UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO – JUNIO 2017

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS

TEMA:

ANALISIS DE LA SEGURIDAD INFORMATICA EN LA COOPERATIVA DE AHORRO Y CREDITO "SAN ANTONIO" DE LA UNION.

EGRESADA:

SARA LEONELA ALMEIDA SUAREZ

TUTOR:

ING. JOSE TEODORO MEJIA VITERI, MSC

AÑO 2017

INTRODUCCION

La seguridad informática juega un papel muy importante en todas las empresas u organizaciones que existen porque permite proteger la integridad, privacidad y confidencialidad de la información que se tiene guardada en el sistema informático.

Hoy en día muchos de estos lugares están siendo afectados por no tomar precauciones necesarias, no se le da importancia en lo que respecta a este tema. piensan que no les ocurrirá algo grave pero, en momentos menos esperados los equipos y la información se ven afectados por amenazas que asechan a las organizaciones.

La cooperativa de ahorro y crédito "San Antonio" de la Unión cuyo objetivo social es brindar servicios a las necesidades financieras de sus socios y a personas terciarias por medio de las actividades propias de las entidades de crédito. Cuenta con un total de 500 socios.

Este análisis se realizó para evaluar los riesgos de los activos de los 4 departamentos de la cooperativa de ahorro y crédito los cuales son: gerencia, atención al cliente, cajero, y asesor de crédito se realizó el inventario de todos los activos de hardware y software, se valoró dependiendo de la importancia y capacidad que tienen, también se reconocieron cuáles son las amenazas y vulnerabilidades que asechan a los activos de aquella institución y por último se procedió analizar los riesgo que se presentan en cada activo, de la cooperativa de ahorro y crédito.

Desarrollo

En el año 2000 comenzó a funcionar La cooperativa de ahorro y crédito "San Antonio" de la Unión es una organización con el objetivo de prestar servicios a socios y terceros los cuales pueden hacer sus depósitos de ahorros y hacer su crédito**.**

Cuenta con un personal de 5 personas el cual labora en el lugar ya mencionado, Este análisis se ha elaborado para saber si los activos y la información están propensos a riesgo si la seguridad informática en la cooperativa de ahorro y crédito "San Antonio" de la Unión es alta o baja.

Se basó en dos tipos de investigaciones tales como las de campo y la bibliográfica.

La investigación de campo porque se ha obtenido información relevante acerca de la seguridad informática esta permitió conocer cuáles son los activos de hardware y software, las causas, los efectos y cuáles son los métodos técnicas e instrumentos que se utilizó en la cooperativa de ahorro y crédito.

La investigación bibliográfica por que se fundamentó en temas existentes y permitió profundizar aquellas teorías relacionadas a nuestro análisis de seguridad informática.

La población está conformada por el personal que labora en dicha institución.

La información se ha obtenido mediante entrevistas y también por observación propia.

Las entrevistas fueron hechas al personal que labora en dicha institución para obtener información necesaria para nuestro análisis y también se visitó el lugar donde pudimos visualizar muchos casos que se presentaban.

Según (Aguilera López, 2010, pág. 9) La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Sin embargo el hecho de enfocarse en la seguridad informática de las empresa esto, no quiere decir que no se va a tener problemas porque a diario se presentan nuevas amenazas y vulnerabilidades que pueden a instituciones pequeñas o grandes con el fin de poder obtener el lucro para sus vidas, pero se tratara de minimizar riesgos y perdidas tanto económica como información importante de estos lugares.

El análisis y gestión de riesgo es un método formal para investigar los riesgos de un SI y recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. (Heredero, López Hermoso Agius, Romo Romero, & Medina Salgado, 2012, pág. 285)

Según Eterovic (2011)

"Existen algunas metodologías para la planificación de la reducción de riesgo, planificación de prevención de accidentes, visualización y detección de las debilidades existentes en los sistemas, ayuda en la toma de mejores decisiones en materia de seguridad de la información"

Hay algunas metodologías para el análisis de riesgos de información en las instituciones, se hablara de cuatro de ellas: Margarit, Octave, Mehari y de ISO 27005.

Según de Pablos Heredero (2006) "OCTAVE, metodología del SEI (Software Engineering Institute) que desde un punto de vista organizativo y técnico analiza los riesgos y propone un plan de mitigación.

Según Desongles Corrales "MARGERIT, 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"

Según (Gaspar Martínez, 2010) mehari es: (Méthode Harmoniée d'Analyse des Risques). Método armonizado de Análisis de Riesgo desarrollado por CLUSIF que clasifica los riesgos según sus causas.

> La Organización internacional de Estandarización (ISO) se dio a la tarea de elaborar y emitir las normas ISO/IEC 27000 que complementan el uso e implementación de un ISMS. Los requerimientos de la norma 27000 se pueden aplicar a cualquier tipo de organización sin importar su tamaño, el sector al que pertenece o el objetivo de la organización. (Baca Urbina, Solares Soto, & Acosta Gonzaga, Administración Informática I: Análisis y Evaluación de Tecnologías de Información, 2014)

ISO/IEC 27001: según (ALEGRE RAMOS & CERVIGÓN HURTADO, 2011) "esta norma es la principal de la serie, la seguridad de la información es la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento".

"ISO/IEC 27002: Un código de buenas prácticas para la gestión de la seguridad de la información. Ayuda a poner en marcha las practicas necesarias para cumplir los requisitos exigidos para la certificación ISO/IEC 27001". (CASTRO GIL , DÍAZ ORUETA , ALZÓRRIZ ARMENDÁRIZ , & SANCRISTÓBAL RUIZ , 2014)

"ISO/IEC 27003: Guía de implementación. Describe los aspectos a tener en cuenta para la implantación de un SGSI, fue publicada en febrero del 2009 y aun no existe traducción al español".

"**ISO/IEC 27004:** Un nuevo estándar sobre métricas de gestión de seguridad de información". (CASTRO GIL , DÍAZ ORUETA , ALZÓRRIZ ARMENDÁRIZ , & SANCRISTÓBAL RUIZ , 2014)

ISO/IEC 27005: Trata los aspectos relacionados a la "Gestión de riesgos "tema de suma Importancia en toda esta familia. (Corletti Estrada, 2011)

Para el análisis de la seguridad informática en la cooperativa de ahorro y crédito de la Unión se ha basado en la norma ISO 27005 se debe hacer la identificación de activos luego la valoración de los mismos también se deben reconocer cuales son las amenazas y vulnerabilidades que se presentan en ese lugar y los riesgos que pueden haber para luego poder hallar una solución a dicho problema.

En la Identificación de los Activos Se deberá tener una lista de todos activos con que cuenta la cooperativa, cuáles son las amenazas que se presentan, las vulnerabilidades y luego proceder al análisis de riesgo.

En la **Tabla 1** se muestra los activos de soporte de gerencia de la cooperativa de ahorro y crédito "San Antonio "de la parroquia la Unión.

ACTIVOS DE SOPORTE DE GERENCIA

Activos de hardware	Activos de software	Activo de información
Portátil	Sistema financiero integrado Ofimática.	Licencia de Windows server 2010
1 Central de aire	Base de datos	Unidades USB o pendrives.
1 Impresora	Antivirus	Documentos en papeles
	Sistema Operativo	
	Correo	
	Internet	

Tabla 1: Activos de soporte del departamento de gerencia de la Cooperativa de ahorro y crédito "San Antonio" de la Unión. **Fuente:** Elaboración propia.

ACTIVOS DE SOPORTE DEL DEPARTAMENTO DE CREDITO

Activos de hardware	Activos de software	Activo de información
1 Equipo de escritorio	Sistema financiero integrado Ofimática.	Licencia de Windows server 2010
1 Central de aire	Base de datos	Unidades USB o pendrives.
1 Impresora	Antivirus	Documentos en papeles
Router	Sistema Operativo	
Swich	Correo	
	Internet	

Tabla 2: Activos de soporte del departamento de crédito de la Cooperativa de ahorro y crédito "San Antonio" de la Unión. **Fuente:** Elaboración propia..

ACTIVOS DE SOPORTE DEL DEPARTAMENTO DE CAJA

Activos de hardware	Activos de software	Activo de información
1 Equipo de escritorio	Sistema financiero integrado Ofimática.	Licencia de Windows server 2010
1 Central de aire	Base de datos	Unidades USB o pendrives.
1 Impresora	Antivirus	Documentos en papeles
	Sistema Operativo	
	Correo	
	Internet	

Tabla 3: Activos de soporte del departamento de caja de la Cooperativa de ahorro y crédito "San Antonio" de la Unión. **Fuente:** Elaboración propia.

ACTIVOS DE SOPORTE DEL DEPARTAMENTO DE ATENCION AL SOCIO

Activos de hardware	Activos de software	Activo de información
1 Equipo de escritorio	Sistema financiero integrado Ofimática.	Licencia de Windows server 2010
1 Central de aire	Base de datos	Unidades USB o pendrives.

1 Impresora	Antivirus Sistema Operativo Correo Internet	Documentos en papeles

Tabla 4: Activos de soporte del departamento de atención al socio de la Cooperativa de ahorro y crédito "San Antonio" de la Unión. **Fuente:** Elaboración propia.

Se ha identificado todos los activos correspondientes a cada uno de los 4 departamentos, ahora se establecerán los parámetros y valoración en cuanto a la dependencia que tenga cada activo y su funcionalidad también se verán si estos están expuestos a problemas en cuanto a la integridad, confidencialidad y disponibilidad de sus servicios.

En un libro de (Computación para docentes) afirma que:

> Confidencialidad: debe de tener la capacidad de proteger la información ante el intento de acceso o divulgación a otros usuarios no autorizados.
>
> Integridad: la información debe estar completa y no ser alterada o modificada sin autorización.
>
> Disponibilidad: la información debe encontrarse a disposición de quienes tengan que acceder a ella, ya sean personas, procesos o aplicaciones, en el momento en que se la necesite.

PARAMENTROS Y VALORACION		**DEPENDENCIA**	**FUNCIONALIDAD**	**INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD**
1	**MUY BAJO**	No existe activo que depende de este para brindar sus servicios	activo con una capacidad tecnológica muy baja para brindar sus servicios	La, modificación, divulgación y no disponibilidad de su archivo de configuración afecta un 20% la entrega de servicios

2	**BAJO**	Existe un mínimo de activo que depende de este para brindar sus servicios	activo con una capacidad tecnológica baja para brindar sus servicios	La, modificación, divulgación y no disponibilidad de su archivo de configuración afecta un 40% la entrega de servicios
3	**MEDIO**	Existe una cantidad limitada de activo que depende de este para brindar sus servicios	activo con una capacidad tecnológica media para brindar sus servicios	La, modificación, divulgación y no disponibilidad de su archivo de configuración afecta un 60% la entrega de servicios
4	**ALTO**	la Existe una mayoría de activo que depende de este para brindar sus servicios	activo con una capacidad tecnológica alta para brindar sus servicios	La, modificación, divulgación y no disponibilidad de su archivo de configuración afecta un 80% la entrega de servicios
5	**CRÍTICO**	Existe el total de activo que depende de este para brindar sus servicios	activo con una capacidad tecnológica muy alta para brindar sus servicios	La, modificación, divulgación y no disponibilidad de su archivo de configuración afecta un 100% la entrega de servicios

Tabla 5: Parámetros y valoración de los activos **Fuente:** Elaboración propia.

En la **Tabla 3** se detalla la valoración de los activos de la cooperativa de ahorro y crédito “San Antonio “de la parroquia la Unión.

Se ha establecido las funciones de cada activo y se procederá a darle su valoración, esto depende del costo que tendrán si hay pérdida de confidencialidad, disponibilidad e integridad por medio de algún problema que se presente y saber el promedio.

VALORACION DE ACTIVOS DE SOPORTE DE GERENTE

ACTIVOS DE SOPORTE	FUNCION	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PROMEDIO
Portátil	Permite acceder a los servicios.	4	4	3	4
1 Central de aire	Permite tener en un ambiente frescos nuestros equipos informáticos	2	2	5	3
1 Impresora	Permite imprimir documentos.	2	2	5	3
Sistema financiero integrado Ofimática.	Permite trabajar con todas las herramientas que necesita una oficina.	2	2	5	3
Base de datos	permite ordenar y tener libre acceso de la información que necesitemos	4	4	5	4
Antivirus	Detecta y da aviso de archivos maliciosos y los elimina	2	2	2	2
Sistema Operativo	administra y gestiona un equipo computarizado y los diversos aparatos periféricos que lo compongan	4	4	5	4
Correo Electrónico	Permite enviar y recibir correos	3	3	3	3
Internet	Permite comunicarnos a diferentes lugares	2	3	5	3
Licencia de Windows server 2010	Permite trabajar con todas las herramientas necesarias para realizar tareas en una oficina.	3	4	5	4
Unidades USB o pendrives.	Permite transportar información a diferentes lugares.	3	3	3	3
Documentos en papeles	Permite tener en forma manual la información.	3	3	3	3

Tabla 6: valoración en cuanto a la perdida de confidencialidad, integridad y disponibilidad del departamento de gerencia **Fuente:** Elaboración propia.

VALORACION DE ACTIVOS DE SOPORTE DE CREDITO

ACTIVOS DE SOPORTE	FUNCION	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PROMEDIO
Equipos de escritorio	Permite acceder a los servicios.	4	4	3	4
1 Central de aire	Permite tener en un ambiente frescos nuestros equipos informáticos	2	2	5	3
1 Impresora	Permite imprimir documentos.	2	2	5	3
Sistema financiero integrado Ofimática.	Permite trabajar con todas las herramientas que necesita una oficina.	2	2	5	3
Base de datos	permite ordenar y tener libre acceso de la información que necesitemos	4	4	5	4
Antivirus	Detecta y da aviso de archivos maliciosos y los elimina	2	2	2	2
Sistema Operativo	administra y gestiona un equipo computarizado y los diversos aparatos periféricos que lo compongan	4	4	5	4
Correo Electrónico	Permite enviar y recibir correos	3	3	3	3
Internet	Permite comunicarnos a diferentes lugares	2	3	5	3
Licencia de Windows server 2010	Permite trabajar con todas las herramientas necesarias para realizar tareas en una oficina.	3	4	5	4
Unidades USB o pendrives.	Permite transportar información a diferentes	3	3	3	3

	lugares.				
Documentos en papeles	Permite tener en forma manual la información.	3	3	3	3
Switch	Permite conectar dispositivos de red	3	2	5	3
Router	Es un dispositivo que permite conectar redes	3	2	5	3

Tabla 7: valoración en cuanto a la perdida de confidencialidad, integridad y disponibilidad del departamento de credito **Fuente:** Elaboración propia.

ACTIVOS DE SOPORTE DEL DEPARTAMENTO DE CAJA

ACTIVOS DE SOPORTE	FUNCION	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PROMEDIO
Equipos de escritorio	Permite acceder a los servicios.	4	4	3	4
1 Central de aire	Permite tener en un ambiente frescos nuestros equipos informáticos	2	2	5	3
1 Impresora	Permite imprimir documentos.	2	2	5	3
Sistema financiero integrado Ofimática.	Permite trabajar con todas las herramientas que necesita una oficina.	2	2	5	3
Base de datos	permite ordenar y tener libre acceso de la información que necesitemos	4	4	5	4
Antivirus	Detecta y da aviso de archivos maliciosos y los elimina	2	2	2	2
Sistema Operativo	administra y gestiona un equipo computarizado y los diversos aparatos periféricos que lo compongan	4	4	5	4
Correo	Permite enviar y recibir	3	3	3	3

Electrónico	correos				
Internet	Permite comunicarnos a diferentes lugares	2	3	5	3
Licencia de Windows server 2010	Permite trabajar con todas las herramientas necesarias para realizar tareas en una oficina.	3	4	5	4
Unidades USB o pendrives.	Permite transportar información a diferentes lugares.	3	3	3	3
Documentos en papeles	Permite tener en forma manual la información.	3	3	3	3

Tabla 8: valoración en cuanto a la perdida de confidencialidad, integridad y disponibilidad del departamento de caja **Fuente:** Elaboración propia.

VALORACION DE ACTIVOS DE SOPORTE ATENCION AL SOCIO

ACTIVOS DE SOPORTE	FUNCION	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	PROMEDIO
Equipos de escritorio	Permite acceder a los servicios.	4	4	3	4
1 Central de aire	Permite tener en un ambiente frescos nuestros equipos informáticos	2	2	5	3
1 Impresora	Permite imprimir documentos.	2	2	5	3
Sistema financiero integrado Ofimática.	Permite trabajar con todas las herramientas que necesita una oficina.	2	2	5	3
Base de datos	permite ordenar y tener libre acceso de la información que necesitemos	4	4	5	4
Antivirus	Detecta y da aviso de archivos maliciosos y los elimina	2	2	2	2
Sistema Operativo	administra y gestiona un equipo computarizado y los diversos aparatos	4	4	5	4

	periféricos que lo compongan				
Correo Electrónico	Permite enviar y recibir correos	3	3	3	3
Internet	Permite comunicarnos a diferentes lugares	2	3	5	3
Licencia de Windows server 2010	Permite trabajar con todas las herramientas necesarias para realizar tareas en una oficina.	3	4	5	4
Unidades USB o pendrives.	Permite transportar información a diferentes lugares.	3	3	3	3
Documentos en papeles	Permite tener en forma manual la información.	3	3	3	3

Tabla 8: valoración en cuanto a la perdida de confidencialidad, integridad y disponibilidad del departamento de atención al socio **Fuente:** Elaboración propia.

Según (Iglesias Mouteira, 2006) "Una amenaza es cualquier factor que pueda causar potencialmente un daño a una organización mediante la exposición, modificación o destrucción de información, o mediante la denegación de servicios críticos".

Esta se da por alguna debilidad que se pueda tener o alguna vulnerabilidad que se presente lo cual puede ocasionar daños a los activos y afectar a la empresa.

En esta tabla se presentan las amenazas en los activos de la cooperativa de ahorro y crédito "San Antonio" de la Unión.

ACTIVOS	**AMENAZAS**
1 Portátil	Caídas Errores del administrador Errores de configuración Robo de equipo Falta de mantenimiento Uso no autorizado del equipo

3 Equipos de escritorio	Daño por suministro de energía Caídas Errores del administrador Errores de configuración Robo de equipo Falta de mantenimiento Uso no autorizado del equipo Suplantación del administrador
3 Impresoras	Caídas Mal uso
Central De Aire	Radiación electromagnética Daño por suministro de energía
Instalación Eléctrica	Radiación electromagnética
Swich	Daño por suministro de energía Caídas Errores del administrador Errores de configuración Robo de equipo Uso no autorizado del equipo
Router	Daño por suministro de energía Caídas Errores del administrador Errores de configuración Robo de equipo Uso no autorizado del equipo
Software	Daño por suministro de energía Error de configuración Uso no autorizado del software
Base de datos	Daño por suministro de energía Error de configuración Uso no autorizado de la base de datos
Antivirus	Error de mantenimiento a la aplicaciones (Software)
Sistema Operativo	Error de configuración
Correo	Software malicioso Error de actualizaciones
Internet	Daños por agua Daño por suministro de energía

Unidades USB o pendrives.	Falla de Servicios Error de mantenimiento a la aplicaciones (Software) Virus Perdida
Documentos en papeles	Daños por agua Perdida

Tabla 9: Activos con sus respectivas amenazas **Fuente:** Elaboración propia.

En Seguridad Informática, la palabra Vulnerabilidad hace referencia a una debilidad en un sistema permitiéndole a un atacante violar la Confidencialidad, Integridad, Disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones (Guzmán, 2011). Una vez que se allá identificado los puntos débiles se podrá contrarrestar un poco con los riesgos que se puedan presentarse en la cooperativa de ahorro y crédito.

Esta tabla presenta la escala de valoración y descripción de las amenazas que se presentan poco o muy a menudo.

PARAMETROS/VALORACION		**DESCRIPCIÓN**
1	**MUY BAJO**	Amenazas capaces de explotar vulnerabilidades en un 20%.
2	**BAJO**	Amenazas capaces de explotar vulnerabilidades en un 40%.
3	**MEDIO**	Amenazas capaces de explotar vulnerabilidades en un 60%.
4	**ALTO**	Amenazas capaces de explotar vulnerabilidades en un 80%.
5	**CRÍTICO**	Amenazas capaces de explotar

	vulnerabilidades en un 100%.

Tabla 10: Probabilidad que ocurra la amenaza. **Fuente**: elaboración propia

Ahora se establecerá que tan frecuente son las amenazas y la facilidad de explotación de cada activo

ACTIVOS	AMENAZAS	VULNERABILIDADES	FRECUENCIA QUE OCURRE UNA AMENAZAS	FACILIDAD DE EXPLOTACION
Portátil	Caídas	Descuido del equipo	BAJO	BAJO
	Errores del administrador	Falta de conocimiento	MEDIO	MEDIO
	Errores de configuración	Falta de conocimiento	MEDIO	MEDIO
	Robo de equipo	Descuido por parte del perteneciente	BAJO	BAJO
	Falta de mantenimiento	Falla por falta de mantenimiento	ALTO	ALTO
	Uso no autorizado del equipo	Contraseñas débiles	ALTO	ALTO
3 Equipos de escritorio	Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO
	Caídas	Descuido del equipo	BAJO	BAJO
	Errores del administrador	Falta de conocimiento	MEDIO	MEDIO
	Errores de configuración	Falta de conocimiento	MEDIO	MEDIO
	Robo de equipo	Descuido por parte del perteneciente	BAJO	BAJO
	Falta de mantenimiento	Falla por falta de mantenimiento	ALTA	ALTA
	Uso no autorizado del equipo	Contraseñas débiles	ALTA	ALTA
3 Impresoras	Caídas	Descuido del equipo	BAJO	BAJO
	Mal uso	Falta de conocimiento	BAJO	BAJO
Central De Aire	Radiación electromagnética	Sensibilidad a radiación electromagnética	BAJO	BAJO

	Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO
Instalación Eléctrica	Radiación electromagnética	Sensibilidad a radiación electromagnética	BAJO	BAJO
Swich	Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO
	Caídas	Descuido del equipo	BAJO	BAJO
	Errores del administrador	Falta de conocimiento	MEDIO	MEDIO
	Errores de configuración	Falta de conocimiento	MEDIO	MEDIO
	Robo de equipo	Descuido por parte del personal administrativo	BAJO	BAJO
	Uso no autorizado del equipo	Descuido por parte del personal administrativo	BAJO	BAJO
Router	Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO
	Caídas	Descuido del equipo	BAJO	BAJO
	Errores del administrador	Falta de conocimiento	MEDIO	MEDIO
	Errores de configuración	Falta de conocimiento	MEDIO	MEDIO
	Robo de equipo	Descuido por parte del personal administrativo	MEDIO	MEDIO
	Uso no autorizado del equipo	Descuido por parte del personal administrativo	BAJO	BAJO
Software	Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO
	Error de configuración	Falta de conocimiento	MEDIO	MEDIO
	Uso no autorizado del software	Descuido por parte del administrador	MEDIO	MEDIO
Base de datos	Daño por suministro de	Cortes o insuficiencia de	BAJO	BAJO

	energía	energía		
	Error de configuración	Falta de conocimiento	MEDIO	MEDIO
	Uso no autorizado de la base de Datos	Descuido por parte del administrador	BAJO	BAJO
Antivirus	Error de mantenimiento a las aplicaciones (Software)	No Actualizar el antivirus	MEDIO	MEDIO
Sistema Operativo	Error de configuración	Falta de conocimiento	MEDIO	MEDIO
Correo	Software malicioso	Protección inadecuada	MEDIO	MEDIO
	Error de actualizaciones	Falta de conocimiento	MEDIO	MEDIO
Internet	Daños por agua	Expuesta a daños por agua	BAJO	BAJO
	Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO
	Falla de Servicios	Baja Señal	BAJO	BAJO
Unidades USB o pendrive.	Perdida	Descuido del propietario	BAJO	BAJO
	Daños por agua	Descuido del propietario	BAJO	BAJO
Documentos en papeles	Perdida	Descuido del propietario	BAJO	BAJO

Tabla 11: frecuencia que ocurren las amenazas en cada activo y facilidad de explotación **Fuente:**

Elaboración propia.

Riesgo "Es una situación con dos características:

-probabilidad de ocurrencia y

-Efecto negativo que no deseamos, directamente relacionado con la pérdida financiera"

(Quiroz, pág. 51) . El riesgo se presenta cuando se está expuesto a condiciones críticas

por ejemplos alguna amenaza o vulnerabilidad. Hoy en día todas las organizaciones están expuestas a riesgos que podrían afectar gravemente el estado económico.

Clasificación de Riesgo

PARAMETROS	RANGO
BAJO	0-2
MEDIO	3-5
ALTO	6-8

Tabla 12: clasificación de riesgo **Fuente:** Elaboración propia.

La siguiente tabla permitirá el cálculo de riesgo sobre los activos de la cooperativa

	Probabilidad De Ocurrencia- De Amenaza	BAJA			MEDIA			ALTA		
	Facilidad De Explotación	L	M	H	L	M	H	L	M	H
Valor Del Activo	1	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

Tabla 13: Evaluación del Riesgo. **Fuente:** ISO 27005

Detalle de los activos que se ven afectados en la cooperativa de ahorro y crédito “San Antonio” de la Unión según sus parámetros.

ACTIVOS	VALOR DEL ACTIVO	AMENAZAS	VULNERABILIDADES	FRECUENCIA QUE OCURRE UNA AMENAZA	FACILIDAD DE EXPLOTACION	RIESGO
Portátil	4	Caídas	Descuido del equipo	BAJO	BAJO	MEDIO
		Errores del administrador	Falta de conocimiento	MEDIO	MEDIO	MEDIO
		Errores de configuración	Falta de conocimiento	MEDIO	MEDIO	MEDIO
		Robo de equipo	Descuido por parte del propietario	BAJO	BAJO	MEDIO
		Falta de mantenimiento	Falla por falta de mantenimiento	ALTO	ALTO	ALTO
		Uso no autorizado del equipo	Contraseñas débiles	ALTO	ALTO	ALTO
3 Equipos de escritorio	4	Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO	MEDIO
		Caídas	Descuido del equipo	BAJO	BAJO	MEDIO
		Errores del administrador	Falta de conocimiento	MEDIO	MEDIO	MEDIO
		Errores de configuración	Falta de conocimiento	MEDIO	MEDIO	MEDIO
		Robo de equipo	Descuido por parte del propietario	BAJO	BAJO	MEDIO
		Falta de mantenimiento	Falla por falta de mantenimiento	ALTA	ALTA	ALTO
		Uso no autorizado del equipo	Contraseñas débiles	ALTA	ALTA	ALTO

3 Impresoras	3	Caídas	Descuido del equipo	BAJO	BAJO	BAJO
		Mal uso	Falta de conocimiento	BAJO	BAJO	BAJO
Central De Aire	3	Radiación electromagnética	Sensibilidad a radiación electromagnética	BAJO	BAJO	BAJO
		Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO	BAJO
Instalación Eléctrica	3	Radiación electromagnética	Sensibilidad a radiación electromagnética	BAJO	BAJO	BAJO
Swich	3	Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO	BAJO
		Caídas	Descuido del equipo	BAJO	BAJO	BAJO
		Errores del administrador	Falta de conocimiento	MEDIO	MEDIO	MEDIO
		Errores de configuración	Falta de conocimiento	MEDIO	MEDIO	MEDIO
		Robo de equipo	Descuido por parte del personal administrativo	BAJO	BAJO	BAJO
		Uso no autorizado del equipo	Descuido por parte del personal administrativo	BAJO	BAJO	BAJO
Router	3	Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO	BAJO
		Caídas	Descuido del equipo	BAJO	BAJO	BAJO
		Errores del administrador	Falta de conocimiento	MEDIO	MEDIO	MEDIO
		Errores de configuración	Falta de conocimiento	MEDIO	MEDIO	MEDIO
		Robo de equipo	Descuido por parte del personal administrativo	MEDIO	MEDIO	MEDIO

		Uso no autorizado del equipo	Descuido por parte del personal administrativo	BAJO	BAJO	BAJO
Software	4	Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO	MEDIO
		Error de configuración	Falta de conocimiento	MEDIO	MEDIO	MEDIO
		Uso no autorizado del software	Descuido por parte del administrador	MEDIO	MEDIO	MEDIO
Base de datos	4	Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO	MEDIO
		Error de configuración	Falta de conocimiento	MEDIO	MEDIO	MEDIO
		Uso no autorizado de la base de Datos	Descuido por parte del administrador	BAJO	BAJO	MEDIO
Antivirus	2	Error de mantenimiento a las aplicaciones (Software)		MEDIO	MEDIO	BAJO
Sistema Operativo	4	Error de configuración	Falta de conocimiento	MEDIO	MEDIO	MEDIO
Correo	3	Software malicioso	Protección inadecuada	MEDIO	MEDIO	MEDIO
		Error de actualizaciones	Falta de conocimiento	MEDIO	MEDIO	MEDIO
Internet	3	Daños por agua	Expuesta a daños por agua	BAJO	BAJO	BAJO
		Daño por suministro de energía	Cortes o insuficiencia de energía	BAJO	BAJO	BAJO
		Falla de Servicios	Baja señal	BAJO	BAJO	BAJO
Unidades USB	3	Virus	Computadoras infectadas	ALTO	ALTO	ALTO
		Perdida	Descuido del propietario	BAJO	BAJO	BAJO

Documentos en papeles	3	Daños por agua	Descuido del propietario	BAJO	BAJO	BAJO
		Perdida	Descuido del propietario	BAJO	BAJO	BAJO

Tabla 14: Evaluación del Riesgo. **Fuente**: Elaboración propia

El impacto de Riesgo Puede ser expresado por las consecuencias o daños que afectan un activo: atentado contra la integridad o la imagen de marca, perdida de disponibilidad o de volumen del negocio. (François, 2016, pág. 42)

Esto puede afectar mucho tanto en lo económico como en la reputación de dicha organización ya que si se presentan riesgos y esto ocasiona daños en los activos también se ven afectados los socios de la cooperativa porque ellos no solo tienen dinero hay sino que también confían que es un lugar confiable y seguro.

CONCLUSIONES

El análisis de la seguridad informática que se elaboró en la cooperativa de ahorro y crédito de la Unión permitió conocer el nivel de riesgo de cada uno de los activos que pertenecen a dicha institución.

Este trabajo toma como herramienta la norma ISO 27005 la cual permite el análisis de riesgo de la seguridad de la información se hizo la identificación de los activos luego se los valoró dependiendo la disponibilidad, integridad y confidencialidad de los datos también se identificaron las amenazas y vulnerabilidades que se enfrentan los activos y por último se evaluó si el riesgo es alto o bajo.

Los activos que se ven con mayor afectación de un alto riesgo son los equipos de escritorio y la portátil por la falta de mantenimiento y contraseñas débiles lo que ocasiona que los equipos tengan fallas, y también que personas no autorizadas puedan manipular información estrictamente confidencial.

Se debe plantear medidas preventivas o políticas de seguridad de acuerdo con la situación económica de la institución para poder asegurar los activos de la cooperativa y poder minimizar o contrarrestar riesgos que afectan a la información y equipos informáticos.

Bibliografía

Aguilera López, P. (2010). *Seguridad informática.* Editex.

ALEGRE RAMOS, M. D., & CERVIGÓN HURTADO, A. G. (2011). *SEGURIDAD INFORMATICA ED.11 Paraninfo.* Madrid: Paraninfo.

Baca Urbina, G., Solares Soto, P. F., & Acosta Gonzaga, E. (2014). *Administración Informática I: Análisis y Evaluación de Tecnologías de Información.* Mexico: Grupo Editorial Patria.

CASTRO GIL , M. A., DÍAZ ORUETA , G., ALZÓRRIZ ARMENDÁRIZ , I., & SANCRISTÓBAL RUIZ , E. (2014). *PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES.* Madrid: UNED.

Computación para docentes. (s.f.). USERSHOP.

Corletti Estrada, A. (2011). *Seguridad por niveles: Seguridad de acuerdo al modelo de capas TCP/IP.* Madrid: darFE.

de Pablos Heredero, C. (2006). *Dirección y gestión de los sistemas de información en la empresa: una visión integradora.* Madrid: ESIC.

Desongles Corrales, J. (s.f.). *Ayudantes Tecnicos. Opcion Informatica. Junta de Andalucia. Temario Volumen Ii.e-book.* España: MAD-Eduforma.

Eterovic, J. E. (25 de 01 de 2011). *Technical note.* Obtenido de Technical note: http://www.cyta.com.ar/ta1001/v10n1a3.htm

François, J. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* ENI.

Gaspar Martínez, J. . (2010). *El plan de continuidad de negocio: Una guia práctica para su elaboracción.* Mexico: Ediciones Díaz de Santos.

Guzmán, A. (01 de noviembre de 2011). *seguridadanggie*. Obtenido de Seguridad Informatica: http://seguridadanggie.blogspot.com/2011/11/vulnerabilidad.html

Heredero, C. d., López Hermoso Agius, J. J., Romo Romero, S. M., & Medina Salgado, S. (2012). *Organización y transformación de los sistemas de información en la empresa.* España: ESIC .

Iglesias Mouteira, R. (2006). *Instalacion de redes informáticas de ordenadores. Guía de técnicas y procedimientos para la verificación y puesta a punto.* España: Vigo.

Quiroz, L. G. (s.f.). *Informática y auditoría para las ciencias empresariales.* UNAB.

ENTREVISTA A LA ENCARGADA DEL DEPARTAMENTO DE GERENCIA

PAZMIÑO FIGUEROA FLOR JISELA

1- **¿Cuáles son los activos de hardware que tiene el departamento?**

2- **¿Cuántas computadoras hay en el departamento?**

3- **¿Cada que tiempo se les da mantenimiento a las computadoras?**

Mensual ( )
Semestral ( )
Anual ( )
No hace ( )

4- **¿El departamento tiene acceso a Internet?**

5- **¿con que sistema operativo trabaja las computadoras?**

6- **¿Cuáles son las amenazas que atacan los activos?**

7- **¿Qué fallas presentan los activos?**

8- **¿Alguna vez se ha hecho algún análisis de riesgo de la información dentro de la cooperativa o del departamento?**

9- **¿ha sufrido robo de información o de dinero dentro de la cooperativa?**