de Trabajo (Vol. 9) ofrece varias posibles respuestas a la pregunta para cada característica. Si una de las opciones coincide con la situación actual de la organización, marque con una "X" en el cuadro titulado "Actual " junto a esa opción.

Asegúrese de que usted llene los espacios en blanco proporcionados por la opción que seleccione. Puede cambiar las palabras proporcionadas o añadir palabras adicionales como sea necesario.

Nota: Se le proporcionará con líneas en blanco al final de las Cuestiones de colaboración y verificación características. Si usted tiene una respuesta única para cómo su organización se dirige a uno de los características, registran el enfoque de los espacios en blanco proporcionados y marque una "X" en el recuadro titulado "Actual" al lado de los espacios en blanco.

No marque una "X" en el cuadro titulado " Cambio" en este momento. Se tendrá en cuenta los cambios en su estrategia de protección de la organización.

11. Complete la Hoja de Trabajo de Protección de Estrategia para todas las áreas de práctica de seguridad operacional.

Asegúrese de que la dirección todas las características aplicables para cada práctica de seguridad operacional del área.

S5.2 Selección Mitigación Enfoques

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo	• Criterios de Evaluación de Impacto • Criterios de Evaluación de Probabilidad • Información de activos crítico • Procedimientos de seguridad • Revisión de Infraestructura • Notas y Recomendaciones

Definiciones

Enfoque Mitigación - cómo una organización tiene la intención de abordar un riesgo. Una organización tiene las siguientes opciones para cada riesgo: aceptar, mitigar o retrasar.

Aceptar - una decisión tomada durante el análisis de riesgo a tomar ninguna medida para hacer frente a un riesgo y aceptar la deben ocurrir el riesgo consecuencias. Los riesgos que se aceptan generalmente tienen un bajo impacto en la organización.

Mitigar - una decisión tomada durante el análisis de riesgos para hacer frente a un riesgo mediante la implementación de actividades diseñadas para contrarrestar la amenaza subyacente. Los riesgos que se mitigan suelen tener un alto impacto en una organización.

Aplazar - una situación en la que el riesgo no ha sido aceptado ni mitigado. El impacto en la organización debido a un riesgo diferido está por encima de un umbral mínimo, pero no tan grande como para ser una prioridad inmediata.

Riesgos diferidos se observaron y reevaluados en algún momento en el futuro.

Área de Mitigación - una zona de prácticas de seguridad que está designado para ser mejorado con el fin de mitigar uno más de los riesgos de seguridad de una organización.

La decisión de aceptar un riesgo, mitigarlo, o aplazar la decisión se basa en un número de factores.

Valor de impacto es a menudo el principal impulsor al tomar la decisión. La probabilidad puede ser utilizado para determinar qué riesgos para mitigar primero.

Desafortunadamente, no existe un proceso de toma de decisiones bloqueo de paso que se aplica en todas las circunstancias. El perfil de riesgo creado para cada activo crítico durante OCTAVE - S es una herramienta de apoyo a la decisión. Presenta amenazas, los valores de impacto para múltiples áreas de impacto, los valores de probabilidad, y los estados de semáforo de la áreas de práctica de seguridad , lo que ilustra una imagen de los riesgos que afectan a ese activo crítico . Un equipo de análisis utiliza el perfil de riesgo para apoyar las decisiones paliativas que se hace.

S5.2 Selección Mitigación Enfoques

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo	• Criterios de Evaluación de Impacto • Criterios de Evaluación de Probabilidad • Información de activos crítico • Procedimientos de seguridad • Revisión de Infraestructura • Notas y Recomendaciones

Instrucciones

Transferir el estado de la luz de parada para cada zona de prácticas de seguridad de las Prácticas de Seguridad a la sección " Áreas de Práctica de Seguridad " del perfil de riesgo de cada activo crítico.

Nota: Algunas de las áreas de práctica de seguridad están " bloqueados " para cada riesgo. Estas áreas son poco probable que sean seleccionadas como áreas de mitigación. No registrar el estado de semáforo para un área que está " bloqueada ", a menos que haya determinado que es aplicable a un riesgo bajo sus circunstancias actuales.

Nota: No existe un enfoque único para el análisis de la información que ha grabado a lo largo de la evaluación. Un enfoque se documenta en estas directrices. Se puede seleccionar el método que mejor se adaptarse a las preferencias de su equipo de análisis, así como las prácticas aceptadas de su organización. Su objetivo final es seleccionar tres áreas de práctica de seguridad tales como áreas de mitigación. Basado en los riesgos de seguridad de su organización, así como la financiación y el personal restricciones, es posible decidir seleccionar menos o más de tres áreas de mitigación. Utilice su mejor juicio.

1. Revise la información contenida en las siguientes hojas :
• Perfil de riesgo hoja de trabajo (para cada activo crítico)
• Crítico Activos Hoja de trabajo (para cada activo crítico)
• Prácticas de Seguridad Hoja de Trabajo
• Revisión de Infraestructura Hoja de trabajo

Es posible que necesite un contexto adicional para interpretar el impacto, la probabilidad y la vulnerabilidad de información en las pestañas superiores. Revise sus definiciones de impacto y los niveles de gravedad de probabilidad en las siguientes hojas :
• Criterios de Evaluación de Impacto Hoja de Trabajo
• Criterios de Evaluación Probabilidad Hoja de Trabajo

2. Revisar toda la información que ha grabado a lo largo de la evaluación de los Bonos y Recomendación. Preste especial atención a las recomendaciones que le realizados en relación con las posibles actividades de mitigación.

Nota: Puede revisar la información que ha grabado durante la evaluación antes de seleccionar mitigación se acerca. Las hojas de trabajo destacadas anteriormente constituyen el conjunto mínimo de información que usted necesitará durante esta actividad.

3. Considere las siguientes preguntas :
• ¿Qué está impulsando la selección de las áreas de mitigación?
• ¿Las áreas de impacto que sean más importantes para su organización?
• ¿Cómo va a factorizar la probabilidad en sus decisiones?
• ¿Qué requisitos de seguridad es más importante para cada activo crítico?
• ¿Qué áreas específicas de preocupación que necesita para hacer frente?
• ¿Qué áreas de práctica específicas de seguridad necesitan la mayoría de las mejoras?
• ¿Qué no específica vulnerabilidades organizacional es necesario abordar?
• ¿Qué otros factores pueden influir en la selección de las áreas de mitigación?

Revisión riesgos para sus activos críticos, manteniendo las preguntas anteriores en mente. Empiece a pensar en la manera de abordar cada riesgo. Tienes que empezar a pensar en lo que corre el riesgo de que la intención de mitigar, que tiene la intención de aceptar, y que tiene la intención de ver y volver a evaluar en algún momento de la futuro.

S5.2 Selección Mitigación Enfoques (cont.)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo	• Criterios de Evaluación de Impacto • Criterios de Evaluación de Probabilidad • Información de activos crítico • Procedimientos de seguridad • Revisión de Infraestructura • Notas y Recomendaciones

Instrucciones

4. Considere la siguiente pregunta:

• ¿Qué riesgos necesita ser mitigado?

Marque con una "X" en el cuadro titulado " Mitigación " para cada riesgo que tiene la intención de mitigar. Piense en el futuro como usted está seleccionando qué riesgos para mitigar. Si selecciona demasiadas áreas, podría ser abrumado durante la planificación de la mitigación.

5. Considere la siguiente pregunta para todos los riesgos que aún no se haya asignado una mitigación enfoque :

• ¿Qué riesgos se va a aceptar?

Piense en el impacto en la organización, debido a cada riesgo. Determinar qué impactos son lo suficiente bajos que no prevén la necesidad de tomar alguna acción proactiva para prevenirlos.

Marque con una 'X ' en la casilla titulada "Aceptar " para estos riesgos en el área designada en el Perfil de riesgo.

6. Para los riesgos que aún no se ha asignado un enfoque de mitigación (es decir , aquellos que aún no designado como " Mitigar " o "Aceptar ") , considere la siguiente pregunta:

• ¿Existen riesgos adicionales que necesite para mitigar?

Recuerde que debe considerar los controladores de toma de decisiones al considerar áreas adicionales para seleccionar.

Marque con una "X" en el cuadro titulado " Mitigación " para cada riesgo adicional de que usted seleccione.

7. Para este punto, usted ha seleccionado los riesgos que la organización va a mitigar y también identificó los corre el riesgo de que la organización aceptará. También tiene probablemente algunos riesgos que no han sido ni aceptado ni mitigado.

Para aquellos riesgos que no hayan sido aceptados ni mitigado, ha decidido que la impactos potenciales resultantes de estos riesgos no eran lo suficientemente bajo como para aceptar ni lo suficientemente grande como para ser designado como prioridad la mitigación actual. Marque con una "X" en el cuadro titulado " Aplazar " para éstos riesgos. Riesgos diferidos se observaron y reevaluados en algún momento en el futuro.

Ahora ha asignado un enfoque de mitigación para cada riesgo. Después, usted necesita para seleccionar la mitigación áreas.

S5.2 Selección Mitigación Enfoques (cont.)

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Perfil de riesgo	• Criterios de Evaluación de Impacto • Criterios de Evaluación de Probabilidad • Información de activos crítico • Procedimientos de seguridad • Revisión de Infraestructura • Notas y Recomendaciones

Instrucciones

8. Considere las siguientes preguntas al revisar los riesgos a todos los activos críticos , también teniendo en mente los controladores de toma de decisiones :

• ¿Áreas de práctica de valores que tienen más margen de mejora? ¿De qué manera estas áreas afectan los riesgos que deben ser mitigados?

• Las áreas de práctica de valores que, si se selecciona para la mitigación, podría mitigar muchos riesgos para más de un activo crítico?

• ¿Existe alguna reglamentación o políticas que deben tenerse en cuenta al seleccionar las áreas de mitigación? Si es así, qué áreas se va a seleccionar?

Seleccione tres (3) áreas de práctica de seguridad como áreas de mitigación. Asegúrese de considerar todas las limitaciones (por ejemplo, fondos y personal) cuando usted hace su selección. Si el caso lo requiere, puede seleccionar menos o más de tres áreas de práctica de seguridad. Usted debe usar su mejor juicio al decidir el número de zonas para seleccionar.

Nota: Una vez que usted decide implementar mejoras en un área de práctica de seguridad para mitigar su los riesgos de seguridad de la organización, esas áreas de práctica se conocen como áreas de mitigación.

Para cada riesgo que se haya decidido a mitigar, en el círculo de riesgo apropiado de perfil, cuáles de las áreas de práctica de seguridad seleccionados mitigará este riesgo.

S5.3 Desarrollar Planes de Mitigación de Riesgo

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Plan de Mitigación	• Perfil de riesgo en su caso activo crítico • Procedimientos de seguridad • Estrategia de Protección • Lista de acciones • Notas y Recomendaciones • Información activo crítico

Definiciones

Plan de mitigación de riesgo - un plan que tiene por objeto reducir el riesgo a un activo crítico. Los planes de mitigación del riesgo tienden a incorporar actividades o medidas, destinadas a contrarrestar las amenazas a esos bienes.

Un equipo de análisis crea un plan de mitigación por separado para cada área de práctica de seguridad es seleccionado como área de mitigación durante la actividad anterior (Actividad S5.2).

Hay dos tipos de actividades de mitigación: actividades de mitigación generales y actividades de mitigación enfocadas.

Actividades de mitigación generales provocan un cambio en el enfoque de una zona de prácticas de seguridad característica. Actividades de mitigación enfocadas

• no requieren un cambio en el enfoque para la característica de una zona de prácticas de seguridad

• mejorar la forma en el enfoque actual para la característica de una zona de prácticas de seguridad, implementado actividades de mitigación enfocadas a menudo a activos específicos o se concentran en mejoras específicas.

Los planes de mitigación de riesgos a menudo están vinculados a la supervivencia de la empresa. En general, están diseñados para reducir los riesgos que podrían impedir que una organización logre su misión abordando el subyacente a las amenazas. Una actividad de mitigación puede frente a las amenazas en una o más de las siguientes maneras :

• Reconocer las amenazas a medida que ocurren.

• Resistir las amenazas para evitar que se produzcan.

• Recuperación de amenazas después de que ocurren.

Los planes de mitigación de riesgos comprenden los siguientes elementos :

• La actividad de mitigación - define las actividades de un equipo de análisis se recomienda implementar en una zona de prácticas de seguridad

• Algoritmo - documenta las razones para la selección de cada actividad de mitigación. La razón debe documentar si la actividad tiene la intención de reconocer las amenazas , resistirse a ellos , o recuperarse de ellas.

• La responsabilidad de mitigación - identifica que deben estar involucrados en la ejecución de cada actividad

• apoyo adicional - documenta cualquier apoyo adicional que se necesitará cuando la implementación de cada actividad (por ejemplo , la financiación , el compromiso del personal , patrocinio)

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA CIVIL Y MECÁNICA
Cdla. Universitaria (Huachi) / Telf: (03) 2841-144 / Telefax: (03) 2841-062/ Casilla 334/ Email: ficm@uta.edu.ec
Ambato – Ecuador

S5.3 Desarrollar Planes de Mitigación de Riesgo

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Plan de Mitigación	• Perfil de riesgo en su caso activo crítico • Procedimientos de seguridad • Estrategia de Protección • Lista de acciones • Notas y Recomendaciones • Información activo crítico

Instrucciones

1. Revise la información contenida en las siguientes hojas :
• Perfil de riesgo (para cada activo crítico)
• Prácticas de Seguridad.
• Protección Estrategia
• Lista de Acción
• Información de Activos Críticos (para cada activo crítico)

Es posible que necesite un contexto adicional para interpretar el impacto, la probabilidad y la vulnerabilidad información en las pestañas superiores. Revise sus definiciones de impacto, probabilidad y vulnerabilidad niveles de severidad en las siguientes hojas :
• Criterios de Evaluación de Impacto
• Criterios de Evaluación Probabilidad

2. Revisar toda la información que ha grabado a lo largo de la evaluación de los Bonos y Recomendación. Preste especial atención a las recomendaciones que le realizados en relación con las posibles actividades de mitigación.

Nota: Puede revisar la información que ha grabado durante la evaluación antes de seleccionar la mitigación. Las hojas de trabajo destacadas anteriormente constituyen el conjunto mínimo de información que usted necesitará durante esta actividad.

3. En este paso, creará planes de mitigación para cada área de práctica de seguridad que haya seleccionado durante la actividad anterior. Para cada área seleccionada, revise el rango de reducción de ese candidato, actividades en el candidato de mitigación, guía de actividades para esa área. La guía proporciona las posibles actividades de mitigación, pero no es una lista exhaustiva. No sea limitado por las actividades enumeradas en la guía.

4. Considere la siguiente pregunta para cada área de la mitigación seleccionada:
• ¿Qué actividades de mitigación reduciría el riesgo (s) que llevó a la selección de esta área?
• ¿Cuál es la justificación de la selección de cada actividad?
• ¿Quién debe participar en la ejecución de cada actividad? ¿Por qué?
• ¿Qué se necesita apoyo adicional cuando la implementación de cada actividad (por ejemplo, la financiación, el compromiso del personal, patrocinio)?

Desarrollar un plan de mitigación para cada área seleccionada.

Nota: Busque casos en que se anticipa que una actividad provocará un cambio en la estrategia de protección (es decir, las actividades de mitigación generales). Asegúrese de que anote esta información en el área de "Mitigación de actividad" para esa actividad.

S5.4 Identificar cambios en la Estrategia de Protección

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Estrategia de Protección	• Plan de Mitigación • Procedimientos de seguridad • Notas y Recomendaciones

Definiciones

Estrategia de protección de una organización define los métodos utilizados por la organización para permitir, iniciar, implementar y mantener su seguridad interna, proporcionando una dirección para la información futura, los esfuerzos de seguridad. La estrategia de protección se estructura de acuerdo a las áreas de práctica de seguridad resaltadas en la tabla de abajo .

Áreas de Práctica Estratégicas

1. Conciencia de Seguridad y Formación
2. Estrategia de Seguridad
3. Gestión de la Seguridad
4. Políticas y Reglamentos de Seguridad
5. Gestión de la Seguridad de Colaboración
6. Planes de Contingencia / Recuperación de Desastres

Áreas de Práctica Operacional

7. Control de Acceso Físico
8. Monitoreo y Auditoría Física de la seguridad
9. Sistema y Red de Gestión
10. Monitoreo y Auditoría de Seguridad Informática
11. Autenticación y autorización
12. Gestión de vulnerabilidades
13. Encriptación
14. Arquitectura de Seguridad y Diseño
15. Gestión de Incidentes

Durante la actividad S5.1 de OCTAVE -S, un equipo de análisis define la protección actual de su organización estratégica. Durante la actividad S5.2, el equipo selecciona las áreas de práctica de seguridad deben ser mejoradas para mitigar los riesgos más altos de prioridad de la organización. Luego, durante la actividad S5.3, el equipo desarrolla planes de mitigación para cada área de práctica de seguridad seleccionada como área de mitigación.

Los planes de mitigación de riesgos pueden incluir dos tipos de actividades: actividades de mitigación generales y actividades de mitigación específicas. Actividades de mitigación generales suelen desencadenar un cambio en la organización de la estrategia de protección, mientras que las actividades enfocadas a mejorar la forma en la estrategia de protección actual es implementada. Cada cambio en la estrategia de protección debe ser documentado. Documentar los cambios de estrategia de protección de una organización es el objetivo de la Actividad S5.4.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA CIVIL Y MECÁNICA
Cdla. Universitaria (Huachi) / Telf: (03) 2841-144 / Telefax: (03) 2841-062/ Casilla 334/ Email: ficm@uta.edu.ec
Ambato – Ecuador

S5.4: Identificar cambios en la Estrategia de Protección

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Estrategia de Protección	• Plan de Mitigación • Procedimientos de seguridad • Notas y Recomendaciones

Instrucciones

1. Revise la información contenida en las siguientes hojas :
• Plan de Mitigación (Revise cada plan)
• Protección Estratégica (Revisión de la estrategia actual)
• Prácticas de Seguridad
• Notas y Recomendaciones

Nota: Puede revisar la información que ha grabado durante la evaluación antes de realizar esta actividad. Las hojas de trabajo destacadas anteriormente constituyen el conjunto mínimo de información que usted necesitará durante esta actividad.

2. Cada zona de prácticas de seguridad comprende varias características. La excepción es la característica Responsabilidad (para áreas de práctica de seguridad operacional), que se muestra después de el diagrama de Políticas Documentadas.

3. Considere las siguientes preguntas para cada actividad de mitigación que identificó durante la actividad S5.3:
• ¿Esta actividad de mitigación indican un cambio en la protección de la organización estratégica?
• ¿Qué característica de la zona de prácticas de seguridad se verían afectados? ¿Cómo serían afectados?

Si determina que una actividad de mitigación afecta a una de las características de un área de práctica de seguridad, marque con una "X" en el cuadro titulado "Cambiar" al lado del nuevo enfoque sobre la Protección Estratégica.

Asegúrese de que usted llene los espacios en blanco proporcionados por la opción que seleccione. Puede cambiar las palabras proporcionadas o añadir palabras adicionales como sea necesario.

Nota: Se le proporcionará con líneas en blanco al final de todas las características. Si usted tiene una única respuesta por el enfoque de su organización para una característica, recuerde la estrategia en los espacios en blanco siempre y marque una "X" en el cuadro titulado "Cambiar" al lado de los espacios en blanco.

4. Revisar la estrategia de la hoja de trabajo. Examine la estrategia actual, así como cualquier cambio en la estrategia que usted ha identificado. Considere la siguiente pregunta al revisar la estrategia de protección:
• ¿Desea hacer cambios adicionales en la estrategia de protección?

Si su respuesta es sí, entonces marcar esos cambios en la estrategia de la hoja de trabajo de protección.

Después, usted necesita decidir para qué riesgos , si los hay, está impulsando este cambio en la estrategia de protección .

Vuelva a la hoja de trabajo Perfil de riesgo. Tenga en cuenta que los riesgos condujeron a la selección de la nueva estrategia encerrando en un círculo el área de práctica de seguridad correspondiente en el perfil de riesgo apropiado.

Es posible que un cambio en la estrategia de protección esté siendo impulsado por circunstancias distintas del riesgo (por ejemplo, la política, la regulación). Si este es el caso, no es necesario dar la vuelta a las áreas de práctica de seguridad sobre el perfil de riesgo.

En cualquier caso, identificar una o más actividades que producirán el cambio de la estrategia de protección.

Identificar y documentar en el plan de mitigación para el área de práctica de seguridad adecuada.

Nota: Para cualquier cambio en la estrategia de protección que está impulsado por circunstancias distintas del riesgo, asegúrese de documentar esos factores en el área de "Justificación" para esa actividad.

S5.5 Identificar próximos pasos

Hoja de Trabajo de Actividades	Hoja de Trabajo de referencia
Pasos siguientes	• Estrategia de Protección • Plan de Mitigación • Lista de acciones

Definiciones

Creación de un conjunto de pasos a seguir marca el final de OCTAVE-S. Esta actividad requiere que el equipo de análisis debe considerar lo que debe hacerse para facilitar la aplicación de los resultados de la evaluación. Los próximos pasos suelen abordar las cuatro áreas siguientes:

• Patrocinio de gestión para la mejora de la seguridad - la definición de lo que la administración debe hacer para apoyar la implementación de los resultados de OCTAVE-S

• supervisar la aplicación - la identificación de lo que la organización va a hacer en un seguimiento del progreso y asegurar que los resultados de OCTAVE-S se implementan

• la ampliación de la actual evaluación de riesgos de seguridad de información - para determinar si la organización necesita ampliar la actual evaluación OCTAVE-S para incluir activos críticos adicionales o áreas operacionales adicionales

• siguiente información de la evaluación de riesgos de seguridad - la determinación de cuando la organización llevará a cabo su próxima evaluación OCTAVE-S

Instrucciones

1. Revisión (como mínimo) la información contenida en las siguientes hojas:
• Plan de Mitigación
• Protección Estratégica
• Lista de Acción

Considere las siguientes preguntas:
• ¿Qué debe hacer la gestión para apoyar la aplicación de los resultados de OCTAVE-S?
• ¿Cuál el seguimiento del progreso que debe hacer la organización y asegurar que los resultados de esta evaluación se implementen?
• ¿Va a ampliar la actual evaluación OCTAVE-S para incluir activos críticos adicionales? ¿Cuáles?
• ¿Cuándo la organización realizará su próxima evaluación OCTAVE-S?

Nota: Las preguntas anteriores se centran en lo que piensan los altos directivos que hacer para activar y fomentar la aplicación de los resultados de la evaluación, así como la mejora de la seguridad en curso.
Determine qué medidas que la organización debe adoptar para aplicar los resultados de esta evaluación.

2. En este punto, usted ha completado una evaluación OCTAVE-S. Asegúrese de formalmente documentar los resultados de esta evaluación. El formato para la documentación de los resultados de OCTAVE-S debe adaptarse a las pautas normales de documentación de la organización y debe ser adaptada para satisfacer las necesidades de la organización.

Nota: Es importante establecer un registro permanente de los resultados de la evaluación. La información que graba puede servir como material de partida para posteriores evaluaciones y también es útil cuando el seguimiento del estado de los planes y acciones después de la evaluación.