RESUMEN

La presente tesis, Análisis y Gestión de Riesgos de los Sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, tiene por objetivo la aplicación del modelo MAGERIT versión 2 -Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información-, el que contribuirá a que la institución posea un conocimiento claro sobre los riesgos que pueden presentarse en sus sistemas de información.

El modelo MAGERIT fue desarrollado por el Consejo Superior de Administración Electrónica de España, como respuesta al crecimiento acelerado de la tecnología de información y al mayor uso que hacen las Organizaciones, con la finalidad de concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de mitigarlos a tiempo.

Las fases que contempla el modelo MAGERIT son:

1. Planificación del Proyecto.- establece el marco general de referencia para el proyecto
2. Análisis de Riesgos.- permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos
3. Gestión de Riesgos.- permite la selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados

Al aplicar la Metodología MAGERIT, es indispensable implementar la herramienta PILAR Basic, la cual conjuga los activos de un sistema, identifica las posibles amenazas e incorpora las salvaguardas que permitan minimizar el riesgo.

Con la aplicación de la herramienta se podrá conocer el nivel de riesgo actual de los activos, y con la aplicación de nuevas salvaguardas o mejorando las ya implantadas, se podrá conocer el riesgo reducido.

Autores:
Antonio Lucero G.
John Valverde P.

PALABRAS CLAVE:

- Análisis
- Gestión
- Riesgo
- MAGERIT
- PILAR Basic

ABSTRACT

This present thesis, “Análisis y Gestión de Riesgos de los Sistemas de Información de la Cooperativa de Ahorro y Crédito Jardín Azuayo” has the objective to apply model, MAGERIT version 2- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – which will allow the mentioned institution have a clear idea about the risks that may arise in their information systems, identifying critical areas that require greater control.

The model MAGERIT was developed by the CSAE (Consejo Superior de Administración Electrónica) in Spain, as a response to the rapid growth of technology information and the increasing use of IT by organizations. It was also designed with the final purpose of allowing those who are responsible for the information systems to become more conscious of the existence of risks and the need to mitigate them promptly.

The phases that the MAGERIT model envisions are:

1. Planning of the Project .- sets a reference of the general framework for the project
2. Risk Analysis.- allows you to determine how it is, the worth, and how protected the assets are.
3. Risk Management.- allows the selection and implementation of safeguards to know, to prevent, to avoid, and to reduce or control the risks identified.

In order to implement the MAGERIT methodology, it is essential to implement the PILLAR Basic tool, which combines the assets of a system, identifies the potential threats, and incorporates the safeguards that enable institutions to minimize risks.

With the implementation of the tool institutions will be able to know the level of the current risk of the assets. Also with the application of new safeguards or improving the already established ones, you can know the reduced risks.

ÍNDICE

LISTADO DE GRÁFICOS

LISTADO DE TABLAS

LISTADO DE FIGURAS

LISTADO DE ANEXOS

UNIVERSIDAD DE CUENCA

Fundada en 1867

Yo, Antonio José Lucero Gómez, reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Contador Publico Auditor. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Antonio Lucero G.
1400708382

UNIVERSIDAD DE CUENCA

Fundada en 1867

Yo, Antonio José Lucero Gómez, certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor/a.

Antonio Lucero G.
1400708382

UNIVERSIDAD DE CUENCA

Fundada en 1867

Yo, John Oswaldo Valverde Padilla, reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Contador Publico Auditor. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

John Valverde P.
1400739304

UNIVERSIDAD DE CUENCA

Fundada en 1867

Yo, John Oswaldo Valverde Padilla, certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor/a.

John Valverde P.
1400739304

UNIVERSIDAD DE CUENCA

FACULTAD DE CIENCIAS ECONOMICAS Y ADMINISTRATIVAS

ESCUELA DE CONTABILIDAD Y AUDITORIA

“ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO JARDÍN AZUAYO, UTILIZANDO LA METODOLOGIA MAGERIT”

Tesis previa a la obtención del título de Contador Público Auditor

AUTORES:

ANTONIO JOSÉ LUCERO GÓMEZ

JOHN OSWALDO VALVERDE PADILLA

DIRECTOR:

ING. WILSON CUEVA

CUENCA – ECUADOR

2011 - 2012

DECLARACIÓN

Nosotros **ANTONIO JOSÉ LUCERO GÓMEZ Y JOHN OSWALDO VALVERDE PADILLA,** declaramos que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificado profesional; y hemos consultado las referencias bibliográficas que contiene en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondiente a este trabajo a la **UNIVERSIDAD DE CUENCA,** según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y en la normatividad institucional vigente.

---	---
Antonio J. Lucero Gómez	John O. Valverde Padilla

AGRADECIMIENTO

Queremos agradecer primeramente a nuestro querido Dios, por permitirnos alcanzar una meta más en nuestras vidas. A nuestros padres por darnos su amor y apoyo incondicional; a nuestros maestros que nos guiaron e impartieron conocimientos para desenvolvernos con profesionalismo; a nuestro Director de Tesis Ing. Wilson Cueva, quien ha sido un excelente amigo y guía, brindándonos su total apoyo y tiempo para culminar con el proyecto; a todo el personal de la Cooperativa de Ahorro y Crédito Jardín Azuayo, por facilitarnos con la información necesaria para el desarrollo de nuestro trabajo, a nuestros amigos por compartir experiencias inolvidables.

Antonio - John

DEDICATORIA

Dedico todo el esfuerzo de este trabajo a Dios por darme sabiduría y fortaleza para lograr mis objetivos, además de su infinita bondad y amor.

A mis padres Luis y María, por haberme apoyado en todo momento, por sus consejos, por sus enseñanzas, por su cariño, comprensión, paciencia y amor que me han brindado para la culminación de mi carrera profesional.

A mis hermanos por su cariño y apoyo incondicional en todas las etapas de mi vida.

A mis familiares y amigos Gracias por su apoyo y las palabras de ánimo que me dieron para el desarrollo de mi formación tanto profesional como personal.

Antonio Lucero Gómez

DEDICATORIA

Este trabajo lo dedico a Dios por darme la fuerza y dedicación para alcanzar mis metas.

A mis padres, Víctor y Zoila, que siempre me han dado su cariño, sus buenas enseñanzas y su apoyo incondicional para la culminación de mi carrera profesional.

A mis hermanos: Luis, Rodolfo, Nely, Narcisa y Jorge, por su gran cariño y apoyo en mi carrera; a mis familiares y amigos, que de una u otra manera me han apoyado y dado fuerzas para culminar con mis estudios.

John Valverde

INTRODUCCIÓN

El presente tema de tesis consiste en realizar un Análisis y Gestión de Riesgos de los Sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo, el mismo que tiene por objetivo la aplicación del modelo MAGERIT versión 2 -Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información-, metodología que contribuirá a que la institución posea un conocimiento claro sobre los riesgos que pueden presentarse en sus sistemas de información, identificando las áreas críticas que requieran un mayor control. La tesis se ha dividido en cinco capítulos.

En el capítulo 1 Antecedentes; trataremos una breve descripción del objeto de estudio, así como aspectos conceptuales de la Metodología MAGERIT y su herramienta PILAR Basic para el análisis y gestión de riesgos.

En el capítulo 2 Planificación del Proyecto; se establecen las consideraciones necesarias para arrancar el proyecto de Análisis y Gestión de Riesgos, se investiga la oportunidad de realizarlo, se define los objetivos que ha de cumplir y el dominio que abarcará, se planifican los medios materiales y humanos para su realización y se procede al lanzamiento del proyecto.

En el capítulo 3 Análisis de Riesgos; es la parte central del proyecto en donde se identifica los activos relevantes de la Organización, se identifican las amenazas sobre aquellos activos, se identifica las salvaguardas existentes, las vulnerabilidades, y se estima el impacto y el riesgo al que están expuestos los activos del sistema.

En el capítulo 4 Gestión de Riesgos; se identifica los riesgos críticos y se toma las medidas de seguridad necesarias para enfrentarlos, implantando salvaguardas de seguridad ya sean nuevas salvaguardas o mejorando las ya existentes, y elaborando un plan de seguridad, con el fin de prevenir, impedir reducir y/o controlar los riesgos identificados en la Organización.

En el capítulo 5 Conclusiones y Recomendaciones; contiene las opiniones y acciones a seguir, como resultado del Análisis y Gestión de Riesgos del presente proyecto.

CAPÍTULO 1

ANTECEDENTES

1.1. DESCRIPCIÓN DEL OBJETO DE ESTUDIO

1.1.1. ANTECEDENTES

Breve Reseña Histórica

La Cooperativa de Ahorro y Crédito Jardín Azuayo (COAC JA) nació en Paute en febrero de 1996, en el contexto de la reconstrucción del cantón Paute, luego de los daños causados por el desastre de La Josefina (1993), hizo que las poblaciones afectadas enfrenten una emergencia de grandes proporciones, ante lo cual con el apoyo del Centro de Educación y Capacitación del Campesinado del Azuay (CECCA) y la Iglesia, a fin de mejorar su situación se planteó como alternativas, crear una Cooperativa, de esta manera el 27 de mayo de 1996 nace La Cooperativa de Ahorro y Crédito Jardín Azuayo mediante el acuerdo 0836 del Ministerio de Bienestar Social e ingresó a la Superintendencia de Bancos y Seguros en enero del 2007. Empezó con 120 socios fundadores.

La reconstrucción fue una oportunidad para plantear un nuevo estilo de desarrollo con una base en la comunidad que permita mejorar sus formas de producir, se potencie sus capacidades, transforme el ahorro local y extra local en créditos que dinamicen las condiciones de vida del socio (a) y su entorno.

Jardín Azuayo trabaja de manera sostenible y solvente, generando nuevos actores sociales con conciencia ciudadana, solidaria y global, profundizando la confianza, apoyada en sus directivas locales, que permiten consolidarse como una institución propia en cada lugar en el que está presente.

Actualmente Jardín Azuayo cuenta con 27 oficinas ubicadas en las provincias de Azuay, Cañar, Morona Santiago, Loja y El Oro, (30 puntos de atención) y más de 205.000 socios. Cada oficina está conformada

con sus directivos y empleados que coordinadamente gestionan el progreso de la Institución, contribuyendo al desarrollo local de los pueblos.[1]

1.1.2. PENSAMIENTO ESTRATÉGICO[2]

1.1.2.1. Misión

Es lo que somos y lo que hacemos para alcanzar nuestra Visión:

La Misión de la COAC Jardín Azuayo es: *"Fomentamos el desarrollo de una cultura Cooperativa haciendo de nuestra Institución una escuela de Cooperativismo, con organización, participación, comunicación, información e interacción en redes Institucionales. Desarrollamos productos y servicios sociales y financieros acordes a la demanda con tecnología adecuada, cobertura nacional e internacional, que permitan la recirculación de los recursos locales y regionales con sentido de equidad entre socios y entre regiones."*

1.1.2.2. Visión

La Visión de la COAC Jardín Azuayo para el 2013 es:

"Somos una sociedad de personas con cultura cooperativa que buscamos nuestro buen vivir, el de nuestras comunidades y el de la sociedad en general, privilegiando a los sectores populares, con una organización solidaria, confiable, solvente, referente del Cooperativismo nacional e internacional; con este fin desarrollamos actividades sociales y financieras eficientes, competitivas y de calidad, integrando pueblos y culturas."

1.1.2.3. Objetivos Generales

Entre los principales objetivos de la cooperativa tenemos:

- Fomentar en los socios mejores condiciones de trabajo y el aumento de la producción y la productividad, mediante la prestación de servicios financieros competitivos y oportunos;

[1] www.jardinazuayo.fin.ec
[2] La Misión, Visión, Principios y Valores fue tomado del Plan Estratégico 2009-2013

- Fomentar el ahorro de los socios y sus comunidades;
- Fomentar los principios cooperativos como base fundamental del funcionamiento y desarrollo de la cooperativa;
- Procurar fuentes de financiamiento interno y externo, para el desarrollo Institucional y de sus asociados;
- Potenciar la formación y capacitación de directivos y socios;
- Promover el desarrollo integral de los socios y sus comunidades;
- Apoyar en capacitación a organizaciones productivas integradas por socios de la cooperativa.

1.1.2.4. Valores y Principios Institucionales

Valores:

Transparencia.- mostramos como somos-sin reservas. Hace relación a la Ética, entendiendo como la lógica de lo racional, la actuación con la verdad, en cuyo fortalecimiento es importante la socialización de la información y la capacitación.

Honestidad.- claridad, transparencia, cumplimiento. Expresado a través de la realización del trabajo diario, que se realiza con absoluta claridad para ayudar al crecimiento de quienes lo reciben y también de quienes lo generan.

Compromiso.- apropiarnos de las responsabilidades adquiridas. Exige fortalecer la gobernabilidad, entendida como la capacidad y compromiso de los consejos directivos por enfrentar los cambios y generar condiciones para el cumplimiento del presente plan estratégico. Sin duda que elevar la convicción y compromiso, es un proceso continuo de mejoramiento, en ello juega un rol importante la capacitación y los sistemas de comunicación como herramientas que generan implicación social, pues sin ello, toda programación será una propuesta cargada de buena voluntad social.

Responsabilidad.- cumplir oportunamente con nuestros deberes y derecho. Expresada a través del trabajo en equipo (Directivos,

Empleados, Gerencia, Socios) que en conjunto buscan tomar y ejercer las mejores decisiones para brindar servicios eficientes, con calidad, que les permitan a los socios mejorar su futuro.

Confianza.- la confianza, se relaciona con la seguridad que tiene los socios en sus ahorros, de ser parte, propietario, socio de la Cooperativa. De pertenecer y contribuir a que la Cooperativa tenga buen desempeño nivel Financiero y Social.

Fidelidad.- sentido de pertenencia, lealtad, compromiso, confianza, conoce, apropiación consecuente con objetivos Institucionales.

Democracia.- se relaciona con la equidad, encierra el hecho de democratizar los servicios financieros, que estos sean accesibles para todos respetando e integrando pueblos y cultura.

Evoca la participación colectiva.

Buscando el bienestar de la mayoría.

Respeto al Medio Ambiente.- en sintonía con una nueva conciencia planetaria, integrados a una comunidad de vida, responsables con el cuidado de nuestra casa común.

Principios Cooperativos:

- Adhesión abierta y voluntaria.
- Gestión democrática de los socios y socias.
- Participación económica de los socios y socias.
- Autonomía e independencia
- Educación, capacitación e información
- Cooperación entre Cooperativas
- Compromiso con la comunidad

1.1.3. ESTRUCTURA DE LA COOPERATIVA

Gráfico 1-1: Estructura Organizativa de la Cooperativa de Ahorro y Crédito Jardín Azuayo

Fuente:http://www.jardinazuayo.fin.ec/index.php?option=com_content&view=article&id=85&Itemid=29

La Coac “Jardín Azuayo” funciona con una Asamblea General de Representantes elegidos en cada oficina en función del número de socios, asambleas generales de oficina, asambleas locales de socios. De las asambleas locales salen los integrantes de las comisiones locales que apoyan el trabajo de la oficina en administración y créditos y los delegados para las asambleas generales de cada oficina, y su presidente. Los presidentes de cada oficina pasan a conformar el Consejo de Administración. Las asambleas de oficina tienen, también, el encargo de elegir a los delegados para la asamblea general en concordancia con el número de socios.

El Consejo de Administración de la Cooperativa “Jardín Azuayo” funciona con cinco miembros elegidos entre los presidentes y un comité

consultivo integrado por los presidentes restantes que sugiere y recomienda acciones, reduciendo el riesgo de concentración de decisiones. El Comité de Auditoría está conformado por cinco miembros: dos miembros del consejo de administración, un profesional externo a la Institución, el Auditor Interno y el Gerente. El Comité de Crédito lo integran el gerente y dos miembros elegidos por el Consejo, este comité fija políticas crediticias y delega responsabilidades a los comités de oficina y locales.[3]

1.1.4. ACTIVIDADES

La Cooperativa es una entidad de intermediación financiera dedicada a la captación de recursos de sus socios a través de libretas de ahorro y certificados de depósito a plazo fijo; y el otorgamiento de créditos en su mercado de influencia, satisfaciendo de esta manera las demandas de créditos ordinarios y extraordinarios vinculados a actividades de Desarrollo, Vivienda.

1.1.5. RECURSOS

1.1.5.1. Recursos Materiales.- la Cooperativa cuenta con los siguientes clasificación de activos:

- Terreno
- Edificio
- Vehículos
- Muebles y Enseres
- Equipo de Oficina
- Equipo de Computación
- Comunicación

1.1.5.2. Recursos Humanos.-

[3] www.jardinazuayo.fin.ec

PROVINCIAS	OFICINA/VENTANILLA	N° EMPLEADOS
Azuay	Chordeleg	4
	Cuenca	16
	El Valle	6
	Ricaurte	4
	Totoracocha	6
	Yanuncay	6
	Gualaceo	11
	Nabón - Shiña	7
	Oña	4
	Palmas - Sevilla de Oro	4
	Paute (Matriz)	14
	Pucará	4
	San Fernando	2
	Santa Isabel	9
	Sigsig	12
Cañar	Azogues	8
	Cañar	8
	El tambo	5
	La Troncal	13
	Suscal	5
Morona Santiago	Gualaquiza	7
	Limón Indanza SJ Bosco	10
	Macas	13
	Méndez	7
	Sucúa	7
Loja	Saraguro	5
El Oro	Pasaje	11
	COORDINACIÓN	81
	Total	289

Tabla 1-1: Distribución del Personal por Provincias

Fuente: Cooperativa de Ahorro y Crédito Jardín Azuayo
Elaborado por: autores

1.1.5.3. Recursos Financieros.- la COAC Jardín Azuayo se mantiene económicamente a través de los servicios de Ahorro y del Crédito.

a) Ahorro.-

- Ahorro a la Vista
- Certificados de Depósitos
- Mi alcancía Segura

b) Crédito.-

- Crédito Ordinario
- Crédito Extraordinario
- Crédito sin Ahorro
- Crédito para Desarrollo

1.1.5.4. Recursos Tecnológicos.- los principales recursos de la Institución son:

- Sistema Financiero Integrado Jardín Azuayo
- Internet
- Sistema de comunicación mediante IP
- Servidor de correo electrónico Zimbra
- Servicio de archivo compartido por iFolder
- Hardware:
  - Servidor de Base de Datos
  - Computadoras de escritorio, portátiles
  - Impresoras matriciales y laser, entre otros

1.2. ASPECTOS CONCEPTUALES

1.2.1. ANÁLISIS Y GESTIÓN DE RIESGOS

Previo a un Análisis y Gestión de Riesgos dentro de una Organización, es importante conocer el concepto de Seguridad, el mismo que se define como: "*la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o mal intencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles."*[4]

Por tal razón, la misión de la Organización es proteger la información, lo cual hace indispensable considerar las dimensiones de seguridad:

- **Disponibilidad.-** permite que el personal autorizado tenga acceso a la información y a sus activos asociados cuando sea necesario.

  La falta de disponibilidad podría interrumpir el servicio, afectando directamente a la productividad de la organización.

- **Integridad.-** garantiza exactitud, completitud y corrección de la información.

  Si la información aparece manipulada, corrupta o incompleta, las funciones de la Organización quedarían afectadas y por ende su desempeño.

- **Confidencialidad.-** certeza de que la información llegue únicamente a las personas autorizadas.

  La falta de confidencialidad podría dar lugar a la salida y entrada de información a personas no autorizadas, así como accesos no autorizados.

[4] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.7

- **Autenticidad.**- que la persona que se hace responsable de la información o prestación de servicio sea confiable y no exista duda sobre él, para evitar que se generen suplantación de identidad y engaños que buscan realizar un fraude.

Las características antes mencionadas son las que pretenden conseguir toda Organización, pero esto no se llega a alcanzar, por lo tanto es necesario poner medios y esfuerzos para conseguirlas, aplicando un Análisis y Gestión de Riesgos.

Para entender esta metodología partiremos con las definiciones de:

- **Riesgo.-** *"estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización"*.[5] Dicho concepto nos indica lo que le podría suceder a nuestros activos si no son protegidos adecuadamente.

  Es necesario conocer las características importantes de cada activo, así como el peligro en las que se encuentran, para lo cual será necesario analizar el sistema.

- **Análisis de Riesgos.-** *"proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización".*[6]

  El análisis de riegos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento.

  El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos.

  Una vez identificado y analizado los riesgos es necesario tomar decisiones con el fin de contrarrestar dichos riesgos.

[5] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.8

[6] Ibíd.

- **Gestión de Riesgos.**- "*selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados".*[7]

  La gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis.

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 acepta la dirección.

En toda organización siempre existirá cierto nivel de riesgo y no podrá ser reducida a cero, debido a que la seguridad absoluta no existe, por tanto siempre hay que aceptar un cierto nivel de riesgo, el mismo que debe ser conocido y sometido a su más bajo nivel.

La Organización al aceptar cierto nivel de riesgo es consciente y sabe de las condiciones en las cuales trabaja, dando la confianza al sistema de ajustarse con las actividades diarias, con el fin de tener menos incertidumbre.

Para elaborar el Análisis y Gestión de Riesgos en una Organización, se debe de establecer una metodología, la misma que permita gestionar la Seguridad de Información. El modelo MAGERIT es la metodología mejor recomendada para el análisis y gestión de riesgos, el cual permite realizar una evaluación profunda de la Seguridad de los Sistemas de Información en una Organización.

[7] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.8

1.2.2. DESCRIPCIÓN DE LA METODOLOGÍA MAGERIT – versión 2

1.2.2.1. Introducción a MAGERIT

El CSAE (Consejo Superior de Administración Electrónica) de España, ha elaborado y promueve MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas) 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 de servicio.[8]

La razón de ser de MAGERIT está pues directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que garanticen la autenticación, confidencialidad, integridad y disponibilidad de los sistemas de información y generan confianza cuando se utilicen tales medios.[9]

Una organización no alcanzará sus objetivos, metas y misión si no tiene a su alcance los elementos informáticos básicos e indispensables que le ayuden y soporten sus decisiones.

1.2.2.2. Breve conceptualización

MAGERIT es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.[10]

1.2.2.3. Objetivos de MAGERIT[11] – versión 2

MAGERIT persigue los siguientes objetivos:

[8] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.6
[9] Ibíd.
[10] http://www.ar-tools.com/index.html
[11] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.6,7

Directos:

1. Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
2. Ofrecer un método sistemático para analizar tales riesgos.
3. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

Indirectos:

4. Preparar a la organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

1.2.2.4. Elementos de MAGERIT v.2[12]

A continuación definimos brevemente los elementos considerados significativos por MAGERIT para el estudio de los Sistemas de Información.

- **Activos:** recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la Dirección.
- **Amenazas:** eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o perdidas inmateriales en sus activos.
- **Vulnerabilidad de un activo:** potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
- **Impacto de un activo:** consecuencia sobre éste de la materialización de un activo.

[12] http://www.cii-murcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.pdf

- **Riesgo:** posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.
- **Servicio de salvaguarda:** acción que reduce el riesgo.
- **Mecanismo de salvaguarda:** procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

La siguiente figura muestra los elementos y sus interrelaciones:

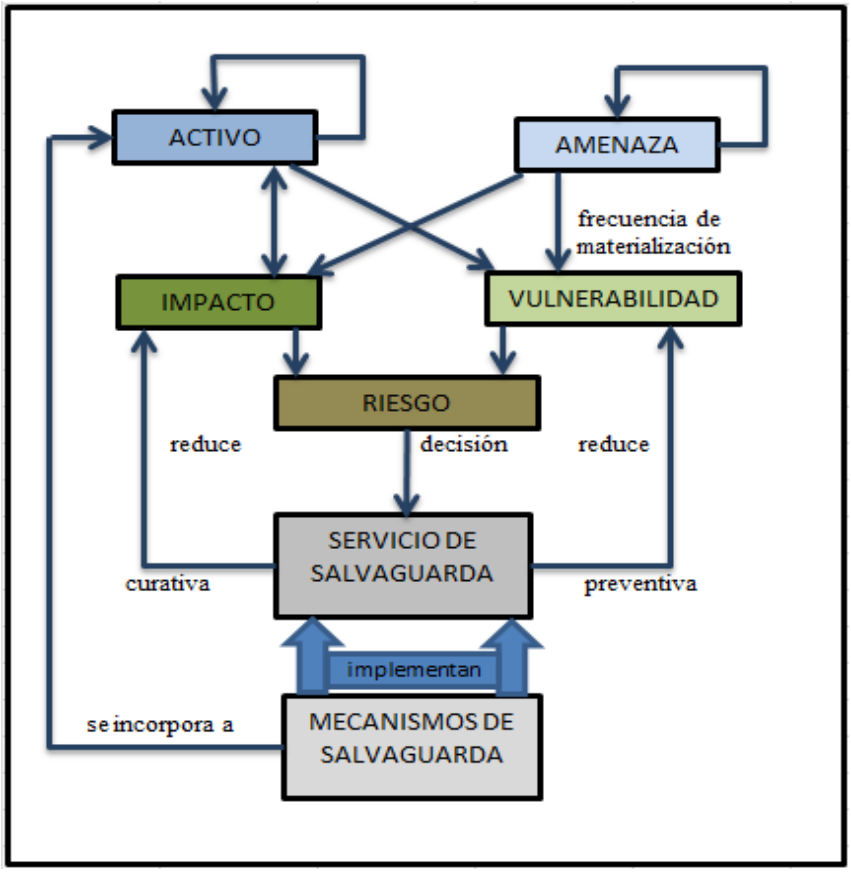


Figura 1-1: Elementos del MAGERIT

Fuente:http://www.cii-murcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.pdf
Elaborado por: autores

1.2.2.5. Aplicación de MAGERIT v.2

- Es aplicable a la totalidad del ciclo de vida del sistema de información
- Se puede llevar a cabo en diferentes momentos, con diferentes grados de precisión, detalle y rigor

- Dependiendo del tamaño de la organización y de la complejidad del sistema de información

MAGERIT permite:[13]

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

En una Organización, para poder aplicar la Metodología MAGERIT, es indispensable implementar la herramienta PILAR Basic, la cual conjuga los activos de un sistema, identifica las posibles amenazas e incorpora las salvaguardas que permitan minimizar el riesgo.

PILAR, acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una aplicación informática desarrollada bajo especificación del Centro Criptológico Nacional - Centro Nacional de Inteligencia (CCN-CNI), para soportar el análisis de riesgos de sistemas de información siguiendo la metodología MAGERIT, la herramienta comercial está ampliamente utilizada en la Administración Pública Española y en la actualidad también en organismos no gubernamentales.

13 http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

Objetivos de PILAR[14]

- Realizar el análisis según la metodología MAGERIT
- Diseño del plan de mejora de la seguridad

PILAR Basic ofrece un conjunto de herramientas que permiten: [15]

- Bien un análisis general, estudiando las diferentes dimensiones de seguridad (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad)
- Bien un análisis de continuidad, centrándose en la disponibilidad del sistema de información para atajar interrupciones de servicio ante incidencias o desastres.

Además la herramienta PILAR Basic, permite realizar un seguimiento continuo del sistema de la Organización, con el fin de que el sistema enfrente riesgos actuales y futuros y así tener mayor confianza del sistema que posee.

[14] http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=161

[15] MÉNDEZ, Andrés, MAÑAS, José Antonio, 2010, MANUAL DE USUARIO PILAR BASIC versión 4.4, Ministerio de Administraciones Públicas, España, p. 5

CAPÍTULO 2

PLANIFICACIÓN DEL PROYECTO

2.1. OBJETIVOS

Antes de iniciar con el Análisis y Gestión de Riesgos (AGR) de los sistemas de información (S.I) de la oficina Coordinación y Cuenca de la Cooperativa de Ahorro y Crédito (COAC) Jardín Azuayo, es importante que conozcamos la situación que presentan los S.I., lo cual podemos conocer mediante la etapa de Planificación, la misma que tiene como objetivo principal establecer el marco general de referencia para todo el proyecto.

El proyecto de AGR será desarrollado con la metodología MAGERIT bajo la aplicación de la herramienta PILAR Basic 4.4.

Como objetivos complementarios a lograrse en esta etapa podemos identificar los siguientes:

- Motivar y concienciar a la Gerencia de la Organización
- Razonar y validar la oportunidad de realizar un proyecto AGR
- Dar a conocer la voluntad de la Gerencia para la realización del proyecto
- Crear condiciones adecuadas y necesarias para el buen desarrollo del proyecto

Para un trabajo eficiente de la etapa de Planificación, se necesitará la colaboración y participación de todo el personal involucrado con los sistemas de información.

Para el desarrollo del proceso de Planificación de Análisis y Gestión de Riesgos, aplicaremos los siguientes pasos: [16]

- Estudio de oportunidad
- Determinación del alcance del proyecto

[16] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.38

- Planificación del proyecto
- Lanzamiento del proyecto

2.2. ESTUDIO DE OPORTUNIDAD

Esta actividad tiene por objetivo suscitar el interés de la Dirección de la Organización en la realización de un proyecto de Análisis y Gestión de Riesgos.

En la Cooperativa de Ahorro y Crédito Jardín Azuayo la Gerencia suele ser consciente de las ventajas que aportan las técnicas electrónicas, informáticas y telemáticas a su funcionamiento, pero no de los nuevos problemas de seguridad que estas técnicas implican.

Con la aplicación de entrevistas realizadas al personal de informática y de riesgos de la COAC Jardín Azuayo, nos hemos percatado que no se han generado incidentes significativos relacionados a la Seguridad de la Información; lo que podemos indicar como un problema es la falta de control de los soportes de información, donde la información queda vulnerable para los usuarios que tengan acceso a ella.

Otros problemas a considerar son el crecimiento acelerado de la Base de Datos, control ineficiente de los activos de tecnología, dificultad en el proceso de aplicación de nuevos sistemas, infraestructura inadecuada de los sistemas de información.

Tiene un nivel de seguridad adecuado en cuanto al respaldo de la información.

2.3. DETERMINACIÓN DEL ALCANCE DEL PROYECTO

Una vez que se ha constatado la oportunidad de realizar el proyecto de Análisis y Gestión de Riesgos y el apoyo de la Dirección, esta actividad procede a identificar los objetivos que debe cumplir el proyecto y a definir su dominio y límites.

Los objetivos se sistematizan en tres fases:

- Planificación global de la seguridad

- Análisis de la situación actual y especificación de necesidades funcionales de seguridad
- Diseño de los mecanismos de salvaguarda

El dominio del proyecto se centra en el Departamento Informático de la Cooperativa de Ahorro y Crédito Jardín Azuayo, oficina Coordinación y Cuenca.

Personal del Departamento Informático involucrado en la realización del proyecto:

- Ingeniero Hernán Urgilés – Coordinador de Auditoría
- Ingeniero Fabián Cuesta – Auditor Informático
- Ingeniero David Ávila – Infraestructura y Telecomunicaciones
- Ingeniero Jorge Bonete – Administración de Base de Datos
- Ingeniero Marco Paredes – Ingeniería de Software
- Ingeniero Omar Vélez – Programador desarrollador
- Ingeniero Fabricio Barreto – Soporte a Usuarios, entre otros.

La restricción estipulada por la COAC Jardín Azuayo es al acceso a la información confidencial como medida de protección.

2.4. PLANIFICACIÓN DEL PROYECTO

Esta actividad estima los elementos de Planificación del proyecto, es decir sus cargas de trabajo, el grupo de usuarios, los participantes y su modo de actuación y el plan de trabajo para la realización del proyecto.

En la COAC Jardín Azuayo para la realización de las entrevistas se solicitarán una cita a cada entrevistado en un plazo no mayor a 15 días laborables.

Las entrevistas nos ayudaran a determinar por ámbito a los usuarios afectados y a planificar la intervención de ellos en el proyecto.

El proyecto AGR de los Sistemas de información de la Cooperativa de Ahorro y Crédito Jardín Azuayo está constituido por los siguientes órganos:

- Equipo de Estudio.- está constituido por un Director de proyecto; y dos egresados en Contabilidad y Auditoría.
- Grupo de usuarios.- está formado por los utilizadores, actuales, del Sistema de Información.

2.5. LANZAMIENTO DEL PROYECTO

Esta actividad completa las tareas preparatorias del lanzamiento del proyecto de Análisis y Gestión de Riesgos: empezando por seleccionar y adaptar los cuestionarios que se utilizaran en la recogida de datos, así como especificar los criterios y las técnicas a emplear en el Análisis y Gestión de Riesgos; y terminando por asignar los recursos necesarios para para la realización del proyecto y por la campaña informativa de sensibilización a los implicados en el proyecto.

Para la recogida de información se ha realizado una adaptación a las fichas del Apéndice 2 del libro II – Catálogo de Elementos MAGERIT-versión 2, debido a la especificidad de este proyecto. Las fichas de recolección de información deben verse por tanto, más que un recordatorio para el análisis que un documento a auto rellenar directamente por los responsables del Dominio. (Ver Anexo 1. Fichas para la recolección de datos)

La técnica utilizada para la recogida de información se adaptan con el objeto de identificar correctamente los elementos de trabajo: activos, amenazas, vulnerabilidades, impactos, salvaguardas existentes, restricciones generales; la necesidad de una adaptación siempre existe debido al problema de la seguridad que puede y debe tratar MAGERIT.

La situación de la seguridad de los sistemas de información de la COAC Jardín Azuayo es producto de la incorporación de las salvaguardas tomadas para prevenir o reducir unos riesgos hasta ahora no analizados de forma sistemática. Por el momento no ha tenido fallos operacionales informáticos de envergadura que hayan forzado a tomar precauciones drásticas.

Sin embargo, la falta de análisis sobre riesgos no ha permitido priorizar hasta ahora estas numerosas medidas adquiridas, dicho análisis permitirá

racionalizar las medidas actuales y completarlas con algunas otras. El estudio previo encargado se basa parcialmente en esta situación paradójica de abundancia y a la vez carencia de medidas de seguridad, lo que exige un Análisis global de riesgos.

La COAC Jardín Azuayo dispone los recursos a utilizarse para el desarrollo del proyecto, disponibilidad de equipos, tiempos planificados, medios materiales-herramientas, traslado de documentos y manuales etc.

Se ha realizado la comunicación a las unidades afectadas sobre el lanzamiento del proyecto. Se realizó un dialogo con el Jefe de Talento Humano señor Henry Quezada, sobre el proyecto y su contenido, quien nos supo informar que la unidad implicada conoce sobre el proyecto y que están prestos a apoyarnos para el desarrollo del mismo. Además se envió un oficio a la Gerencia en el cual se indicaba el proyecto, sus objetivos, la metodología y demás parámetros formales para una ejecución correcta y formal del proyecto de Análisis y Gestión de Riesgos.

Indicado lo anterior, se nos informó que el proyecto está autorizado y listo para su ejecución.

CAPÍTULO 3

ANÁLISIS DE RIESGOS

Como es de conocimiento general, toda organización se encuentra expuesta a riesgos; debido a que no existe un entorno 100% seguro, ya que la exposición de riesgos es constante. Por tal motivo toda organización deberá estar alerta a cualquier cambio o situación extraña y que considera que podría afectar negativamente a un activo, a un dominio o a toda su organización.

Esta etapa se constituye en el núcleo central de MAGERIT, y su correcta aplicación condiciona la validez y utilidad de todo el proyecto.

Objetivos del Análisis de Riesgos:

1. Identificar los activos relevantes que poseen la organización
2. Identificar las amenazas a las que están expuestos dichos activos
3. Determinar si existen salvaguardas para los activos
4. Estimar el impacto si una amenaza llegara a materializarse

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos evaluando de manera metódica para llegar a conclusiones con fundamento.

Elementos del Análisis de Riesgos:

1. Activos, no son más que los elementos del sistema de información (o las que se encuentran relacionado con este) que generan valor a la organización.
2. Amenazas, son eventos que les puede pasar a los activos provocando daños a la organización.
3. Salvaguardas, son mecanismos de defensa utilizados para que aquellas amenazas no causen tanto daño.

Con los elementos anteriormente mencionados se puede identificar:

1. El impacto, lo que podría pasar
2. El riesgo, lo que probablemente pase

La siguiente figura recoge lo mencionado anteriormente:

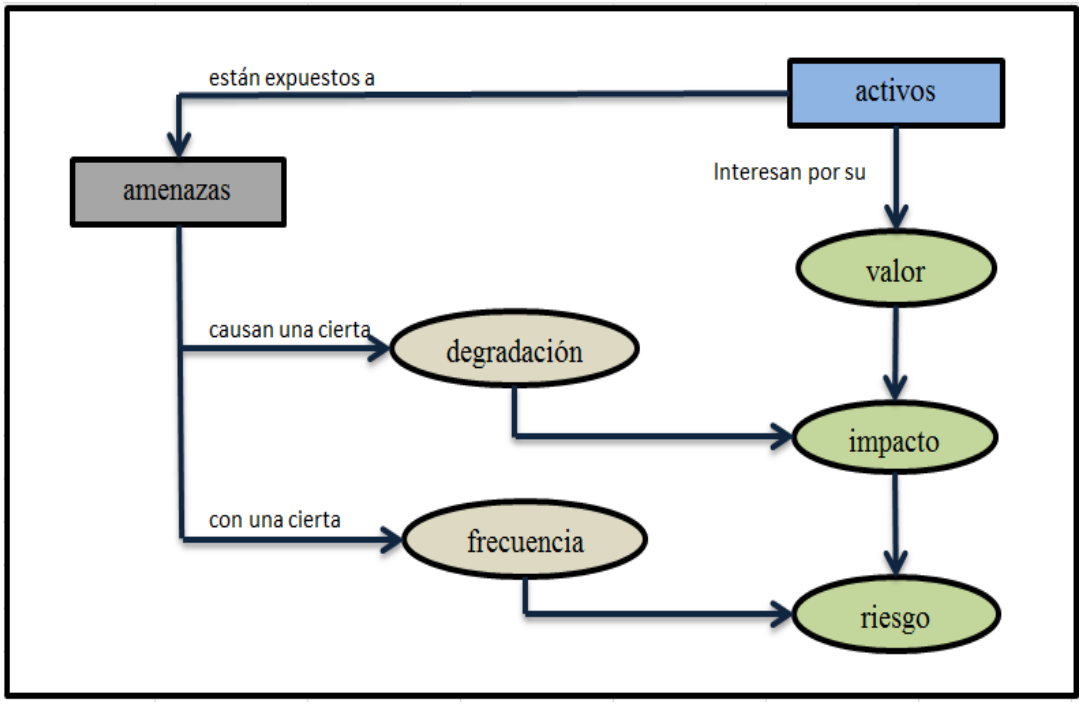


Figura 3-1: Análisis de Riesgos

Fuente: MAGERIT – versión 2
Elaborado por: autores

Para el desarrollo de esta etapa, la recolección de la información será desarrollada mediante encuestas y entrevistas a los usuarios responsables de los sistemas de información de la COAC Jardín Azuayo, también se considerarán las inspecciones físicas realizadas a la organización.

Esta actividad tiene una importancia crucial por dos motivos: la información a recoger condiciona el conocimiento del equipo del proyecto; y la recogida en sí es una operación delicada que exige una confianza mutua profunda (la transmisión de información es siempre delicada y más sí concierne a la seguridad).

3.1. IDENTIFICACIÓN DE ACTIVOS

Se denomina activos, los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su Dirección.

El activo esencial es la información que maneja el sistema; es decir los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes que integran los Sistemas de Información como son:[17]

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) que permiten hospedar datos, aplicaciones, y servicios.
- Las redes de comunicaciones que permiten intercambiar datos.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

La identificación de activos es importante ya que permite materializar con precisión el alcance del proyecto, permite valorar los activos con exactitud e identificando y valorando las amenazas a las que están expuestos dichos activos.

3.1.1. [S] SERVICIOS

Función que satisface una necesidad de los usuarios (del servicio). Para la prestación de un servicio se requiere una serie de medios.

[17] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.17

Los servicios aparecen como activos de un análisis de riesgos bien como servicios finales (prestados por la organización a terceros), bien como servicios instrumentales (donde tanto los usuarios como los medios son propios), bien como servicios contratados (a otra organización que les proporciona con sus propios medios).[18]

Para los usuarios internos, la organización presta los siguientes servicios:

- Telefonía IP
- Portal web
- Acceso Remoto
- Servidor de correo electrónico Zimbra
- Servicio de archivo compartido por iFolder
- Internet

Para los usuarios externos, la institución cuenta con los siguientes servicios:

- Ahorro
- Crédito
- Cajero automático
- Otros - pagos:
    - Planillas de teléfono (Pacifictel - CNT)
    - Planillas de luz
    - Pensiones
    - SOAT
    - Recaudación Otecel (movistar)
    - RISE
    - Sueldos a empleados

3.1.2. [SW] APLICACIONES (Software)

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su

[18] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.6

desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.[19]

Entre las aplicaciones que ostenta la institución tenemos los siguientes:

- Sistema Financiero Integrado Jardín Azuayo (FISJA)
- Ofimática
- Antivirus
- Otros software:
    - BP Wind
    - Proyect
    - Paquete de Adobe
    - My SQL
    - VLC
    - Paquete de Photoshop

3.1.3. [HW] EQUIPOS INFORMÁTICOS (Hardware)

Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.[20]

Dentro de los equipos informáticos que posee la institución tenemos los siguientes:

- Servidor de base de datos
- Equipos virtuales
- Router
- Switch
- Radios

[19] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.8

[20] Ibíd., p.9

- Firewall
- Computadores de escritorio
- Computadores portátiles
- Impresoras a laser
- Impresoras matriciales
- Equipos de contingencia:
    - Cámaras fotográficas
    - GPS

3.1.4. [COM] REDES DE COMUNICACIONES

Incluyendo tanto instalaciones dedicadas como servicio de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de trasporte que llevan datos de un sitio a otro.[21]

Entre los medios de transporte de información tenemos los siguientes:

- Telefonía IP
- Red LAN
- Red WWAN
- Internet

3.1.5. [SI] SOPORTES DE INFORMACIÓN

En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.[22]

En la institución generalmente se utilizan los siguientes soportes de información:

- Dispositivos USB
- Material impreso

[21] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.10

[22] Ibíd.

- Microfilm
- Discos formato DVD
- Discos formato CD

3.1.6. [AUX] EQUIPAMIENTO AUXILIAR

En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.[23]

En la institución se cuenta son los siguientes equipos auxiliares:

- Fuentes de alimentación
- Sistemas de alimentación ininterrumpida
- Generador eléctrico
- Equipo de climatización
- Cableado de datos
- Robots
- Mobiliario
- Caja Fuerte
- Otros equipamientos auxiliares:
    - Biometría
    - Acceso temporizado
    - Detector de incendios
    - Extintor de incendios
    - Cámaras de vigilancia, entre otros.

3.1.7. [SS] SERVICIOS SUBCONTRATADOS

La Cooperativa de Ahorro y Crédito Jardín Azuayo tiene convenios con otras instituciones para satisfacer la demanda de la ciudadanía, entre los servicios subcontratados se tiene:

- IRNET
- COOPSEGUROS

[23] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.10

- Red COONECTA
- Ventanilla compartida

3.1.8. [L] INSTALACIONES

En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.[24]

La infraestructura donde se localiza los sistemas de información y comunicación se denomina Unidad de Sistemas, Redes y Telecomunicaciones, ubicado en la calle Sucre 5-42, siendo un local con adecuaciones, por ser de tipo casa. Posteriormente la Cooperativa se trasladó de local, manteniendo los mismos los sistemas de información y comunicación, radicándose actualmente en la calle Benigno Malo 9-75 y Gran Colombia.

3.1.9. [P] PERSONAL

En este epígrafe aparecen las personas relacionadas con los sistemas de información.[25]

Dentro del personal de la institución, podemos citar los siguientes:

- Ingeniero David Ávila – Infraestructura y Telecomunicaciones
- Ingeniero Jorge Bonete – Administración de Base de Datos
- Ingeniero Marco Paredes – Ingeniería de Software
- Ingeniero Omar Vélez – Programador /desarrollador
- Ingeniero Fabricio Barreto – Soporte a Usuarios, entre otros.

Los activos descritos anteriormente se pueden observar con sus respectivas características y comentarios en el Anexo 2. Modelo de Valor.

[24] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.11

[25] Ibíd.

3.2. IDENTIFICACIÓN DE AMENAZAS

Luego de la identificación de los activos se deben de identificar las amenazas que pueden afectar a cada activo, por lo que una amenaza puede desencadenar muchas más.

Las amenazas son *eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o perdidas inmateriales en sus activos*.[26]

La herramienta PILAR Basic aplicada, asigna de forma automática las amenazas, su frecuencia de materialización y el impacto que supondría.

Las amenazas que genera la biblioteca de PILAR Basic no serán tomadas en su totalidad, debido a que consideraremos las amenazas obtenidas de las encuestas realizadas a los responsables de los sistemas de información de la institución.

La frecuencia y degradación de las amenazas se vió necesario realizar de forma manual para una mayor comprensión; lo que se tomó en cuenta para su elaboración fueron las capas.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. Se caracteriza con una fracción del valor del activo: [27]

NIVELES	DEGRADACIÓN
25%	Poco
50%	Medio
75%	Alto
100%	Muy Alto

Tabla 3-1: Escala de Degradación
Elaborado por: autores

[26] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.102
[27] Ibíd., p.22

La frecuencia es cada cuánto se materializa la amenaza, se modela como una tasa anual de ocurrencia, siendo valores típicos:[28]

PERIODICIDAD	FRECUENCIA
360	A diario
12	Mensualmente
4	Cuatro veces al año
2	Dos veces al año
1	Una vez al año
1/12	Cada varios años

Tabla 3-2: Escala de Frecuencia
Elaborado por: autores

En la siguiente tabla se puede observar las diferentes amenazas a las que están expuestos los activos:

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
CAPA DEL NEGOCIO	-Ahorro	-Corte de suministro eléctrico -Fallo de servicios de comunicaciones -Errores del administrador	1	25%
	-Crédito	-Corte de suministro eléctrico -Fallo de servicios de comunicaciones -Errores del usuario		
	-Cajero automático	-Desastres naturales -Acceso no autorizado -Ataque destructivo -Avería de origen físico o lógico -Corte de suministro eléctrico -Condiciones inadecuadas de temperatura o humedad -Fallo de servicios de comunicaciones -Errores del administrador -Suplantación de la identidad del usuario		

[28] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.27

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
SERVICIOS INTERNOS	-Telefonía IP	-Desastres naturales -Avería de origen físico o lógico -Falla de servicios de comunicaciones -Degradación de los soportes de almacenamiento de la información -Emanaciones electromagnéticas -Errores de los usuarios -Errores de configuración -Errores de re-encaminamiento -Errores de mantenimiento/ actualización de programas (software) -Errores de mantenimiento/ actualización de equipos (hardware) -Manipulación de la configuración -Uso no previsto	2	25%
	-Portal Web	-Desastres naturales -Acceso no autorizado -Avería de origen físico o lógico -Corte del suministro eléctrico - Falla de servicios de comunicaciones -Errores del administrador -Suplantación de la identidad del usuario		
	-Acceso Remoto	- Errores del administrador -Degradación de la información -Divulgación de la información -Suplantación de la identidad del usuario -Acceso no autorizado -Destrucción de la información -Ataque destructivo		

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
	-Servidor de correo electrónico Zimbra	-Avería de origen físico o lógico - Corte del suministro eléctrico -Fallo de servicios de comunicaciones -Errores del administrador -Fugas de información -Errores de mantenimiento/ actualización de programas(software) -Suplantación de la identidad del usuario -Denegación de servicio		
	-Servicio de archivo compartido por iFolder	-Fuego -Avería de origen físico o lógico - Falla de servicios de comunicaciones -Interrupción de otros servicios o suministros esenciales -Degradación de los soportes de almacenamiento de la información -Fugas de información -Alteración de la información -Destrucción de la información -Errores de mantenimiento/ actualización de programas (software) -Suplantación de la identidad del usuario -Introducción de falsa información -Destrucción de la información -Denegación de servicio		

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
	-Internet	-Corte de suministro eléctrico -Errores de los usuarios -Errores del administrador -Errores de configuración - Errores de mantenimiento/ actualización de programas (software) -Manipulación de la configuración		
APLICACIONES	-FISJA	-Daños por agua -Acceso no autorizado -Difusión de software dañino -Falla de servicios de comunicaciones -Errores de los usuarios -Errores de configuración -Introducción de falsa información -Errores de mantenimiento/ actualización de programas (software) -Modificación de información -Introducción de falsa información	4	25%
	-Ofimática	-Avería de origen físico o lógico -Corte del suministro eléctrico -Degradación de los soportes de almacenamiento de la información -Errores de los usuarios -Errores del administrador -Errores de configuración -Difusión de software dañino - Errores de mantenimiento/ actualización de programas (software) -Manipulación de la configuración		

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
	-Antivirus	-Avería de origen físico o lógico -Errores de los usuarios -Errores de configuración - Errores de mantenimiento/ actualización de programas (software) -Difusión de software dañino		
	-Otros software	-Avería de origen físico o lógico -Corte del suministro eléctrico -Degradación de los soportes de almacenamiento -Errores de los usuarios -Errores del administrador -Errores de configuración -Difusión de software dañino -Errores de mantenimiento/ actualización de programas (software) -Manipulación de la configuración		
EQUIPOS	-Servidor de Base de Datos	-Desastres naturales -Avería de origen físico o lógico -Cortes del suministro eléctrico -Condiciones inadecuadas de temperatura o humedad -Denegación del servicio -Degradación de los soportes de almacenamiento de la información -Errores de los usuarios -Errores del administrador -Errores de configuración -Abuso de privilegios de acceso -Uso no previsto -Acceso no autorizado -Modificación de información	4	50%

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
		-Introducción de falsa información -Indisponibilidad del personal		
	-Equipos virtuales	-Fuego -Avería de origen físico o lógico -Corte del suministro eléctrico -Condiciones inadecuadas de temperatura o humedad -Fallo de servicios de comunicaciones -Degradación de los soportes de almacenamiento de la información -Errores del administrador -Errores de configuración -Errores de mantenimiento/ actualización de programas (software) -Errores de mantenimiento/ actualización de equipos (hardware) -Caída del sistema por agotamiento físico de recursos -Indisponibilidad del personal -Manipulación de la configuración -Robo de equipos		
	-Router	-Daños por agua -Corte de suministro eléctrico -Errores de mantenimiento/ actualización de programas (software) -Manipulación de la configuración -Abuso de privilegios y acceso -Acceso no autorizado -Robo de equipos -Ataque destructivo		

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
	-Switch	-Fuego -Daños por agua -Corte de suministro eléctrico -Errores de mantenimiento/ actualización de programas (software) -Abuso de privilegios de acceso -Acceso no autorizado -Introducción de falsa información -Robo de equipos -Ataque destructivo		
	-Radios	-Fuego -Daño por agua -Avería de origen físico o lógico -Corte del suministro eléctrico -Errores de mantenimiento/ actualización de programas (software) -Pérdida de equipos -Manipulación de la configuración -Suplantación de l identidad del usuario -Abuso de privilegios de acceso -Acceso no autorizado -Modificación de información -Robo de equipos		
	-Firewall	-Corte del suministro de eléctrico -Condiciones inadecuadas de temperatura o humedad		

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
	-Computadoras de escritorio	-Fuego -Daños por agua -Corte del suministro eléctrico -Errores de los usuarios -Errores del administrador -Errores de configuración -Difusión de software dañino -Errores de mantenimiento/ actualización de equipos (hardware) -Perdida de equipos -Manipulación de la configuración -Suplantación de la identidad del usuario		
	-Computaras portátiles	-Fuego -Daños por agua -Corte del suministro eléctrico -Errores de los usuarios -Errores del administrador -Errores de configuración -Difusión de software dañino -Errores de mantenimiento/ actualización de equipos (hardware) -Perdida de equipos -Manipulación de la configuración -Suplantación de la identidad del usuario		
	-Impresora a laser	-Daños por agua -Avería de origen físico o lógico -Interrupción de otros servicios o suministros esenciales -Errores de los usuarios -Errores de configuración -Manipulación de la configuración -Pérdida de equipos		

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
	-Impresora matricial	-Fuego -Daños por agua -Avería de origen físico o lógico -Interrupción de otros servicios o suministros esenciales -Errores de los usuarios -Errores de configuración -Manipulación de la configuración -Pérdida de equipos		
	-Equipos de contingencia	-Daños por agua -Condiciones inadecuadas de temperatura o humedad -Errores de los usuarios -Pérdida de equipos -Robo de equipos		
COMUNICACIONES	-Telefonía IP	-Desastres naturales -Avería de origen físico o lógico -Falla de servicios de comunicaciones -Degradación de los soportes de almacenamiento de la información -Emanaciones electromagnéticas -Errores de los usuarios -Errores de configuración -Errores de re-encaminamiento -Errores de mantenimiento/ actualización de programas (software) -Errores de mantenimiento/ actualización de equipos (hardware) -Manipulación de la configuración -Uso no previsto -Interceptación de información (escucha)	4	25%

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
	-Red LAN	-Daños por agua -Corte de suministro eléctrico -Condiciones inadecuadas de temperatura o humedad -Fallo de servicios de comunicaciones -Errores de mantenimiento/ actualización de programas (software) -Caída del sistema por agotamiento de recursos -Indisponibilidad del personal -Manipulación de la configuración		
	-Red WWAN	-Daños por agua -Avería de origen físico o lógico -Corte de suministro eléctrico -Condiciones inadecuadas de temperatura o humedad -Fallos de servicios de comunicaciones -Emanaciones electromagnéticas -Errores del administrador -Errores de configuración -Vulnerabilidad de los programas (software) -Errores de mantenimiento/ actualización de programas (software) -Errores de mantenimiento/ actualización de los equipos (hardware) -Análisis de tráfico -Abuso de privilegios de acceso -Uso no previsto -Indisponibilidad del personal		

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
	-Internet	-Daños por agua -Corte de suministro eléctrico -Condiciones inadecuadas de temperatura o humedad -Fallo de servicios de comunicaciones -Errores de mantenimiento/ actualización de programas (software) -Caída del sistema por agotamiento de recursos -Indisponibilidad del personal -Manipulación de la configuración		
ELEMENTOS AUXILIARES	-Fuentes de alimentación	-Desastres naturales -Avería de origen físico o lógico -Errores de los usuarios -Errores de configuración -Errores de mantenimiento/ actualización de programas (software) -Errores de mantenimiento/ actualización de equipo (hardware)	1	25%
	-Sistema de alimentación ininterrumpida	-Desastres naturales -Contaminación electromagnética -Corte de suministro eléctrico -Falla de servicio de comunicaciones -Emanaciones electromagnéticas -Errores de los usuarios -Errores de mantenimiento/ actualización de programas (software) -Errores de mantenimiento/ actualización de equipo (hardware)		

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
	-Generador eléctrico	-Desastres naturales -Desastres industriales -Contaminación mecánica -Avería de origen físico o lógico -Errores de los usuarios -Errores de configuración -Errores de mantenimiento/ actualización de equipo (hardware)		
	-Equipo de climatización	-Desastres naturales -Desastres industriales -Avería de origen físico o lógico -Corte de suministro eléctrico -Errores de los usuarios -Errores de configuración -Errores de mantenimiento/ actualización de equipo (hardware)		
	-Cableado de datos	-Desastres naturales -Contaminación mecánica -Contaminación electromagnética -Corte de suministro eléctrico -Condiciones inadecuadas de temperatura o humedad -Deficiencias en la organización -Falla de servicio de comunicaciones -Emanaciones electromagnéticas -Errores de los usuarios		
	-Robots	-Desastres naturales -Contaminación electromagnética -Corte de suministro eléctrico -Falla de servicio de comunicaciones -Emanaciones electromagnéticas -Errores de los usuarios		

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
	-Mobiliario	-Desastres naturales -Contaminación electromagnética -Corte de suministro eléctrico -Falla de servicio de comunicaciones -Emanaciones electromagnéticas -Errores de los usuarios		
	-Caja Fuerte	-Desastres naturales -Contaminación electromagnética -Corte de suministro eléctrico -Falla de servicio de comunicaciones -Emanaciones electromagnéticas -Errores de los usuarios		
	-Otros equipamientos auxiliares	-Desastres naturales -Contaminación electromagnética -Corte de suministro eléctrico -Falla de servicio de comunicaciones -Emanaciones electromagnéticas -Errores de los usuarios		
SERVICIOS SUBCONTRATADOS	-IRNET	-Errores de los usuarios	1/12	25%
	-COOPSEGURO	-Fugas de información		
	-RED COONECTA	-Caída del sistema por agotamiento de recursos -Acceso no autorizado -Errores de los usuarios -Errores de la configuración -Suplantación de la identidad del usuario		
	-Ventanilla Compartida	-Errores del administrador -Errores de la configuración		
INSTALACIONES	-Unidad de sistemas, redes y telecomunicaciones	-Fuego -Daños por agua -Cortes de suministro eléctrico -Condiciones inadecuadas de temperatura o humedad -Deficiencias en la organización	1/12	25%

CAPAS	ACTIVOS	AMENAZAS	FRECUENCIA	DEGRADACIÓN
PERSONAL	-Administración de Base de datos (producción-pruebas)	-Deficiencia de la organización -Divulgación de la información -Extorción -Ingeniería social	n/a	n/a
	-Infraestructura y Telecomunicaciones	-Deficiencia de la organización - Divulgación de la información -Extorción -Ingeniería social		
	-Desarrolladores/ Programadores	-Deficiencia de la organización - Divulgación de la información -Extorción -Ingeniería social		
	-Ingeniería de software	-Deficiencia de la organización - Divulgación de la información -Extorción -Ingeniería social		
	-Soporte a usuarios	-Deficiencia de la organización - Divulgación de la información -Extorción -Ingeniería social		

Tabla 3-3: Identificación de Amenazas

Elaborado por: autores

3.3. IDENTIFICACIÓN DE SALVAGUARDAS

Una vez identificado las amenazas, se identificará los mecanismos de salvaguarda implantados en aquellos activos, describiendo las dimensiones de seguridad que estos ofrecen (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad).

Salvaguarda son *procedimiento, dispositivo, físico o lógico, que reduce el riesgo*.[29]

[29] http://www.cii-murcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.pdf

En la siguiente tabla se observa las diferentes salvaguardas que tienen los activos:

CAPA	ACTIVOS	SALVAGUARDAS	DIMENSIÓN
CAPA DEL NEGOCIO	-Ahorro	-Según la Corporación del Seguro de Depósitos COSEDE, fortalece el aseguramiento de depósitos bancarios, sea a través de procesos de resolución bancaria, o reintegrándolos en la mayor proporción técnica posible	-Disponibilidad -Autenticidad -Trazabilidad
	-Crédito	-De Coopseguros S.A: Seguro de vida sobre préstamos.- bajo esta póliza pueden asegurarse los préstamos y/o saldos de préstamos concedidos por la Cooperativa a sus Asociados o Clientes, siendo su principal objetivo proteger a la institución, a los familiares, garantes y/o garantías que, a su fallecimiento o incapacidad total y permanente, el saldo insoluto de la deuda quedará cancelado en su totalidad por Coopseguros	
	-Cajero Automático	-Protección del equipo dentro de la organización: monitoreo, respaldos periódicos, aire acondicionado, UPS, cámara de seguridad, antivirus, actualizaciones (parches), mantenimiento -Acceso limitado	
SERVICIOS INTERNOS	-Telefonía IP	- Protección del equipo dentro de la organización	-Disponibilidad -Confidencialidad -Autenticidad -Trazabilidad
	-Portal Web	-Protección del equipo dentro de la organización	
	-Acceso Remoto	- Protección del equipo dentro de la organización -Activación/desactivación cuando sea necesario	
	-Servidor de correo electrónico Zimbra	-Protección del equipo dentro de la organización	
	-Servicio de archivo compartido por iFolder	-Protección del equipo dentro de la organización	
	-Internet	-Protección del equipo dentro de la organización	

CAPAS	ACTIVOS	SALVAGUARDAS	DIMENSIÓN
APLICACIONES	-FISJA	-Protección del equipo dentro de la organización -Stand By	-Disponibilidad -Integridad -Autenticidad -Trazabilidad
	-Office	-Protección del equipo dentro de la organización	
	-Antivirus	-Protección del equipo dentro de la organización	
	-Otros software	-Protección del equipo dentro de la organización	
EQUIPOS	-Servidor de Base de Datos	-Stand By -RMAN	-Disponibilidad - Confidencialidad -Autenticidad
	-Equipos virtuales	-Protección del equipo dentro de la organización	
	-Router	-Claves -Interruptor de reseteo - Protección del equipo dentro de la organización	
	-Switch	-Claves - Protección del equipo dentro de la organización	
	-Radios	-Acceso remoto - Protección del equipo dentro de la organización	
	-Firewall	-Protección del equipo dentro de la organización	
	-Computadoras de escritorio	-Protección del equipo dentro de la organización	
	-Computaras portátiles	-Protección del equipo dentro de la organización	
	-Impresora a laser	-Protección del equipo dentro de la organización	
	-Impresora matricial	-Protección del equipo dentro de la organización	
	-Equipos de contingencia	-Protección del equipo dentro de la organización	
COMUNICACIONES	-Telefonía IP	-Protección del equipo dentro de la organización	-Disponibilidad - Confidencialidad
	-Red LAN	-Protección del equipo dentro de la organización	
	-Red WWAN	-Protección del equipo dentro de la organización -Subnetting -Seguridad del equipo -Filtrado de redes -Paquetes y puertos	
	-Internet	-Filtrado de contenido -Firewall -SSL para Https	

CAPAS	ACTIVOS	SALVAGUARDAS	DIMENSIÓN
ELEMENTOS AUXILIARES	-Fuentes de alimentación	-Recarga de baterías	-Disponibilidad -Autenticidad
	-Sistema de alimentación ininterrumpida	-Seguridad lógica y física -Seguros con proveedores -Monitoreo y gestión electrónica y física	
	-Generador eléctrico	-Protección del equipo dentro de la organización -Transferencia automática	
	-Equipo de climatización	-Protección del equipo dentro de la organización	
	-Cableado de datos	-Seguridad lógica y física -Monitoreo y gestión electrónica y física	
	-Robots	-Seguridad lógica y física -Seguros con proveedores -Monitoreo y gestión electrónica y física	
	-Mobiliario	-Seguridad lógica y física -Monitoreo y gestión electrónica y física	
	-Caja Fuerte	-Seguridad lógica y física -Seguros con proveedores -Monitoreo y gestión electrónica y física	
	-Otros equipamientos auxiliares	-Seguridad lógica y física -Seguros con proveedores -Monitoreo y gestión electrónica y física	
SERVICIOS SUBCONTRATADOS	-IRNET	-Protección del equipo dentro de la organización	-Disponibilidad -Autenticidad
	-COOPSEGUROS	-Protección del equipo dentro de la organización -Doble salida con dos proveedores: Telconet y Punto net	
	-RED COONECTA	-Respaldos de los servidores -Logs	
	-VENTANILLA COMPARTIDA	-Respaldos de los servidores -Logs	
INSTALACIONES	-Unidad de sistemas, redes y telecomunicaciones	-Alarmas -Ventilación (aire acondicionado) -UPS -Protecciones metálicas -Extintores	-Disponibilidad

CAPAS	ACTIVOS	SALVAGUARDAS	DIMENSIÓN
PERSONAL	-Administración de Base de datos (producción-pruebas)	-Plan de contingencia	-Integridad -Confidencialidad -Autenticidad
	-Infraestructura y Telecomunicaciones	- Plan de contingencia	
	-Desarrolladores/ programadores	- Plan de contingencia	
	-Ingeniería de software	- Plan de contingencia	
	-Soporte a usuarios	- Plan de contingencia	

Tabla 3-4: Identificación de Salvaguardas

Elaborado por: autores

3.4. IDENTIFICACIÓN DE VULNERABILIDADES

Una vez identificado las amenazas y las salvaguardas existentes de los activos, la siguiente actividad es la identificación de vulnerabilidades.

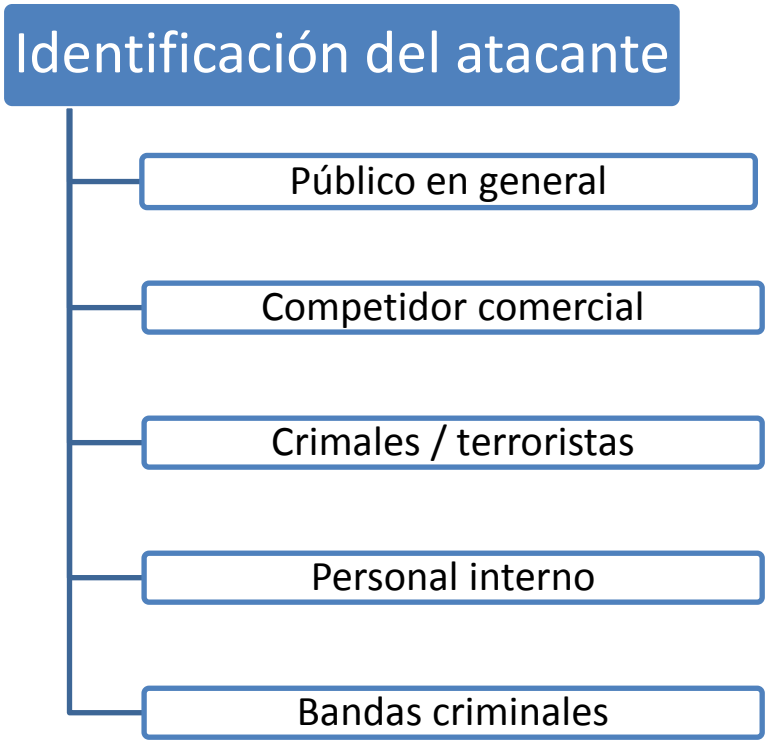
Vulnerabilidad *es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo*.[30]

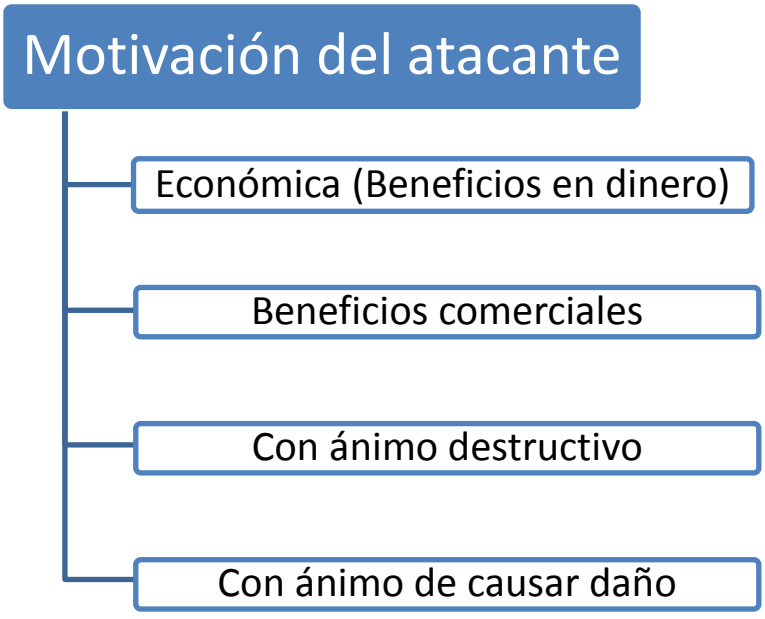
PILAR Basic ha sustituido, los valores de probabilidad y degradación por una serie de criterios que permiten reflejar el entorno en el que se encuentran los activos.

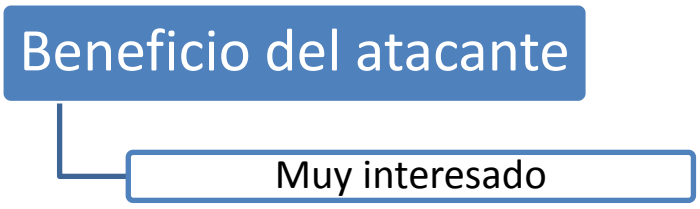
En la Gestión de Vulnerabilidades que genera la herramienta PILAR Basic, se podrá definir qué criterios pueden influir sobre un dominio (y por lo tanto sobre todos los activos que se encuentran en dicho dominio)

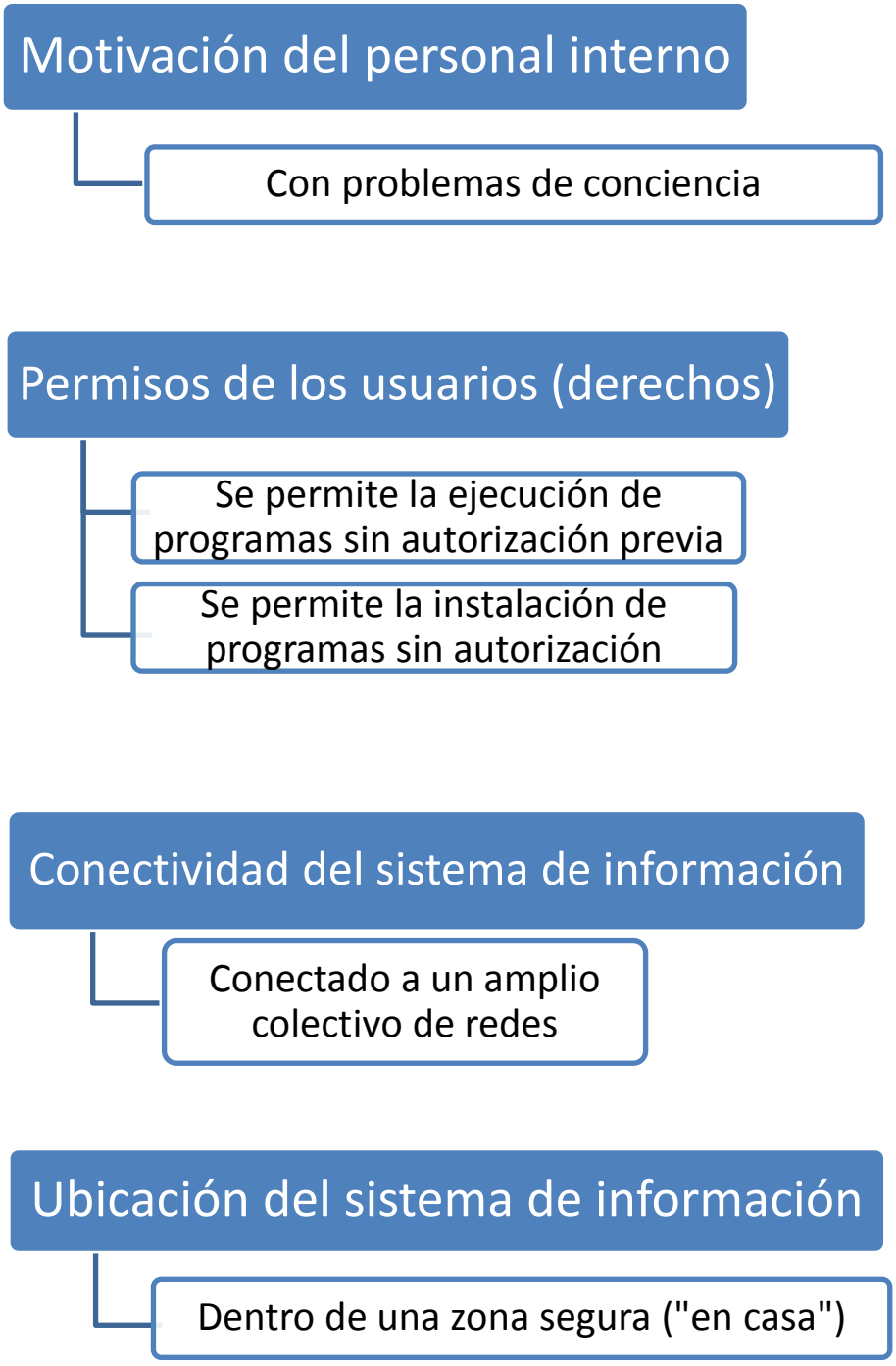
Las Vulnerabilidades identificadas por medio de las encuestas, (Ver Anexo 3.Vulnerabilidad de los Dominios), que podrían generar que una amenaza se materialice son las siguientes:

[30] http://www.cii-murcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.pdf


Identificación del atacante
Público en general
Competidor comercial
Crimales / terroristas
Personal interno
Bandas criminales


Motivación del atacante
Económica (Beneficios en dinero)
Beneficios comerciales
Con ánimo destructivo
Con ánimo de causar daño


Beneficio del atacante
Muy interesado


Motivación del personal interno
Con problemas de conciencia
Permisos de los usuarios (derechos)
Se permite la ejecución de programas sin autorización previa
Se permite la instalación de programas sin autorización
Conectividad del sistema de información
Conectado a un amplio colectivo de redes
Ubicación del sistema de información
Dentro de una zona segura ("en casa")

3.5. IDENTIFICACIÓN DE IMPACTOS

El objetivo en esta actividad es, conocer el alcance del daño producido en el dominio (y por lo tanto sobre todos los activos que se encuentran en dicho dominio), como resultado de la materialización de las amenazas sobre los activos.

La identificación de impactos o valoración de dominios se desarrollara con repercusiones a las dimensiones de valoración que son: (D) Disponibilidad, (I) Integridad, (C) Confidencialidad, (A) Autenticidad y (T) Trazabilidad de la información.

Las dimensiones de valoración son características o atributos que hacen valioso un activo.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que se recibe en una cierta dimensión es la medida del perjuicio para la organización si los activos se ven dañados en dicha dimensión.

Los criterios de valoración que utiliza PILAR Basic son cuatro (Alto, Medio, Bajo y Despreciable), la escala de valoración que hemos implementado es la siguiente:

VALOR		CRITERIO
7 - 10	Alto	Daño grave a la organización
4 - 7	Medio	Daño importante a la organización
1 - 4	Bajo	Daño menor a la organización
0 - 1	Despreciable	Irrelevante a efectos prácticos

Tabla 3-5: Escala de criterios de valoración
Elaborado por: autores

A continuación se indican las cinco dimensiones con sus criterios de valoración, obtenidas de las encuestas realizadas. (Ver Anexo 4. Valoración de Dominios)

DISPONIBILIDAD

Es el aseguramiento de que los usuarios autorizados tienen acceso cuando lo requiera a la información y a sus activos asociados.

Indica la repercusión que tendría en la institución el hecho de que se dejara de prestar el servicio

ALTO

- Impida la investigación de delitos graves o facilite su comisión
- Probablemente cause una interrupción seria de las actividades propias de la organización con un impacto significativo en otras organizaciones
- Administración y gestión: problamente impediría la operación efectiva de la organización
- Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
- Intereses comerciales o económicos: de alto interés para la competencia, causa de graves pérdidas económicas
- Obligaciones legales: probablemente cause un imcumplimiento grave de una ley o regulación
- Información personal: probablemente afecte gravemente a un grupo de individuos
- Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

INTEGRIDAD

Es la garantia de la exactitud y completitud de la información y los métodos de su procesamiento.

Indica la repercusión que tendría en la institución el hecho de que la información que se maneja para prestar el servicio fuera incorrecta o imcompleta

ALTO

- Impida la investigación de delitos graves o facilite su comisión
- Administración y gestión: problamente impediría la operación efectiva de la organización
- Intereses comerciales o económicos: causa de graves pérdidas económicas
- Obligaciones legales: probablemente cause un imcumplimiento grave de una ley o regulación
- Información personal: probablemente afecte gravemente a un grupo de individuos

CONFIDENCIALIDAD

Es el aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

Indica la repercusión que tendría en la institución el hecho de que la información que se maneja para prestar el servicio fuera accedida por personas no autorizadas

MEDIO

- Probablemente sea causa una cierta publicidad negativa: por afectar negativamente a las relaciones con otras organizaciones, por afectar negativamente a las relaciones con el público
- Intereses comerciales o económicos: de cierto interés para la competencia, de cierto valor comercial
- Información personal: probablemente quebrante leyes o regulaciones

AUTENTICIDAD

Es es aseguramiento de la identidad u origen .

Indica la repercusión que tendría en la institución el hecho de que no se pudiera confirmar la identidad de quién accedió al servicio o a la información

ALTO

- Administración y gestión: problamente impediría la operación efectiva de la organización
- Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones, con el público en general
- Intereses comerciales o económicos: causa de graves pérdidas económicas
- Obligaciones legales: probablemente cause un imcumplimiento grave de una ley o regulación
- Información personal: probablemente afecte gravemente a un grupo de individuos
- Información personal: probablemente quebrate seriamente la ley o algún reglamento de protección de información personal
- Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

TRAZABILIDAD

Es el aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

Indica la repercusión que tendría en la institución el hecho de que no se pudiera conocer a quién se le presta un servicio o a que información y cuando accedió un usuario

MEDIO

- Probablemente cause la interrupción de actividades propias de la organización con impacto en otras organizaciones
- Intereses comerciales o económicos: causa de graves pérdidas financieras o mermas de ingresos, facilita ventajas desproporcionadas a individuos u organizaciones, constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
- Información personal: probablemente afecte a un grupo de individuos
- Dificulte la investigación o facilite la comisión de delitos

3.6. IDENTIFICACIÓN DEL RIESGO

En esta actividad, luego del análisis de los activos en lo que se refiere a las amenazas, salvaguardas existentes, vulnerabilidades e identificación de impactos, se identificará los activos que poseen niveles de riesgo considerables.

La escala para calificar los riesgos de acuerdo a la herramienta aplicada PILAR Basic son:

- [5] Critico
- [4] Muy alto
- [3] Alto
- [2] Medio
- [1] Bajo
- [0] Despreciable

Cada activo se encontrará con un nivel de riesgo y su valoración como resultado de la calificación de las salvaguardas implementadas en PILAR Basic.

La calificación de los riesgos por activo que PILAR Basic nos genera está clasificada de acuerdo a la valoración de dominios (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad).

En el siguiente cuadro se puede observar los activos con su nivel de riesgo y su valoración.

NIVEL DE RIESGO					
DESPRECIABLE [0]	BAJO [1]	MEDIO [2]	ALTO [3]	MUY ALTO [4]	CRÍTICO [5]

ACTIVOS	DIMENSIONES				
	D	I	C	A	T
Capa del Negocio					
Ahorro	3.2	2.8	1.0	3.4	0.8
Crédito	3.2	2.8	1.0	3.4	0.8
Cajero automático	3.2	2.8	1.0	3.4	0.8

NIVEL DE RIESGO					
DESPRECIABLE [0]	BAJO [1]	MEDIO [2]	ALTO [3]	MUY ALTO [4]	CRÍTICO [5]

ACTIVOS	DIMENSIONES				
	D	I	C	A	T
Servicios Internos					
Telefonía IP	3.1	2.7	0.9	3.3	0.7
Portal Web	3.3	2.9	1.1	3.5	0.8
Acceso Remoto	3.2	2.8	1.0	3.4	0.7
Servidor de correo electrónico (Zimbra)	3.1	2.7	0.9	3.3	0.6
Servidor de archivo compartido por iFolder	3.2	2.8	1.0	3.4	0.7
Internet	1.9	2.4	0.7	2.6	0.8
Equipamiento: **Aplicaciones**					
Sistema Financiero Integrado Jardín Azuayo	3.3	2.3	1.0	2.8	0.7
Ofimática	1.9	2.4	0.7	2.6	0.8
Antivirus	3.2	2.5	1.0	2.7	1.0
Otros Software	3.2	2.5	1.0	2.7	1.0
Equipos					
Servidor de base de datos	2.9	1.7	0.0	1.8	0.0
Equipos virtuales	2.2	0.0	0.0	1.2	0.0
Router	2.9	0.0	0.0	1.2	0.0
Switch	2.9	0.0	0.0	1.2	0.0
Radios	2.9	0.0	0.0	1.2	0.0
Firewall	2.9	0.0	0.0	1.2	0.0
Computadoras de escritorio	2.9	0.0	0.0	1.2	0.0
Computadoras portátiles	2.8	0.0	0.0	1.2	0.0
Impresora a laser	2.3	0.0	0.0	1.3	0.0
Impresora matricial	3.0	0.0	0.0	1.3	0.0
Equipos de contingencia	2.9	0.0	0.0	1.2	0.0

NIVEL DE RIESGO					
DESPRECIABLE [0]	BAJO [1]	MEDIO [2]	ALTO [3]	MUY ALTO [4]	CRÍTICO [5]

ACTIVOS	DIMENSIONES				
	D	I	C	A	T
Comunicaciones					
Telefonía IP	3.2	0.4	0.5	2.2	0.1
Red LAN	3.0	0.2	0.2	1.9	0.0
Red WWAN	3.0	0.2	0.2	1.9	0.0
Internet	1.9	0.2	0.0	2.0	0.0
Elementos Auxiliares					
Fuentes de alimentación	2.9	0.0	0.0	0.0	0.0
Sistema de alimentación ininterrumpida	1.1	0.0	0.0	0.0	0.0
Generador eléctrico	1.1	0.0	0.0	0.0	0.0
Equipo de climatización	1.1	0.0	0.0	0.0	0.0
Cableado de datos	3.8	0.0	0.0	0.7	0.0
Robots	2.9	0.0	0.0	0.7	0.0
Mobiliario	2.9	0.0	0.0	0.7	0.0
Caja fuerte	2.9	0.0	0.0	0.7	0.0
Otros equipamientos auxiliares	2.9	0.0	0.0	0.7	0.0
Servicios subcontratados					
IRNET	3.2	2.8	1.0	3.3	0.7
COOP Seguros	3.2	2.8	1.0	3.3	0.7
RED COONECTA	3.2	2.8	1.0	3.4	0.8
Ventanilla compartida	3.2	2.8	1.0	3.4	0.7
Instalaciones					
Unidad de sistemas, redes y telecomunicaciones	2.6	1.9	0.1	2.0	0.2
Personal					
Administración de base de datos (Producción - Pruebas)	1.5	2.0	0.3	2.0	0.3
Infraestructura y telecomunicaciones	1.5	2.0	0.3	2.0	0.3

NIVEL DE RIESGO					
DESPRECIABLE [0]	BAJO [1]	MEDIO [2]	ALTO [3]	MUY ALTO [4]	CRÍTICO [5]

ACTIVOS	DIMENSIONES				
	D	I	C	A	T
Desarrolladores / programadores	1.5	2.0	0.3	2.0	0.3
Ingeniería de software	0.0	0.2	0.0	0.3	0.0
Soporte a usuarios	0.6	0.8	0.0	0.8	0.0

Tabla 3-6: Identificación del Riesgo

Elaborado por: autores

CAPÍTULO 4

GESTIÓN DE RIESGOS

La gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis.

En coordinación con los objetivos, estrategias y políticas de la organización, las actividades de gestión de riesgo permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la dirección.

Por lo tanto, constituyendo los sistemas de información un elemento clave para el éxito empresarial, se hace necesario disponer de sistemas de protección adecuados frente a sus amenazas internas y externas, con el fin de asegurar su adecuado uso, así como para reducir y evitar posibles responsabilidades laborales, civiles y/o penales.

Las salvaguardas en esta fase son fundamentales, entendiéndolas como aquellos *procedimientos o mecanismos tecnológicos que reducen el riesgo*.[31]

La gestión de riesgos es la *selección e implantación de salvaguardas para para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.*[32]

En la siguiente figura se indica cómo influyen las salvaguardas en la gestión de riesgo:

[31] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.108

[32] Ibíd., p.105

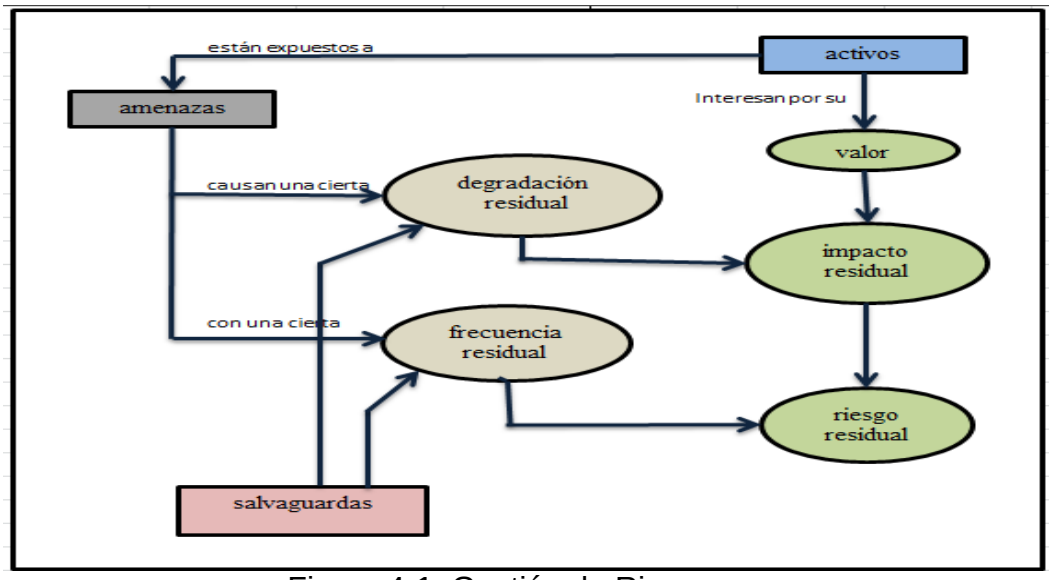


Figura 4-1: Gestión de Riesgos
Fuente: MAGERIT – versión 2
Elaborado por: autores

El plan de seguridad contempla lo siguiente:

- Fortalecer las salvaguardas existentes
- Implementar nuevas salvaguardas

Se gestiona para:

- Preservar los principios fundamentales de la información: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Conocer a qué estamos expuestos; es decir, las amenazas que pueden atentar contra dichos principios.
- Procurar evitar daños que afecten los principios de la información.
- Minimizar dichos daños en caso de que ocurriesen.

Las salvaguardas se relacionan con el riesgo de dos formas:

1. Reduciendo la frecuencia de las amenazas.
   Conocidas como salvaguardas preventivas, las ideales llegan a impedir completamente que la amenaza se materialice
2. Limitando el daño causado.
   Existen salvaguardas que limitan la posible degradación, otras que frenan el ataque a que la degradación no avance y, salvaguardas

que permiten su pronta recuperación cuando la amenaza lo ha destruido.

En cualquiera de los tres casos la amenaza se materializa, pero las consecuencias se limitan.

Las salvaguardas se caracterizan debido a los beneficios que éstas aportan; es decir, por su eficacia frente al riesgo que pretendan mitigar.

La salvaguarda ideal es que sea 100% eficaz. Entre una eficacia del 0% (imperfecta) y entre del 100% (perfecta), se estimará un grado de eficacia real en cada caso concreto.

Tipos de salvaguarda:

- Salvaguarda preventiva
- Salvaguarda de emergencia
- Salvaguarda de recuperación

Se debe considerar prioritariamente las salvaguardas de tipo preventivo que buscan que la amenaza no ocurra o su daño sea bajo; es decir, impedir incidentes o ataques.

No todo es conocido en la práctica, ni lo conocido es económicamente razonable impedirlo. Tanto para enfrentar lo desconocido como a lo que permanece expuesto, es indispensable contar con elementos que detecten el inicio de un incidente y permitan reaccionar de manera rápida impidiendo que se genere un desastre.

Lo más común es actuar de forma preventiva para que las cosas no ocurran o causen daño, pero no siempre es posible. Lo que no debe dejarse es que ningún 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.

4.1. TOMA DE DECISIONES

4.1.1. IDENTIFICACIÓN DE RIESGOS CRÍTICOS

En toda organización los activos están expuestos a riesgos, pero lo importante es conocer cuáles de los activos poseen un mayor nivel de riesgo con el fin de implementar salvaguardas para evitar que las amenazas se materialicen.

Una vez evaluado los activos y conocido el riesgo a los que están expuestos los mismos, hemos seleccionado los activos que poseen un nivel alto de riesgo.

A continuación se indica lo anteriormente dicho:

NIVEL DE RIESGO					
DESPRECIABLE [0]	BAJO [1]	MEDIO [2]	ALTO [3]	MUY ALTO [4]	CRÍTICO [5]

ACTIVOS	DIMENSIONES				
	D	I	C	A	T
Capa del Negocio					
Cajero automático	3.2	2.8	1.0	3.4	0.8
Servicios Internos					
Portal Web	3.3	2.9	1.1	3.5	0.8
Equipamiento: **Aplicaciones**					
Sistema Financiero Integrado Jardín Azuayo	3.3	2.3	1.0	2.8	0.7
Equipos					
Servidor de base de datos	2.9	1.7	0.0	1.8	0.0
Comunicaciones					
Telefonía IP	3.2	0.4	0.5	2.2	0.1
Red WWAN	3.0	0.2	0.2	1.9	0.0
Elementos Auxiliares					
Cableado de datos	3.8	0.0	0.0	0.7	0.0
Servicios subcontratados					
RED COONECTA	3.2	2.8	1.0	3.4	0.8
Instalaciones					
Unidad de sistemas, redes y telecomunicaciones	2.6	1.9	0.1	2.0	0.2
Personal	1.5	2.0	0.3	2.0	0.3

Tabla 4-1: Identificación de Riesgos Críticos (current)
Elaborado por: autores

4.2. PLAN DE SEGURIDAD

El plan de seguridad, es una actividad de la Gestión de Riesgos, que indica las decisiones que se van a efectuar en la mejora de la seguridad, en un determinado tiempo para un caso específico de la gestión, dicha actividad tiene para su realización las siguientes tareas:

- Programa de seguridad
- Plan de seguridad

4.2.1. PROGRAMAS DE SEGURIDAD

El programa de seguridad, es una tarea que tiene como objetivo principal elaborar un conjunto de programas de seguridad, fundamentados en las valoraciones de los riesgos, para implementar una serie de salvaguardas que mitiguen el impacto y/o riesgo a un nivel residual mínimo.

Los programas de seguridad tratan de implantar o mejorar la implantación de una serie de salvaguardas que lleven impacto y riesgo a niveles residuales asumidos por la Dirección. Los niveles residuales se mencionan luego de la gestión de los activos con riesgos críticos.

A continuación se gestionan los activos con riesgos críticos:

Capa del Negocio

- Cajero automático.- Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

  Un nivel de riesgo Alto (3.2) en cuanto a disponibilidad, teniendo la amenaza con mayor nivel de riesgo el acceso no autorizado; si ésta llegase a materializarse el atacante podría acceder a los recursos del sistema burlando los sistemas de identificación y autorización.

La consecuencia de la amenaza en el cajero automático en cuanto a disponibilidad generaría que el servicio quede indispuesto, provocando que la imagen de la cooperativa sea mal vista por usuarios insatisfechos con un servicio que no se puede acceder a él.

Un nivel de riesgo Alto (3.4) en cuanto a autenticidad, teniendo la amenaza con mayor nivel de riesgo la suplantación de la identidad del usuario, pudiendo ser personal interno, personal ajeno a la Cooperativa o por personal contratado temporalmente; si ésta amenaza llegase a materializarse el atacante disfrutaría de los privilegios del usuario suplantado para sus fines propios.

La medida para reducir el riesgo actual (current) de este activo, es la siguiente:

- Mejorar la protección del equipo dentro de la organización: en lo que se refiere a la seguridad lógica, con una protección de acceso controlado donde se limite los intentos fallidos de acceso.

Servicios Internos

- Portal web.- Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

  Un nivel de riesgo Alto (3.3) en cuanto a disponibilidad, teniendo la amenaza con mayor nivel de riesgo el acceso no autorizado; si ésta llegase a materializarse el atacante podría acceder a los recursos del sistema burlando los sistemas de identificación y autorización.

  La consecuencia de la amenaza del servicio portal web en cuanto a disponibilidad generaría que el servicio quede inhabilitado, impidiendo que los socios puedan realizar servicios en línea y obtener información adicional.

Un nivel de riesgo Alto (3.5) en cuanto a autenticidad, teniendo la amenaza con mayor nivel de riesgo la suplantación de la identidad del usuario, pudiendo ser personal interno como externo a la cooperativa.

La consecuencia de la amenaza en cuanto a autenticidad provocaría que el atacante disfrute de los privilegios del usuario suplantado para sus fines propios.

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

- Implementar medidas de control de acceso para aumentar la seguridad de los servicios en línea como: protección de acceso controlado donde se limite los intentos fallidos de acceso e implementación de tarjetas de coordenadas.

Equipamiento

Aplicaciones

- Sistema Financiero Integrado Jardín Azuayo.- Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

Un nivel de riesgo Alto (3.3) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo el acceso no autorizado, difusión de software dañino, errores de configuración y errores de los usuarios; si éstas llegasen a materializarse: el atacante podría acceder a los recursos del sistema burlando los sistemas de identificación y autorización, propagar virus, espías, gusanos, troyanos, bombas lógicas etc.; en errores no intencionados el introducir datos de configuración errónea provocaría la perdida de privilegios de acceso, fallo en el flujo de actividad, etc., y los errores comunes de los usuarios (personal) al usar los servicios, datos, etc., provocaría fallos de la información.

Las consecuencias de las amenazas en la disponibilidad generaría la pérdida de la exactitud y completitud de la información ocasionando que la aplicación genere resultados erróneos.

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

- Mejorar las medidas de control de acceso para aumentar la seguridad de la información, como el control mediante firewall.
- Mejorar la protección de la aplicación: monitorear la protección del código dañino.
- Implementar un registro de errores no intencionales.

Equipos

- Servidor de base de datos.- Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

  Un nivel de riesgo Medio (2.9) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo la condición inadecuada de temperatura o humedad y denegación del servicio; si la primera amenaza llegase a materializarse el servidor de base de datos trasladaría la información demasiado tarde a quien lo requiera, debido a la deficiencia de adaptación del local donde se encuentra, por exceso de calor, frio o humedad. La amenaza denegación de servicio provoca que el sistema caiga debido a una carencia de recursos suficientes.

  Las consecuencias de las amenazas en la disponibilidad del servidor de base de datos provocarían que la información generada en los departamentos no ingrese ni salga de la base de datos de manera oportuna.

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

- Implementar el Estándar TIA-942 (Telecomunications Industry Association) para Data Center, encaminado una atención al control periódico de los niveles de temperatura y control físico.

Comunicaciones

- Telefonía IP.- Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

Un nivel de riesgo Alto (3.2) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo los errores de configuración, los errores de re-encaminamiento e interceptación de información (escucha); si existe un error en la configuración las comunicaciones podrían llegar a tener un error de re-encaminamiento provocando que la información no llegue a donde lo requiera o simplemente la comunicación no se realiza. Si la tercera amenaza llegase a materializarse el atacante, al interceptar la información emitida por la telefonía IP, podría utilizar toda esa información para sus fines propios.

Las consecuencias de las amenazas en la disponibilidad generarían que la comunicación IP falle y por ende no esté disponible el servicio.

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

- Protección del equipo dentro de la organización: mejorar el control centralizado con revisiones periódicas de la configuración.

- Implementar una prohibición de establecimiento de conversaciones confidenciales en lugares públicos o sin adecuadas medidas de protección.
- Prohibición de dejar mensajes confidenciales en contestadoras automáticas.

➢ Red WWAN.- Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

Un nivel de riesgo Alto (3.0) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo los fallos de servicios de comunicaciones, errores del administrador y análisis de tráfico; si la primera amenaza llegase a materializarse generaría que se pierda la capacidad de trasmitir datos de un sitio a otro debido a la destrucción física de los medios físicos de transporte. Si la segunda amenaza se llegase a materializar a causa de unas equivocaciones de personas con responsabilidades de instalación y operación, la red WWAN no llegaría a los usuarios, impidiendo que puedan realizar sus labores oportunamente. Y si la tercera amenaza se materializa, el atacante sin necesidad de analizar el contenido de las comunicaciones es capaz de extraer conclusiones solamente conociendo el origen, destino, volumen y frecuencia de los intercambios.

Las consecuencias de las amenazas en la disponibilidad generarían que la red WWAN pierda la capacidad de trasmitir datos de un sitio a otro generando dificultad en la realización de trabajos.

Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

- Implementar un control de los medios físicos de transporte de comunicaciones.

- Protección del equipo dentro de la organización: mejorar las pruebas de operaciones.
- Mejorar la seguridad del filtrado de redes.

Elementos auxiliares

- Cableado de Datos.- Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

  Un nivel de riesgo Alto (3.8) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo la contaminación mecánica, contaminación electromagnética, condiciones inadecuadas de temperatura o humedad y deficiencias en la organización; si las amenazas se materializan debido a una deficiente instalación del cableado por parte de la organización, provocarían que el cableado y equipos interrelacionados sufran emanaciones electromagnéticas y daños físicos por el polvo, suciedad, cables expuestos a daños no intencionados por el personal.

  Las consecuencias de las amenazas en la disponibilidad impedirían que, con un daño en el cableado, las conexiones entre redes dejen de funcionar y también podrían generar daños físicos a los equipos; generando dificultades para realizar los trabajos y poder enviar información.

  Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

  - Implementar planes actualizados del cableado
  - Implementar procedimientos para la modificación del cableado
  - Implementar la segregación de cableado de alimentación y de comunicación para evitar interferencias

- Implementar un control de todos los accesos al cableado
- Mejorar el monitoreo y gestión electrónica y física

Servicios subcontratados

- Red COONECTA.- Para este servicio que presta la Cooperativa, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

  Un nivel de riesgo Alto (3.2) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo la caída del sistema por agotamiento de recursos y el acceso no autorizado. Si la primera amenaza llegase a materializarse provocarían que los socios no puedan realizar retiros en los cajeros automáticos de la institución y los cajeros afiliados a la Red COONECTA y BanRed debido un deficiente control de la contratación de servicios; y si la segunda amenaza se materializa el atacante accedería al sistema burlando su autenticidad haciendo que el sistema funcione con fallas o simplemente no funcione.

  Las consecuencias de las amenazas en la disponibilidad impedirían que los socios dispongan del servicio de los cajeros.

  Un nivel de riesgo Alto (3.4) en cuanto a autenticidad, teniendo la amenaza con mayor nivel de riesgo la suplantación de la identidad del usuario. Si la amenaza llegase a materializarse, la consecuencia en la dimensión, provocaría que el atacante disfrute de los privilegios para sus fines propios o para terceros.

  Las medidas para reducir el riesgo actual (current) de este servicio, son las siguientes:

  - Implementar controles de monitorización y verificación del rendimiento.

- Implementar acuerdos para informar, notificar, investigar las incidencias y fallos de seguridad.

Instalaciones

- Unidad de sistemas, redes y telecomunicaciones.- Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

  Un nivel de riesgo Medio (2.6) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo el fuego, daños por agua y deficiencias en la organización. Si las amenazas llegasen a materializarse el nivel de impacto sería alto, causando daños físicos y económicos.

  Las consecuencias de las amenazas en la disponibilidad impedirían que el personal disponga de las instalaciones para poder ejercer sus actividades, debido a los daños en sus activos.
  Un nivel de riesgo Medio (2.0) en cuanto a autenticidad, teniendo la amenaza con mayor nivel el acceso no autorizado. Si la amenaza llegase a materializarse el atacante puede ser el causante de producir daños irreversibles.

  La consecuencia de la amenaza en la autenticidad provocaría que el atacante desconocido origine daños físicos y económicos.

  Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

  - Supervisar la norma de conducta (prohibición de fumar, beber, comer, etc.)
  - Implementar un plan de protección frente a desastres
  - Implementar una separación de áreas de seguridad y de acceso público
  - Implementar un control de las áreas de carga y descarga
  - Implementar un control de acceso: mecanismo de huella dactilar

- Mejorar el control de visitas
- Implementar una protección de conductos y aberturas
- Implementar las medidas de seguridad de los sistemas de información

Personal

- Personal.- los riesgos que abarcan: la administración de base de datos (producción-pruebas), infraestructura y telecomunicaciones, desarrolladores/programadores, ingeniería de software y soporte a usuarios, son los siguientes: deficiencia de la organización, divulgación de información, extorción e ingeniería social.

  Si la primera amenaza se materializa existiría información desorganizada e interpretaciones erróneas, cuando no estén claras las responsabilidades de quien tiene que hacer exactamente qué y cuándo. Si las demás amenazas llegan a materializarse, la información sustraída puede ser utilizada como extorción o como abuso de la buena fe para beneficios propios del atacante.

  Las consecuencias de las amenazas causarían: cambios de conducta en el personal, inasistencia al trabajo, preocupaciones sin poder cumplir sus responsabilidades e inseguridad en el manejo de la información.

  Las medidas para reducir el riesgo actual (current) de este activo, son las siguientes:

  - Implementar una política de gestión de personal (en materia de seguridad)
  - Mejorar la asignación de responsabilidades
  - Implementar procedimientos para el cambio de puesto de trabajo
  - Implementar comprobaciones de puestos de gran responsabilidad

- Implementar una normativa de desempeño del puesto-propiedad intelectual

Con la aplicación de las salvaguardas el nivel de riesgo actual (current) disminuiría a un nivel de riesgo objetivo (target), como se indica en la siguiente tabla:

NIVEL DE RIESGO					
DESPRECIABLE [0]	BAJO [1]	MEDIO [2]	ALTO [3]	MUY ALTO [4]	CRÍTICO [5]

ACTIVOS	DIMENSIONES				
	D	I	C	A	T
Capa del Negocio					
Cajero automático	0.0	0.0	0.0	0.0	0.0
Servicios Internos					
Portal Web	0.0	0.0	0.0	0.0	0.0
Equipamiento: **Aplicaciones**					
Sistema Financiero Integrado Jardín Azuayo	0.0	0.0	0.0	0.0	0.0
Equipos					
Servidor de base de datos	0.8	0.0	0.0	0.0	0.0
Comunicaciones					
Telefonía IP	0.5	0.0	0.0	0.0	0.0
Red WWAN	0.6	0.0	0.0	0.0	0.0
Elementos Auxiliares					
Cableado de datos	2.0	0.0	0.0	0.0	0.0
Servicios subcontratados					
RED COONECTA	0.0	0.0	0.0	0.0	0.0
Instalaciones					
Unidad de sistemas, redes y telecomunicaciones	0.0	0.0	0.0	0.0	0.0
Personal	0.0	0.0	0.0	0.0	0.0

Tabla 4-2: Riesgo Residual

Elaborado por: autores

La aplicación de las salvaguardas implica recurrir en costos, los cuales estarán en función de los materiales a emplearse, del recurso humano a disponer tanto

interno como externo, y del tiempo que se extienda en la aplicación de dichas salvaguardas.

Se deberá tomar en cuenta antes de la aplicación de la salvaguarda, la variable costo-beneficio, con el fin de poder controlar que el costo de la aplicación de la salvaguarda no supere al costo de la amenaza en caso de que se materialice.

La Cooperativa de Ahorro y Crédito Jardín Azuayo a su criterio analizará la factibilidad de la aplicación de las salvaguardas y el beneficio que éstas aportarán con el fin de disminuir el riesgo; así también, a su libre criterio seleccionarán los recursos convenientes a utilizarse para la aplicación de las salvaguardas, con sus costos respectivos y el tiempo que estimen prudente.

4.2.2. PLAN DE SEGURIDAD

Es una actividad con el objetivo de ordenar en un lapso de tiempo los programas de seguridad considerando la criticidad, gravedad de los impactos y/o riesgos que se van a mitigar, con una prioridad relevante a los activos en situaciones críticas, como también la disponibilidad del personal para la implementación de las actividades del plan.

Los planes pueden llevarse en un plazo de tiempo, ya sea a corto o a largo plazo, dependiendo de la perspectiva y objetivos específicos en los que se materialicen los programas de seguridad.

Un control de seguridad que la Cooperativa de Ahorro y Crédito Jardín Azuayo debe implementar es la norma ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la Información. La herramienta PILAR Basic nos genera un reporte de dicha norma. (Ver Anexo 5. Código de buenas prácticas para la Gestión de la Seguridad de la Información)

Al realizar el plan de seguridad se debe considerar los siguientes aspectos; los activos a tratar, acciones y cronograma, como se describe a continuación:

Activos.- se generará una lista de los activos a mitigar, cuyo objetivo principal es proveer a los miembros del equipo un sentido claro de los activos a gestionar, como también proveer a la gerencia una información de los activos que están siendo analizados y gestionados.

Acciones.- la institución ejecutará el plan de seguridad como otra de las tareas y actividades que realiza, apoyada en un análisis y gestión de riesgos en donde se determinará qué acciones específicas se deben realizar pudiendo ser los planes de seguridad y controles de seguridad y los responsables de ejecutar dichos acciones.

Cronograma.- es el tiempo de duración de las acciones a realizarse en determinado tiempo, indicando el inicio y final de las actividades y tareas de dichas acciones.

Con los elementos definidos anteriormente, se elabora el plan de seguridad como se indica en la siguiente tabla:

ACTIVO	ACCIONES	RESPONSABLES	TIEMPO ESTIMADO
	PLAN DE CONTINGENCIA DE LOS ACTIVOS:		
-Cajero automático -Portal web -FISJA -Servidor de base de datos -Telefonía IP -Red WWAN -Cableado de datos -Red COONECTA -Unidad de sistemas de redes y telecomunicaciones	1. PLAN DE EMERGENCIA	Ing. Andrea Yánez Coordinadora de Seguridad, Ing. John Machuca Coordinador de Riesgos	Tiempo a realizar: 12 meses
Cajero automático -Portal web -FISJA	2. PLAN DE CONTINUIDAD	Ing. John Machuca Coordinador de Riesgos	Tiempo a realizar: 6 meses

ACTIVO	ACCIONES	RESPONSABLES	TIEMPO ESTIMADO
-Servidor de base de datos -Telefonía IP -Red WWAN -Cableado de datos -Red COONECTA -Unidad de sistemas de redes y telecomunicaciones			
Cajero automático -Portal web -FISJA -Servidor de base de datos -Telefonía IP -Red WWAN -Cableado de datos -Red COONECTA -Unidad de sistemas de redes y telecomunicaciones	3. PLAN DE RECUPERACIÓN	Ing. John Machuca Coordinador de Riesgos	Tiempo a realizar: 8 meses
Personal de: -Administración de base de datos -Infraestructura y telecomunicaciones -Desarrolladores/ Programadores -Ingeniería de software -Soporte a usuarios -Departamento de Riesgos -Auditor informático	PLAN DE CONCIENCIACIÓN DEL USO DE LAS TI	Ing. Guillermo Cabrera Coordinador del área de sistemas, Ing. Richard Yunga Capacitador del personal - Talento Humano	Tiempo a realizar: 6 meses
Personal de: -Administración de base de datos -Infraestructura y telecomunicaciones -Desarrolladores/ Programadores -Ingeniería de software -Soporte a usuarios - Departamento de Riesgos -Auditor informático	PLAN DE FORMACIÓN CONTINUA DE LAS TI	Ing. Richard Yunga Capacitador del personal - Talento Humano	Tiempo a realizar: 6 meses

Tabla 4-3: Plan de Seguridad

Elaborado por: autores

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- El presente trabajo sirve como una aplicación de la metodología MAGERIT – versión 2 basada en su herramienta PILAR Basic, para la ejecución del Análisis y Gestión de Riesgos, extendida hacia cualquier institución pública o privada que posea activos.

- La prevención, detección y mitigación de los riesgos, es imprescindible, razón por la que se deberá aplicar una metodología con sus respectiva herramienta, con la finalidad de mitigar los riesgos usando perfiles de seguridad y salvaguardas adecuadas que recomienda la herramienta PILAR Basic.

- La herramienta PILAR Basic, fue de vital importancia para comprender que los Sistemas de Información están expuestos a amenazas que pueden causar daños significativos a las operaciones de la organización, el mismo que tiene un interfaz amigable de aplicación para el usuario.

- Una vez terminado el Análisis y Gestión de Riesgos a la Cooperativa de Ahorro y Crédito Jardín Azuayo, y realizada la calificación de los riesgos a los activos: cajero automático, portal web, Sistema Financiero Integral Jardín Azuayo, servidor de base de datos, telefonía IP, red WWAN, cableado de datos y Red COONECTA, todos con sus respectivas amenazas, se concluye que éstos son los activos con un mayor nivel de riesgo en la organización, debido a la falta de implementación de salvaguardas de seguridad como recomiendan los estándares y Código de buenas prácticas para la Gestión de la Seguridad de la Información.

- La Cooperativa de Ahorro y Crédito Jardín Azuayo no cuenta con un plan de seguridad de la información por lo que existe una alta probabilidad de que las amenazas se materialicen.

- La Institución, está consciente del riesgo que poseen sus sistemas de información, por lo que, la Gerencia a partir del presente trabajo, realizó la implementación de ciertas salvaguardas que les permitirá proteger su información.

- El apoyo, tanto de la Gerencia como del personal de la unidad de sistemas, redes y telecomunicaciones, fue indispensable para la elaboración de la tesis, ya que con coordinaciones nos facilitaron la información que nos permitió evaluar y gestionar los activos tecnológicos.

- Concluimos que actualmente en nuestro medio no se pone real énfasis en temas referentes al Análisis y Gestión de Riesgos de los Sistemas de Información, lo que ocasiona que no se tenga un conocimiento adecuado de dichos temas y no se cuente con el personal especializado para realizar dicho análisis.

5.2. RECOMENDACIONES

- Se recomienda utilizar la Metodología MAGERIT – versión 2, en el Análisis y Gestión de Riesgos, complementando con la herramienta PILAR Basic, que es una herramienta propia automatizada y basada en la metodología, que permite trabajar con varios activos, amenazas y salvaguardas.

- Se recomienda que la administración tome en cuenta estándares como: ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la Información, COBIT e ITIL (mejores prácticas de prestación de servicios TI y auditoría) y CISCO (estándares internacionales de redes y telecomunicaciones).

- A las Organizaciones que realicen el Análisis y Gestión de Riesgos de los Sistemas de Información, les sugerimos que lo hagan por lo menos, una vez al año, razón por la cual podrán conocer sus fortalezas o debilidades e implementar salvaguardas para reducir las debilidades encontradas.

- A los estudiantes que tenga interés en realizar un Análisis y Gestión de Riesgos, les sugerimos que constantemente mantengan reuniones con los delegados en el manejo de la información y con el personal involucrado en el proyecto que labora en la organización, para que el resultados se ajusten a la realidad.

SOBRE LOS ACTIVOS:

- Se recomienda implementar salvaguardas preventivas hasta que se implemente el plan de seguridad, con el objetivo de proteger al activo en todo tiempo.

- Se recomienda la implementación de las siguientes salvaguardas en cada activo, para reducir las probabilidades de que las amenazas se materialicen:

Capa del Negocio

Cajero Automático

- Aumentar la seguridad con una protección de acceso controlado, donde se limite los intentos fallidos de acceso al cajero, en un número máximo de tres (3) intentos; de esta manera se evitará que los atacantes disfruten de los privilegios de la persona suplantada para sus fines propios.
- Incrementar el número de dígitos de la clave.

Servicios Internos

Portal Web

- Mejorar la seguridad virtual con una protección de acceso controlado, donde se limite los intentos fallidos de acceso a la cuenta del socio (servicio en línea), en un número máximo de tres (3) intentos; de esta manera se evitará que los atacantes disfruten de los privilegios de la persona suplantada para sus fines propios.
- Incrementar el número de dígitos de la clave.
- Implementar medidas de control de acceso al servicio en línea como por ejemplo:
  - Contestando una de varias preguntas de seguridad (ejemplo: lugar de nacimiento, mascota favorita, libro preferido, etc.) y seleccionando una imagen de identificación. Estas dos medidas de control el usuario lo aplicará por una sola vez, y en ingresos posteriores al servicio en línea, el usuario solamente constatará la pregunta e imagen identificada antes de ingresar su clave.
  - Tarjeta de coordenadas, ayudará como un segundo factor de autenticación o clave, la cual contiene una serie de números

(coordenadas), ordenados en filas tituladas con números y las columnas con letras. Las coordenadas serán pedidas en cada sesión y de manera aleatoria después de ingresada la clave de seguridad de la Cooperativa.

- En el servicio en línea incrementar una opción de re-impresión de comprobantes de las transferencias realizadas.
- Concienciar a los socios la importancia del cambio periódico de claves y el peligro que generaría no hacerlo.

Equipamiento

Aplicaciones

Sistema Financiero Integrado Jardín Azuayo

- Mejorar las medidas de control de acceso; monitorear periódicamente la protección del código dañino; llevar un registro de errores no intencionales, todo esto con el fin de que ayude a mejorar la eficacia de la cooperativa en sus procesos automáticos.
- Se recomienda que todas las conexiones externas deben pasar a través de los cortafuegos con el fin de prevenir el uso y el acceso de usuarios no autorizados a los ordenadores.

Equipos

Servidor de base de datos

- Implementar el Estándar TIA-942 (Telecomunications Industry Association) para Data Center, el cual brindará los parámetros para un control físico para que el sistema no caiga debido a la carencias de recursos, y un control periódico de los niveles de temperatura en que se encuentra el servidor, con el fin de evitar que el activo sufra daños por exceso de calor, frio o humedad.
- Debido al acelerado crecimiento del número de socios y a la abundante información recopilada ocasiona que la base de datos existente se sature, por lo que recomendamos ampliar la base de

datos para que la información se encuentre organizada y completa.

Comunicaciones

- Se recomienda una actualización de los planes de continuidad ya que son muy importantes porque garantizan que el sistema nunca caiga, generando satisfacción a los servicios que presta a los socios.

Telefonía IP

- Se debe mejorar el control centralizado con revisiones periódicas de la configuración lo que ayudará a que la información llegue a su destino y evite errores de re-encaminamiento.
- Cuando se hablen temas de vital importancia o confidenciales por la telefonía IP, tratar de tener cautela de las personas que puedan escuchar la información, con el fin de evitar que se den fugas de las mismas.

Red WWAN

- Se recomienda mecanismo de cifrado basado en clave pública ya que permite controlar los riesgos para que las transacciones electrónicas que se realicen en las redes abiertas e inseguras como internet puedan ocurrir con total confianza y garantía. Esta tecnología es fundamental para mejorar los procesos del negocio, permitiendo optimizar los tiempos, la gestión de errores y reducir sus costes.
- Se recomienda que todas las conexiones externas deben pasar a través de los cortafuegos con el fin de prevenir el uso y el acceso de usuarios no autorizados a los ordenadores.

Soportes de información

- Se recomienda para proteger la información sensible y valiosa, un control o eliminación de los dispositivos de entrada como los USB

y CD-ROM para proteger la integridad y confidencialidad de los datos.

Elementos auxiliares

Cableado de datos

- Se recomienda implementar el Estándar TIA-942 (Telecomunications Industry Association), el cual brindará los requerimientos y lineamientos necesarios para el diseño e instalación de centros de cómputo.

Climatización

- Se recomienda implementar un equipo de climatización porque la cooperativa no cuenta con una adecuada ventilación para los equipos informáticos, ocasionando que el ambiente de trabajo no sea el adecuado para los empleados que laboran en la institución.

Servicios subcontratados

Red COONECTA

- Se recomienda incorporar para los servicios subcontratados el documento SLA (Service Level Agreement - Acuerdo de Nivel de Servicio), que es un documento anexo al Contrato de Prestación de Servicios, en donde se estipulan las condiciones y parámetros que comprometen al prestador del servicio a cumplir con unos niveles de calidad de servicio frente al contratante de los mismos.

  Es importante que en el SLA se especifiquen los términos y parámetros sobre los que se adquiere el compromiso en el servicio, se indique el modo de cálculo del índice de cumplimiento, cuál es el objetivo pactado; indicando el valor o márgenes de referencia, cuáles son las posibles compensaciones por incumplimiento y por último las exclusiones o limitaciones en dichos cálculos.

Instalaciones

Unidad de sistemas, redes y telecomunicaciones

- Se recomienda implementar el Estándar TIA-942 (Telecomunications Industry Association), el cual brindará los requerimientos y lineamientos necesarios para el diseño e instalación de centros de cómputo, el cual cuenta con los requerimientos de: instalación de suelo antiestático, sistema central de refrigeración, unidades de aire acondicionado, sistema de distribución de suministros eléctricos auxiliares (UPS), sistema automático de detección de alarmas de incendios, sistema de control de seguridad perimetral, sistema de vigilancia, sistema de control de accesos y todas las normas de seguridad que necesita el área de sistema de información.

Personal

Personal

- Se recomienda implementar una política y procedimientos de gestión de personal (en materia de seguridad)
- Mejorar la asignación de responsabilidades de seguridad a todos los puestos de trabajo
- Implementar procedimientos para el cambio de puesto de trabajo, ya que se maneja de forma intuitiva y dentro de los mismos no se establece la actualización de los acuerdos de confidencialidad en los nuevos puestos debido a la importancia de la información.
- Implementar comprobaciones para el personal con puestos de gran responsabilidad
- Implementar una normativa de obligado cumplimiento en el desempeño del puesto-propiedad intelectual, esto incentivaría a que los trabajos sean realizados con mayor esmero.

ANEXOS

ANEXO 1

FICHAS PARA LA RECOPILACIÓN DE DATOS

[S] SERVICIOS	
NOMBRE:	
DESCRIPCIÓN: …… ……	
RESPONSABLE:	
Tipo (marque todos los adjetivos que procedan): ( ) [anon] anónimo (sin requerir identificación del usuario) ( ) [pub] al público en general (sin relación contractual) ( ) [ext] a usuarios externos (bajo una relación contractual) ( ) [int] interno (usuarios y medios de la propia organización) ( ) [cont] contratado a terceros (se presta con medios ajenos) ( ) [www] world wide web ( ) [telnet] acceso remoto a cuenta local ( ) [email] correo electrónico ( ) [voip] voz sobre ip ( ) [file] almacenamiento de ficheros ( ) [print] servicio de impresión ( ) [ftp] transferencia de ficheros ( ) [backup] servicio de copias de respaldo (backup) ( ) [edi] intercambio electrónico de datos ( ) [dir] servicio de directorio ( ) [dns] servidor de nombres de dominio ( ) [idm] gestión de identidades ( ) [ipm] gestión de privilegios ( ) [crypto] servicios criptográficos ( ) [key_gen] generación de claves ( ) [integrity] protección de la integridad ( ) [encryption] cifrado ( ) [auth] autenticación ( ) [sign] firma electrónica ( ) [time] fechado electrónico ( ) [pki] PKI - infraestructura de clave pública ( ) [ca] autoridad de certificación ( ) [ra] autoridad de registro ( ) [ba] autoridad de validación ( ) [tsa] autoridad de fechado electrónico ( ) [aa] autoridad de atributos ( ) [other] otros…	**CARACTERISTICAS:** ……

SALVAGUARDAS EXISTENTES:……
……

AMENAZAS:

[N] Desastres Naturales
- [N.1] Fuego
- [N.2] Daños por agua
- [N.*]Desastres naturales

[I] De origen industrial
- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios o suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados
- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización (log)
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de (re-)encaminamiento
- [E.10] Errores de secuencia
- [E.14] Fugas de información
- [E.15] Alteración de la información
- [E.16] Introducción de falsa información
- [E.17] Degradación de la información
- [E.18] Destrucción de la información
- [E.19] Divulgación de la información
- [E.20] Vulnerabilidad de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Perdidas de equipos
- [E.28] Indisponibilidad del personal

[A] Ataques deliberados
- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] (Re-) encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de trafico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación de información
- [A.16] Introducción de falsa información
- [A.17] Corrupción de la información

[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[SW] APLICACIONES (Software)

NOMBRE:

DESCRIPCIÓN:
……
……

CARACTERISTICAS:
……
……
……

RESPONSABLE:

Tipo (marque todos los adjetivos que procedan):
( ) [prp] desarrollo propio (in house)
( ) [sub] desarrollo a medida (subcontratado)
( ) [std] estándar (off the shelf)
- ( ) [browser] navegador web
- ( ) [www] servidor de presentación
- ( ) [app] servidor de aplicaciones
- ( ) [email_client] cliente de correo electrónico
- ( ) [email_server] servidor de correo electrónico
- ( ) [directory] servidor de directorio
- ( ) [file] servidor de ficheros
- ( ) [dbms] sistema de gestión de bases de datos
- ( ) [tm] monitor transaccional
- ( ) [office] ofimática
- ( ) [av] anti virus
- ( ) [os] sistema operativo
  - ( ) [windows] Windows
  - ( ) [solaris] Solaris
  - ( ) [linux] linux
  - ( ) [other] otros…
- ( ) [ts] servidor de terminales
- ( ) [backup] sistema de backup
- ( ) [other] otros…

SALVAGUARDAS EXISTENTES:……
……

AMENAZAS:

[N] Desastres Naturales
- [N.1] Fuego
- [N.2] Daños por agua
- [N.*]Desastres naturales

[I] De origen industrial
- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios o suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados
- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización (log)
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de (re-)encaminamiento
- [E.10] Errores de secuencia
- [E.14] Fugas de información
- [E.15] Alteración de la información
- [E.16] Introducción de falsa información
- [E.17] Degradación de la información
- [E.18] Destrucción de la información
- [E.19] Divulgación de la información
- [E.20] Vulnerabilidad de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Perdidas de equipos
- [E.28] Indisponibilidad del personal

[A] Ataques deliberados
- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] (Re-) encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de trafico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación de información
- [A.16] Introducción de falsa información
- [A.17] Corrupción de la información

[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[HW] EQUIPAMIENTO INFORMÁTICO (Hardware)

NOMBRE:

DESCRIPCIÓN:

……
……

CARACTERÍSTICAS:

MARCA:…….. VERSION……..
MODELO:……. AÑO…….

RESPONSABLE:

Tipo (marque todos los adjetivos que procedan):

( ) [host] grandes equipos (host)
( ) [mid] equipos medios
( ) [pc]informática personal
( ) [vhost]equipos virtuales
( ) [cluster] cluster
( ) [mobile] informática móvil
( ) [pda]agendas electrónicas
( ) [easy]fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
  ( ) [print] medios de impresión
  ( ) [scan] escáner
  ( ) [crypto] dispositivo criptográfico
  ( ) [other] otros…
( ) [bd] dispositivo de frontera
( ) [network] soporte de la red
  ( ) [modem] módem
  ( ) [hub] concentrador
  ( ) [switch] conmutador
  ( ) [router] encaminador
  ( ) [bridge]puente
  ( ) [gtwy] pasarela
  ( ) [firewall] cortafuegos
  ( ) [wap] punto de acceso wireless
  ( ) [other] otros…
( ) [pabx]centralita telefónica
( ) [other] otros…

SALVAGUARDAS EXISTENTES:……
……
……

AMENAZAS:

[N] Desastres Naturales
- [N.1] Fuego
- [N.2] Daños por agua
- [N.*]Desastres naturales

[I] De origen industrial
- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios o suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados
- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización (log)
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de (re-)encaminamiento
- [E.10] Errores de secuencia
- [E.14] Fugas de información
- [E.15] Alteración de la información
- [E.16] Introducción de falsa información
- [E.17] Degradación de la información
- [E.18] Destrucción de la información
- [E.19] Divulgación de la información
- [E.20] Vulnerabilidad de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Perdidas de equipos
- [E.28] Indisponibilidad del personal

[A] Ataques deliberados
- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] (Re-) encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de trafico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación de información
- [A.16] Introducción de falsa información
- [A.17] Corrupción de la información
- [A.18] Destrucción de la información

[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[COM] COMUNICACIONES
NOMBRE:
DESCRIPCIÓN: …… ……
CARACTERISTICAS: MARCA:…….. CANTIDAD…….. MODELO:…… …….. ……
RESPONSABLE:
Tipo (marque todos los adjetivos que procedan): ( ) [PSTN] red telefónica ( ) [ISDN] RDSI (red digital) ( ) [X25] X25 (red de datos) ( ) [ADSL] ADSL ( ) [pp] punto a punto ( ) [radio] red inalámbrica ( ) [wifi] Wifi ( ) [mobile] telefonía movil ( ) [sat] por satélite ( ) [LAN] red local ( ) [VLAN] LAN virtual ( ) [MAN] red metropolitana ( ) [WAN] red de área amplia ( ) [Internet] Internet ( ) [vpn] red privada virtual ( ) [other] otros…

SALVAGUARDAS EXISTENTES:……
……
……

AMENAZAS:

[N] Desastres Naturales
- [N.1] Fuego
- [N.2] Daños por agua
- [N.*]Desastres naturales

[I] De origen industrial
- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios o suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados
- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización (log)
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de (re-)encaminamiento
- [E.10] Errores de secuencia
- [E.14] Fugas de información
- [E.15] Alteración de la información
- [E.16] Introducción de falsa información
- [E.17] Degradación de la información
- [E.18] Destrucción de la información
- [E.19] Divulgación de la información
- [E.20] Vulnerabilidad de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Perdidas de equipos
- [E.28] Indisponibilidad del personal

[A] Ataques deliberados
- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] (Re-) encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de trafico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación de información
- [A.16] Introducción de falsa información
- [A.17] Corrupción de la información

[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[SI] SOPORTES DE INFORMACION
NOMBRE:
DESCRIPCIÓN: …… ……
CARACTERÍSTICAS: MARCA:…… …… CAPACIDAD:…… …… CANTIDAD:…… …….. ……
RESPONSABLE:
Tipo (marque todos los adjetivos que procedan): ( ) [electronic] electrónicos ( ) [disk] discos ( ) [vdisk] discos virtuales ( ) [san] almacenamiento en red ( ) [disquette] disquetes ( ) [cd] cederrón (CD-ROM) ( ) [usb] dispositivos USB ( ) [dvd] DVD ( ) [tape] cinta magnética ( ) [mc] tarjetas de memoria ( ) [ic] tarjetas inteligentes ( ) [other] otros… ( ) [non_electronic] no electrónicos ( ) [printed] material impreso ( ) [tape] cinta de papel ( ) [film] microfilm ( ) [cards] tarjetas perforadas ( ) [other] otros…

SALVAGUARDAS EXISTENTES:……
……
……

AMENAZAS:

[N] Desastres Naturales
- [N.1] Fuego
- [N.2] Daños por agua
- [N.*]Desastres naturales

[I] De origen industrial
- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios o suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados
- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización (log)
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de (re-)encaminamiento
- [E.10] Errores de secuencia
- [E.14] Fugas de información
- [E.15] Alteración de la información
- [E.16] Introducción de falsa información
- [E.17] Degradación de la información
- [E.18] Destrucción de la información
- [E.19] Divulgación de la información
- [E.20] Vulnerabilidad de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Perdidas de equipos
- [E.28] Indisponibilidad del personal

[A] Ataques deliberados
- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] (Re-) encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de trafico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación de información
- [A.16] Introducción de falsa información
- [A.17] Corrupción de la información
- [A.18] Destrucción de la información

[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[AUX] EQUIPAMIENTO AUXILIAR

NOMBRE:

DESCRIPCIÓN:
……
……

CARACTERISTICAS:
MARCA:…….
TIPO……..
……
……..

RESPONSABLE:

Tipo (marque todos los adjetivos que procedan):
( ) [power] fuentes de alimentación
( ) [ups] sai - sistemas de alimentación ininterrumpida
( ) [gen] generadores eléctricos
( ) [ac] equipos de climatización
( ) [cabling] cableado
  ( ) [wire] cable eléctrico
  ( ) [fiber] fibra óptica
( ) [robot] robots
  ( ) [tape] ... de cintas
  ( ) [disk] ... de discos
( ) [supply] suministros esenciales
( ) [destroy] equipos de destrucción de soportes de información
( ) [furniture] mobiliario: armarios, etc
( ) [safe] cajas Fuertes
( ) [other] otros…

SALVAGUARDAS EXISTENTES:……
……
……

AMENAZAS:

[N] Desastres Naturales
- [N.1] Fuego
- [N.2] Daños por agua
- [N.*]Desastres naturales

[I] De origen industrial
- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios o suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados
- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización (log)
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de (re-)encaminamiento
- [E.10] Errores de secuencia
- [E.14] Fugas de información
- [E.15] Alteración de la información
- [E.16] Introducción de falsa información
- [E.17] Degradación de la información
- [E.18] Destrucción de la información
- [E.19] Divulgación de la información
- [E.20] Vulnerabilidad de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento/actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Perdidas de equipos
- [E.28] Indisponibilidad del personal

[A] Ataques deliberados
- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] (Re-) encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de trafico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación de información
- [A.16] Introducción de falsa información

[A.17] Corrupción de la información
[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[SS] SERVICIOS SUBCONTRATADOS

NOMBRE:

DESCRIPCIÓN:
……
……

CARACTERÍSTICAS:
SERVICIO:……

RESPONSABLE:

Tipo (marque todos los adjetivos que procedan):
( ) [anon] anónimo (sin requerir identificación del usuario)
( ) [pub] al público en general (sin relación contractual)
( ) [ext] a usuarios externos (bajo una relación contractual)
( ) [int] interno (usuarios y medios de la propia organización)
( ) [cont] contratado a terceros (se presta con medios ajenos)

( ) [www] world wide web
( ) [telnet] acceso remoto a cuenta local
( ) [email] correo electrónico
( ) [voip] voz sobre ip
( ) [file] almacenamiento de ficheros
( ) [print] servicio de impresión
( ) [ftp] transferencia de ficheros
( ) [backup] servicio de copias de respaldo (backup)
( ) [edi] intercambio electrónico de datos

( ) [dir] servicio de directorio
( ) [dns] servidor de nombres de dominio
( ) [idm] gestión de identidades
( ) [ipm] gestión de privilegios
( ) [crypto] servicios criptográficos
  ( ) [key_gen] generación de claves
  ( ) [integrity] protección de la integridad
  ( ) [encryption] cifrado
  ( ) [auth] autenticación
  ( ) [sign] firma electrónica
  ( ) [time] fechado electrónico

SALVAGUARDAS EXISTENTES:……
……
……

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de (re-)encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.16] Introducción de falsa información
[E.17] Degradación de la información
[E.18] Destrucción de la información
[E.19] Divulgación de la información
[E.20] Vulnerabilidad de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Perdidas de equipos
[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] (Re-) encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de trafico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información
[A.16] Introducción de falsa información
[A.17] Corrupción de la información
[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[L] INFRAESTRUCTURA

NOMBRE:

DESCRIPCIÓN:

……
……
……

CARACTERÍSTICAS:

TIPO:……..
DIRECCIÓN:……
TELEFONOS:……
……
……
……

RESPONSABLE:

Tipo (marque todos los adjetivos que procedan):

( ) [site] emplazamiento
( ) [building] edificio
( ) [local] local
( ) [mobile] plataformas móviles
  ( ) [car] vehículo terrestre: coche, camión, etc.
  ( ) [plane] vehículo aéreo: avión, etc.
  ( ) [ship] vehículo marítimo: buque, lancha, etc.
  ( ) [shelter] contenedores
( ) [channel] canalización
( ) [other] otros…

SALVAGUARDAS EXISTENTES:……
……
……

AMENAZAS:

[N] Desastres Naturales
- [N.1] Fuego
- [N.2] Daños por agua
- [N.*]Desastres naturales

[I] De origen industrial
- [I.1] Fuego
- [I.2] Daños por agua
- [I.*] Desastres industriales
- [I.3] Contaminación mecánica
- [I.4] Contaminación electromagnética
- [I.5] Avería de origen físico o lógico
- [I.6] Corte del suministro eléctrico
- [I.7] Condiciones inadecuadas de temperatura o humedad
- [I.8] Fallo de servicios de comunicaciones
- [I.9] Interrupción de otros servicios o suministros esenciales
- [I.10] Degradación de los soportes de almacenamiento de la información
- [I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados
- [E.1] Errores de los usuarios
- [E.2] Errores del administrador
- [E.3] Errores de monitorización (log)
- [E.4] Errores de configuración
- [E.7] Deficiencias en la organización
- [E.8] Difusión de software dañino
- [E.9] Errores de (re-)encaminamiento
- [E.10] Errores de secuencia
- [E.14] Fugas de información
- [E.15] Alteración de la información
- [E.16] Introducción de falsa información
- [E.17] Degradación de la información
- [E.18] Destrucción de la información
- [E.19] Divulgación de la información
- [E.20] Vulnerabilidad de los programas (software)
- [E.21] Errores de mantenimiento / actualización de programas (software)
- [E.23] Errores de mantenimiento / actualización de equipos (hardware)
- [E.24] Caída del sistema por agotamiento de recursos
- [E.25] Perdidas de equipos
- [E.28] Indisponibilidad del personal

[A] Ataques deliberados
- [A.4] Manipulación de la configuración
- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] (Re-) encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de trafico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación de información
- [A.16] Introducción de falsa información
- [A.17] Corrupción de la información
- [A.18] Destrucción de la información

[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

[P] PERSONAL
NOMBRE:
DESCRIPCIÓN: …… ……
CARACTERÍSTICAS: RESPONSABLES:…… ……
RESPONSABLE:
Tipo (marque todos los adjetivos que procedan): ( ) [ue] usuarios externos ( ) [ui] usuarios internos ( ) [op] operadores ( ) [adm] administradores de sistemas ( ) [com] administradores de comunicaciones ( ) [dba] administradores de BBDD ( ) [sec] administradores de seguridad ( ) [des] desarrolladores/programadores ( ) [sub] subcontratas ( ) [prov] proveedores ( ) [other] otros…

SALVAGUARDAS EXISTENTES:……
……
……

AMENAZAS:

[N] Desastres Naturales
[N.1] Fuego
[N.2] Daños por agua
[N.*]Desastres naturales

[I] De origen industrial
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica

[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios o suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de (re-)encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información
[E.15] Alteración de la información
[E.16] Introducción de falsa información
[E.17] Degradación de la información
[E.18] Destrucción de la información
[E.19] Divulgación de la información
[E.20] Vulnerabilidad de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.25] Perdidas de equipos
[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] (Re-) encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de trafico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación de información
[A.16] Introducción de falsa información
[A.17] Corrupción de la información
[A.18] Destrucción de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.24] Denegación de servicio
[A.25] Robo de equipos
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

ANEXO 2

MODELO DE VALOR

proyecto: [AR_JA] ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO JARDIN AZUAYO

1. Datos del proyecto

AR_JA	ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO JARDIN AZUAYO
Descripción	Análisis a los Sistemas de Información
Dirección	Sucre 5-42 entre Hermano Miguel y Mariano Cueva Benigno Malo 9-75 y Gran Colombia
Teléfonos	2840 259
Responsable	Sr. Antonio José Lucero Gómez y Sr. John Oswaldo Valverde Padilla
Organización	COOPERATIVA DE AHORRO Y CRÉDITO JARDÍN AZUAYO
Lugar del examen	Coordinación y Cuenca
Versión	1
Fecha	21-11-2011
biblioteca	[std] Biblioteca INFOSEC (22.1.2009)

Descripción

El presente trabajo es realizado en la Cooperativa de Ahorro y Crédito Jardín Azuayo en la oficia Cuenca y su Coordinación, la Institución está controlada por la Superintendencia de Bancos y Seguros

Licencia

[edu] Universidad de Cuenca
Cuenca - Ecuador
[... 1.1.2013]

2. Dimensiones

- o [D] disponibilidad
- o [I] integridad de los datos
- o [C] confidencialidad de los datos
- o [A] autenticidad de los usuarios y de la información
- o [T] trazabilidad del servicio y de los datos

3. Dominios de seguridad

dominio de seguridad	[D]	[I]	[C]	[A]	[T]
[base] COAC Jardín Azuayo	A	A	M	A	M

4. Activos

4.1. Capa - [B] Capa de negocio

[AH_JA] AHORRO
[CR_JA] CRÉDITO
[CA_JA] CAJERO AUTOMÁTICO

4.2. Capa - [IS] Servicios internos

[IP_JA] TELEFONÍA IP
[WEB_JA] PORTAL WEB
[AR_JA] ACCESO REMOTO
[ZM_JA] SERVIDOR DE CORREO ELECTRÓNICO (ZIMBRA)
[iFL_JA] SERVICIO DE ARCHIVO COMPARTIDO POR iFOLDER
[IEX_JA] INTERNET

4.3. Capa - [E] Equipamiento

[SW] Aplicaciones
- [FISJA_JA] SISTEMA FINANCIERO INTEGRADO JARDÍN AZUAYO
- [OFF_JA] OFIMÁTICA
- [AV_JA] ANTIVIRUS
- [OTR_JA] OTROS SOFTWARE

[HW] Equipos
- [SBD_JA] SERVIDOR DE BASE DE DATOS
- [VHOST_JA] EQUIPOS VIRTUALES
- [ROUTER_JA] ROUTER
- [SWITCH_JA] SWITCH
- [BRIDGE_JA] RADIOS
- [FIREWALL_JA] FIREWALL
- [DESKTOP_JA] COMPUTADORAS DE ESCRITORIO
- [LAPTOP_JA] COMPUTADORAS PORTÁTILES
- [PRINT1_JA] IMPRESORA A LASER
- [PRINT2_JA] IMPRESORA MATRICIAL
- [CTG_JA] EQUIPOS DE CONTINGENCIA

[COM] Comunicaciones
- [COM_JA] TELEFONÍA IP
- [LAN_JA] RED LAN
- [WAN_JA] RED WWAN
- [INTERNET_JA] INTERNET

[AUX] Elementos auxiliares
- [POWER_JA] FUENTES DE ALIMENTACIÓN
- [SAI_JA] SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA
- [GEN_JA] GENERADOR ELÉCTRICO
- [EC_JA] EQUIPO DE CLIMATIZACIÓN
- [CABLING_JA] CABLEADO DE DATOS
- [ROBOTS_JA] ROBOTS
- [MOB_JA] MOBILIARIO
- [CF_JA] CAJA FUERTE
- [OTHER_JA] OTROS EQUIPAMIENTOS AUXILIARES

4.4. Capa - [SS] Servicios subcontratados

[SS.01_JA] IRNET
[SS.02_JA] COOPSEGUROS
[SS.03_JA] RED COONECTA
[SS.04_JA] VENTANILLA COMPARTIDA

4.5. Capa - [L] Instalaciones

[L_JA] UNIDAD DE SISTEMAS, REDES Y TELECOMUNICACIONES

4.6. Capa - [P] Personal

[DBA_JA] ADMINISTRACIÓN DE BASE DE DATOS (PRODUCCIÓN-PRUEBAS)
[ITL_JA] INFRAESTRUCTURA Y TELECOMUNICACIONES
[DES_JA] DESARROLLADORES / PROGRAMADORES
[ISOFT_JA] INGENIERÍA DE SOFTWARE
[UI_JA] SOPORTE A USUARIOS

5. Activos

5.1. [AH_JA] AHORRO

- o [S] Servicios
- o [S.pub] al público en general (sin relación contractual)
- o [S.ext] a usuarios externos (bajo una relación contractual)

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

A LA VISTA	Interés anual del 4%; Cualquier cantidad gana interés; no se cobra mantenimiento de cuenta
CERTIFICADO DE DEPÓSITO A PLAZO (Póliza)	A 30, 60, 90, 180, 270, 365 o más días se gana el 6%, 6.25%, 6.50%, 7%, 7.50%, 9% respectivamente
PROGRAMADO - MI ALCANCÍA SEGURA	Mi pequeña alcancía de 1 a 5 años el 8% de interés y mi gran alcancía a más de 5 años el 8.50% de interés

Descripción

Para realizar los depósitos usted debe presentar:
-libreta de ahorros
-la papeleta de depósito (color verde), si su depósito incluye cheques, deberá llenar el detalle de los mismos en el reverso de la papeleta.

Para realizar los retiros usted necesita:
-cédula de identidad
-libreta de ahorros
-papeleta de retiro (color amarillo)

(En cada oficina se tienen montos máximos de retiro, entre 500 y 1.000 dólares por lo cual se debe anticipar el retiro en la respectiva oficina con 24 horas hábiles de anterioridad; se puede también retirar con cheque sin anticipación)

5.2. [CR_JA] CRÉDITO

- o [S] Servicios
- o [S.pub] al público en general (sin relación contractual)
- o [S.ext] a usuarios externos (bajo una relación contractual)

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

ORDINARIO	Base de ahorro del 10% del valor que necesite; Ti= 12,77% anual; Plazo máximo= $5.000 en 4 años y $30.000 en 5 años
EXTRAORDINARIO o EMERGENTE	Ti=11,22% anual; Monto máximo= $1.000; Plazo máximo= 12 meses
SIN AHORRO	Individual: Ti= 15% anual, Monto máximo= $30.000 en 5 años, de acuerdo a cupos y disponibilidad; Grupal: Ti=14,04%, Monto máximo= $10.000 a 4 años, de acuerdo a cupos y disponibilidad
DE DESARROLLO	Ti=10,15%, Monto máximo= $45.000 a 4 años
DE VIVIENDA	Ti=12,09%, Monto máximo=$20.000 a 10 años

Descripción

CRÉDITO ORDINARIO.- son los créditos provenientes de los ahorros de los socios o de fuentes externas, con el propósito de apoyar en la dinamización de las economías locales.
El crédito ordinario de Jardín Azuayo está orientado a beneficiar a los socios pues: a) es un medio o alternativo menos costosa de obtener recursos monetarios, b) da la oportunidad a las personas sean estas jurídicas, naturales u organizaciones de hecho de financiar sus operaciones o gastos, c) baja tasa de interés en relación a otras instituciones financieras.

CRÉDITO EXTRAORDINARIO.- son aquellas que se otorgan a los socios en condiciones especiales y se concederán en situaciones emergentes como: enfermedad, calamidad doméstica, siniestro debidamente comprobado o para gastos de educación. La calificación de emergencia puede corresponder al socio, a su cónyuge, a sus hijos y a sus padres si dependen del socio. Solo en el caso de éstos créditos es permitido mantener al mismo tiempo dos créditos vigentes con la COAC Jardín Azuayo. A través de este crédito los socios se benefician de la siguiente manera: a) no necesita tener una base de ahorro para acceder al crédito, b) disponibilidad inmediata del crédito, c) obtiene una baja tasa de interés en comparación a otras alternativas.

CRÉDITO SIN AHORRO.- Son operaciones que se otorgan a las persona naturales, jurídicas u organizaciones de hecho que cumplan con la condición de ser socios, sin que previamente deban realizar el depósito de ahorro exigido para los créditos ordinarios.

CRÉDITO DE DESARROLLO.- Son créditos que la Cooperativa otorga a organizaciones jurídicas o de hecho sin fines de lucro para invertir en proyectos de desarrollo. Pueden solicitar con ahorro previo o sin ahorro. Para optar por este tipo de crédito las organizaciones deberán presentar el proyecto de desarrollo. A través de esta alternativa los socios se beneficiarán de la siguiente manera: a) Mediante la obtención de fondos para sus proyectos de desarrollo, b) Tasas de interés bajas en comparación con el mercado, c) No necesita tener una base de ahorro.

CRÉDITO DE VIVIENDA.- Son créditos que la Cooperativa otorga a sus socios con el propósito de adquirir, mejorar o construir su vivienda y se exige garantía hipotecaria. Estos tipos de crédito son a largo plazo, permitiendo con ello a los socios mayores facilidades para los pagos. La concesión de estos tipos de crédito se da en función de cupos. A través de esta opción los socios se beneficiarán de la siguiente manera: a) Acceso a recursos económicos a largo plazo para construcción, remodelación o compra de vivienda, b) Baja tasa de interés en comparación a otras alternativas, c) No necesita tener una base de ahorro para acceder al crédito.

5.3. [CA_JA] CAJERO AUTOMÁTICO

- o [S] Servicios
- o [S.pub] al público en general (sin relación contractual)
- o [S.crypto] servicios criptográficos
- o [S.crypto.auth] autenticación

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MODELO	Lovi type NCR SelfSer 22
PANTALLA	Interna de 15" touchscreen
SISTEMA OPERATIVO	Windows XP Pro, core 2 duo
CAPACIDAD DISCO DURO	80 GB
DISPENSADOR	4 cassettes
IMPRESORA QUE USA	Receipt print - 80 mm
RESOLUCIÓN DE IMPRESORA	203 dpi graphics terminal printer

Descripción

Son Cajeros automáticos modelo Lovi, están colocados en diferentes agencias. Disponen de 12 cajeros a nivel de toda la Cooperativa hasta el momento; existe un cajero en la oficina cuenca.

5.4. [IP_JA] TELEFONÍA IP

- o [S] Servicios
- o [S.int] interno (usuarios y medios de la propia organización)
- o [S.voip] voz sobre ip

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	Cisco Call Manager Express
MODELO	2801 de cisco
CANTIDAD	32
TIPO	Base, Inhalámbrico

Descripción

Control de servicios a través de equipo IP y sus beneficios, Call Manager, tripartita, transferencia, etc.

5.5. [WEB_JA] PORTAL WEB

- o [S] Servicios
- o [S.pub] al público en general (sin relación contractual)
- o [S.www] world wide web
- o [S.dns] servidor de nombres de dominio

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

SISTEMA OPERATIVO	Suse 4D de 64 bits
PROCESADOR	Micro procesador core 2 duo
MEMORIA RAM	24 GB
DISCO DURO	40 GB
CONEXIÓN	Directa con la Base de Datos Central para realizar transacciones en línea

Descripción

Con el portal web la cooperativa provee a sus socios información con respecto a los nuevos servicios que posee, así como transacciones vía web, consulta de saldos, recarga de saldos entre los principales.

5.6. [AR_JA] ACCESO REMOTO

- o [S] Servicios
- o [S.int] interno (usuarios y medios de la propia organización)
- o [S.telnet] acceso remoto a cuenta local

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

SISTEMA OPERATIVO	linux
PUERTO	23/tcp
FUNCION	protocolo cliente / servicio

Descripción

Se tiene dos formas de acceso remoto, por SSH y team view que permite dar soporte de forma remota usando claves fijas y aleatorias, también se usa telnet para acceder a equipos como activos de red.

5.7. [ZM_JA] SERVIDOR DE CORREO ELECTRÓNICO (ZIMBRA)

- o [S] Servicios
- o [S.int] interno (usuarios y medios de la propia organización)
- o [S.email] correo electrónico

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

DESARROLLADOR	Zimbra Inc
VERSIÓN	7
GENERO	Group Ware
SISTEMA OPERATIVO	Windows, Linux
INTERFAZ	Soap

Descripción

El servidor presta funcionalidades de servidor de envio y recepción de correo electrónico, agenda personal y colaborativa, servicio de mensajería instantánea a los colaboradores de la Cooperativa.

5.8. [iFL_JA] SERVICIO DE ARCHIVO COMPARTIDO POR iFOLDER

- o [S] Servicios
- o [S.int] interno (usuarios y medios de la propia organización)
- o [S.file] almacenamiento de ficheros

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	Novell
VERSIÓN	3.8 sobre Suse Interprice 11
CAPACIDAD	4 GB por usuario
VIRTUALIZACIÓN	VMWARE

Descripción

Servicio de archivos compartidos compatible con windows y linux, mendiante instalación de software cliente, acceso mediante HTTPs y cliente propio, capacidad de administración de cuotas y usuarios permitidos, integración con LDAP.

5.9. [IEX_JA] INTERNET

- o [SW] Aplicaciones (software)

- o [SW.std] estándar (off the shelf)
- o [SW.std.browser] navegador web
- o [SW.std.os] sistema operativo
- o [SW.std.os.windows] windows

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

DISEÑO	HTML, CSSS, XML
INTERFAZ DE USUARIO	FTP
PROTOCOLO	HTTP, FTP
SISTEMA OPERATIVO	Windows
ÁMBITO	Software libre
VERSIÓN	7 y 8

Descripción

Navegación internet, browser para acceso al sistema y configuración de router, radios, etc

5.10. [SW.FISJA_JA] SISTEMA FINANCIERO INTEGRADO JARDÍN AZUAYO

- o [D] Datos / Información
- o [D.vr] datos vitales
- o [D.biz] datos de interés para el negocio
- o [D.int] datos de gestión interna
- o [D.log] registro de actividad (log)
- o [SW] Aplicaciones (software)
- o [SW.prp] desarrollo propio (in house)
- o [SW.sub] desarrollo a medida (subcontratado)
- o [SW.std] estándar (off the shelf)
- o [SW.std.browser] navegador web
- o [SW.std.app] servidor de aplicaciones
- o [SW.std.dbms] sistema de gestión de bases de datos
- o [SW.std.os] sistema operativo
- o [SW.std.os.windows] windows
- o [SW.std.os.linux] linux

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

NOMENCLATURA	FISJA
CREACIÓN	2005
LENGUAJE DE PROGRAMACIÓN	Oracle 11G
PREFORMA	Oracle Develop Suite 10G
SOPORTE	Oracle Aplication Server
PLATAFORMA	Windows, Linux

Descripción

Controla y automatiza las tareas de Ahorro y Crédito, control de equipos y usuarios de la Institución

5.11. [SW.OFF_JA] OFIMÁTICA

- o [SW] Aplicaciones (software)
- o [SW.std] estándar (off the shelf)
- o [SW.std.office] ofimática
- o [SW.std.os] sistema operativo
- o [SW.std.os.windows] windows
- o [SW.std.os.linux] linux

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

BAJO WINDOWS	Microsoft Office, versión 2007 y 2010
BAJO LINUX	Open Office, versión 3
ÁMBITO	libre

Descripción

Sirven para trabajos de oficina: procesamiento de texto, hojas de cálculo, presentaciones electrónicas etc.

5.12. [SW.AV_JA] ANTIVIRUS

- o [D] Datos / Información
- o [D.vr] datos vitales
- o [D.other] otros ...
- o [SW] Aplicaciones (software)
- o [SW.std] estándar (off the shelf)
- o [SW.std.av] anti virus
- o [SW.std.os] sistema operativo
- o [SW.std.os.windows] windows
- o [SW.std.os.linux] linux

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

SOFTWARE 1	Kapersky 6.0
SOFTWARE 2	Eset Nod 32 Bussines Edition

Descripción

Son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos.

5.13. [SW.OTR_JA] OTROS SOFTWARE

- o [D] Datos / Información
- o [D.vr] datos vitales

- o [D.biz] datos de interés para el negocio
- o [D.other] otros ...
- o [SW] Aplicaciones (software)
- o [SW.std] estándar (off the shelf)
- o [SW.std.os] sistema operativo
- o [SW.std.os.windows] windows
- o [SW.std.os.linux] linux
- o [SW.std.other] otros ...

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

SOFTWARE 1	BPwind
SOFTWARE 2	Proyect
SOFTWARE 3	Paquete de Adobe
SOFTWARE 4	My SQL
SOFTWARE 5	VLC
SOFTWARE 6	Paquete de Photoshop

Descripción

Existen muchos software que se utiliza en la Institución entre las principales tenemos las mencionadas.

5.14. [HW.SBD_JA] SERVIDOR DE BASE DE DATOS

- o [HW] Equipamiento informático (hardware)
- o [HW.host] grandes equipos (host)
- o [HW.data] que almacena datos

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

NOMBRE	Oracle Standar One
MARCA	IBM P7
VERSIÓN	11G
MODELO	Core

Descripción

La base de datos contiene la información de los sistemas de caja, directivos, operaciones, etc,

5.15. [HW.VHOST_JA] EQUIPOS VIRTUALES

- o [HW] Equipamiento informático (hardware)
- o [HW.vhost] equipos virtuales

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	IBM
MODELO	HS22, BMWARE X86 INFRAESTRUCTURE
AÑO	2010
VERSIÓN	ESXi4.2
CANTIDAD	25

Descripción

Estos equipos están virtualizados en cuchillas blade HS22 en un blad type H y depende de los servicios que se quieran instalar dentro de estas cuchillas. Pueden utilizarse dos máquinas virtuales como diez máquinas virtuales o más, todo depende de la memoria.

5.16. [HW.ROUTER_JA] ROUTER

- o [HW] Equipamiento informático (hardware)
- o [HW.network] soporte de la red
- o [HW.network.router] encaminador
- o [HW.network.gtwy] pasarela
- o [HW.network.wap] punto de acceso wireless

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	CISCO
MODELO	2801
AÑO	2008
CANTIDAD	2

Descripción

Un Router es el hardware que sirve para rutear direcciones, dar salida a internet a un switch o directamente a una PC.

Sus principales características son:

-Permiten interconectar tanto redes de área local como redes de área extensa.
-Proporcionan un control del tráfico y funciones de filtrado a nivel de red, es decir, trabajan con direcciones de nivel de red, como por ejemplo, con direcciones IP.

5.17. [HW.SWITCH_JA] SWITCH

- o [HW] Equipamiento informático (hardware)
- o [HW.network] soporte de la red
- o [HW.network.switch] conmutador

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	CISCO
MODELO	2960
AÑO	2010
CANTIDAD	4

Descripción

Un Switch es el hardware que sirve para conectar dos o más PC's para compartir recursos.

5.18. [HW.BRIDGE_JA] RADIOS

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.bridge] puente

Dominio de seguridad

- [base] COAC Jardín Azuayo

Datos

MARCA	CISCO, MOTOROLA
MODELO	1300-PTP300
AÑO	2008
CANTIDAD	2X2

Descripción

Un puente o bridge es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red hacia otra, con base en la dirección física de destino de cada paquete.

5.19. [HW.FIREWALL_JA] FIREWALL

- [HW] Equipamiento informático (hardware)
- [HW.network] soporte de la red
- [HW.network.firewall] cortafuegos

Dominio de seguridad

- [base] COAC Jardín Azuayo

Datos

MARCA	Clon de pc
SISTEMA OPERATIVO	Linux
VERSIÓN	clear OS
CANTIDAD	1

Descripción

Un cortafuegos (o firewall en inglés) es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo

tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

5.20. [HW.DESKTOP_JA] COMPUTADORAS DE ESCRITORIO

- o [HW] Equipamiento informático (hardware)
- o [HW.mid] equipos medios
- o [HW.pc] informática personal

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	Intel - Samsung
PROCESADOR	Core Duo y Core i3
MEMORIA RAM	1GB A 2GB
DISCO DURO	320 GB
VERSIÓN	DH55PJ, DG31PR, DHG1WW

Descripción

Son Pc clon de escritorio para instalar windows o linux, por lo general se maneja equipos intel puros, sirven para ejecutar las operaciones diarias.

5.21. [HW.LAPTOP_JA] COMPUTADORAS PORTÁTILES

- o [HW] Equipamiento informático (hardware)
- o [HW.pc] informática personal
- o [HW.mobile] informática móvil

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	Toshiba - Dell
MODELO	Satellite - Inspiron
PROCESADOR	Core Duo, Core i3
MEMORIA RAM	2 a 6 GB
DISCO DURO	320 a 600 GB
AÑO	2009 Y 2011

Descripción

Sirven para realizar trabajos diarios aplicativo - Institucional.

5.22. [HW.PRINT1_JA] IMPRESORA A LASER

- o [HW] Equipamiento informático (hardware)
- o [HW.mid] equipos medios
- o [HW.easy] fácilmente reemplazable

- o [HW.peripheral] periféricos
- o [HW.peripheral.print] medios de impresión

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	Xerox / Samsung
MODELO	X3435 / ML-2010
AÑO	2009 / 2011
CANTIDAD	60

Descripción

Son impresoras que sirven para reportes del módulo crédito, SOAT.

5.23. [HW.PRINT2_JA] IMPRESORA MATRICIAL

- o [HW] Equipamiento informático (hardware)
- o [HW.mid] equipos medios
- o [HW.peripheral] periféricos
- o [HW.peripheral.print] medios de impresión
- o [HW.peripheral.scan] escáner

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	Epson
MODELO	FX-890
AÑO	2008

Descripción

En las oficinas se manejan las impresoras epson, este modelo es muy robusto y por ende soporta gran volumen de impresión diaria.

5.24. [HW.CTG_JA] EQUIPOS DE CONTINGENCIA

- o [HW] Equipamiento informático (hardware)
- o [HW.peripheral] periféricos
- o [HW.peripheral.crypto] dispositivo criptográfico

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

EQUIPOS	cámaras fotográficas, GPS
MARCA	Sony, canon, hp, etc.

Descripción

Estos equipos ayudan al momento del avalúo de los terrenos y a la protección de equipos host.

5.25. [COM.COM_JA] TELEFONÍA IP

- o [COM] Redes de comunicaciones
- o [COM.radio] red inalámbrica

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	Cisco Call Manager Express
MODELO	2801 de cisco
CANTIDAD	32

Descripción

Controla servicios a través de equipo IP y sus beneficios, Call Manager tripartita, transferencias, etc.

5.26. [COM.LAN_JA] RED LAN

- o [COM] Redes de comunicaciones
- o [COM.LAN] red local

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

INTERCONEXIÓN	Computadoras y periféricos
DISTANCIA	200 metros
CATEGORÍA	6

Descripción

Existen dos redes LAN, una para voz y una red para datos dentro de la Cooperativa.

5.27. [COM.WAN_JA] RED WWAN

- o [COM] Redes de comunicaciones
- o [COM.WAN] red de área amplia

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	Motorola
MODELO	PTP800, PTP400, PTP300, PTP100, 1300 Y 350 (cisco)
SISTEMA	Basado en microondas
DISTANCIA	100 A 1000 kilómetros
TOPOLOGÍA	Estrella

Descripción

Red tipo radio frecuencia en banda abierta 2.4 ghz hasta 5.8 ghz, en 5 provincias australes.

5.28. [COM.INTERNET_JA] INTERNET

- o [COM] Redes de comunicaciones
- o [COM.Internet] Internet
- o [COM.vpn] red privada virtual

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

TIPO	Inhalámbrico
MODELO	1 en 1 sin comprensión
CANTIDAD	1
ISP INTERNET SERVICE PROVIDE	Punto Net, CNT, Telconet

Descripción

Sirven para acceso transaccional y servicios de Transferencias de archivos con otras Instituciones Financieras (FTP- File Transfer Protocol).

5.29. [AUX.POWER_JA] FUENTES DE ALIMENTACIÓN

- o [AUX] Equipamiento auxiliar
- o [AUX.power] fuentes de alimentación

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	APC
TIPO	10 KVA
CANTIDAD	2 por equipo
SOBREMESA	200 a 250 w

Descripción

Es un sistema de UPS para Data Center que ayuda a su mejor funcionamiento.
Cada equipo tiene dos fuentes de alimentación como medida de contingencia.

5.30. [AUX.SAI_JA] SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

- o [AUX] Equipamiento auxiliar
- o [AUX.ups] sai - sistemas de alimentación ininterrumpida

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	APC
SERIE	GT
DISPOSITIVO	VFV voltaje y frecuencia independiente

Descripción

Es un dispositivo que gracias a sus baterías proporcionan energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.

5.31. [AUX.GEN_JA] GENERADOR ELÉCTRICO

- [AUX] Equipamiento auxiliar
- [AUX.gen] generadores eléctricos

Dominio de seguridad

- [base] COAC Jardín Azuayo

Datos

MARCA	Wilson
TIPO	150 KVA
CANTIDAD	1

Descripción

Este equipo es indispensable cuando la falta de energía es larga y se necesita provisión a las zonas críticas.

5.32. [AUX.EC_JA] EQUIPO DE CLIMATIZACIÓN

- [AUX] Equipamiento auxiliar
- [AUX.ac] equipos de climatización

Dominio de seguridad

- [base] COAC Jardín Azuayo

Datos

MARCA	Samsung, LG
TIPO	Data Center industrial

Descripción

Su objetivo es mantener el funcionamiento óptimo de los equipos y servidores.

5.33. [AUX.CABLING_JA] CABLEADO DE DATOS

- [AUX] Equipamiento auxiliar
- [AUX.cabling] cableado de datos
- [AUX.cabling.wire] cable eléctrico
- [AUX.cabling.fiber] fibra óptica

Dominio de seguridad

- [base] COAC Jardín Azuayo

Datos

MARCA	Panduit
CATEGORIA	6A

Descripción

El cableado de datos es fundamental para la transferencia de archivos y por ende para el funcionamiento de la Institución.

5.34. [AUX.ROBOTS_JA] ROBOTS

- o [AUX] Equipamiento auxiliar
- o [AUX.robot] robots
- o [AUX.robot.tape] ... de cintas

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

MARCA	IBM
DISCO	MARCA IMATION

Descripción

Es un tipo de medio o soporte de almacenamiento de datos que se graba en pistas cobre una banda plástica con un material magnetizado. El tipo de información que se puede almacenar en las cintas es variado.

5.35. [AUX.MOB_JA] MOBILIARIO

- o [AUX] Equipamiento auxiliar
- o [AUX.furniture] mobiliario

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

GABINETE	RACK
IBM	servidor
TECKDATA	red

5.36. [AUX.CF_JA] CAJA FUERTE

- o [AUX] Equipamiento auxiliar
- o [AUX.safe] cajas fuertes

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

CARACTERISTICAS	INDUSTRIALES Y TEMPORIZADOS
MATERIAL	acero templado y hormigón
PESO	más de 100 kilogramos de peso

Descripción

Es un compartimiento de seguridad que ha sido implementado para que su apertura sea muy difícil para personas no autorizadas y así poder guardar elementos de valor.

5.37. [AUX.OTHER_JA] OTROS EQUIPAMIENTOS AUXILIARES

- o [AUX] Equipamiento auxiliar
- o [AUX.other] otros ...

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

EQUIPO	Biometría
EQUIPO	Acceso temporizado
EQUIPO	Detector de incendios
EQUIPO	Extintor de incendios
EQUIPO	Cámaras de vigilancia

Descripción

Los equipamientos fundamentales con los que cuenta la Institución están mencionados anteriormente.

5.38. [SS.01_JA] IRNET

- o [S] Servicios
- o [S.pub] al público en general (sin relación contractual)
- o [S.www] world wide web

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

ENLACE	Web
SERVICIO	Pago de Remesas
INGRESO AL SISTEMA	Vía web mediante clave

Descripción

La Red Internacional de Remesas del Consejo Mundial de Cooperativas de Ahorro y Crédito (IRnet®) es una plataforma para que las cooperativas de ahorro y crédito ofrezcan a sus socios y socios potenciales en todo el mundo acceso a transferencias de fondos nacionales e internacionales seguras y accesibles (remesas).

La red se creó en respuesta a una mayor demanda de dinero y servicios de transferencias y para combatir las comisiones exorbitantes que se cobran por utilizar dichos servicios.

5.39. [SS.02_JA] COOPSEGUROS

- o [S] Servicios
- o [S.pub] al público en general (sin relación contractual)

o [S.www] world wide web

Dominio de seguridad

o [base] COAC Jardín Azuayo

Datos

SERVICIO	SOAT
INGRESO AL SISTEMA	Vía web usando claves de acceso para ingresar a la pantalla de cobros

Descripción

Es una empresa dedicada a la venta de seguros de vehículos SOAT (Seguro Obligatorio de Accidentes de Tránsito).

5.40. [SS.03_JA] RED COONECTA

o [S] Servicios
o [S.ext] a usuarios externos (bajo una relación contractual)
o [S.int] interno (usuarios y medios de la propia organización)

Dominio de seguridad

o [base] COAC Jardín Azuayo

Datos

SERVICIO	Se usa para interconectar los cajeros de la Institución a la Red de COONECTA y a su vez con los cajeros de BanRed

Descripción

Es una Red que interconecta a todas las cooperativas del país y brinda servicios de conexión con otras cooperativas y BanRed es especial para cajeros automáticos.

5.41. [SS.04_JA] VENTANILLA COMPARTIDA

o [S] Servicios
o [S.int] interno (usuarios y medios de la propia organización)

Dominio de seguridad

o [base] COAC Jardín Azuayo

Datos

SERVICIO	A través de la Red COONECTA, se puede realizar los depósitos y retiros en más de 17 Cooperativas en todo el país

Descripción

La ventanilla compartida es un servicio que se coordina con la Red COONECTA para enlazarse con las diferentes cooperativas para el pago.

5.42. [L_JA] UNIDAD DE SISTEMAS, REDES Y TELECOMUNICACIONES

o [L] Instalaciones
o [L.site] emplazamiento

o [L.local] local

Dominio de seguridad

o [base] COAC Jardín Azuayo

Datos

TIPO	Casa con adecuaciones
DIRECCION	Sucre 5-42 Benigno Malo 9-75
TELEFONO	2849-718

Descripción

En esta infraestructura se realiza planificación, desarrollo y soporte de servicios informáticos.

5.43. [DBA_JA] ADMINISTRACIÓN DE BASE DE DATOS (PRODUCCIÓN-PRUEBAS)

o [P] Personal
o [P.dba] administradores de BBDD

Dominio de seguridad

o [base] COAC Jardín Azuayo

Datos

RESPONSABLE	Ing. Víctor Astudillo
RESPONSABLE	Ing. Jorge Bonete

Descripción

Son los encargados de la producción y realizar las pruebas necesarias en la Base de Datos.

5.44. [ITL_JA] INFRAESTRUCTURA Y TELECOMUNICACIONES

o [P] Personal
o [P.com] administradores de comunicaciones
o [P.other] otros ...

Dominio de seguridad

o [base] COAC Jardín Azuayo

Datos

RESPONSABLE	Ing. José David Ávila
RESPONSABLE	Ing. Edison Tirado
RESPONSABLE	Ing. Marcos Real
RESPONSABLE	Ing. Javier Crespo
RESPONSABLE	Magister Santiago Vásquez

Descripción

Son los encargados de los servidores de aplicaciones y la red de telecomunicaciones.

5.45. [DES_JA] DESARROLLADORES / PROGRAMADORES

- o [P] Personal
- o [P.des] desarrolladores / programadores

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

RESPONSABLE	Ing. María Eugenia Montero
RESPONSABLE	Ing. Vanessa Morales
RESPONSABLE	Ing. Omar Vélez
RESPONSABLE	Ing. Paúl Zhañay

Descripción

Son los encargados en desarrollar las interfaces de usuario con el código correspondiente de los aplicativos.

5.46. [ISOFT_JA] INGENIERÍA DE SOFTWARE

- o [P] Personal
- o [P.other] otros ...

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

RESPONSABLE	Ing. Marco Paredes
RESPONSABLE	Ing. Santiago Araujo
RESPONSABLE	Ing. Romel Cando
RESPONSABLE	Ing. Verónica Vélez

Descripción

Son los encargados del diseño de aplicaciones, previo al análisis de los requerimientos.

5.47. [UI_JA] SOPORTE A USUARIOS

- o [P] Personal
- o [P.ui] usuarios internos

Dominio de seguridad

- o [base] COAC Jardín Azuayo

Datos

RESPONSABLE	Ing. Andrea Tenezaca
RESPONSABLE	Ing. Fabian Chuquimarca
RESPONSABLE	Ing. Fabricio Barreto

Descripción

Se encargan de brindar soporte de primer nivel y re direccionar las unidades del departamento a quien corresponda un requerimiento.

ANEXO 3

VULNERABILIADAD DE LOS DOMINIOS

Vulnerabilidad.- los activos, por su propia naturaleza, se ven influidos por una serie de amenazas. La probabilidad de que se materialice una de dichas amenazas y la degradación que le supone a un activo es lo que se conoce como vulnerabilidad.

PILAR Basic ha sustituido, los valores de probabilidad y degradación por una serie de criterios que permiten reflejar el entorno en el que se encuentran los activos.

En la Gestión de Vulnerabilidades descritas posteriormente, se podrá definir qué criterios pueden influir sobre un dominio (y por lo tanto sobre todos los activos que se encuentran en dicho dominio)

Responsable de la encuesta:
……

(Subrayar los criterios pertinentes)

[101] Identificación del atacante – quienes son los atacantes a los activos
- [101.a] público en general
- [101.b] competidor comercial
- [101.c] proveedor de servicios
- [101.d] grupos de presión política / activistas / extremistas
- [101.e] periodistas
- [101.f] criminales / terroristas
- [101.g] personal interno
- [101.h] bandas criminales
- [101.i] grupos terroristas
- [101.j] servicios de inteligencia

[102] Motivación del atacante
- [102.a] económica (beneficios en dinero)
- [102.b] beneficios comerciales
- [102.c] personal propio con problemas de conciencia
- [102.d] personal propio con conflictos de interés
- [102.e] personal propio con pertenencia a un grupo extremista
- [102.f] con ánimo destructivo
- [102.g] con ánimo de causar daño
- [102.h] con ánimo de provocar pérdidas

[103] Beneficio del atacante
- [103.a] moderadamente interesado
- [103.b] muy interesado
- [103.c] extremadamente interesado

[104] Motivación del personal interno

[104.a] todo el personal está fuertemente motivado
[104.b] baja calificación profesional / escasa información
[104.c] sobrecargos de trabajo
[104.d] con problemas de conciencia
[104.e] con conflictos de intereses
[104.f] personal asociado a grupos extremistas

[105] Permisos de los usuarios (derechos)
[105.a] se permite el acceso a internet
[105.b] se permite la ejecución de programas sin autorización previa
[105.c] se permite la instalación de programas sin autorización previa
[105.d] se permite la conexión de dispositivos móviles

[111] Conectividad del sistema de información
[111.a] sistema aislado
[111.b] conectado a un conjunto reducido y controlado de redes
[111.c] conectado a un amplio colectivo de redes conocidas
[111.d] conectado a internet

[112] Ubicación del sistema de información
[112.a] dentro de una zona segura (“en casa”)
[112.b] en un área de acceso abierto
[112.c] en un entorno hostil

ANEXO 4
VALORACIÓN DE DOMINIOS

Se desarrollará con supuestos, de acuerdo a las Dimensiones de Valoración: (D) Disponibilidad, (I) Integridad, (C) Confidencialidad, (A) Autenticidad y (T) Trazabilidad de la información y los servicios que la institución presta con dicha información.

Aquí se valorará sobre la Base de los Dominios, cuya base abarca todos los activos del Sistema de Información de la Cooperativa.

Criterios de valoración: ALTO, MEDIO, BAJO Y DESPRECIABLE (se escogerá un criterio para cada dimensión de valoración)

Responsable de la Encuesta: …….
(Encerrar en un círculo la opción que usted elija conveniente)

DISPONIBILIDAD

Es el aseguramiento de que los usuarios autorizados tienen acceso cuando lo requiera a la información y sus activos asociados.

Indicar la repercusión que tendría en la Institución el hecho de que se dejara de prestar el servicio.

[A] ALTO

[crm] Impida la investigación de delitos graves o facilite su comisión
[da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
[adm] Administración y gestión: probablemente impediría la operación efectiva de la Organización
[lg] Probablemente causaría una publicidad negativa generalizada
[a] por afectar gravemente a las relaciones con otras organizaciones
[b] por afectar gravemente a las relaciones con el público en general
[cei] Intereses comerciales o económicos:
[a] de alto interés para la competencia
[b] de elevado valor comercial
[c] causa de graves pérdidas económicas
[d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones
[e] constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
[lro] Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
[pi1] Información personal: probablemente afecte gravemente a un grupo de individuos
[pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[si] Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[lbl] Información clasificada: confidencial

[ue] CONFIDENTIEL UE

[M] MEDIO

[da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
[adm] Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la Organización
[lg] Probablemente sea causa una cierta publicidad negativa
[a] por afectar negativamente a las relaciones con otras organizaciones
[b] por afectar negativamente a las relaciones con el público
[lro] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación
[cei] Intereses comerciales o económicos:
[a] de cierto interés para la competencia
[b] de cierto valor comercial
[c] causa de pérdidas financieras o mermas de ingresos
[d] facilita ventajas desproporcionadas a individuos u organizaciones
[e] constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
[pi1] Información personal: probablemente afecte a un grupo de individuos
[pi1] Información personal: probablemente afecte gravemente a un individuo
[pi2] Información personal: probablemente quebrante leyes o regulaciones
[si] Seguridad: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
[crm] Dificulte la investigación o facilite la comisión de delitos
[lbl] Información clasificada: difusión limitada
[ue] RESTREINT UE

[B] BAJO

[da] Probablemente cause la interrupción de actividades propias de la Organización
[adm] Administración y gestión: probablemente impediría la operación efectiva de una parte de la Organización
[lg] Probablemente afecte negativamente a las relaciones internas de la Organización
[cei] Intereses comerciales o económicos:
[a] de bajo interés para la competencia
[b] de bajo valor comercial
[pi1] Información personal: probablemente afecte a un individuo
[pi2] Información personal: pudiera quebrantar de forma leve leyes o regulaciones
[lro] Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
[si] Seguridad: pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[lbl] Información clasificada: sin clasificar

[D] DESPRECIABLE

[2] sería causa de inconveniencias mínimas a las partes afectadas
[3] supondría pérdidas económicas mínimas
[4] no supondría daño a la reputación o buena imagen de las personas u organizaciones

INTEGRIDAD

Es la garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

Indicar la repercusión que tendría en la Institución el hecho de que la información que se maneja para prestar el servicio fuera incorrecta o incompleta.

[A] ALTO

[crm] Impida la investigación de delitos graves o facilite su comisión
[da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
[adm] Administración y gestión: probablemente impediría la operación efectiva de la Organización
[lg] Probablemente causaría una publicidad negativa generalizada
[a] por afectar gravemente a las relaciones con otras organizaciones
[b] por afectar gravemente a las relaciones con el público en general
[cei] Intereses comerciales o económicos:
[a] de alto interés para la competencia
[b] de elevado valor comercial
[c] causa de graves pérdidas económicas
[d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones
[e] constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
[lro] Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
[pi1] Información personal: probablemente afecte gravemente a un grupo de individuos
[pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[si] Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[lbl] Información clasificada: confidencial
[ue] CONFIDENTIEL UE

[M] MEDIO

[da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
[adm] Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la Organización
[lg] Probablemente sea causa una cierta publicidad negativa
[a] por afectar negativamente a las relaciones con otras organizaciones
[b] por afectar negativamente a las relaciones con el público

[lro] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación
[cei] Intereses comerciales o económicos:
[a] de cierto interés para la competencia
[b] de cierto valor comercial
[c] causa de pérdidas financieras o mermas de ingresos
[d] facilita ventajas desproporcionadas a individuos u organizaciones
[e] constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
[pi1] Información personal: probablemente afecte a un grupo de individuos
[pi1] Información personal: probablemente afecte gravemente a un individuo
[pi2] Información personal: probablemente quebrante leyes o regulaciones
[si] Seguridad: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
[crm] Dificulte la investigación o facilite la comisión de delitos
[lbl] Información clasificada: difusión limitada
[ue] RESTREINT UE

[B] BAJO

[da] Probablemente cause la interrupción de actividades propias de la Organización
[adm] Administración y gestión: probablemente impediría la operación efectiva de una parte de la Organización
[lg] Probablemente afecte negativamente a las relaciones internas de la Organización
[cei] Intereses comerciales o económicos:
[a] de bajo interés para la competencia
[b] de bajo valor comercial
[pi1] Información personal: probablemente afecte a un individuo
[pi2] Información personal: pudiera quebrantar de forma leve leyes o regulaciones
[lro] Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
[si] Seguridad: pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[lbl] Información clasificada: sin clasificar

[D] DESPRECIABLE

[2] sería causa de inconveniencias mínimas a las partes afectadas
[3] supondría pérdidas económicas mínimas
[4] no supondría daño a la reputación o buena imagen de las personas u organizaciones

CONFIDENCIALIDAD

Es el aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

Indicar la repercusión que tendría en la Institución el hecho de que la información que se maneja para prestar el servicio fuera accedida por personas no autorizadas.

[A] ALTO

[crm] Impida la investigación de delitos graves o facilite su comisión
[da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
[adm] Administración y gestión: probablemente impediría la operación efectiva de la Organización
[lg] Probablemente causaría una publicidad negativa generalizada
[a] por afectar gravemente a las relaciones con otras organizaciones
[b] por afectar gravemente a las relaciones con el público en general
[cei] Intereses comerciales o económicos:
[a] de alto interés para la competencia
[b] de elevado valor comercial
[c] causa de graves pérdidas económicas
[d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones
[e] constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
[lro] Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
[pi1] Información personal: probablemente afecte gravemente a un grupo de individuos
[pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[si] Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[lbl] Información clasificada: confidencial
[ue] CONFIDENTIEL UE

[M] MEDIO

[da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
[adm] Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la Organización
[lg] Probablemente sea causa una cierta publicidad negativa
[a] por afectar negativamente a las relaciones con otras organizaciones
[b] por afectar negativamente a las relaciones con el público
[lro] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación
[cei] Intereses comerciales o económicos:
[a] de cierto interés para la competencia
[b] de cierto valor comercial

[c] causa de pérdidas financieras o mermas de ingresos
[d] facilita ventajas desproporcionadas a individuos u organizaciones
[e] constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
[pi1] Información personal: probablemente afecte a un grupo de individuos
[pi1] Información personal: probablemente afecte gravemente a un individuo
[pi2] Información personal: probablemente quebrante leyes o regulaciones
[si] Seguridad: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
[crm] Dificulte la investigación o facilite la comisión de delitos
[lbl] Información clasificada: difusión limitada
[ue] RESTREINT UE

[B] BAJO

[da] Probablemente cause la interrupción de actividades propias de la Organización
[adm] Administración y gestión: probablemente impediría la operación efectiva de una parte de la Organización
[lg] Probablemente afecte negativamente a las relaciones internas de la Organización
[cei] Intereses comerciales o económicos:
[a] de bajo interés para la competencia
[b] de bajo valor comercial
[pi1] Información personal: probablemente afecte a un individuo
[pi2] Información personal: pudiera quebrantar de forma leve leyes o regulaciones
[lro] Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
[si] Seguridad: pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[lbl] Información clasificada: sin clasificar

[D] DESPRECIABLE

[2] sería causa de inconveniencias mínimas a las partes afectadas
[3] supondría pérdidas económicas mínimas
[4] no supondría daño a la reputación o buena imagen de las personas u organizaciones

AUTENTICIDAD

Es el aseguramiento dela identidad u origen.

Indicar la repercusión que tendría en la Institución el hecho de que no se pudiera confirmar la identidad de quien accedió al servicio o a la información.

[A] ALTO

[crm] Impida la investigación de delitos graves o facilite su comisión
[da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
[adm] Administración y gestión: probablemente impediría la operación efectiva de la Organización
[lg] Probablemente causaría una publicidad negativa generalizada
[a] por afectar gravemente a las relaciones con otras organizaciones
[b] por afectar gravemente a las relaciones con el público en general
[cei] Intereses comerciales o económicos:
[a] de alto interés para la competencia
[b] de elevado valor comercial
[c] causa de graves pérdidas económicas
[d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones
[e] constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
[lro] Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
[pi1] Información personal: probablemente afecte gravemente a un grupo de individuos
[pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[si] Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[lbl] Información clasificada: confidencial
[ue] CONFIDENTIEL UE

[M] MEDIO

[da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
[adm] Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la Organización
[lg] Probablemente sea causa una cierta publicidad negativa
[a] por afectar negativamente a las relaciones con otras organizaciones
[b] por afectar negativamente a las relaciones con el público
[lro] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación
[cei] Intereses comerciales o económicos:
[a] de cierto interés para la competencia
[b] de cierto valor comercial
[c] causa de pérdidas financieras o mermas de ingresos

[d] facilita ventajas desproporcionadas a individuos u organizaciones
[e] constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
[pi1] Información personal: probablemente afecte a un grupo de individuos
[pi1] Información personal: probablemente afecte gravemente a un individuo
[pi2] Información personal: probablemente quebrante leyes o regulaciones
[si] Seguridad: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
[crm] Dificulte la investigación o facilite la comisión de delitos
[lbl] Información clasificada: difusión limitada
[ue] RESTREINT UE

[B] BAJO

[da] Probablemente cause la interrupción de actividades propias de la Organización
[adm] Administración y gestión: probablemente impediría la operación efectiva de una parte de la Organización
[lg] Probablemente afecte negativamente a las relaciones internas de la Organización
[cei] Intereses comerciales o económicos:
[a] de bajo interés para la competencia
[b] de bajo valor comercial
[pi1] Información personal: probablemente afecte a un individuo
[pi2] Información personal: pudiera quebrantar de forma leve leyes o regulaciones
[lro] Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
[si] Seguridad: pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[lbl] Información clasificada: sin clasificar

[D] DESPRECIABLE

[2] sería causa de inconveniencias mínimas a las partes afectadas
[3] supondría pérdidas económicas mínimas
[4] no supondría daño a la reputación o buena imagen de las personas u organizaciones

TRAZABILIDAD

Es el aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

Indicar la repercusión que tendría en la Institución el hecho de que no se pudiera conocer a quién se le presta un servicio o a qué información y cuándo accedió un usuario.

[A] ALTO

[crm] Impida la investigación de delitos graves o facilite su comisión
[da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
[adm] Administración y gestión: probablemente impediría la operación efectiva de la Organización
[lg] Probablemente causaría una publicidad negativa generalizada
[a] por afectar gravemente a las relaciones con otras organizaciones
[b] por afectar gravemente a las relaciones con el público en general
[cei] Intereses comerciales o económicos:
[a] de alto interés para la competencia
[b] de elevado valor comercial
[c] causa de graves pérdidas económicas
[d] proporciona ganancias o ventajas desmedidas a individuos u organizaciones
[e] constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
[lro] Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación
[pi1] Información personal: probablemente afecte gravemente a un grupo de individuos
[pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
[si] Seguridad: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
[lbl] Información clasificada: confidencial
[ue] CONFIDENTIEL UE

[M] MEDIO

[da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
[adm] Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la Organización
[lg] Probablemente sea causa una cierta publicidad negativa
[a] por afectar negativamente a las relaciones con otras organizaciones
[b] por afectar negativamente a las relaciones con el público
[lro] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación
[cei] Intereses comerciales o económicos:
[a] de cierto interés para la competencia

[b] de cierto valor comercial
[c] causa de pérdidas financieras o mermas de ingresos
[d] facilita ventajas desproporcionadas a individuos u organizaciones
[e] constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
[pi1] Información personal: probablemente afecte a un grupo de individuos
[pi1] Información personal: probablemente afecte gravemente a un individuo
[pi2] Información personal: probablemente quebrante leyes o regulaciones
[si] Seguridad: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
[crm] Dificulte la investigación o facilite la comisión de delitos
[lbl] Información clasificada: difusión limitada
[ue] RESTREINT UE

[B] BAJO

[da] Probablemente cause la interrupción de actividades propias de la Organización
[adm] Administración y gestión: probablemente impediría la operación efectiva de una parte de la Organización
[lg] Probablemente afecte negativamente a las relaciones internas de la Organización
[cei] Intereses comerciales o económicos:
[a] de bajo interés para la competencia
[b] de bajo valor comercial
[pi1] Información personal: probablemente afecte a un individuo
[pi2] Información personal: pudiera quebrantar de forma leve leyes o regulaciones
[lro] Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
[si] Seguridad: pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[lbl] Información clasificada: sin clasificar

[D] DESPRECIABLE

[2] sería causa de inconveniencias mínimas a las partes afectadas
[3] supondría pérdidas económicas mínimas
[4] no supondría daño a la reputación o buena imagen de las personas u organizaciones

ANEXO 5

CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN [27002:2005]

proyecto: [AR_JA] ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO JARDIN AZUAYO

1. Datos del proyecto

AR_JA	ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO JARDIN AZUAYO
Descripción	Análisis a los Sistemas de Información
Dirección	Sucre 5-42 entre Hermano Miguel y Mariano Cueva Benigno Malo 9-75 y Gran Colombia
Teléfonos	2840 259
Responsable	Sr. Antonio José Lucero Gómez y Sr. John Oswaldo Valverde Padilla
Organización	COOPERATIVA DE AHORRO Y CRÉDITO JARDÍN AZUAYO
Lugar del examen	Coordinación y Cuenca
Versión	1
Fecha	21-11-2011
biblioteca	[std] Biblioteca INFOSEC (22.1.2009)

Descripción

El presente trabajo es realizado en la Cooperativa de Ahorro y Crédito Jardín Azuayo en la oficia Cuenca y su Coordinación, la Institución está controlada por la Superintendencia de Bancos y Seguros

Licencia

[edu] Universidad de Cuenca
Cuenca - Ecuador
[... 1.1.2013]

2. Dominios de seguridad

o [base] COAC Jardín Azuayo

3. Fases del proyecto

o [current] situación actual
o [target] situación objetivo

4. Dominio de seguridad: [base] COAC Jardín Azuayo

4.1. [5] Política de seguridad

control	[current]	[target]
[5] Política de seguridad	82%	99%
[5.1] Política de seguridad de la información	82%	99%
[5.1.1] Documento de política de seguridad de la información	70%	98%
[5.1.2] Revisión de la política de seguridad de la información	93%	100%

4.2. [6] Aspectos organizativos de la seguridad de la información

control	[current]	[target]
[6] Aspectos organizativos de la seguridad de la información	42%	83%
[6.1] Organización interna	48%	87%
[6.1.1] Comité de gestión de la seguridad de la información	10%	90%
[6.1.2] Coordinación para la seguridad de la información	50%	95%
[6.1.3] Asignación de responsabilidades relativas a la seguridad de la información	0%	50%
[6.1.4] Proceso de autorización de recursos para el tratamiento de la información	95%	100%
[6.1.5] Acuerdos de confidencialidad	25%	70%
[6.1.6] Contacto con las autoridades	95%	100%
[6.1.7] Contacto con grupos de interés específicos	78%	100%
[6.1.8] Revisión independiente de la seguridad de la información	30%	95%
[6.2] Relaciones con terceros	36%	79%
[6.2.1] Identificación de riesgos derivados del acceso de terceros	50%	95%
[6.2.2] Tratamiento de la seguridad en las relaciones con clientes	5%	47%
[6.2.3] Tratamiento de la seguridad en contratos con terceros	53%	95%

4.3. [7] Gestión de activos

control	[current]	[target]
[7] Gestión de activos	33%	93%
[7.1] Responsabilidad sobre los activos	61%	96%
[7.1.1] Inventario de activos	60%	96%
[7.1.2] Propiedad de los activos	73%	97%
[7.1.3] Condiciones de uso de los activos	49%	96%
[7.2] Clasificación de la información	5%	90%
[7.2.1] Directrices de clasificación	0%	90%
[7.2.2] Etiquetado y tratamiento de la información	10%	90%

4.4. [8] Seguridad relacionada con los recursos humanos

control	[current]	[target]
[8] Seguridad relacionada con los recursos humanos	29%	86%
[8.1] Previa a la contratación	9%	78%
[8.1.1] Funciones y responsabilidades	28%	94%
[8.1.2] Investigación de antecedentes	0%	90%
[8.1.3] Términos y condiciones laborales	0%	50%
[8.2] Mientras dure la contratación	7%	83%
[8.2.1] Responsabilidades de la Dirección	0%	70%
[8.2.2] Concienciación, formación y capacitación en seguridad de la información	10%	90%
[8.2.3] Medidas disciplinarias	10%	90%
[8.3] Fin de la contratación o cambio de puesto de trabajo	71%	98%

[8.3.1] Responsabilidad del cese o cambio	70%	100%
[8.3.2] Devolución de activos	50%	95%
[8.3.3] Cancelación de los derechos de acceso	92%	98%

4.5. [9] Seguridad física y del entorno

control	[current]	[target]
[9] Seguridad física y del entorno	25%	83%
[9.1] Áreas seguras	30%	82%
[9.1.1] Perímetro de seguridad física	33%	90%
[9.1.2] Controles físicos de entrada	0%	50%
[9.1.3] Aseguramiento de oficinas, salas e instalaciones	63%	95%
[9.1.4] Protección frente a amenazas externas	25%	70%
[9.1.5] Reglamentación del trabajo en áreas seguras	33%	93%
[9.1.6] Áreas abiertas al público, zonas de entrega, carga y descarga	25%	92%
[9.2] Seguridad del equipamiento	20%	85%
[9.2.1] Ubicación y protección de los equipos	26%	87%
[9.2.2] Suministros	3%	77%
[9.2.3] Seguridad del cableado	0%	50%
[9.2.4] Mantenimiento de equipos	50%	95%
[9.2.5] Seguridad de los equipos fuera de las instalaciones	0%	95%
[9.2.6] Retirada o reutilización de equipos (pasan a otras manos)	50%	95%
[9.2.7] Activos que salen de las instalaciones (removal of property)	10%	95%

4.6. [10] Gestión de comunicaciones y operaciones

control	[current]	[target]
[10] Gestión de comunicaciones y operaciones	35%	95%
[10.1] Responsabilidades y procedimientos de operación	63%	98%
[10.1.1] Documentación de los procedimientos de operación	90%	95%
[10.1.2] Gestión de cambios	23%	98%
[10.1.3] Segregación de tareas	90%	100%
[10.1.4] Separación de los recursos de desarrollo, prueba y operación	50%	98%
[10.2] Gestión de servicios prestados por terceros	18%	94%
[10.2.1] Prestación de los servicios	0%	90%
[10.2.2] Supervisión y revisión de los servicios	45%	92%
[10.2.3] Gestión de cambios en los servicios	10%	100%
[10.3] Planificación y aceptación de sistemas	46%	96%
[10.3.1] Gestión de capacidades	50%	95%
[10.3.2] Aceptación de nuevos sistemas	42%	96%
[10.4] Protección frente a código dañino y código descargable	100%	100%
[10.4.1] Protección frente a código dañino	100%	100%
[10.4.2] Protección frente a código descargado (ej.	n.a.	n.a.

applets)		
[10.5] Copias de seguridad	3%	95%
[10.5.1] Copias de seguridad	3%	95%
[10.6] Gestión de la seguridad de las redes	20%	93%
[10.6.1] Controles de red	30%	95%
[10.6.2] Seguridad de los servicios de red	10%	92%
[10.7] Tratamiento de soportes de información	10%	90%
[10.7.1] Gestión de soportes	n.a.	n.a.
[10.7.2] Retirada de soportes	n.a.	n.a.
[10.7.3] Procedimientos de tratamiento de la información	n.a.	n.a.
[10.7.4] Seguridad de la documentación del sistema	10%	90%
[10.8] Intercambios de información	28%	94%
[10.8.1] Normas y procedimientos	3%	97%
[10.8.2] Acuerdos de intercambio	10%	90%
[10.8.3] Soportes físicos en tránsito	n.a.	n.a.
[10.8.4] Mensajería electrónica	10%	90%
[10.8.5] Interconexión de sistemas de información	90%	100%
[10.9] Servicios de comercio electrónico	9%	96%
[10.9.1] Comercio electrónico	10%	95%
[10.9.2] Transacciones en línea	7%	93%
[10.9.3] Información puesta a disposición pública	10%	100%
[10.10] Supervisión	54%	97%
[10.10.1] Pistas de auditoría	90%	95%
[10.10.2] Supervisión del uso de los sistemas	0%	95%
[10.10.3] Protección de registros (logs)	90%	100%
[10.10.4] Registros de administración y operación	47%	95%
[10.10.5] Registro de fallos	95%	100%
[10.10.6] Sincronización de relojes	0%	95%

4.7. [11] Control de acceso

control	[current]	[target]
[11] Control de acceso	51%	96%
[11.1] Requisitos del control de acceso	78%	99%
[11.1.1] Política de control de acceso	78%	99%
[11.2] Gestión de usuarios	54%	98%
[11.2.1] Registro de usuarios	76%	100%
[11.2.2] Gestión de privilegios	0%	95%
[11.2.3] Gestión de contraseñas	50%	98%
[11.2.4] Revisión de derechos de acceso	90%	100%
[11.3] Responsabiliades de los usuarios	59%	97%
[11.3.1] Uso de contraseñas	87%	100%
[11.3.2] Equipo desatendido	0%	95%
[11.3.3] Puesto de trabajo limpio y pantalla en blanco	90%	95%
[11.4] Control de acceso a la red	26%	97%
[11.4.1] Política de uso de los servicios de red	50%	95%
[11.4.2] Autenticación de usuarios en acceso remoto	10%	95%
[11.4.3] Identificación de equipos en la red	84%	99%

[11.4.4] Puertas de diagnóstico y configuración remota	10%	100%
[11.4.5] Segregación de redes	10%	100%
[11.4.6] Control de conexión a la red	10%	95%
[11.4.7] Control de encaminamiento	10%	95%
[11.5] Control del acceso a sistemas en operación	64%	91%
[11.5.1] Procedimientos de inicio de sesión (log-on)	0%	50%
[11.5.2] Identificación y autorización de usuarios	57%	100%
[11.5.3] Gestión de contraseñas	94%	100%
[11.5.4] Uso de los recursos del sistema	50%	95%
[11.5.5] Desconexión automática de la sesión	95%	100%
[11.5.6] Limitación del tiempo de conexión	90%	100%
[11.6] Control de acceso a datos y aplicaciones	44%	94%
[11.6.1] Restricción del acceso a la información	84%	99%
[11.6.2] Aislamiento de sistemas críticos	5%	90%
[11.7] Equipos móviles y tele-trabajo	30%	95%
[11.7.1] Equipos móviles	50%	95%
[11.7.2] Teletrabajo	10%	95%

4.8. [12] Adquisición, desarrollo y mantenimiento de los sistemas de información

control	[current]	[target]
[12] Adquisición, desarrollo y mantenimiento de los sistemas de información	39%	97%
[12.1] Requisitos de seguridad	68%	96%
[12.1.1] Análisis y especificación de requisitos	68%	96%
[12.2] Garantías de procesamiento de información	38%	95%
[12.2.1] Validación de datos de entrada	0%	95%
[12.2.2] Control de tratamiento interno	10%	95%
[12.2.3] Integridad de los mensajes	90%	100%
[12.2.4] Validación de los datos de salida	50%	90%
[12.3] Controles criptográficos	27%	97%
[12.3.1] Política de uso	28%	96%
[12.3.2] Gestión de claves	26%	98%
[12.4] Seguridad de los archivos del sistema	30%	97%
[12.4.1] Control de programas en producción	0%	100%
[12.4.2] Protección de los datos de prueba	90%	100%
[12.4.3] Control de acceso al código fuente	0%	90%
[12.5] Seguridad en los procesos de desarrollo y soporte	31%	98%
[12.5.1] Procedimientos de control de cambios	50%	100%
[12.5.2] Revisión técnica de las aplicaciones tras cambios del S.O.	50%	100%
[12.5.3] Restricciones a los cambios de aplicaciones en producción	10%	100%
[12.5.4] Fugas de información	45%	100%
[12.5.5] Desarrollo externalizado (outsourcing)	0%	90%
[12.6] Gestión de vulnerabilidades	43%	98%
[12.6.1] Control de vulnerabilidades técnicas	43%	98%

4.9. [13] Gestión de incidentes de seguridad de información

control	[current]	[target]
[13] Gestión de incidentes de seguridad de información	61%	96%
[13.1] Comunicación de incidencias y debilidades	50%	94%
[13.1.1] Comunicación de incidencias	50%	95%
[13.1.2] Comunicación de debilidades	50%	92%
[13.2] Gestión de incidentes y mejoras	73%	98%
[13.2.1] Responsabilidades y procedimientos	78%	98%
[13.2.2] Aprendiendo del pasado	95%	100%
[13.2.3] Recopilación de evidencias	45%	96%

4.10. [14] Gestión de la continuidad del negocio

control	[current]	[target]
[14] Gestión de la continuidad del negocio	67%	97%
[14.1] Seguridad de la información en relación a la gestión de la continuidad	67%	97%
[14.1.1] Inclusión de la seguridad de la información en los planes de continuidad	70%	98%
[14.1.2] Continuidad y evaluación de riesgos	50%	97%
[14.1.3] Desarrollo e implantación de planes de continuidad incluyendo la seguridad de la información	93%	100%
[14.1.4] Marco de planificación de la continuidad	74%	96%
[14.1.5] Prueba, mantenimiento y re-evaluación de los planes de continuidad	50%	95%

4.11. [15] Cumplimiento

control	[current]	[target]
[15] Cumplimiento	73%	98%
[15.1] Satisfacción de requisitos legales	53%	97%
[15.1.1] Identificación de legislación aplicable	47%	95%
[15.1.2] Derechos de propiedad intelectual (IPR)	63%	97%
[15.1.3] Protección de los documentos de la organización	50%	95%
[15.1.4] Protección de datos e información de carácter personal	56%	97%
[15.1.5] Prevención frente al mal uso de los medios de tratamiento de la información	75%	98%
[15.1.6] Regulación de controles criptográficos	29%	99%
[15.2] Cumplimiento de políticas, normas y reglamentos técnicos	90%	99%
[15.2.1] Cumplimiento de políticas y normas	90%	100%
[15.2.2] Verificación del cumplimiento técnico	90%	98%
[15.3] Consideraciones sobre auditoría de los sistemas de información	75%	98%
[15.3.1] Controles de auditoría	50%	95%
[15.3.2] Protección de las herramientas de auditoría	100%	100%

GLOSARIO

- **Abuso de privilegios de acceso.-** Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.[33]

- **Acceso no autorizado.-** El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. [34]

- **Acreditación.-** Acción de facultar a un sistema o red de información para que procese datos sensibles, determinando el grado en el que el diseño y la materialización de dicho sistema cumple los requerimientos de seguridad técnica preestablecidos.[35]

- **Activo.-** Recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y a alcance los objetivos propuestos por su dirección.[36]

- **Alteración de la información.-** Es la alteración accidental de la información.[37]

- **Amenaza.-** Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.[38]

- **Análisis.-** La acción y el efecto de separar un todo en los elementos que lo componen con el objeto de estudiar su naturaleza, función o significado.[39]

---

[33] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.36

[34] Ibíd., p.37

[35] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.102

[36] Ibíd.

[37] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.33

[38] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.102

[39] http://es.wiktionary.org/wiki/an%C3%A1lisis

- **Análisis de Riesgos.-** Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.[40]
- **Análisis de tráfico.-** El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.[41]

- **Ataque.-** Cualquier acción deliberada encaminada a violar los mecanismos de seguridad de un sistema de información.[42]

- **Ataque destructivo.-** Puede ser vandalismo, terrorismo o acción militar que puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.[43]

- **Auditoría.-** Inspección formal para verificar si un Estándar o un conjunto de Guías se está siguiendo, que sus Registros son precisos, o que las metas de Eficiencia y Efectividad se están cumpliendo. Una Auditoría la puede realizar tanto un grupo interno como uno externo.[44]

- **Autenticidad.-** Aseguramiento de la identidad u origen.[45]

- **Avería de origen físico o lógico.-** Son los fallos en los equipos y/o fallos en los programas. Puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema.[46]

[40] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.103
[41] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.37
[42] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.104
[43] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.40
[44] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-Glosario_y_abreviaturas/401/index.html
[45] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p. 104
[46] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.29

- **Biometría.-** Dispositivo que utiliza parámetros biológicos característicos de las personas como la huella dactilar, el iris del ojo o la voz para la autenticación.[47]
- **Caída del sistema por agotamiento físico de recursos.-** La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.[48]

- **Capa.-** Sirve para agrupar un conjunto de activos, con el objetivo de facilitar el trabajo con los mismos, por lo que no tiene ninguna repercusión en el análisis de riesgos.[49]

- **Certificación.-** Confirmación del resultado de una evaluación, y que los criterios de evaluación utilizados fueron correctamente aplicados.[50]

- **CISCO.-** La Certificación Cisco es un plan de capacitación en tecnología de redes que la empresa Cisco ofrece. Se divide en tres niveles, de menor a mayor complejidad: Cisco Certified Network Associate, Cisco Certified Network Professional y Certificado Cisco de Experto en Internet.[51]

- **COBIT.-** Es una estructura que provee una herramienta para los propietarios de los procesos del negocio para descargar eficiente y efectivamente sus responsabilidades de control sobre los sistemas informáticos.[52]

- **Código dañino.-** es un software que tiene como objetivo infiltrarse en o dañar un ordenador sin el conocimiento de su dueño y con finalidades

[47] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-Glosario_y_abreviaturas/401/index.html

[48] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.34

[49] MÉNDEZ, Andrés, MAÑAS, José Antonio, 2010, MANUAL DE USUARIO PILAR BASIC versión 4.4, Ministerio de Administraciones Públicas, España, p. 95

[50] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p. 104

[51] http://www.google.com.ec/#hl=es&rlz=1R2TSND_esEC423&tbs=dfn:1&sclient=psy-ab&q=certificacion+cisco&rlz=1R2TSND_esEC423&pbx=1&oq=certificacion+cisco&aq=f&aqi=&aql=&gs_sm=3&gs_upl=21232l23400l3l24336l14l9l0l0l0l0l0l0ll0l0&bav=on.2,or.r_gc.r_pw.r_qf.,cf.osb&fp=f89e31c4e36c9ff3&biw=1366&bih=556

[52] http://www.netconsul.com/riesgos/cci.pdf

muy diversas ya que en esta categoría encontramos desde un troyano hasta un spyware.[53]

- **Condiciones inadecuadas de temperatura o humedad.-** Son las deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frio, exceso de humedad.[54]
- **Confidencialidad.-** Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.[55]

- **Contaminación electromagnética.-** Son las interferencias de radios, campos magnéticos, luz ultravioleta.[56]

- **Contaminación mecánica.-** Son vibraciones, polvo, suciedad.[57]

- **Corte de suministro eléctrico.-** Es la cese de la alimentación de potencia.[58]

- **Costo-Beneficio.-** Criterio para especificar cuando una tecnología o medida delibera un bien o servicio a igual o menor costo que la práctica que lo produce actualmente.[59]

- **Daños por agua.-** Son las inundaciones: posibilidad de que el agua acabe con el recurso del sistema.[60]

- **Deficiencias en la organización.-** Es cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.[61]

[53] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-Glosario_y_abreviaturas/401/index.html

[54] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.30

[55] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p. 104

[56] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.29

[57] Ibíd.

[58] Ibíd.

[59] http://cambio_climatico.ine.gob.mx/glosario.html

[60] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.27

- **Degradación.-** Mide el daño causado por un incidente en el supuesto de que ocurriera.[62]

- **Denegación de servicio.-** Es la carencia de recursos suficientes que provoca la caída del sistema cuando la carga de trabajo es desmesurada.[63]
- **Desastres industriales.-** Son otros desastres debido a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas y accidentes de tráfico.[64]

- **Desastres naturales.-** Son otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.[65]

- **Destrucción de información.-** Son la perdida accidental de información.[66]

- **Difusión de software dañino.-** Es la propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.[67]

- **Dimensiones de seguridad.-** Es una característica o atributo que hace valioso a un activo, y sobre el que se valora a un activo.[68]

- **Disponibilidad.-** Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.[69]

- **Divulgación de la información.-** Es la revelación de la información.[70]

---

[61] Ibíd., p. 32
[62] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.22
[63] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.39
[64] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.33
[65] Ibíd., p.28
[66] Ibíd., p. 34
[67] Ibíd., p. 36
[68] MÉNDEZ, Andrés, MAÑAS, José Antonio, 2010, MANUAL DE USUARIO PILAR BASIC versión 4.4, Ministerio de Administraciones Públicas, España, p. 95
[69] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.105

- **Dominio.-** Conjunto de activos sometidos a un tratamiento homogéneo, bajo una cierta política de seguridad común.[71]

- **Emanaciones electromagnéticas.-** Es el hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del atacante.[72]

- **Errores de configuración.-** Es la introducción de datos de configuración erróneas.[73]

- **Errores de mantenimiento/Actualización de equipos (hardware).-** Son defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.[74]

- **Errores de mantenimiento/Actualización de programas (software).-** Son defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.[75]

- **Errores de re-encaminamiento.-** Es el envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a dónde o por dónde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.[76]

- **Errores del administrador.-** Son las equivocaciones de personas con responsabilidades de instalación y operación.[77]

- **Errores del usuario.-** Son las equivocaciones de las personas cuando usan los servicios, datos, etc.[78]

---

[70] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.39

[71] MÉNDEZ, Andrés, MAÑAS, José Antonio, 2010, MANUAL DE USUARIO PILAR BASIC versión 4.4, Ministerio de Administraciones Públicas, España, p. 95

[72] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.31

[73] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.32

[74] Ibíd., p.34

[75] Ibíd.

[76] Ibíd., p.32

[77] Ibíd., p. 31

- **Estándar TIA-942.-** Es un estándar que brinda los requerimientos y lineamientos necesarios para el diseño e instalación de Data Center o centros de cómputo.[79]

- **Extorción.-** Es la presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.[80]

- **Fallo de servicios de comunicaciones.-** Es la cese de la capacidad de trasmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centro de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.[81]

- **Firewall.-** Dispositivo de red físico o lógico que se utiliza para permitir, denegar o analizar las comunicaciones entre redes de datos, de acuerdo con las políticas de seguridad de la organización o del usuario.[82]

- **Frecuencia.-** Es cada cuánto se materializa la amenaza, se modela como una tasa anual de ocurrencia, siendo valores típicos.[83]

- **Fuego.-** Son incendios: posibilidad de que el fuego se acabe con los recursos del sistema.[84]

- **Gestión.-** Es coordinar todos los recursos disponibles para conseguir determinados objetivos.[85]

- **Gestión de Riesgos.-** Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.[86]

---

[78] Ibíd.
[79] http://www.grupoelectrotecnica.com/pdf/estandaresdatacenter.pdf
[80] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.40
[81] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.30
[82] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-Glosario_y_abreviaturas/401/index.html
[83] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.22
[84] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.27
[85] http://www.amazonas.gov.co/glosario.shtml?apc=I----&s=b

- **Impacto.-** Consecuencia que sobre un activo tiene la materialización de una amenaza.[87]
- **Impacto residual.-** Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad.[88]

- **Incidente.-** Evento con consecuencias en detrimento de la seguridad del sistema de información.[89]
- **Incertidumbre.-** Es el grado de desconocimiento o falta de información, porque existen desacuerdos sobre lo que se sabe o podría saberse.[90]

- **Indisponibilidad del personal.-** Es la ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los excesos.[91]

- **Ingeniería social.-** Es el abuso de la buena fe de las persona para que realicen actividades que interesan a un tercero.[92]

- **Integridad.-** Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.[93]

- **Interceptación de información (escucha).-** Es cuando el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.[94]

[86] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.105
[87] Ibíd.
[88] MÉNDEZ, Andrés, MAÑAS, José Antonio, 2010, MANUAL DE USUARIO PILAR BASIC versión 4.4, Ministerio de Administraciones Públicas, España, p. 95
[89] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.106
[90] http://es.wiktionary.org/wiki/incertidumbre
[91] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.40
[92] Ibíd., p. 41
[93] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.106
[94] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.38

- **Interrupción de otros servicios o suministros esenciales.-** Son otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, etc.[95]

- **Introducción de falsa información.-** Es la inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio.[96]

- **ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la Información.-** Establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización.
  ISO / IEC 27002:2005 contiene las mejores prácticas de los objetivos de control y los controles en las siguientes áreas de gestión de seguridad de la información:
  - política de seguridad;
  - organización de seguridad de la información;
  - de gestión de activos;
  - recursos de la seguridad humana;
  - seguridad física y ambiental;
  - las comunicaciones y la gestión de las operaciones;
  - control de acceso;
  - la adquisición de sistemas de información, desarrollo y mantenimiento;
  - seguridad de la información de gestión de incidentes;
  - gestión de la continuidad;
  - cumplimiento.[97]

- **ITIL.-** Information Technology Infrastructure Library, es una colección de las mejores prácticas observadas en la industria de TI. Es un conjunto de libros en los cuales se encuentran documentados todos los procesos referentes a la provisión de servicios de tecnología de información hacia las organizaciones.

  ITIL por medio de procedimientos, roles, tareas, y responsabilidades que se pueden adaptar a cualquier organización de TI, genera una descripción detallada de mejores prácticas, que permitirán tener mejor comunicación y administración en la organización de TI. Proporciona los

[95] Ibíd., p.30
[96] Ibíd., p.38
[97] http://www.iso.org/iso/catalogue_detail?csnumber=50297

elementos necesarios para determinar objetivos de mejora y metas que ayuden a la organización a madurar y crecer.[98]

- **MAGERIT.-** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), Es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.[99]

- **Manipulación de la configuración.-** Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.[100]
- **Medios electrónicos.-** Cualquier tecnología que permita la transmisión, generación, almacenamiento, envío, resguardo, transformación, modificación, comunicación pública o privada sin limitar tecnologías actuales o futuras.[101]
- **Medios informáticos.-** Todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento y la Optimización del trabajo con Ordenadores y Periféricos, tanto a nivel Individual, como Colectivo u Organizativo, sin dejar de lado el buen funcionamiento de los mismos.[102]
- **Medios telemáticos.-** Un espacio abstracto de adquisición de información, del cual surge información y se recibe información.[103]
- **Modelo de Valor.-** Informe: Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.[104]

- **Modificación de información.-** Es la alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.[105]

[98] http://www.soporteremoto.com.mx/help_desk/articulo04.html
[99] http://www.ar-tools.com/index.html
[100] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.35
[101] http://www.bpc.com.mx/?page_id=70
[102] http://informacion.wordpress.com/2006/06/06/%C2%BFque-son-los-recursos-informaticos/
[103] http://www.slideshare.net/tannia1928/medios-telematicos
[104] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.107
[105] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.38

- **PILAR Basic.-** acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una herramienta desarrollada bajo la especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología MAGERIT.[106]
- **Plan de continuidad.-** Prevención, reacción y recuperación frente a detenciones del servicio.[107]
- **Plan de emergencia.-** Planeación e intervención de acciones en al antes, durante y después de presentarse una emergencia. Enfocado a la prevención.[108]
- **Plan de recuperación.-** Procedimiento definido para que se reanuden los procesos de negocio tras una interrupción significativa de los mismos.[109]
- **Plan de seguridad.-** Conjunto de programas de seguridad que permiten materializar las decisiones de gestión de riesgos.[110]

- **Programa de seguridad.-** Agrupación de tareas orientadas a afrontar el riesgo del sistema. La agrupación se realiza por conveniencia, bien porque se trata de tareas que en singular carecerían de eficacia, bien porque se trata de tareas con un objetico común, bien porque se trata de tareas que competen a una única unidad de acción.[111]
- **Riesgo.-** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.[112]
- **Riesgo residual.-** Riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.[113]

[106] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.129
[107] https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/index.html
[108] http://www.google.com.ec/#hl=es&tbo=1&rlz=1R2TSND_esEC423&tbs=dfn:1&sclient=psy-ab&q=plan+de+emergencia&rlz=1R2TSND_esEC423&pbx=1&oq=plan+de+emergencia&aq=f&aqi=g10&aql=&gs_sm=3&gs_upl=2139l2795l4l3125l6l4l0l0l0l2l252l830l0.2.2l4l0&tbo=1&bav=on.2,or.r_gc.r_pw.r_qf.,cf.osb&fp=a3266cec0758bb3&biw=1366&bih=556
[109] https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/index.html
[110] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.107
[111] Ibíd.
[112] Ibíd.
[113] Ibíd.

- **RMAN.-** Recovery Manager" (RMAN) es un programa potente y versátil que permite realizar una copia de datos. Con el comando RMAN BACKUP, RMAN por defecto crea un conjunto de copia de seguridad y con el comando RESTORE se restauraría la información, todo esto en un formato "propietario" por lo que se necesita RMAN para la recuperación.[114]
- **Robo de equipos.-** La sustracción del equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.[115]
- **Salvaguarda.-** Procedimiento o mecanismo tecnológico que reduce el riesgo.[116]
- **Seguridad de la Información.-** Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables.[117]
- **Seguridad física.-** Conjunto de medidas usadas para proporcionar protección física a los recursos de información contra amenazas intencionadas o accidentales.[118]
- **Seguridad lógica.-** se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.[119]
- **Seguridad.-** la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o mal intencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.[120]
- **Sistemas de Información.-** Son los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento.[121]

[114] http://limbail.wordpress.com/2010/04/12/rman-que-es-rman/
[115] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.39
[116] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.108
[117] https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/index.html
[118] https://www.ccn-cert.cni.es/publico/serieCCN-STIC401/index.html
[119] http://es.wikipedia.org/wiki/Seguridad_l%C3%B3gica
[120] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.108
[121] Ibíd.

- **SSL para Https.-** SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.[122]
- **Stand By.-** Se denomina *stand by* (en español consumo en espera) al consumo en espera de diferentes aparatos electrónicos, tales como televisión, reproductores d[123]e audio o vídeo, aire acondicionado, algunos modelos de frigoríficos, algunas vitrocerámicas, alimentadores/cargadores, PC, etc. En *stand by*, el aparato se encuentra conectado a la espera de recibir órdenes, por lo que consume energía eléctrica.

- **Subneting.-** es una colección de direcciones IP que permiten definir el número de redes y de host que se desean utilizar en una subred determinada.[124]

- **Suplantación de la identidad del usuario.-** Es cuando un atacante consigue hacerse pasar por un usuario autorizado, disfrutando de los privilegios de este para sus fines propios.[125]
- **Tarjeta de coordenadas.-** es una herramienta de seguridad adicional a la clave de seguridad bancaria requerida para realizar operaciones que impliquen movimiento de fondos o contratación de productos y servicios a través de servicios a distancia (banca electrónica o banca telefónica).

  Conforma un segundo factor de autenticación de la cuenta bancaria, pero a diferencia del PIN o clave, que es fijo, es dinámica. Cuando una clave es dinámica es más difícil para los estafadores electrónicos robar claves para hacer transferencias por Internet. Cada vez que lo intenten necesitarán una coordenada distinta, que es aleatoria y vence con cada sesión.
  La Tarjeta de Coordenadas es una tarjeta de plástico, del tamaño de una tarjeta de crédito, que contiene una matriz o serie de números (generalmente pares de datos) impresos, es decir, ordenados en filas y columnas. Las filas están tituladas con números ascendentes a partir del

[122] http://es.wikipedia.org/wiki/Transport_Layer_Security
[123] http://es.wikipedia.org/wiki/Stand_by
[124] http://www.monografias.com/trabajos35/subnetting-vlsm/subnetting-vlsm.shtml
[125] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.35

1 y las columnas con letras ascendentes alfabéticamente comenzando desde la A. En algunas entidades, el orden es inverso.[126]

- **Trazabilidad.-** Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.[127]

- **UPS.-** Un sistema de alimentación ininterrumpida, SAI (en inglés *Uninterruptible Power Supply*, *UPS*), es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.[128]

- **Uso no previsto.-** Es la utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, base de datos personales, programas personales, almacenamiento de datos personales, etc.[129]

- **Valor.-** De un activo. Es una estimación del coste inducido por la materialización de una amenaza.[130]

- **Vulnerabilidad.-** Estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada.[131]
- **Vulnerabilidad de los programas (software).-** Son defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la identidad de los datos o la capacidad misma de operar.[132]

[126] http://es.wikipedia.org/wiki/Tarjeta_de_coordenadas
[127] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.109
[128] http://es.wikipedia.org/wiki/Sistema_de_alimentaci%C3%B3n_ininterrumpida
[129] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.36
[130] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.109
[131] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España, p.109
[132] LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II – Catálogo de Elementos, Ministerio de Administraciones Públicas, España, p.34

BIBLIOGRAFÍA

LIBROS:

ACHIG, Lucas, 2000, Investigación Social, Teoría Metodológica, Técnicas y Evaluación, U Ediciones, Cuenca-Ecuador

LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier, 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. I – Método, Ministerio de Administraciones Públicas, España

LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier, 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. II –Catálogo de Elementos, Ministerio de Administraciones Públicas, España

LOPEZ, Francisco, AMUTIO, Miguel, CANDAU, Javier, 2006, MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. III – Guía de Técnicas, Ministerio de Administraciones Públicas, España

MÉNDEZ, Andrés, MAÑAS, José Antonio, 2010, MANUAL DE USUARIO PILAR BASIC versión 4.4, Ministerio de Administraciones Públicas, España

DOCUMENTOS:

COAC Jardín Azuayo, Estatuto

COAC Jardín Azuayo, Reglamento Interno

COAC Jardín Azuayo, Planificación Estratégica 2009-2013

COAC Jardín Azuayo, Manual para Socios

PÁGINAS WEB:

www.jardinazuayo.fin.ec

http://www.ar-tools.com/

https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=187&lang=es

http://www.cii-murcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.pdf

http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_Area_Descargas&langPae=es&iniciativa=184

http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=161