CENTRO DE DIAGNOSTICO AUTOMOTOR DE CUCUTA LIMITADA- CEDAC

PLAN DE VALORIZACION Y TRATAMIENTO DE RIESGOS DE SEGURIDAD

CUCUTA 2024

INTRODUCCION

La entidad maneja un activo de vital importancia para su funcionamiento que es la información, a diario las bases de datos del CEDAC se incrementan considerablemente y se hace de vital importancia proteger esta información contra alteraciones, robo, borrado o incluso divulgación no autorizada que pueda poder en riesgo la imagen de la empresa o causarle una perdida económica, por esto es muy importante realizar una adecuada evaluación de los riesgos que puedan tener los activos de información.

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación[1]:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 1. Criterios de Clasificación
Fuente: Guía gestión del riesgo SEGURIDAD Y PRIVACIDAD DE LA INFORMACION Min TIC

[1] Guía gestión del riesgo SEGURIDAD Y PRIVACIDAD DE LA INFORMACION Min TIC

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 2. Niveles de Clasificación

Fuente: Guía gestión del riesgo SEGURIDAD Y PRIVACIDAD DE LA INFORMACION Min TIC.

OBJETIVO

- Generar un procedimiento que sirva como guía, el cual permita describir la metodología y actividades para la identificación de amenazas, análisis y valoración de riesgos de seguridad de la información en el CEDAC.

- Determinar las salvaguardas adecuados siguiendo la metodología Magerit de acuerdo a las amenazas identificadas en los activos y la valoración del riesgo de cada una de estas

METODOLOGÍA

Para desarrollar este trabajo se va a utilizar la Metodología MAGERIT, la cual contempla las siguientes etapas:

ETAPA 1. Caracterización de Activos

ACTIVIDAD 1.1 Identificación de Activos
ACTIVIDAD 1.2 Dependencia entre activos
ACTIVIDAD 1.3 Valoración de activos

ETAPA 2. Caracterización de las amenazas

ACTIVIDAD 2.1 Identificación de las amenazas
ACTIVIDAD 2.2 Valoración de las amenazas

ETAPA 3. Caracterización de las salvaguardas

ACTIVIDAD 3.1 Identificación de las salvaguardas pertinentes
ACTIVIDAD 3.2 Valoración de las salvaguardas

ETAPA 4. Estimación del estado del riesgo

ACTIVIDAD 4.1 Estimación del Impacto
ACTIVIDAD 4.2 Estimación del riesgo

IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS

Tabla 3 IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS

GRUPO MAGERIT	NOMBRE DEL ACTIVO	CÓDIGO
SERVICIOS INTERNOS [SERVICE]	Internet	[INTERNET]
	TNS	[TNS]
	NUBE	[NB]
	NAS	[NAS]
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema	[PASSWORD]
	Copias de Seguridad	[BACKUP]
SOFTWARE [SW]	Antivirus	[AV]
	Office	[OFFICE]
	SART	[SART]
	Sistema operativo	[SO]
HARDWARE [HW]	Equipos de Escritorio	[PC]
	Equipos Portátiles	[MOBILE]
	Servidores	[SRV]
	Impresoras	[PRINT]
	Routers	[ROUTER]
	Celulares	[CEL]
	Switch	[SWITCH]

SOPORTES DE INFORMACIÓN [MEDIA]	Discos Duros Extraíbles	[BACKUP]
	USB	[USB]
	Material Impreso	[VR]
EQUIPAMIENTO AUXILIAR [AUX]	UPS	[UPS]
	Aires Acondicionados	[AC]
	Rack	[RACK]
	Cableado	[CABLING]
REDES DE COMUNICACIONES [COM]	Red Local	[LAN]
	Red Inalámbrica	[WIFI]
INSTALACIONES [L]	Edificio	[BUILDING]
PERSONAL [P]	Funcionarios	[FU]
	Contratistas	[CT]
	Administrador de Sistemas	[ADM]

Tabla 3: Listado de activos del CEDAC según clasificación MAGERIT

Dependencia entre los activos

El objetivo de esta tarea es determinar la dependencia entre los activos más importantes de la organización. Cuando se habla de dependencia, quiere decir que en el momento en que una amenaza sea materializada en un activo inferior, pueda afectar a un activo de orden superior.

Para la empresa es de suma importancia el servicio de internet y el software de revisión técnico mecánica, ya que sin ellos no se podría llevar a cabo el objetivo misional de la entidad que es el de realizar la revisión técnico mecánica y emisiones contaminantes.

Los documentos impresos en su mayor parte hacen parte del sistema de calidad, facturación y contratación que constituyen un nivel superior, puesto que son de vital importancia para la entidad.

Los activos de bajo nivel son todos los equipos de comunicación como central telefónica, teléfonos, radios, ya que en caso de que alguno de estos falle no representa un cese de la actividad, la empresa podría seguir prestando sus servicios.
Cabe resaltar que los activos de información de la entidad se encuentran contenidos dentro de la misma edificación, la cual cuenta con seguridad para el control, de acceso de personas ajenas a la empresa.

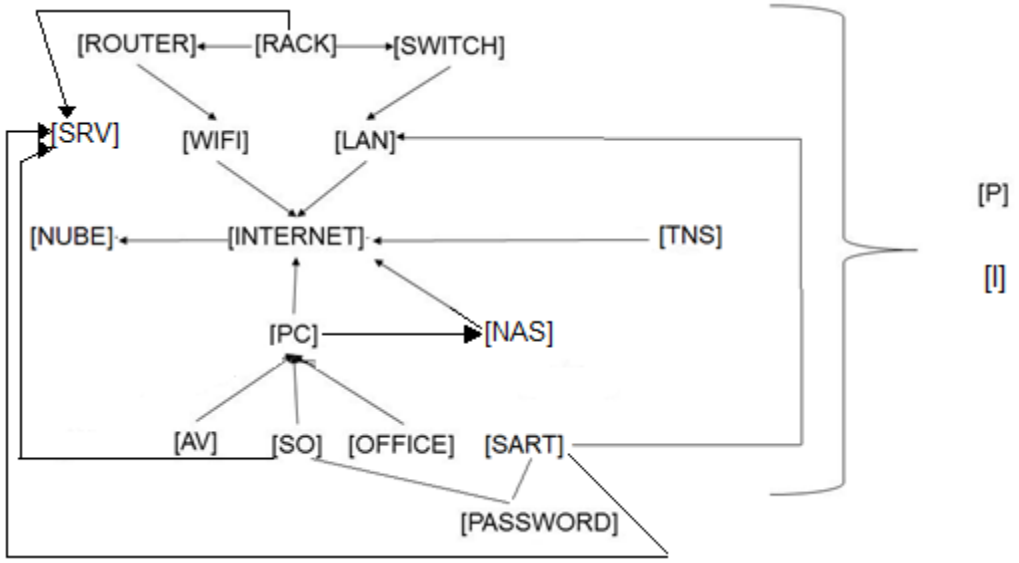

Imagen 1: Dependencia entre activos
Fuente: El autor

Valoración de los activos

El objetivo de esta tarea es determinar la valoración de cada activo de información importante de la organización, con respecto a las dimensiones disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Es decir, que se evalúa cada activo sobre las características mencionada anteriormente.

Los criterios de valoración a tener en cuenta, son los establecidos en Magerit Versión 3 – Catalogo de Elementos:

VALOR		CRITERIO
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a factores prácticos

Tabla 4. Criterios de Valoración
Fuente: Magerit V3 Catálogo de Elementos

Dimensiones de Valoración:

- Disponibilidad [D]
- Integridad [I]
- Confidencialidad [C]
- Autenticidad [A]
- Trazabilidad [T]

GRUPO DE ACTIVO	ACTIVO	DIMENSIONES				
		[I]	[C]	[D]	[T]	[A]
SERVICIOS INTERNOS [SERVICE]	Internet [INTERNET]			10	10	10
	TNS[TNS]			3	3	3
	NUBE[NB]			8		
	NAS[NAS]	10	10	10	10	10
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema [PASSWORD]	7	10			9
	Copias de Seguridad [BACKUP]	10	10	7		
SOFTWARE [SW]	Antivirus [AV]			7		
	Office [OFFICE]			7		
	Sistema Operativo [SO]			7		
	SART [SART]			10		
HARDWARE [HW]	Equipos de Cómputo [PC]	6	3	7		
	Equipos Portátiles [MOBILE]	3	3	3		
	Impresoras [PRINT]			5		
	Routers [ROUTER]			10		7
	Switch [SWITCH]			10		
	Servidores [SRV]	7		10		
SOPORTES DE INFORMACIÓN [MEDIA]	Material Impreso [VR]	3	7	3		
	Discos Duros Extraíbles [BACKUP]	7	7	8		
EQUIPAMIENTO AUXILIAR [AUX]	UPS [UPS]			3		
	Aires Acondicionados [AC]			1		
	Rack [RACK]			6		
	Cableado [CABLING]			7		
	Red Inalámbrica [WIFI]			3		

REDES DE COMUNICACIONES [COM]	Red Local [LAN]			8		
INSTALACIONES [I]	Edificio [BUILDING]			10		
PERSONAL [P]	Funcionarios [FU]		6	3		
	Contratistas [CT]		6	3		
	Administrador de Sistemas [ADM]		8	4		

Tabla 5. Valoración de los activos de información más relevantes de la institución
Fuente: Autor

Identificación de amenazas significativas

Para esta actividad se tiene como objetivo la caracterización de las amenazas, identificación y valoración de las mismas.

Para ello se tendrá en cuenta el catálogo de amenazas establecidas en Magerit Versión 3, Catálogo de Elementos.

Caracterización de Amenazas

Según Magerit Versión 3, las amenazas se clasifican en cuatro categorías:

- Desastres naturales [N]
- De origen Industrial [I]
- Errores y fallos no intencionados [E]
- Ataques Intencionados [A]

Identificación de Amenazas

El objetivo de esta tarea es identificar las amenazas más relevantes que pueden afectar a los activos más representativos de la organización.

GRUPO DE ACTIVO	GRUPO DE ACTIVO	GRUPO DE ACTIVO
SERVICIOS INTERNOS [SERVICE]	Internet [INTERNET]	A.7 Uso no previsto A.24 Denegación del servicio
	TNS[TNS]	E.1 Errores de los usuarios. A.15 Modificación deliberada de la información.
	NUBE[NB]	A.7 Uso no previsto A.24 Denegación del servicio
	NAS[NAS]	A.5 Suplantación de identidad del usuario. A.7 Uso no previsto A.24 Denegación del servicio I.5 Avería de origen físico o lógico N.1 Fuego
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema [PASSWORD]	A.5 Suplantación de identidad del usuario.
	Copias de Seguridad [BACKUP]	E.19 Fugas de Información. A.7 Uso no previsto
SOFTWARE [SW]	Antivirus [AV]	E.8 Difusión de software dañino. E.20 Vulnerabilidades de los programas (software).
	Office [OFFICE]	I.5 Avería de origen físico o lógico. E.20 Vulnerabilidades de los programas (software). E.21 Errores de mantenimiento / actualización de programas (software).
	Sistema Operativo [SO]	I.5 Avería de origen físico o lógico. E.20 Vulnerabilidades de los programas (software).

		E.21 Errores de mantenimiento / actualización de programas (software).
	SART [SART]	E.20 Vulnerabilidades de los programas (software). E.21 Errores de mantenimiento / actualización de programas (software).
HARDWARE [HW]	Equipos de Cómputo [PC]	N.1 Fuego N.2 Daños por agua I.5 Avería de origen físico o lógico. I.6 Corte del suministro eléctrico. E.23 Errores de mantenimiento / actualización de equipos (hardware).
	Equipos Portátiles [MOBILE]	I.5 Avería de origen físico o lógico. E.23 Errores de mantenimiento / actualización de equipos (hardware).
	Impresoras [PRINT]	I.5 Avería de origen físico o lógico. I.6 Corte del suministro eléctrico.
HARDWARE [HW]	Routers [ROUTER]	N.1 Fuego N.2 Daños por agua I.5 Avería de origen físico o lógico. I.6 Corte del suministro eléctrico. A.11 Acceso no autorizado.
	Switch [SWITCH]	N.1 Fuego

		N.2 Daños por agua I.5 Avería de origen físico o lógico. I.6 Corte del suministro eléctrico. A.11 Acceso no autorizado.
	Servidores[SRV]	N.1 Fuego N.2 Daños por agua I.5 Avería de origen físico o lógico. I.6 Corte del suministro eléctrico. E.23 Errores de mantenimiento / actualización de equipos (hardware).
SOPORTES DE INFORMACIÓN [MEDIA]	Material Impreso [VR]	N.* Desastres naturales. E.1 Errores de los usuarios.
	Discos Duros Extraíbles [BACKUP]	I.5 Avería de origen físico o lógico. E.19 Fugas de información. E.25 Pérdida de equipos.
EQUIPAMIENTO AUXILIAR [AUX]	UPS [UPS]	I.* Desastres industriales
	Aires Acondicionados [AC]	I.* Desastres industriales. I.6 Corte del suministro eléctrico.
	Rack [RACK]	I.* Desastres industriales. I.6 Corte del suministro eléctrico. A.11 Acceso no autorizado.
	Cableado [CABLING]	I.* Desastres industriales A.25 Robo
REDES DE COMUNICACIONES [COM]	Red Inalámbrica [WIFI]	I.8 Fallo de servicios de comunicaciones. A.11 Acceso no autorizado. A.24 Denegación del servicio

	Red Local [LAN]	I.8 Fallo de servicios de comunicaciones.
INSTALACIONES [I]	Edificio [BUILDING]	N.* Desastres naturales.
PERSONAL [P]	Funcionarios[FU]	E.28 Indisponibilidad del personal. A.30 Ingeniería Social.
	Contratistas[CT]	E.28 Indisponibilidad del personal. A.30 Ingeniería Social.
	Administrador de Sistemas [ADM]	E.28 Indisponibilidad del personal. A.30 Ingeniería Social.

Tabla 6. Identificación de amenazas por cada uno de los activos de información.
Fuente: Autor

Valoración del riesgo

El objetivo de esta tarea, es determinar la probabilidad de ocurrencia de las amenazas identificadas con respecto a cada activo, y especificar la degradación que podría causar la amenaza en cada una de las dimensiones del activo, si ésta se llegara a materializar.

Para evaluar la probabilidad de ocurrencia de cada amenaza, se tendrá en cuenta los siguientes criterios:

VALOR CUALITATIVO	FRECUENCIA	DESCRIPCIÓN
CS	A Diario	Casi Seguro
MA	Cada Semana	Muy Alto
P	Cada 2 o 3 meses	Posible
PP	Cada Año	Poco Probable
MB	Cada Varios Años	Muy Baja
MR	Cada Siglo	Muy Rara

Tabla 7. Probabilidad de Ocurrencia
Fuente: Autor

VALOR CUALITATIVO	DEGRADACIÓN	DESCRIPCIÓN
MA	Desastroso	Muy Alta

A	Mayor	Alta
M	Moderado	Media
B	Menor	Baja
MB	Insignificante	Muy Baja

Tabla 8. Degradación del activo de información
Fuente: Autor

ACTIVOS	AMENAZA	P	DIMENSION				
			[I]	[C]	[D]	[T]	[A]
SERVICIOS INTERNOS [SERVICE]							
Internet [INTERNET	A.7 Uso no previsto	**PP**	**-**	**-**	**B**	**-**	**-**
	A.24 Denegación del servicio	PP	-	-	A	-	-
TNS[TNS]	E.1 Errores de los usuarios.	PP	A	A	-	A	-
	A.15 Modificación deliberada de la información.	PP	A	A	-	A	-
NUBE[NB]	A.24 Denegación del servicio	PP	-	-	B	-	-

Tabla 9: SERVICIOS INTERNOS [SERVICE]
Fuente: Autor

ACTIVOS	AMENAZA	P	DIMENSION				
			[I]	[C]	[D]	[T]	[A]
DATOS O INFORMACIÓN [D]							
Contraseñas de acceso al sistema [PASSWORD]	A.5 Suplantación de identidad del usuario.	PP	A	A	-	-	-

Copias de Seguridad [BACKUP]	E.19 Fugas de Información	PP		A	-	-	-
	A.7 Uso no previsto	PP	A	A	-	-	-

Tabla 10: DATOS O INFORMACIÓN [D]
Fuente: Autor

ACTIVOS	AMENAZA	P	DIMENSION				
			[I]	[C]	[D]	[T]	[A]
SOFTWARE [SW]							
Antivirus [AV]	E.8 Difusión de software dañino.	**PP**	**-**	**-**	**A**	**-**	**-**
	E.20 Vulnerabilidades de los programas (software).	PP	A	-	A	-	-
Office [OFFICE]	I.5 Avería de origen físico o lógico	PP	-	-	B	-	-
	E.20 Vulnerabilidades de los programas (software).	PP	-	-	B	-	-
	E.21 Errores de mantenimiento / actualización de programas (software).	PP	-	-	B	-	-
Sistema Operativo [SO]	A.24 Denegación del servicio	PP	-	-	B	-	-
SART [SART]	E.20 Vulnerabilidades de los programas (software).	PP	-	-	A	-	-
	E.21 Errores de mantenimiento / actualización de programas (software).	PP	-	-	A	-	-

Tabla 11: SOFTWARE[SW]

Fuente: Autor

ACTIVOS	AMENAZA	P	DIMENSION				
			[I]	[C]	[D]	[T]	[A]
HARDWARE [HW]							
Equipos de Cómputo [PC]	N.1 Fuego	PP	-	-	A	-	-
	N.2 Daños por agua	PP	-	-	A	-	-
	I.5 Avería de origen físico o lógico.	pp	-	-	A	-	-
	I.6 Corte del suministro eléctrico.	P	-	-	A	-	-
	E.23 Errores de mantenimiento / actualización de equipos (hardware).	P	B	-	M	-	-
Equipos Portátiles [MOBILE]	I.5 Avería de origen físico o lógico.	PP	-	-	B	-	-
	E.23 Errores de mantenimiento / actualización de equipos (hardware).	PP	-	-	B	-	-
Impresoras [PRINT]	I.5 Avería de origen físico o lógico.	P			B		
	I.6 Corte del suministro eléctrico.	P	-	-	B	-	-
Routers [ROUTER]	N.1 Fuego	MR	-	-	A	-	-
	N.2 Daños por agua	MR	-	-	A	-	-
	I.5 Avería de origen físico o lógico.	PP	-	-	A	-	-

	I.6 Corte del suministro eléctrico.	P	-	-	M	-	-
	A.11 Acceso no autorizado.	PP	A	A	-	-	-
Switch [SWITCH]	N.1 Fuego	MR	-	-	A	-	-
	N.2 Daños por agua	MR	-	-	A	-	-
	I.5 Avería de origen físico o lógico.	PP	-	-	A	-	-
Switch [SWITCH]	I.6 Corte del suministro eléctrico.	P	-	-	M	-	-
	A.11 Acceso no autorizado.	PP	A	A	-	-	-
Servidores[SRV]	N.1 Fuego	MR	-	-	A	-	-
	N.2 Daños por agua	MR	-	-	A	-	-
	I.5 Avería de origen físico o lógico.	PP	-	-	A	-	-
	I.6 Corte del suministro eléctrico.	P	-	-	M	-	-
	E.23 Errores de mantenimiento / actualización de equipos (hardware).	PP	-	-	A	-	-

Tabla 12: HARDWARE [HW]

Fuente: Autor

ACTIVOS	AMENAZA	P	DIMENSION				
			[I]	[C]	[D]	[T]	[A]
SOPORTES DE INFORMACIÓN [MEDIA]							
Material Impreso [VR]	**N.* Desastres naturales.**	**MR**	**A**	**-**	**A**	**-**	**-**
	E.1 Errores de los usuarios	PP	A	A	A	-	-
Copias de Seguridad [BACKUP]	E.19 Fugas de Información	MR	-	-	A	-	-
	A.7 Uso no previsto	MR	-	A	-	-	-

Tabla 13: SOPORTES DE INFORMACIÓN [MEDIA]
Fuente: Autor

ACTIVOS	AMENAZA	P	DIMENSION				
			[I]	[C]	[D]	[T]	[A]
EQUIPAMIENTO AUXILIAR [AUX]							
UPS [UPS]	I.* Desastres industriales	MR	-	-	A	-	-
Aires Acondicionados [AC]	I.* Desastres industriales.	MR	-	-	MB	-	-
	I.6 Corte del suministro eléctrico.	P	-	-	B	-	-
Rack [RACK]	I.* Desastres industriales.	MR	-	-	A	-	-
	I.6 Corte del suministro eléctrico.	P	-	-	A	-	-
	A.11 Acceso no autorizado.	PP	-	B	B	-	-

Cableado [CABLING]	I.* Desastres industriales	MR	-	-	A	-	-

Tabla 14: EQUIPAMIENTO AUXILIAR [AUX]
Fuente: Autor

ACTIVOS	AMENAZA	P	DIMENSION				
			[I]	[C]	[D]	[T]	[A]
REDES DE COMUNICACIONES [COM]							
Red Inalámbrica [WIFI]	I.8 Fallo de servicios de comunicaciones.	MR	-	-	A	-	-
	A.11 Acceso no autorizado.	MR	-	A	B	-	-
	A.24 Denegación del servicio	P	-	-	A	-	-
Red Local [LAN]	I.8 Fallo de servicios de comunicaciones.	MR			A		

Tabla 15: REDES DE COMUNICACIONES [COM]
Fuente: Autor

ACTIVOS	AMENAZA	P	DIMENSION				
			[I]	[C]	[D]	[T]	[A]
INSTALACIONES [I]							
Edificio [BUILDING]	N.* Desastres naturales.	MR			A		

Tabla 16: INSTALACIONES [I]
Fuente: Autor

ACTIVOS	AMENAZA	P	DIMENSION				
			[I]	[C]	[D]	[T]	[A]
PERSONAL [P]							
Funcionarios[FU]	E.28 Indisponibilidad del personal.	P			B		
	A.30 Ingeniería Social.	P	A	A	A		
Contratistas[CT]	E.28 Indisponibilidad del personal.	P			B		
	A.30 Ingeniería Social.	P	A	A	A		
Administrador de Sistemas [ADM]	E.28 Indisponibilidad del personal.	P			M		
	A.30 Ingeniería Social.	MR	A	A	A		

Tabla 17: PERSONAL [P]
Fuente: Autor

DETERMINACIÓN DE SALVAGUARDAR PARA LA MITIGACIÓN DE LOS RIESGOS

Esta actividad es de suma importancia ya que con ellos se pretende gestionar aquellos activos que son críticos para el correcto funcionamiento de la entidad y establecer unas salvaguardas que ayuden a mitigar los riesgos de seguridad de la información.

Esta actividad constituye de dos tareas, la identificación de salvaguardas eficaces para la organización y la valoración de estas salvaguardas.

La identificación de salvaguardas se hace con base en la investigación e identificación anterior de los riesgos potenciales y se tiene en cuenta el libro Magerit Versión 3. Catálogo de Elementos.

Tabla 18: identificación de salvaguardas

SALVAGUARDA: Protecciones generales u horizontales [H.tools.AV] Herramienta contra código dañino	
JUSTIFICACIÓN: Se deben proteger los equipos de cómputo contra cualquier código malicioso, con lo cual se cuenta con un antivirus licenciado Kaspersky Small office,e cual cuenta con protección incluso contra Ramsonwere.	
ACTIVOS EN LOS QUE SE APLICA: □ Software [SW]	**DIMENSIONES:** □ Disponibilidad □ Integridad
AMENAZAS MITIGADAS: □ E.8 Difusión de software dañino. □ E.20 Vulnerabilidades de los programas (software). □ E.21 Errores de mantenimiento / actualización de programas (software). □ I.5 Avería de origen físico o lógico.	
SALVAGUARDA: Protección de los datos/información [D] Copias de Seguridad de los datos (backup).	
JUSTIFICACIÓN: Siendo que para la entidad los datos correspondientes a las revisiones técnico mecánicas, de vital importancia, al igual que toda la información generada del Sistema de Gestión de Calidad, contratación y contabilidad se escogió esta salvaguarda ya que se debe asegurar que la información de los backup generados no se pierda y se resguarde adecuadamente.	
ACTIVOS EN LOS QUE SE APLICA: □ Datos o Información [D]	**DIMENSIONES:** □ Confidencialidad □ Integridad
AMENAZAS MITIGADAS: □ E.19 Fugas de Información. □ A.7 Uso no previsto.	

SALVAGUARDA: Protección de los Servicios [S.A] Aseguramiento de la disponibilidad	
JUSTIFICACIÓN: Esta salvaguarda permite que el servicio que presta la entidad, no se vea afectado por falta de conexión al RUNT o a cualquiera de los sistemas que dependen de internet	
ACTIVOS EN LOS QUE SE APLICA: □ Redes de Comunicaciones [COM]	**DIMENSIONES:** □ Disponibilidad
AMENAZAS MITIGADAS: □ I.8 Fallo de servicios de comunicaciones □ A.24 Denegación del servicio	

SALVAGUARDA: Protección de los equipos [HW] Protección de los equipos informáticos	
JUSTIFICACIÓN: Esta salvaguarda se toma ya que es indispensable proteger los equipos de cómputo así como router o switches del acceso de cualquier persona que pueda alterar su configuración.	
ACTIVOS EN LOS QUE SE APLICA: □ Hardware [HW] □ Equipamiento auxiliar [AUX]	**DIMENSIONES:** □ Integridad □ Disponibilidad
AMENAZAS MITIGADAS: □ A.11 Acceso no autorizado.	
SALVAGUARDA: Protección de los equipos [HW.CM] Cambios (actualizaciones y mantenimiento)	
JUSTIFICACIÓN: Esta salvaguarda responde a la necesidad de proteger los equipos de daños por falta de mantenimiento o por condiciones inadecuadas de las instalaciones.	
ACTIVOS EN LOS QUE SE APLICA: □ Hardware [HW] □ Equipamiento Auxiliar [AUX]	**DIMENSIONES:** □ Integridad □ Disponibilidad
AMENAZAS MITIGADAS: □ N.2 Daños por agua.	

□ I.5 Avería de origen lógico o físico. □ E.253 Errores de mantenimiento / actualización de equipos (hardware).

SALVAGUARDA: Protección de las comunicaciones [COM] Protección de las comunicaciones	
JUSTIFICACIÓN: Esta salvaguarda tiene lugar para proteger el servicio de internet que es de vital importancia para el funcionamiento de la entidad, ya que dé el dependen muchos sistemas necesarios para que la entidad cumpla con su objetivo misional.	
ACTIVOS EN LOS QUE SE APLICA: □ Servicios Internos [SERVICE] □ Redes de Comunicaciones [COM]	**DIMENSIONES:** □ Disponibilidad □ Trazabilidad □ Autenticidad
AMENAZAS MITIGADAS: □ A.7 Uso no previsto. □ A.24 Denegación del servicio. □ I.8 Fallo de servicios de comunicaciones. □ A.11 Acceso no autorizado.	

SALVAGUARDA: Salvaguardas relativas al personal [PS.AT] Formación y concientización	
JUSTIFICACIÓN: Por medio de entrevistas realizadas al personal, se pudo evidenciar la falta de conocimientos con base en seguridad informática, como por ejemplo el desconocimiento de la implementación de mecanismos de seguridad, ingeniería social, etc. Por eso la importancia de esta salvaguarda	
ACTIVOS EN LOS QUE SE APLICA: □ Personal [P] □ Datos o Información [D] □ Servicios Internos [SERVICE] □ Soportes de información [MEDIA]	**DIMENSIONES:** □ Confidencialidad □ Autenticidad □ Integridad □ Trazabilidad

AMENAZAS MITIGADAS: □ A.30 Ingeniería Social. □ A.5 Suplantación de Identidad. □ E.1 Errores de los usuarios. □ A.15 Modificación deliberada de la información. □ E.19 Fugas de Información.
SALVAGUARDA: Protección de Comunicaciones
[COM.DS] Segregación de los redes en dominios
JUSTIFICACIÓN: Esta salvaguarda permitirá que la red se segregue en dominios lógicos que permitirá que tenga entre otras ventajas, autenticación de usuarios, monitorización de tráfico, que no hayan conflictos por IP duplicadas.

ACTIVOS EN LOS QUE SE APLICA:	**DIMENSIONES:**
□ Servicios Internos [SERVICE] □ Redes de Comunicaciones [COM] □ Software [SW]	□ Disponibilidad □ Trazabilidad □ Autenticidad

AMENAZAS MITIGADAS: □ A.7 Uso no previsto. □ E.8 Difusión de software dañino. □ A.11 Acceso no autorizado.

Valoración de las salvaguardas

El objetivo de esta tarea es especificar la eficacia de las salvaguardas necesarias para los activos de información de la institución.

Para ello se tiene en cuenta el nivel de madurez de las salvaguardas como se define en la siguiente tabla:

EFICACIA	NIVEL	SIGNIFICADO
0%	L0	Inexistente
10%	L1	Inicial
50%	L2	Reproducible, pero intuitivo
90%	L3	Proceso definido
95%	L4	Gestionable y medible
100%	L5	Optimizado

Tabla 19: Eficacia y Madurez de las Salvaguardas
Fuente: Magerit V3 Libro 1. Método

Tabla 20: Valoración de la eficacia y madurez de las salvaguardas

SALVAGUARDA	ACTIVO	DIMENSIONES					Estado actual
		[I]	[C]	[D]	[T]	[A]	
Protecciones generales u horizontales: [H.tools.AV] Herramienta contra código dañino	Software [SW]			X			L4
Protección de los datos/información: [D] Copias de Seguridad de los datos (backup)	Datos e información [D]	X	X				L4
Protección de los Servicios: [S.A] Aseguramiento de la disponibilidad	Redes de comunicaciones [COM]			X	X		L2

Protección de los equipos: [HW] Protección de los equipos informáticos	Hardware [HW] Equipamiento Auxiliar [AUX	X		X			L4
Protección de los equipos: [HW.CM] Cambios (actualizaciones y mantenimiento)	Hardware [HW] Equipamiento Auxiliar [AUX]	X		X			L3
Protección de las comunicaciones: [COM] Protección de las comunicaciones	Servicios Internos [SERVICE] Redes de comunicaciones [COM]	X		X			L4
Protección de Comunicaciones: [COM.DS] Segregación de los redes en dominios	Servicios Internos [SERVICE] Redes de comunicaciones [COM] Software [SW]			X	X	X	L1
Salvaguardas relativas al personal: [PS.AT] Formación y concientización	Personal [P] Datos o Información [D] Servicios Internos [SERVICE] Soportes de Información [MEDIA]	X	X	X		X	L1

Estimación del impacto.

El objetivo de esta tarea es establecer el impacto potencial y residual.

El impacto es la medida del daño que pueda causar la materialización de una amenaza sobre un activo de información relevante de la organización.

El impacto potencial se determina teniendo en cuenta la valoración realizado tanto para los activos, como para las amenazas.

El impacto residual se determina teniendo en cuenta la valoración tanto de los activos como de las amenazas, así como también la eficacia y madurez de las salvaguardas establecidas.

La fórmula para el cálculo del impacto residual es:

$$\text{Impacto residual} = \text{impacto potencial} * (1- e^{i})$$

Donde $e^{i}=0$ significa que las salvaguardas son ineficaces, por lo tanto, el impacto es igual. Mientras que $e^{i}=1$ representa un conjunto de salvaguardas completamente eficaz, lo cual reduciría el impacto residual a cero.

Impacto Potencial

Como se mencionó anteriormente, para la realización de esta tarea se tendrá en cuenta el valor de los activos en las diferentes dimensiones (integridad, confidencialidad, integridad, trazabilidad y autenticidad), la valoración de la degradación que causan las amenazas sobre los activos de información relevantes en la organización, y de esta manera determinar el impacto que pueda causarse.

A continuación, se muestra una escala en la que se clasifica el impacto

Tabla 21: escala de valorización del impacto

VALOR	NIVEL DE IMPACTO
9-10	Alto
8	
6-7	Medio
4-5	
1-3	Bajo
0	

Tabla 22: Valorización del impacto potencial sobre cada activo

GRUPO DE ACTIVO	ACTIVO	DIMENSIONES				
		[I]	[C]	[D]	[T]	[A]
SERVICIOS INTERNOS [SERVICE]	Internet [INTERNET]			10	10	10
	TNS[TNS]			3	3	3
	NUBE[NB]			8		
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema [PASSWORD]	7	10			9
	Copias de Seguridad [BACKUP]	10	10	7		
SOFTWARE [SW]	Antivirus [AV]			7		
	Office [OFFICE]			7		
	Sistema Operativo [SO]			7		
	SART [SART]			10		
HARDWARE [HW]	Equipos de Cómputo [PC]	6	3	7		
	Equipos Portátiles [MOBILE]	3	3	3		
	Impresoras [PRINT]			1		
	Routers [ROUTER]			10		7
	Switch [SWITCH]			10		
	Servidores[SRV]	7		10		
SOPORTES DE INFORMACIÓN [MEDIA]	Material Impreso [VR]	3	7	3		
	Discos Duros Extraíbles [BACKUP]	7	7	8		
EQUIPAMIENTO AUXILIAR [AUX]	UPS [UPS]			3		
	Aires Acondicionados [AC]			1		
	Rack [RACK]			6		
	Cableado [CABLING]			7		
REDES DE COMUNICACIONES [COM]	Red Inalámbrica [WIFI]			3		
	Red Local [LAN]			8		
INSTALACIONES [I]	Edificio [BUILDING]			10		
PERSONAL [P]	Funcionarios[FU]		6	3		
	Contratistas[CT]		6	3		
	Administrador de Sistemas [ADM]		8	4		

Impacto Residual

El impacto residual se calcula teniendo en cuenta el impacto potencial calculado sobre el activo y las salvaguardas establecidas para mitigar las amenazas sobre ese activo.

Tabla 23: Impacto residual sobre cada activo

GRUPO DE ACTIVO	ACTIVO	DIMENSIONES				
		[I]	[C]	[D]	[T]	[A]
SERVICIOS INTERNOS [SERVICE]	Internet [INTERNET]			0	0	0
	TNS[TNS]			3	3	3
	NUBE[NB]			0		
DATOS O INFORMACIÓN [D]	Contraseñas de acceso al sistema [PASSWORD]	0	0			0
	Copias de Seguridad [BACKUP]	0	0	0		
SOFTWARE [SW]	Antivirus [AV]			0		
	Office [OFFICE]			0		
	Sistema Operativo [SO]			0		
	SART [SART]			0		
HARDWARE [HW]	Equipos de Cómputo [PC]	0	0	0		
	Equipos Portátiles [MOBILE]	0	0	0		
	Impresoras [PRINT]			1		
	Routers [ROUTER]			0		0
	Switch [SWITCH]			0		
	Servidores[SRV]	0		0		
SOPORTES DE INFORMACIÓN [MEDIA]	Material Impreso [VR]	3	7	3		
	Discos Duros Extraíbles [BACKUP]	0	0	0		
EQUIPAMIENTO AUXILIAR [AUX]	UPS [UPS]			3		
	Aires Acondicionados [AC]			1		
	Rack [RACK]			0		
	Cableado [CABLING]			0		
REDES DE COMUNICACIONES [COM]	Red Inalámbrica [WIFI]			0		
	Red Local [LAN]			0		
INSTALACIONES[I]	Edificio [BUILDING]			10		

PERSONAL [P]	Funcionarios[FU]		6	3		
	Contratistas[CT]		6	3		
	Administrador de Sistemas [ADM]		8	4		

ELABORÓ:	REVISÓ:		APROBÓ:
Martin J Diez C			
MARTIN JAVIER DIEZ D.T. SUPLENTE	JULIETH SALCEDO ASESORA PLANEACION Y GESTION	MARTHA JAIMES ASESORA CONTROL INTERNO	MAIRA ALEJANDRA LOPEZ GERENTE
FECHA: 15/01/2024	**FECHA: 16/01/2024**	**FECHA: 24/01/2024**	**FECHA: 26/01/2024**