ANEXO 10

Caracterización, valoración y clasificación de activos de información de los procesos de atención al usuario, financiera y administrativa-

Matriz de Riesgo

TABLA DE CONTENIDO

LISTA DE TABLAS

1. TÉRMINOS Y DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000**).**

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Salvaguarda: El sistema MAGERIT define el servicio de salvaguarda como la acción genérica que puede producir un riesgo y el mecanismo de salvaguarda como el procedimiento que lo reduce.

2. CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN DE LOS PROCESOS DE ATENCIÓN AL USUARIO, ADMINISTRATIVA Y FINANCIERA

2.1. Identificación Y Clasificación De Activos Informáticos Procesos Dirección Financiera, Dirección Administrativa Y Atención Al Usuario

Con el fin de cumplir con esta fase se procede a realizar un reconocimiento de los activos de información del Concejo Distrital de Cartagena de Indias para la identificación de los activos de información en los procesos de atención al usuario, dirección administrativa y dirección financiera.

Para el análisis y gestión de los riesgos de información y con el fin de proteger la confidencialidad, integridad y disponibilidad de esta se toma como método de análisis y gestión de riesgos informáticos la Metodología MAGERIT 37 versión 3.0, esta metodología de la mano con la norma ISO/IEC 27001 de 2013 la cual permite identificar amenazas y estimar impacto y probabilidad de forma cualitativa.

Con la metodología Margerit también se definen estrategias que permitirán proteger la información y establecer un plan de mitigación de riesgo, donde se diseñan los controles para el tratamiento.

Para la caracterización y valoración de los activos de información se realizó un levantamiento del inventario de activos de información existentes en los procesos de atención al usuario, dirección administrativa y dirección financiera. La caracterización y valoración de los activos se realiza de acuerdo al Libro II de la metodología MAGERIT versión 3, en donde nos presenta el catálogo de elementos:

Tabla N° 1. Inventario de activos informáticos procesos de Dirección Financiera, Dirección Administrativa y Atención al usuario

TIPO	NOMBRE DEL ACTIVO
[SW] Software - Aplicaciones informáticas	1. ZEUS CONTABILIDAD Y ZEUS NOMINA 2. Sistema Contable y Financiero 3. [SO] Sistema Operativo. WINDOWS 7 4. [HER_SW] Herramientas Software. 5. [ANT_VIR] Anti-virus (10 antivirus)
SERVICIOS	6. Conectividad a internet (Wifi, Cable, VPN)
[COM] Redes de comunicaciones	7. [RO_ISP] Router Proveedor de Servicios de Internet. (3)
[HW] Equipamiento informático (hardware)	8. Impresora hp 1102 w (9) 9. PC] Equipos de cómputo (16 equipos)
Equipamiento auxiliar	10. [CAB_RED] Cableado de Red. [UTP CATEGORÍA 6
Instalaciones	11. [GAB] Gabinete de Red (2)
Personal	12. Contratista (1) VANESA PADILLA Mantenimiento de equipos y reparaciones 13. Funcionarios de Dirección Administrativa, Funcionarios de Dirección Financiera, Funcionarios de atención al usuario

Fuente. Los autores. Entrevista realizada al personal de la entidad

2.2. Valoración De Los Activos

Para realizar la valoración de los activos de información acuerdo a la metodología MAGERIT Versión 3; se usa las siguientes dimensiones:

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de la Información.
- [A] Autenticidad
- [T] trazabilidad

De acuerdo a la metodología Margerit para la valoración de los activos se utilizará la Tabla N° 2.

Tabla N° 2. Escala de Valoración de Activos

VALOR			IMPACTO PARA LA ORGANIZACIÓN
10	Extremo	E	Daño extremadamente grave
9	Muy Alto	MA	Daño Muy grave
6-8	Alto	A	Daño Grave
3-5	Medio	M	Daño Importante
1-2	Bajo	B	Daño Menor
0	Despreciable	D	Irrelevante a efectos prácticos

Tomado de: 2012_Magerit_v3_libro2_catálogo de elementos_es_NIPO_630-12-171-8.

2.2.1. Valoración De Activo: Tipo Aplicaciones

Tabla N° 3. Valoración de activos tipo Aplicaciones

ACTIVO	DIMENSIONES DE SEGURIDAD				
	D	I	C	A	T
ZEUS NOMINA Y CONTABILIDAD (1)	MA	MA	MA		
Sistema Contable y Financiero (2)		A	A	A	
[SO] Sistema Operativo Safe (3)	MA	A			
[HER_SW] Herramientas Software (4)	MA	A			
[ANT_VIR] Anti virus (5)	A				

Fuente. Los autores

Tabla N° 4. Valoración Aplicación Zeus

Valoración de activos según criterios de Margerit 3.0
(1) ZEUS CONTABLE Y DE NOMINA
[6.pi1] Probablemente afecte a un grupo de individuos [9 Lro] Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación [10.si] Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios [3.da] Probablemente cause la interrupción de actividades propias de la Organización [8.lbl] Confidencial

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

Tabla N° 5. Valoración Aplicación Sistema contable y financiero

Valoración de activos según criterios de Margerit 3.0
(2) SISTEMA CONTABLE Y FINANCIERO
[4.pi1] Probablemente afecte a un grupo de individuos [7.lro] Probablemente cause un incumplimiento grave de una ley o regulación [10.si] Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios [5.da2] Probablemente cause un cierto impacto en otras organizaciones [8.lbl] Confidencial

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

Tabla N° 6. Valoración Aplicación SAFE

Valoración de activos según criterios de Margerit 3.0
(3) [SO] SISTEMA OPERATIVO SAFE
[6.pi1] Probablemente afecte a un grupo de individuos [9 Lro] Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación [10.si] Probablemente sea causa de un incidente excepcionalmente serio de seguridad [3. da] Probablemente cause la interrupción de actividades propias de la Organización

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

Tabla N° 7. Valoración Herramientas Software

Valoración de activos según criterios de Margerit 3.0
(4) [HER_SW] HERRAMIENTAS SOFTWARE
[6.pi1] Probablemente afecte a un grupo de individuos [9 Lro] Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación [10.si] Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios [3.da] Probablemente cause la interrupción de actividades propias de la Organización [8.lbl] Confidential

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

Tabla N° 8. Valoración Antivirus

Valoración de activos según criterios de Margerit 3.0
(5) [ANT_VIR] ANTI VIRUS
[7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves [7. da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

2.2.2. Valoración De Activos Tipo Servicio

Tabla N° 9. Valoración de Activos Tipo: Servicios

ACTIVO	DIMENSIONES DE SEGURIDAD				
	D	I	C	A	T
[Conectividad a internet (Wifi, Cable, VPN)	M	A			

Fuente. Los autores

Tabla N° 10. Valoración activo Conectividad a Internet

Valoración de activos según criterios de Margerit 3.0
(6) [Conectividad a internet (Wifi, Cable, VPN)
[6.pi1] Probablemente afecte gravemente a un grupo de individuos [10.si] probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios [3.adm] Probablemente impediría la operación efectiva de una parte de la Organización [9. da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones [3.adm] Probablemente impediría la operación efectiva de una parte de la Organización

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

2.2.3. Valoración De Activos Tipo Redes De Comunicaciones

Tabla N° 11. Valoración de Activos Tipo: Redes de Comunicaciones

ACTIVO	DIMENSIONES DE SEGURIDAD				
	D	I	C	A	T
[RO_ISP] Router Proveedor de Servicios de Internet. . (7) MOVISTAR	MA	A			

Fuente. Los autores

Tabla N° 12. Valoración Redes De Comunicaciones - Proveedor de Servicios de Internet

Valoración de activos según criterios de Margerit 3.0
(7) [RO_ISP] ROUTER PROVEEDOR DE SERVICIOS DE INTERNET.
[4. p1] probablemente afecte a un grupo de individuos [7.lro] probablemente cause un incumplimiento grave de una ley o regulación [9.olm] Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística [5.lg. b] Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

2.2.4. Valoración De Activos Tipo: Equipamiento Informático

Tabla N° 13. Valoración de Activos Tipo: Equipo Informático

ACTIVO	DIMENSIONES DE SEGURIDAD				
	D	I	C	A	T
Impresora hp 1102 w (8)	M				
[PC] 16 Equipos de cómputo(9)		A	A	A	A

Fuente. Los autores

Tabla N° 14. Valoración Equipo Informático- Impresora Hp 1102 W

Valoración de activos según criterios de Margerit 3.0
(8) IMPRESORA HP 1102 W
[5.pi1] Probablemente afecte gravemente a un individuo [5.da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

Tabla N° 15. Valoración Equipo Informático- Equipo de cómputo.

Valoración de activos según criterios de Margerit 3.0
(9) [PC] EQUIPOS DE CÓMPUTO
[5.pi1] Probablemente afecte gravemente a un individuo [3.lro] Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación [7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves [5. da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones [3. lg] Probablemente afecte negativamente a las relaciones internas de la Organización

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

2.2.5. Valoración De Activos Tipo: Equipamiento Auxiliar

Tabla N° 16. Valoración de Activos Tipo: Equipo Auxiliar

ACTIVO	DIMENSIONES DE SEGURIDAD				
	D	I	C	A	T
[[CAB_RED] Cableado de Red. UTP CATEGORÍA 6 (10)	A	M			M

Fuente. Los autores

Tabla N° 17. Valoración Equipo Auxiliar - Cableado de Red.

Valoración de activos según criterios de Margerit 3.0
(10) [CAB_RED] Cableado de Red. [UTP CATEGORÍA 6
[4.pi1] Probablemente afecte a un grupo de individuos [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones [7.adm] Probablemente impediría la operación efectiva de la Organización

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

2.2.6. Valoración De Activos Tipo: Instalaciones

Tabla N° 18.Valoración de Activos Tipo: Instalaciones

ACTIVO	DIMENSIONES DE SEGURIDAD				
	D	I	C	A	T
[GAB] Gabinete de Red(11)	B	D			M

Fuente. Los autores

Tabla N° 19. Valoración Instalaciones- Gabinete de Red.

Valoración de activos según criterios de Margerit 3.0
(11) Gabinete de Red
[1.lro] Pudiera causar el incumplimiento leve o técnico de una ley o regulación. [1.si] Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente.

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

2.2.7. Valoración De Activos Tipo: Personal

Tabla N° 20. Valoración de Activos Tipo: Personal

ACTIVO	DIMENSIONES DE SEGURIDAD				
	D	I	C	A	T
[CO] Contratista. (12)	MA	A	A	A	A
Funcionarios administrativa, financiera y atención al usuario. (13)	MA	A	A	A	A

Fuente. Autores del Proyecto Modelos de Información Concejo Distrital.

Tabla N° 21. Valoración Activos- Personal Contratista

Valoración de activos según criterios de Margerit 3.0
(12) Contratista
[4.pi1] Probablemente afecte a un grupo de individuos [7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves [9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones [6.po] Probablemente cause manifestaciones, o presiones significativas [5.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local [3.adm] probablemente impediría la operación efectiva de una parte de la Organización [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización.

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

Tabla N° 22. Valoración Activos- Personal Funcionarios administrativos, financieros y atención al usuario.

Valoración de activos según criterios de Margerit 3.0
(13) Funcionarios administrativos, financieros y atención al usuario
[4.pi1] Probablemente afecte a un grupo de individuos [7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves [9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones [6.po] Probablemente cause manifestaciones, o presiones significativas [5.olm] Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local [3.adm] probablemente impediría la operación efectiva de una parte de la Organización [2.lg] Probablemente cause una pérdida menor de la confianza dentro de la Organización.

Fuente. Los autores de acuerdo a Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Margerit _V3_2

3. CARACTERIZACIÓN Y VALORACIÓN DE LAS AMENAZAS DE LOS PROCESOS DE ATENCIÓN AL USUARIO, DIRECCIÓN FINANCIERA Y DIRECCIÓN ADMINISTRATIVA

Para establecer las amenazas se tomó el catálogo de elementos que presenta la metodología MAGERIT en su libro II Versión 3.0

Para el desarrollo de esta actividad es necesario tener presente los rangos dados en los siguientes cuadros tanto de frecuencia como de degradación.

Tabla N° 23. Probabilidad de ocurrencia

VALOR			CRITERIO
100	Muy Frecuente	MF	A diario
10	Frecuente	F	Mensualmente
1	Normal	FN	Una vez al año
1/10	Poco frecuente	PF	Cada varios años

Fuente: Magerit Libro I versión 3.0.Pag 28 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

3.1. Degradación De La Amenaza – Impacto En El Activo

Tabla N° 24. Medición de la degradación

VALOR	DEGRADACIÓN O IMPACTO	
81- 100%	MA	Degradación MUY ALTA del activo
61- 80%	A	Degradación ALTA considerable del activo
51- 60%	M	Degradación MEDIANA del activo
21-50%	B	Degradación BAJA del activo
0-20%	MB	Degradación MUY BAJA del activo

Fuente: Los autores en base a Magerit versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro III- Guía de Técnicas

3.2. Identificación De Las Amenazas

A continuación, se identifican las amenazas de cada activo de la entidad

Tabla N° 25. Identificación de las amenazas de los activos de información del Concejo Distrital de Cartagena

ACTIVOS	AMENAZAS
Aplicaciones Informáticas	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.4] Errores de configuración [E.8] Difusión de software dañino [E.14] Escapes de información [E.18] Destrucción de información [A.11] Acceso no autorizado [A.15] Modificación de la información
Servicios	[I.8] Fallos de comunicación [E.24] Caída del sistema por agotamiento de recursos [A.11] Acceso no autorizado [A.24] Denegación de servicio
Redes de comunicaciones	[N.*] Desastres Naturales [[I.5] Avería de origen físico o lógico [I.8] Fallo de Servicio de comunicaciones [E.2] Errores del administrador [A.4] Manipulación de Configuración
Equipamiento Informático	[N.1] Fuego [I.5] Avería de origen físico o lógico [E.23] Errores de mantenimiento/ actualización de equipos (hardware) [Acceso no Autorizado [A.23] Manipulación de los equipos

ACTIVOS	AMENAZAS
Equipamiento auxiliar	[I.5] Avería de origen físico o lógico
Instalaciones	[A.26] Ataque destructiva
Personal	[E.15] Alteración accidental de la información

Fuente. Los autores

3.2.1. Valoración de las Amenazas

Tabla N° 26. Valoración de Amenazas Tipo: Aplicaciones Informáticas

AMENAZA	FRECUENCIA	DIMENSIONES DE SEGURIDAD				
		D	I	C	A	T
[E.1] Errores de los usuarios	MF	MA	MA	MA		
[E.2] Errores del administrador	PF	B	B	B		
[E.4] Errores de configuración	FN	A	A			
[E.8] Difusión de software dañino	PF	B	B	B	B	B
[E.14] Escapes de información	F	M	M	A	M	M
[E.18] Destrucción de información	PF	MA		A		
[A.11] Acceso no autorizado	FN	MA				
[A.15] Modificación de la información	PF		MA			

Fuente. Los Autores

3.2.1.1. Identificación y Valoración de Amenazas Tipo: Servicios

Tabla N° 27. Valoración de Amenazas Tipo: Servicios

AMENAZA	FRECUENCIA	DIMENSIONES DE SEGURIDAD				
		D	I	C	A	T
[I.8] Fallos de comunicación	F	A				B
[E.24] Caída del sistema por agotamiento de recursos	F	A				B
[A.11] Acceso no autorizado	F	A				B
[A.5] Suplantación de la identidad del usuario	FN			A	A	

Fuente. Los Autores

3.2.1.2. Valoración de Amenazas Tipo: Redes de Comunicaciones

Tabla N° 28. Valoración de Amenazas Tipo: Redes de Comunicaciones

AMENAZA	FRECUENCIA	DIMENSIONES DE SEGURIDAD				
		D	I	C	A	T
[N.*] Desastres Naturales	PF	MA				MA
[[I.5] Avería de origen físico o lógico	PN	MA				
[I.8] Fallo de Servicio de comunicaciones	PF	A				
[E.2] Errores del administrador	PF	A		A		
[A.4] Manipulación de Configuración.	PF			A	A	

Fuente. Los autores

3.2.1.3. Valoración de Amenazas Tipo: Equipamiento Informático

Tabla N° 29. Valoración de Amenazas Tipo: Equipamiento Informático

AMENAZA	FRECUENCIA	DIMENSIONES DE SEGURIDAD				
		D	I	C	A	T
[N.1] Fuego	PF	MA	MA	MA	MA	MA
[I.5] Avería de origen físico o lógico	PF	A				
[E.23] Errores de mantenimiento/ actualización de equipos (hardware)	FN	A		A		
[A.5] Suplantación de la identidad del usuario	FN	A				
[Acceso no Autorizado	FN			A		
[A.23] Manipulación de los equipos	FN			A		

Fuente. Los autores

3.2.1.4. Valoración de Amenazas Tipo: Equipamiento Auxiliar

Tabla N° 30. Valoración de Amenazas Tipo: Equipamiento auxiliar

ACTIVO/ AMENAZA	FRECUENCIA	DIMENSIONES DE SEGURIDAD				
		D	I	C	A	T
[I.5] Avería de origen físico o lógico	PF	A				

Fuente. Los autores

3.2.1.5. Valoración de Amenazas Dimensiones de seguridad

Tabla N° 31.Valoración de Amenazas Tipo: Instalaciones

ACTIVO/ AMENAZA	FRECUENCIA	DIMENSIONES DE SEGURIDAD				
		D	I	C	A	T
[A.26] Ataque destructivo	PF	A				

Fuente. Los autores

Tabla N° 32. Valoración de Amenazas Tipo: persona

ACTIVO/ AMENAZA	FRECUENCIA	DIMENSIONES DE SEGURIDAD				
		D	I	C	A	T
[E.7] Deficiencia en la organización.	FN	A				
[E.15] Alteración accidental de la información	FN		A			

Fuente. Los autores

4. IDENTIFICACIÓN DE LAS SALVAGUARDAS

Obtenido el nivel de criticidad de los activos incluido en el análisis de riesgos del CONCEJO DISTRITAL DE CARTAGENA DE INDIAS se realiza La caracterización de las salvaguardas basados en el catálogo de elementos que proporciona Magerit v 3.0.

4.1.1. Salvaguardas Activos:

Tabla N° 33. Salvaguardas Activos

Protecciones generales u horizontal
Control de acceso lógico H.AC
Herramienta contra código dañino
Gestión de vulnerabilidades
Protección de los datos / información
Protección de la Información
Copias de seguridad de los datos (backup)
Protección de las claves criptográficas
Gestión de claves criptográficas
Protección de los servicios
Se aplican perfiles de seguridad:
Protección De Las Aplicaciones (Software)
Cambios (Actualizaciones y mantenimiento)
Protección De Los Equipos (Hardware)
Operación
Protección De Las Comunicaciones
Internet: uso de ? acceso a

Fuente. Los autores

Dentro de las salvaguardas de protección general u horizontal se tomó Control de acceso lógico: ya que se busca proteger a los activos del tipo servicios y aplicaciones en

la dimensión de Disponibilidad, Confidencialidad y Autenticidad de los usuarios del servicio, teniendo en cuenta que mecanismos básicos, los cuales no son los ideales y pueden ser fácilmente vulnerados y la Herramienta contra código dañino con esta salvaguarda se busca proteger contra virus, sin embargo la mayoría esta desactualizado

Para salvaguardar la información se seleccionaron protección de la información y copias de seguridad la cual es necesaria para proteger y conservar la información de la entidad.

Para la protección de claves criptográficas se escogió la salvaguarda Gestión de claves Criptográficas ya que al servidor de la entidad se puede acceder fácilmente lo que lo coloca en una situación de vulnerabilidad.

Para proteger los servicios se escogió aplica perfiles de seguridad, la cual actualmente no se realiza y es necesario para afrontar amenazas como difusión de software dañino, errores de usuario.

Para la protección de las aplicaciones (Software) se tomó la salvaguarda cambios (Actualizaciones y mantenimiento) con el fin de determinar el mejoramiento y/o cambios que se realicen de acuerdo a parámetros establecidos.

Para Hardware las salvaguardas operación dado que en el Concejo Distrital de Cartagena no existen procedimientos, ni buenas prácticas para el uso de los equipos de cómputo e impresoras, el uso de estos se da de acuerdo a los conocimientos de los funcionarios y contratistas.

Para la Protección De Las Comunicaciones se tomó Internet: uso de acceso a internet con el fin de restringir el acceso a páginas que pueden afectar el buen funcionamiento de los procesos en la entidad.

4.1.2. Valoración de las salvaguardas

A través de esta valoración se determinará si las salvaguardas son eficientes

Tabla N° 34. Niveles de Madurez

Eficacia	Nivel	Madurez	Estado
0%	L0	Inexistente	inexistente
10%	L1	Inicial/ad hoc	Iniciado
50%	L2	Reproducible/ pero intuitivo	Parcialmente realizado
90%	L3	Proceso definido	En funcionamiento
95%	L4	Gestionado y medible	Monitoreado
100%	65	optimizado	Mejora continua

Fuente. Herramienta PILA 5.2.9

Tabla N° 35. Estimación de los Salvaguardas

SALVAGUARDA	EFICACIA	NIVEL DE MADUREZ	ESTADO	EVIDENCIAS
Protecciones generales u horizontal				
Control de acceso lógico H.AC	50%	Reproducible/ pero intuitivo	Parcialmente realizado	Se tiene autenticación de usuario con claves personales para los programas safe y Zeus. No se cuenta con programas de control de acceso
Herramienta contra código dañino	50%	Reproducible/ pero intuitivo	Parcialmente realizado	Todos los computadores poseen antivirus pero esta desactualizado lo que no permite una eficacia del 100%
Gestión de vulnerabilidades	10%	Inicial/ad hoc	Iniciado	Se realizó la identificación de vulnerabilidades de los sistemas pero no se ha realizado evaluación y corrección en los sistemas de información de la entidad
Protección de los datos / información				
Protección de la Información	0%	Inexistente	Inexistente	No se protege la información de interés de la entidad con ningún procedimiento, no se realizan copias de seguridad

Copias de seguridad de los datos (backup)	0%	Inexistente	Inexistente	No se han realizado copias de seguridad por parte del contratista de sistemas de la entidad
Protección de las claves criptográficas				
Gestión de claves criptográficas	10%	Inicial/ad hoc	Iniciado	La mayoría de computadores poseen claves para resguardar la información, pero las claves no cumplen los criterios de protección, ni se cambian periódicamente.
Protección de los servicios				
Se aplican perfiles de seguridad:	0%	Inexistente	Inexistente	No se aplican perfiles de seguridad
Protección De Las Aplicaciones (Software)				
Cambios (Actualizaciones y mantenimiento)	50%	Reproducible/ pero intuitivo	Parcialmente realizado	El mantenimiento y las actualizaciones de los sistemas se realizan en el momento en que son requeridos, no existe un procedimiento definido para la realización de esta función. La mayoría de las veces se realiza por daños en los computadores

Protección De Los Equipos (Hardware)				
Operación	50%	Reproducible/ pero intuitivo	Parcialmente realizado	Existe controles de acceso de físico para la protección de los equipos, no hay controles para desastres naturales y desastres del entorno. No hay procedimientos para el uso del equipo
Protección De Las Comunicaciones				
Internet: uso de ? acceso a	0%	Inexistente	Inexistente	No existe protección en las comunicaciones, no se ha implementado procedimientos para el acceso a internet, los funcionarios pueden acceder a páginas no autorizadas con facilidad.

Fuente. Los autores de acuerdo a los análisis realizados.

5. EVALUACIÓN, ESTIMACIÓN Y TRATAMIENTO DE LOS RIESGOS

De acuerdo con la valoración de los activos de información, la identificación de las amenazas se procede a evaluar el estado del riesgo, donde se estima el impacto de este sobre los activos de información.

Para la valoración del impacto y magnitud del riesgo se tomará la siguiente escala:

Tabla N° 36. Escala de magnitud del riesgo

MUY ALTO
ALTO
MEDIO
BAJO
MUY BAJO

5.1. Estimación Del Impacto

En esta actividad se determinará la magnitud del daño que se produce en los activos de información en el momento en que se materialice una amenaza, teniendo en cuenta las dimensiones analizadas como son:

Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, haciendo uso de la tabla N°24 donde se mira el impacto y degradación del activo propuestas por la metodología Magerit v.3.

Tabla N° 37. Estimación del impacto

IMPACTO		DEGRADACIÓN				
		1%	10%	50%	80%	100%
VALOR	MUY ALTO	M	A	A	MA	MA
	ALTO	B	M	M	A	A
	MEDIO	MB	B	B	MA	MA
	BAJO	MB	MB	MB	B	B
	MUY BAJO	MB	MB	MB	MB	MB

Fuente: Magerit V.3 – Libro II - Catálogo de Elementos

Tabla N° 22 Valoración impacto en activos de información

ACTIVO	AMENAZA	IMPACTO ACUMULADO					IMPACTO RESIDUAL				
		D	I	C	A	T	D	I	C	A	T
APLICACIONES INFORMATICAS	E.1] Errores de los usuarios										
	[E.2] errores del administrador										
	[E.4] Errores de configuración										
	[E.8] Difusión de software dañino										
	[E.14] Escapes de información										
	[E.18] Destrucción de información										
	[A.11] Acceso no autorizado										
	[A.15] Modificación de la información										
SERVICIOS	[I8] Fallos De comunicación										
	[E24] Caída Del sistema por agotamiento de recursos										
	[A.24] Denegación del servicio										
	[A.11] Acceso no autorizado										

ACTIVO	AMENAZA	IMPACTO ACUMULADO					IMPACTO RESIDUAL				
		D	I	C	A	T	D	I	C	A	T
REDES DE COMUNICACIONES	[N.*] Desastres Naturales										
	[[I.5] Avería de origen físico o lógico										
	[I.8] Fallo de Servicio de comunicaciones										
	[E.2] Errores del administrador										
	[A.4] Manipulación de Configuración.										
EQUIPAMIENTO INFORMATICO	[N.1] Fuego										
	[I.5] Avería de origen físico o lógico										
	[E.23] Errores de mantenimiento/ actualización de equipos (hardware)										
	[A.5] Suplantación de la identidad del usuario										
	[Acceso no Autorizado										

ACTIVO	AMENAZA	IMPACTO ACUMULADO					IMPACTO RESIDUAL				
		D	I	C	A	T	D	I	C	A	T
	[A.23] Manipulación de los equipos										
EQUIPAMIENTO AUXILIAR	[I.5] Avería de origen físico o lógico										
INSTALACIONES	[A.26] Ataque destructiva										
PERSONAL	[E.7] Deficiencia en la organización.										
	[E.15] Alteración accidental de la información										

Fuente. Los autores

5.2. Valoración del riesgo en los activos de información

Para realizar la estimación del riesgo se hace en uso de las siguientes escalas cualitativas, tomando como entradas impacto acumulado y frecuencia

Tabla N° 38. Valores de Frecuencia

VALOR			CRITERIO
100	Muy Frecuente	MF	A diario
10	Frecuente	F	Mensualmente
1	Normal	FN	Una vez al año
1/10	Poco frecuente	PF	Cada varios años

Fuente: Magerit Libro I versión 3.0.Pag 28 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Tabla N° 24. Matriz de evaluación del Riesgo

Riesgo		FRECUENCIA			
		PF	FN	F	MF
Impacto	MA	M	A	MA	MA
	A	B	A	MA	MA
	M	B	M	A	A
	B	MB	B	M	A
	MB	MB	MB	B	B

Fuente: Mejía Quijano (2013) Administración de riesgos un enfoque empresarial. Página 205.

Teniendo en cuenta la tabla N° 24 se analizan con los criterios de estimación del riesgo de acuerdo a la frecuencia en que se puede materializar la amenaza y así se podrán verificar el nivel de riesgo y se diseñarán las acciones a tomar para mitigarlos.

Tabla N° 39. Valoración de riesgo en activos de información

ACTIVO	AMENAZA	FRECUENCIA	IMPACTO			RIESGO	Medida de tratamiento
			D	I	C		
APLICACIONES INFORMÁTICAS	[E.1] Errores de los usuarios	MF					Prevenir el riesgo, proteger la empresa
	[E.2] Errores del administrador	PF					Proteger la empresa
	[E.4] Errores de configuración	FN					Prevenir el riesgo, proteger la empresa , retener las perdidas
	[E.8] Difusión de software dañino	PF					Transferir el riesgo, proteger la empresa
	[E.14] Escapes de información	F					
	[E.18] Destrucción de información	PF					Proteger la empresa
	[A.11] Acceso no autorizado	FN					Prevenir el riesgo, proteger la empresa
	[A.15] Modificación de la información	PF					Proteger la empresa
SERVICIOS	[I.8] Fallos de comunicación	F					Prevenir el riesgo
	[E.24] Caída del sistema por agotamiento de recursos	F					Prevenir el riesgo

ACTIVO	AMENAZA	FRECUENCIA	IMPACTO			RIESGO	Medida de tratamiento
			D	I	C		
	[A.11] Acceso no autorizado	F					Prevenir el riesgo
	[A.5] Suplantación de la identidad del usuario	FN					Proteger la empresa
REDES DE COMUNICACIONES	[N.*] Desastres Naturales	PF					
	[[I.5] Avería de origen físico o lógico	PF					Proteger la empresa, transferir el riesgo
	[I.8] Fallo de Servicio de comunicaciones	PF					Proteger la empresa,
	[E.2] Errores del administrador	PF					Prevenir el riesgo
	[A.4] Manipulación de Configuración.	PF					Proteger la empresa, prevenir el riesgo
EQUIPAMIENTO INFORMÁTICO	[N.1] Fuego	PF					
	[I.5] Avería de origen físico o lógico	PF					
	[E.23] Errores de mantenimiento/ actualización de equipos (hardware)	FN					Proteger la empresa
	[A.5] Suplantación de la identidad del usuario	FN					Proteger la empresa. Prevenir el riesgo

ACTIVO	AMENAZA	FRECUENCIA	IMPACTO			RIESGO	Medida de tratamiento
			D	I	C		
	[Acceso no Autorizado	FN					Proteger la empresa. Prevenir el riesgo
	[A.23] Manipulación de los equipos	FN					Proteger la empresa. Prevenir el riesgo
EQUIPAMIENTO AUXILIAR	[I.5] Avería de origen físico o lógico	PF					
INSTALACIONES	[A.26] Ataque destructivo	PF					Proteger la empresa. Prevenir el riesgo, transferir el riesgo
PERSONAS	[E.7] Deficiencia en la organización.	FN					
	[E.15] Alteración accidental de la información	FN					Proteger la empresa. Prevenir el riesgo

Fuente. Los autores

6. ANÁLISIS COSTO BENEFICIO

Teniendo en cuenta que la seguridad de la información es de gran importancia para la continuidad de las organizaciones, es necesario realizar inversiones en materia económica como también de tiempo y esfuerzo, es por esto que es necesario establecer los beneficios de implementar el sistema de gestión de seguridad de la información analizando su costo.

El costo de la inversión se toma de los valores actuales de los diferentes periodos, teniendo en cuenta las salvaguardas propuestas las cuales se centran en la modificación de procesos lo que conllevaría a la capacitación del personal, lo que la implementación se reflejaría en la mano de obra y en la adquisición o actualización de antivirus.

Para establecer los costos de la implementación del Sistema de seguridad de la información se identifica el perfil de los participantes de la implementación del sistema (descripción, responsabilidades, valor de la tarifa) y se realiza la EDT (estructura desglosada del trabajo) determinando la duración de las actividades en días se estructuro el plan de implementación, estableciendo el valor de la inversión.

Al establecer los costos del proyecto se podrá determinar los beneficios económicos de implementar las salvaguardas teniendo en cuenta que hay factores que no se miden en forma cuantitativamente, sino que se refleja en una disminución de las pérdidas que se pueden dar por incidentes de seguridad, ataques, fallas o errores.

Para valorar los beneficios que genere la implementación de las salvaguardas es necesario cuantificar la inseguridad y estimar las pérdidas de la evaluación de riesgos en un escenario sin salvaguardas y en otro con estas. El beneficio será la diferencia que surja de los dos escenarios.

Tabla N° 40. Costos de implementación del sistema de seguridad de la información Concejo Distrital de Cartagena

Actividades del SGSI	Recursos	Valor Unitario	Cantidad	Valor Total
Reuniones del Comité de seguridad y privacidad de la información	Refrigerios	50.000	10	500.000
Evaluación trimestral de riesgos y revisión de la alta dirección	Horas de trabajo participantes de evaluación y seguimiento	15.833	52	828.516
Seguimientos acciones preventivas, correctivas y lecciones aprendidas	Horas de trabajo responsable de seguimiento al sistema Capacitación de auditores internos Auditoria interna anual	15.833 1.500.000 4.0000.000	120 3 1	316.660 4.500.000 4.000.000
Administración de la documentación (actualización)	Horas de trabajo de la administración de la documentación	15.836	50	791.800
Antivirus	Compra de McAfee Antivirus Total Protección Windows-mac-ios-android Para 10 dispositivos	70.000	2	140.000
Análisis de los incidentes de seguridad	Horas de trabajo del responsable del análisis	15.833	48	759.984
Capacitación y sensibilización en seguridad de la información	Horas de trabajo de la capacitación y de los participantes (grupo de 50 personas) / divulgación (por un año) Papelería	2.500.000 500.000	1	2.500.000
Diagnóstico de plataforma tecnológica	Pruebas de penetración interna o externa	12.000.000	1	12.000.000
			TOTAL	$26.336.960

Fuente. El costo unitario de la hora de trabajo de los funcionarios que participan en las actividades fue solicitado a la dirección administrativa del Concejo Distrital de Cartagena, valor del antivirus cotizado y del diagnóstico de pruebas externa e interna.

Con el fin de medir el impacto que se genera al materializar una amenaza es imprescindible tener en cuenta el mayor número de aspectos implicados en la recuperación. (Sánchez Nicolás, Segura Juan (2006)). En la siguiente tabla se observan los factores que se deben tener en cuenta para calcular los costos de la materialización de las amenazas.

Tabla N° 41. Factores que afectan el Costo de Impacto de Riesgos

Costos de impacto de riesgos	Factores que afectan los costos
Inactividad organizacional	Porcentaje de actividades paralizadas debido al evento
	Número de funcionarios que ven afectadas sus actividades por el evento
	Costo de pérdida de productividad organizacional por hora
Costo de recuperación	Costo por hora de los empleados que se requieran para el restablecimiento de los sistemas afectados
	Tiempo estimado de recuperación (tiempo de recuperación de la información perdida)
	Recuperación de daños causados o equipos o infraestructuras físicas afectadas
Otras perdidas	Perdida irrecuperable de información critica
	Costos por posibles daños a terceros
	Pérdida de imagen organizacional

Fuente. Tomado de Una Guía metodológica para el cálculo del retorno a la Inversión (ROI) Sánchez Nicolás, Segura Juan (2006)

Realizando indagaciones con el contratista del área de sistemas, el director administrativo y el director financiero del Concejo Distrital de Cartagena teniendo en cuenta la valoración de riesgos efectuada se estableció el impacto monetario si se materializa el riesgo sobre los activos de acuerdo a la siguiente escala de impacto económico:

Tabla N° 42. Escala de impacto económico

Nivel de riesgo	CONSECUENCIAS ECONÓMICAS
MA	Más de 10,000,000
A	Entre 5,000,001 y 10,000,000
M	Entre 1,000,001 y 5,000,000
B	entre 500.000 y 1.000,000
MB	menor de 500.000

Fuente. Los autores

Tabla N° 43. Beneficio de la implementación de las salvaguardas

Pérdidas totales por incidentes sin tratar con las salvaguardas propuestas	**6.461.088**
Pérdidas totales por incidentes mitigados con las salvaguardas propuestas	**2.153.696**
Beneficio o ahorro bruto anual generado por las salvaguardas propuestas en el proyecto	**4.307.392**

Fuente. Los autores de acuerdo a análisis realizado en base a la tabla N°28 y entrevistas

En la tabla N° 43 se puede observar que la implementación de las salvaguardas en un incidente de seguridad implica un ahorro significativo por lo tanto es de gran importancia que estos se implementen para la protección de los activos de información de la empresa.

7. MÉTRICAS E INDICADORES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN.

Para el Gobierno Nacional y para las entidades públicas es de gran importancia garantizar sistemas de información en sus entidades, confiables, íntegros y auténticos que protejan el activo más importante que tienen que es la información de ahí la importancia del Diseño del Modelo de seguridad y privacidad de la Información que busca proteger estos activos permitiendo a la organización la permanencia en el mercado.

Teniendo en cuenta que la información es de vital importancia para el logro de los objetivos estratégicos de la entidad, resulta necesario que a la alta dirección le sea proporcionada información necesaria para lograr este cometido.

El Concejo Distrital de Cartagena no es la excepción de ahí la importancia de desarrollar unas métricas o indicadores que nos permitirán monitorear en forma permanente la eficiencia eficacia y operatividad de los distintos componentes del modelo de seguridad y privacidad de la información. Esto permite tener un panorama clave a la hora de la toma de decisiones estratégicas sobre los posibles riegos que puedan presentarse. Para cumplir con este requerimiento se han elaborado los siguientes indicadores que servirán de insumo para mejorar continuamente y tomar las mejores decisiones permitiendo a la entidad contar con un sistema de información adecuado, seguro y confiable.

Tabla N° 44. Métricas del Sistema de seguridad y privacidad de la información

Nombre Indicador	Objetivo	Tipo de Indicador	Forma de calculo	Frecuencia de medida	Responsable	Meta
Funcionarios de la dependencia de dirección financiera que conocen la Política de seguridad de la información	Implementar una política de seguridad de la información, que sea conocida por todos los funcionarios, contratistas, proveedores y terceros involucrados en los procesos tecnológicos dentro de la dependencia.	Estratégico Cumplimiento	Número de Funcionarios del área de financiera que conocen la política de seguridad de la información	semestral	Tomas Romero – Director Financiero	80%
Funcionarios y contratistas de la dependencia Financiera que conocen las políticas de seguridad de la información	Implementar una política de seguridad de la información, que sea conocida por todos los funcionarios, contratistas, proveedores y terceros involucrados en los procesos tecnológicos dentro de la dependencia	Estratégico	Funcionarios y contratista del área de dirección financiera que cumplen la política de seguridad de la información	Trimestral	Oficina Asesora de control Interno	90%
Colaboradores capacitados y concientizados	Capacitar y concientizar a los funcionarios y contratista involucrados en	Estratégico	Número de Funcionarios y/o contratistas capacitados y concientizados/	Trimestral	Talento Humano	100%

Nombre Indicador	Objetivo	Tipo de Indicador	Forma de calculo	Frecuencia de medida	Responsable	Meta
	el manejo de los sistemas de información del área financiera en temas de seguridad		número total de funcionarios			
Porcentaje de riesgos de seguridad de la información para los cuales se han implantado totalmente controles satisfactoriOS.	Evaluar los riesgos de la seguridad de los sistemas de información del área financiera y decidir medidas de tratamiento.	Estratégicos	Numero de riesgos SGI con controles satisfactorios/ número de riesgos de SGI	Bimestral	Oficina De Dirección administra uva	100%
Procedimientos necesarios SGSI documentados, controlados y sensibilizados	Gestionar, documentar y controlar el 100% de los documentos del SGSI	Estratégicos	N° Procedimientos SGSI estandarizados, documentados y sensibilizados/N° Total de requisitos	Semestral	Tecnología de Información	80%
Cumplimiento de los procedimientos documentados, controlados y sensibilizados	Gestionar, documentar y controlar el 100% de los documentos del SGSI	Estratégicos	N° Cumplimiento de procedimientos estandarizados, documentados y sensibilizados/N° Total de procedimiento	Semestral	Tecnología de la información	90%
Conocer el nivel de implementación de los controles de la declaración de aplicabilidad.	Conocer el nivel de implementación de los controles de la declaración de aplicabilidad	Estratégica	controles implementados / Cantidad de controles seleccionados	Anual	Directora financiera	85%

Nombre Indicador	Objetivo	Tipo de Indicador	Forma de calculo	Frecuencia de medida	Responsable	Meta
Costo promedio de solución por incidente	Conocer por parte de la Alta dirección el valor promedio de los costos de los incidentes y lograr disminuir este en un 70%	Estratégico	Costo de la solución de seguridad anualizado / costo de incidentes reales en el año * 365	Anual	Alta dirección	70%
Gestión de riesgos	Administrar los riesgos a los sistemas de información reduciéndolos al 60%	Estratégicos	Número de procedimientos de riesgos programados / procedimientos de riesgos ejecutados	Mensual	Área de Tecnología	60%
Incidentes de seguridad	Administrar y monitorear los incidentes y vulnerabilidades de los sistemas de información del área reduciéndolos mínimo al 85%	Operativo	Cantidad de incidentes de seguridad reportados / cantidad de incidentes de seguridad gestionados	Trimestral	Tecnología	85%
Incidentes atendidos oportunamente	Administrar y monitorear los incidentes y vulnerabilidades de los sistemas de información del área reduciéndolos mínimo al 85%	Operativo	Número de incidentes atendidos oportunamente/ número de incidentes	Mensual	Gerencia de sistemas	90%
Vulnerabilidades atendidos oportunamente	Administrar y monitorear los incidentes y vulnerabilidades de los sistemas	táctico	Número de vulnerabilidades atendidas oportunamente/	Mensual	Gerencia de sistemas	90%

Nombre Indicador	Objetivo	Tipo de Indicador	Forma de calculo	Frecuencia de medida	Responsable	Meta
	de información del área reduciéndolos mínimo al 85%		número de vulnerabilidades			
Activos de información (Zeus nomina- sistema contable, etc.) sin mecanismos de control	Implementar medidas de seguridad para mitigar los riesgos, ejecutar los controles para el tratamiento de riesgos reduciéndolo al 95% dentro de los niveles aceptables	Tácticos	N° de activos sin control/ N total de activos	Semestral	Dirección financiera	95%
Porcentaje de virus detectados y eliminados oportunamente	Verificar la instalación de programas maliciosos con el fin de reducir las incidencias a los sistemas de información del área financiera con el fin de disminuir al 60%	Táctico	Numero de programas maliciosos eliminados /Número de programas maliciosos detectados (virus, antispyware.	Mensual	Área de tecnología (dirección Administrativa)	60%
Vulnerabilidades reportadas adecuadamente	Administrar y monitorear los incidentes y vulnerabilidades de los sistemas de información del área reduciéndolos mínimo al 85%	táctico	Numero de vulnerabilidades reportadas adecuadamente/ total vulnerabilidades	Mensual	Infraestructura y tecnología (dirección Administrativa)	90%
Seguridad física y ambiental	Conocer el nivel de	Operativo	Número de controles	Anual	Ingreso y salida portería	80%

Nombre Indicador	Objetivo	Tipo de Indicador	Forma de calculo	Frecuencia de medida	Responsable	Meta
	implementación de los controles a nivel físico y ambiental de las sedes y personas		propuestos / Número de controles implementados			
Control de acceso	Conocer el nivel de implementación del control de acceso en las redes, sistemas de información y sitios Web.	Operativo	Número de controles propuestos / Número de controles implementados	Anual	Área de sistemas	80%
Controles criptográficos	Conocer el nivel de implementación de los controles criptográficos y la protección general sitios Web y banca electrónica.	Táctico	Controles criptográficos propuestos / controles implementados	Semestral	Área de sistemas – Auditoria de sistemas (dirección Administrativa)	75%
Protección contra software malicioso	Medir la efectividad del sistema contra código malicioso	Operativo	Cantidad de incidentes reportados por software malicioso / cantidad de ataques detectados y bloqueados.	Mensual	Área de sistemas (dirección Administrativa)	90%
Análisis de vulnerabilidades	Conocer el nivel de seguridad en las aplicaciones y redes de datos.	Operativo	Cantidad de hallazgos encontrados en los análisis / Cantidad de vulnerabilidades mitigadas	Semestral	Área de sistemas(dirección Administrativa)	75%
Mantenimiento de equipos	Vigilar que se realicen los	Operativo	Mantenimientos preventivos al	Trimestral	Área de sistemas	95%

Nombre Indicador	Objetivo	Tipo de Indicador	Forma de calculo	Frecuencia de medida	Responsable	Meta
	mantenimientos preventivos adecuados para garantizar la operación		equipo informático realizados/ mantenimientos preventivos al equipo informático programado		(dirección Administrativa)	

Fuente. Los autores

4. RECOMENDACIONES

Es necesario implementar el Sistema de Gestión de la Seguridad de la información para proteger los activos especialmente el más importante “la información” para esto es necesario contar con personal experto en el área de manera permanente.

De igual manera es necesario que la entidad desarrolle controles para mitigar los riesgos de seguridad y privacidad de la información.

Capacitar al personal de sistemas en temas de seguridad informática y estos a su vez capaciten a todos los funcionarios de la entidad, además se debe adoptar y socializar la política de seguridad informática con el fin de mejorar las prácticas en los sistemas de información.

Es necesario que dentro de la Oficina Asesora de Control Interno se incluya una persona experta en el área con el fin de realizar auditorías permanentes a los activos de información para actualizar controles y contribuir con el desarrollo de mejores prácticas relacionadas con la seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

- Gobierno de España, (2012) MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WSNGX5KGOvE

- Sánchez Nicolás, Segura Juan (2006). Una guía metodológica para el cálculo del retorno a la inversión (ROI) en seguridad informática. Un caso de estudio recuperado de http://escuelainformatica.uniacc.cl/wordpress/wp-content/uploads/2013/12/ROIs.pdf