ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“IMPLEMENTACIÓN DE UN PLAN DE TRATAMIENTO DE RIESGOS TECNOLÓGICOS AL CENTRO DE CÓMPUTO DE UNA ORGANIZACIÓN NO GUBERNAMENTAL SIN FINES DE LUCRO SIGUIENDO LA METODOLOGÍA MAGERIT”

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

AUTOR

LUIS ADRIÁN CHÓEZ ACOSTA

GUAYAQUIL, JULIO 2020

AGRADECIMIENTO

A Dios, mi Padre Celestial, porque gracias a Él he alcanzado todas las metas que me he propuesto.

A mi familia por estar a mi lado y acompañarme en todas mis iniciativas.

Al MSIG. Lenin Freire por el apoyo constante desde el inicio de esta maestría.

A Ketty porque siempre ha estado conmigo cuando la he necesitado.

DEDICATORIA

A mis padres Nancy y Luis, porque desde pequeño me inculcaron el amor al estudio y a luchar por alcanzar mis sueños.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenin Freire Cobo
COORDINADOR MSIA

MSIG. Juan Carlos García
PROFESOR DELEGADO
POR EL SUBDECANO DE LA
FIEC

RESUMEN

El presente proyecto buscó mejorar la seguridad de los activos de información del centro de cómputo de una ONG, con sede de Guayaquil, mediante la implementación de un plan de tratamiento de riesgos tecnológicos utilizando la metodología MAGERIT.

La ONG en la que se desarrolló el presente proyecto consciente de la importancia de ofrecer seguridad a la información que posee, brindó todas las facilidades para hacer un inventario de los activos tecnológicos del centro de cómputo de la organización. Además se hizo un análisis de los procesos que maneja el departamento de Sistemas de la ONG, así como los perfiles y responsabilidades del personal técnico del departamento.

Con dicha información, siguiendo la metodología MAGERIT mediante la herramienta PILAR se obtuvo información sobre los riegos que enfrentaba la ONG, y con dichos insumos se elaboró un Plan de Tratamientos para llevar a los riesgos a niveles aceptables.

ÍNDICE GENERAL

ABREVIATURAS

ISO	**:**	Organización Internacional de Estandarización
MAGERIT	**:**	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
ONG	**:**	Organización No Gubernamental
PILAR	**:**	Procedimiento Informático Lógico para el Análisis de Riesgos

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Entre los activos más importantes de cualquier empresa u organización del siglo XXI podemos citar: la información que posee y los medios tecnológicos con que dispone para su utilización y para su resguardo. Es por eso que es de vital importancia gestionar la seguridad de dichos activos, ya que un gran porcentaje del éxito de una organización depende de su correcta administración.

Sin embargo no se pueden eliminar por completo los riesgos a los cuales se enfrenta una organización, debido a que cada día aparecen nuevas amenazas a la disponibilidad, integridad y confidencialidad de la información; por lo que es prioritario que exista una cultura proactiva de seguridad informática y de administración de riesgos tecnológicos.

Una metodología para gestionar los riesgos informáticos es MAGERIT, desarrollada por el gobierno español para organismos gubernamentales, pero que gracias a su facilidad de uso y su eficiencia ha ido ganando preponderancia en el mundo empresarial.

CAPÍTULO 1

GENERALIDADES

1.1. DESCRIPCIÓN DEL PROBLEMA

Actualmente, cualquier institución sea pública o privada tiene riesgos de carácter informático que pueden ocasionar que su información se puede perder o verse comprometida, principalmente en sus sistemas informáticos y en sus servicios comunicacionales.

De acuerdo a la guía ISO 9000:2015, el término riesgo es el “efecto de la incertidumbre sobre la consecución de los objetivos”. [1]

La empresa seleccionada para este proyecto de implementación de un plan de tratamiento de riesgos tecnológicos fue una ONG ecuatoriana especializada en brindar servicios a las comunidades de escasos

recursos. La institución posee activos tecnológicos de carácter informático tales como: equipos de computación, equipos de comunicación, sistemas y servicios informáticos, hardware y servicios de comunicación, etc., los mismos que son administrados por el Departamento de Sistemas, el mismo que no cuenta con un protocolo formal que evite que sus operaciones se suspendan y puedan activarse sin que produzca retrasos o afectación a la empresa.

Esta problemática afecta directamente la continuidad de los servicios informáticos de la organización, la misma que además está expuesta a diferentes tipos de amenazas:

- Causadas por la naturaleza tales como terremotos, incendios, tormentas eléctricas, inundaciones, etc.
- Defectos de fábrica de los equipos.
- Errores en el desarrollo o implementación de un software.
- Producidas accidentalmente por las personas.
- Producidas con premeditación por las personas.

1.2. SOLUCIÓN PROPUESTA

La solución propuesta fue la identificación y evaluación de los activos de la empresa y de las amenazas a los que están expuestos, medir los

riesgos que existen y proponer las salvaguardas necesarias para implementar un plan de tratamiento de los riesgos tecnológicos de orden cualitativo aplicado a los activos del centro de cómputo, que administra los servicios informáticos de la Organización.

La metodología utilizada para la evaluación fue MAGERIT en su versión 3.0, para lo cual se hizo uso de la herramienta PILAR que ha sido desarrollada para realizar análisis y gestión de riesgos en sistemas informáticos.

MAGERIT es una metodología que implementa el proceso de Gestión de Riesgos dentro de un marco de trabajo para que los niveles jerárquicos de las organizaciones tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. Fue desarrollada por el Consejo Superior de Administración Electrónica del Gobierno de España siguiendo la terminología de la normativa ISO 31000. [2]

MAGERIT consiste en 3 libros en versiones inglés, español e italiano:

- Libro I: Método [3]
- Libro II: Catálogo de Elementos [4]

- Libro III: Guía de Técnicas [5] PILAR utiliza gráficos para mostrar los niveles de riesgo e impacto potencial a los cuales está expuesta la organización.

  Entre los beneficios obtenidos por la Organización No Gubernamental sin fines de lucro al implementar la solución tenemos:

  - La disminución del impacto de los riesgos mediante la supervisión y toma de decisiones orientadas a lograr los objetivos de la Organización a fin de evitar las amenazas latentes y corregir vulnerabilidades identificadas.

  - Mayores garantías de continuidad del negocio basadas en la adopción de un plan de seguridad.

  - Entrega de valor a la organización de tal manera que todos los recursos que son destinados a la seguridad deben aplicarse de manera óptima para apoyar los objetivos de negocio y lograr la alineación.

  - Una mayor confianza por parte de clientes, proveedores, auspiciantes y comunidad.

  - Personal del departamento de Sistemas motivado a seguir las normas y protocolos sobre seguridad de la información y recursos tecnológicos. .

CAPÍTULO 2

METODOLOGÍA PARA EL DESARROLLO DE LA SOLUCIÓN

2.1. SITUACIÓN ACTUAL DE LA ORGANIZACIÓN

Para iniciar la evaluación de los riesgos informáticos a los que está sometida la Organización no gubernamental sin fines de lucro donde se realizó la implementación, es fundamental conocer la infraestructura tecnológica y la estructura organizativa del departamento de sistemas, esto permitirá identificar todos los activos expuestos a riesgos y que pueden afectar la continuidad del negocio.

La organización administra su infraestructura tecnológica tanto lógica como física a través del departamento de Sistemas conformado por el

personal de soporte de hardware, soporte de software y desarrollo de aplicaciones, quienes realizan diversas actividades de gestión que coadyuvan en la consecución de los objetivos institucionales como lo indica la Tabla 1.

Tabla 1. Actividades de gestión del personal del departamento de Sistemas

DPTO. DE SISTEMAS	ACTIVIDADES DE GESTIÓN
Soporte de Hardware	• Soporte a usuarios • Mantenimiento de computadoras • Inventario físico de computadoras • Soporte a redes LAN
Soporte de Software	• Soporte a usuarios • Instalación de software • Soporte a sistemas informáticos institucionales

Desarrollo de Aplicaciones	• Desarrollo de servicios y sistemas informáticos • Mantenimiento de sistemas informáticos institucionales • Respaldo de sistemas informáticos institucionales

Fuente: Departamento de Sistemas ONG
Elaboración: Autor

Los servidores de la organización están ubicados en el Centro de Datos o Data Center, esta habitación no posee las seguridades necesarias; cuenta con una climatización ofrecida por un acondicionador de aire destinado para uso del hogar, la mayoría de los equipos están conectados directamente a los tomacorrientes a excepción de los servidores de producción que están conectados a UPS para prevenir cualquier fallo en la continuidad de la energía eléctrica. Al Data Center sólo tienen acceso el personal del Departamento de Sistemas y de Recursos Generales, estos últimos para el mantenimiento del acondicionador de aire.

2.1.1. INVENTARIO DE INFRAESTRUCTURA TECNOLÓGICA

El Departamento de Sistemas mantiene la integridad, disponibilidad y confidencialidad de la información de la organización, de igual manera da soporte a la infraestructura tecnológica, expresadas en las tablas 2, 3 y 4.

Tabla 2. Servidores de la organización

SERVIDOR	SERVICIO
Producción	Sistemas Informáticos de producción. Base de Datos para Sistemas Informáticos de producción.
Pruebas Producción	Sistemas Informáticos de producción para pruebas. Base de Datos para Sistemas Informáticos de producción para pruebas.
Pruebas Desarrollo	Sistemas Informáticos de producción para desarrollo. Base de Datos para Sistemas Informáticos de producción para desarrollo.
Facturación Electrónica	Portal web que almacena los documentos electrónicos: facturas, retenciones, guías de remisión, notas de débito y notas de crédito.
Archivos Respaldo	Servidor de archivos Backup.
Biométrico	Sistema de control de ingreso del personal Sistema de pruebas para candidatos.
Instaladores	Almacenamientos de archivos instaladores de todos los programas que son usados por los usuarios de la organización.
Web Services	Servidor de recepción de pagos.
Comunicaciones	Terminal Server, conexión remota al sistema ERP.
Aplicaciones	Código fuente del sistema ERP.

Fuente: Departamento de Sistemas ONG
Elaboración: Autor

Tabla 3. Inventario de equipos para comunicación de red LAN

EDIFICIO	UBICACIÓN/ CANTIDAD	EQUIPO ACTIVO	ENLACE	SERVICIO DEL ACTIVO	DEPARTAMENTOS / UNIDADES
Matriz	La L	1 Switch de fibra Zyxel Transceiver	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Ventas Cartera EPS
	Planta de Producción	Switch CISCO Catalyst 2960	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Logística Producción Servicios Generales
	Banco de Materiales	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Banco de Materiales
	Capilla	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Talentos Humanos Departamento Médico Pastoral Misión Voluntariado
	Edificio Administrativo Planta Baja	1 Switch Zyxel GS200 1 Switch Zyxel XGS4528f 1 Switch 3COM 1 Switch Dlink 1 Fortinet fortigate 100D 3 Grandstream 1 Transceiver	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Sistemas Vaca Mecánica
	Edificio Administrativo Planta Alta	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Nómina Sistema para control de ingreso de personal Internet Portal web facturación	Recepción Tesorería Contabilidad Departamento Legal Contraloría Direcciones Proyectos Comunicaciones Obra Civil

Sucursal 1	Esmeraldas	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Jefatura Ventas Cartera
Sucursal 2	Babahoyo	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Jefatura Ventas Cartera
Sucursal 3	Quevedo	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Jefatura Ventas Cartera EPS
Sucursal 4	Libertad	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Jefatura Ventas Cartera EPS
Sucursal 5	Machala	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Jefatura Ventas Cartera
Sucursal 6	Daule	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Jefatura Ventas Cartera EPS
Sucursal 7	Quinindé	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Jefatura Ventas Cartera
Sucursal 8	Durán	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	EPS
Sucursal 9	Playas	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	EPS
Sucursal 10	Portoviejo	Switch CISCO Transceiver Switch 3COM	UTP FIBRA	ERP Internet Portal web facturación Antivirus	Jefatura Ventas Cartera

Fuente: Departamento de Sistemas ONG
Elaboración: Autor

Tabla 4**.** Inventario de soluciones informáticas

Nº	SOFTWARE	CÓDIGOS FUENTE	ARQUITECTURA	BASE DE DATOS
1	Sistema ERP Contable	SI	32/64 bits	Oracle 10g
2	Sistema Parametrización de permisos	SI	32/64 bits	
3	Sistema Nómina	SI	32/64 bits	
4	Portal web facturación electrónica	SI	32/64 bits	
5	Sistema para control de ingreso de personal	NO	32/64 bits	
6	Antivirus	NO	32/64 bits	NO APLICA
7	Portal web institucional	NO	32/64 bits	NO APLICA

Fuente: Departamento de Sistemas ONG
Elaboración: Autor

2.2. VALORACIÓN DE LOS ACTIVOS

Para obtener el modelo de valor hay que identificar los activos que son fundamentales en las actividades de la organización, la relación entre ellos, la valoración que se les asigna; y por último los resultados que indican cuán importantes son para la organización.

2.2.1. IDENTIFICACIÓN DE LOS ACTIVOS EN LA HERRAMIENTA PILAR

En primer lugar, de acuerdo con el manual de usuario [6], se identifica los activos mediante un nombre, se los codifica y se los ubica en las categorías que vienen por defecto como lo indica la figura 2.1.

- Activos esenciales
- Servicios internos
- Equipamiento
- Servicios subcontratados
- Instalaciones
- Personal

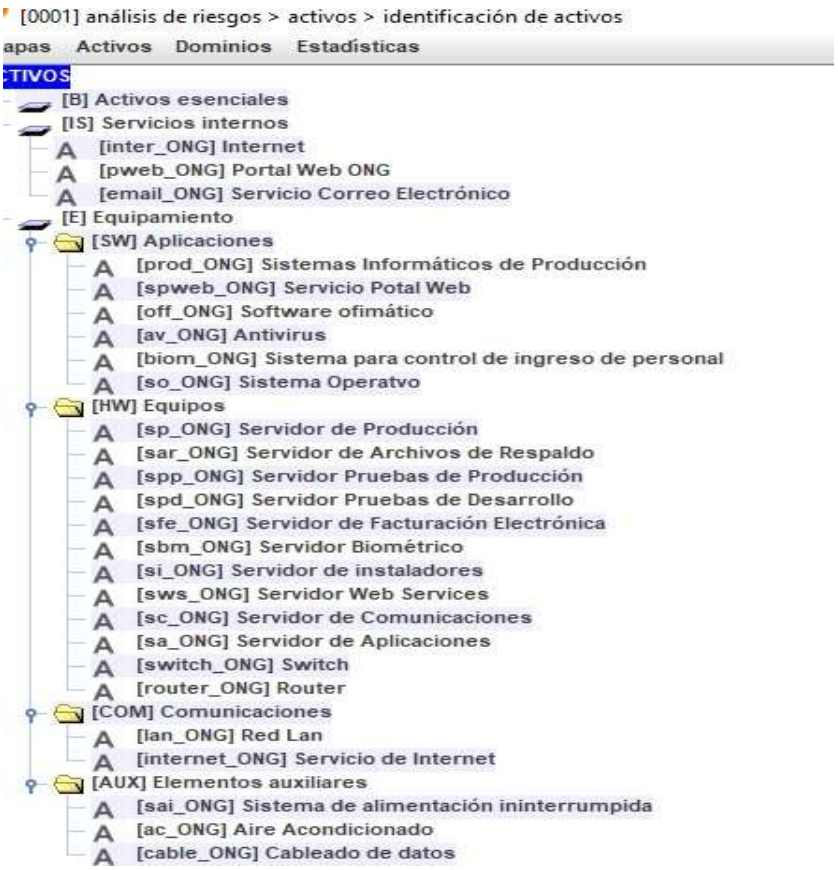


Figura 2.1. Identificación de los activos en Pilar
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

2.2.2. DEPENDENCIA ENTRE ACTIVOS EN LA HERRAMIENTA PILAR

La herramienta Pilar permite establecer dependencias entre cada uno de los activos. Las mismas que hacen entrega de los requisitos de seguridad desde los activos superiores (los que tienen más valor) a los activos que dan soporte al valor como lo indica la figura 2.2.

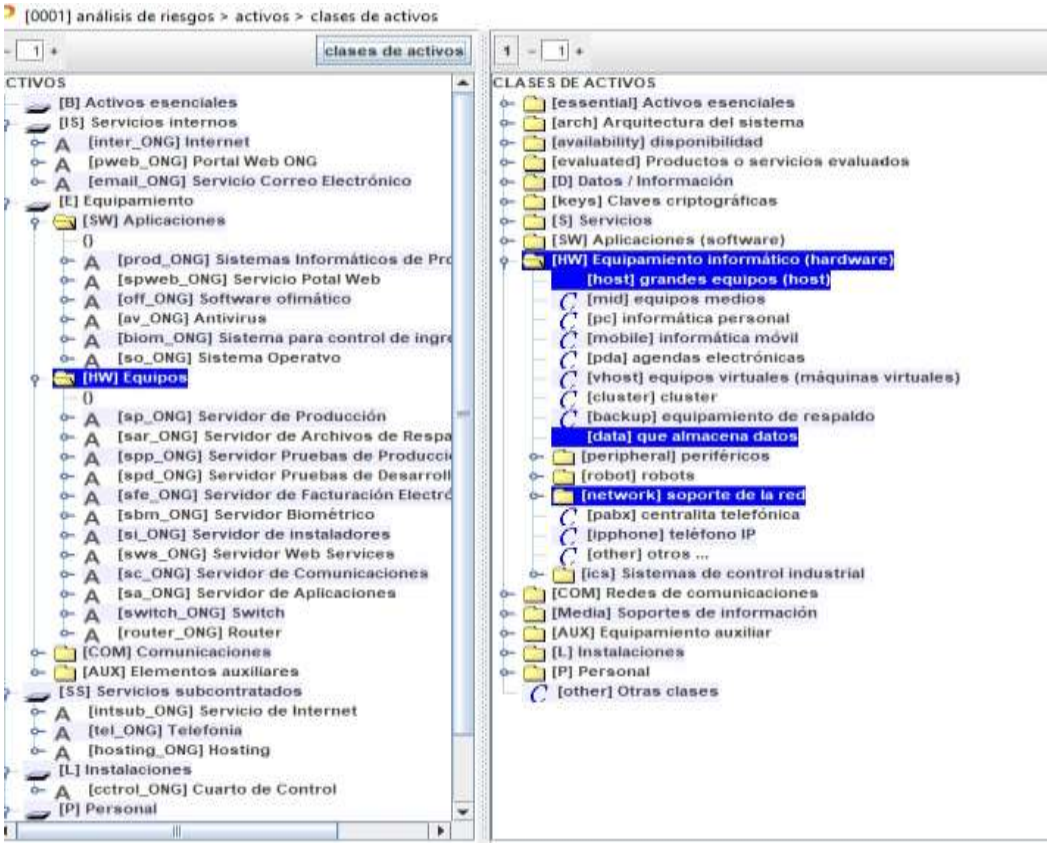


Figura 2.2. Dependencia entre activos
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

2.2.3. VALORACIÓN DE ACTIVOS EN LA HERRAMIENTA PILAR

La herramienta Pilar permite valorar cada uno de los activos en los parámetros de seguridad que se ven expuestos antes las diferentes amenazas. Dichas valoraciones se las hace de acuerdo a los criterios de Disponibilidad (D), Integridad (I), Confidencialidad (C), Autenticidad (A) y Trazabilidad (T) y se lo hace de acuerdo a los criterios de la tabla 5. Las figuras desde la 2.3 hasta la 2.10 muestran las valoraciones de los activos.

Tabla 5**.** Escala de valoración para cada dimensión

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 efectos prácticos

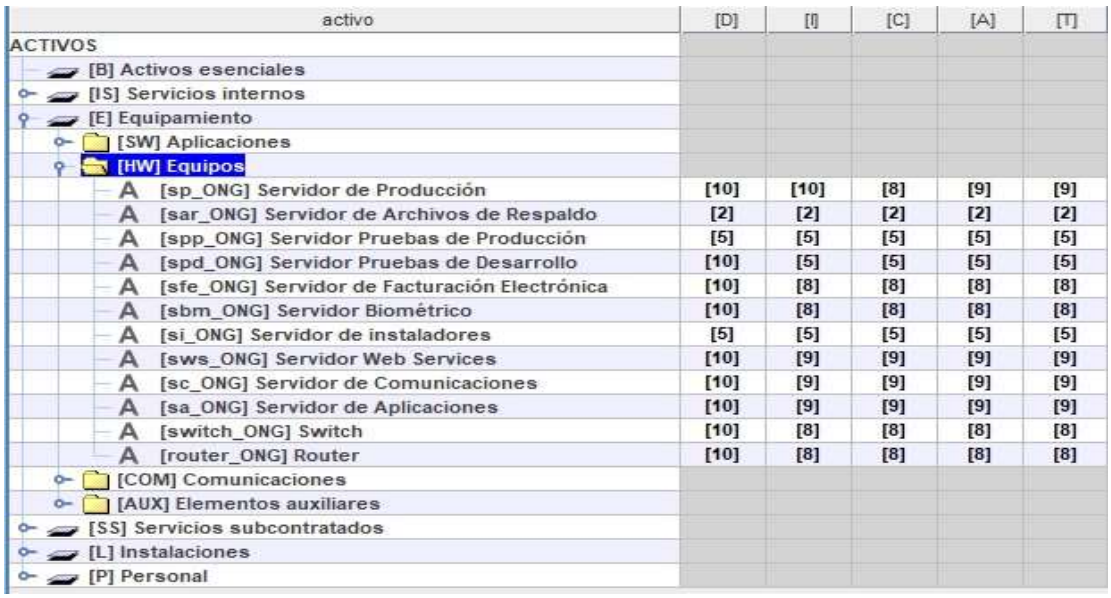
Fuente: Departamento de Sistemas ONG
Elaboración: Autor

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[inter_ONG] Internet	[9]	[7]	[9]	[4]	[9]
[pweb_ONG] Portal Web ONG	[7]	[7]	[5]		
[email_ONG] Servicio Correo Electrónico	[9]	[7]	[9]	[8]	[9]
[E] Equipamiento					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Figura 2.3. Valoración de los activos de servicios informáticos internos
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

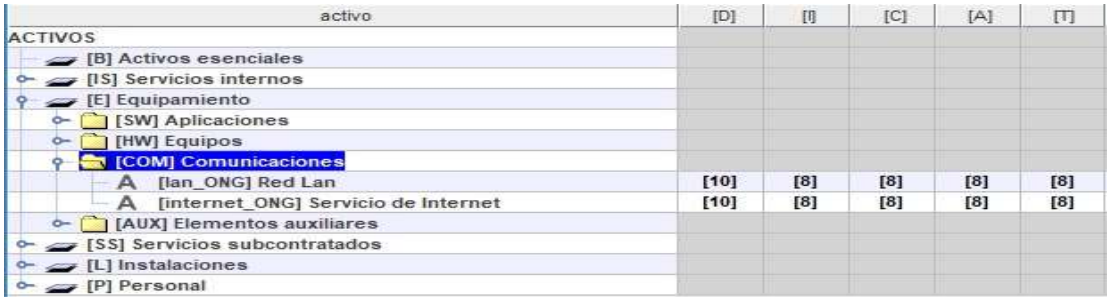
activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[prod_ONG] Sistemas Informáticos de Produc	[10]	[10]	[10]	[9]	[9]
[spweb_ONG] Servicio Potal Web	[10]	[10]	[7]	[4]	[4]
[off_ONG] Software ofimático	[10]				[7]
[av_ONG] Antivirus					[7]
[biom_ONG] Sistema para control de ingreso	[9]	[8]	[3]	[7]	[6]
[so_ONG] Sistema Operatvo	[7]			[7]	[7]
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Figura 2.4. Valoración de aplicaciones informáticas de la organización
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[sp_ONG] Servidor de Producción	[10]	[10]	[8]	[9]	[9]
[sar_ONG] Servidor de Archivos de Respaldo	[2]	[2]	[2]	[2]	[2]
[spp_ONG] Servidor Pruebas de Producción	[5]	[5]	[5]	[5]	[5]
[spd_ONG] Servidor Pruebas de Desarrollo	[10]	[5]	[5]	[5]	[5]
[sfe_ONG] Servidor de Facturación Electrónica	[10]	[8]	[8]	[8]	[8]
[sbm_ONG] Servidor Biométrico	[10]	[8]	[8]	[8]	[8]
[si_ONG] Servidor de instaladores	[5]	[5]	[5]	[5]	[5]
[sws_ONG] Servidor Web Services	[10]	[9]	[9]	[9]	[9]
[sc_ONG] Servidor de Comunicaciones	[10]	[9]	[9]	[9]	[9]
[sa_ONG] Servidor de Aplicaciones	[10]	[9]	[9]	[9]	[9]
[switch_ONG] Switch	[10]	[8]	[8]	[8]	[8]
[router_ONG] Router	[10]	[8]	[8]	[8]	[8]
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Figura 2.5. Valoración de equipos informáticos de la organización
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

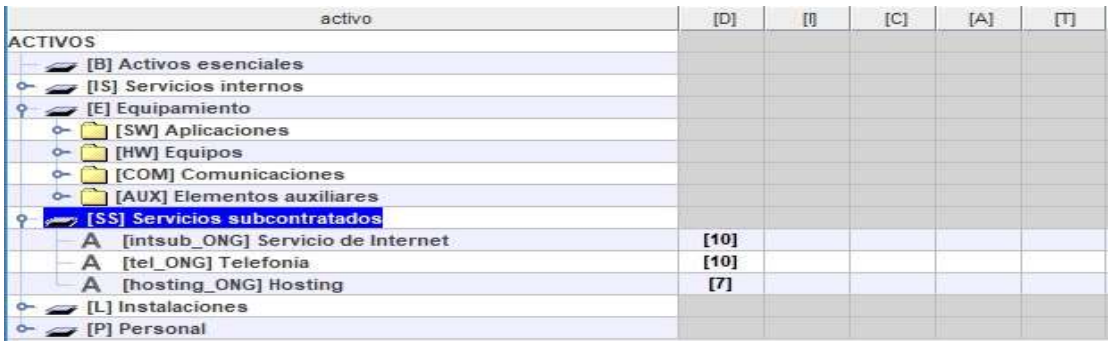


activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[lan_ONG] Red Lan	[10]	[8]	[8]	[8]	[8]
[internet_ONG] Servicio de Internet	[10]	[8]	[8]	[8]	[8]
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Figura 2.6. Valoración de los activos de comunicación
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[sai_ONG] Sistema de alimentación ininterrumpida	[6]				[6]
[ac_ONG] Aire Acondicionado	[7]				[7]
[cable_ONG] Cableado de datos	[7]				[7]
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Figura 2.7. Valoración de equipamiento auxiliar
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
[intsub_ONG] Servicio de Internet	[10]				
[tel_ONG] Telefonia	[10]				
[hosting_ONG] Hosting	[7]				
[L] Instalaciones					
[P] Personal					

Figura 2.8. Valoración de servicios subcontratados
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
[L] Instalaciones					
[cctrol_ONG] Cuarto de Control	[9]	[9]	[8]	[9]	[9]
[P] Personal					

Figura 2.9. Valoración de Instalaciones físicas
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Activos esenciales					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					
[admp_ONG] Administradores de sistemas	[7]		[9]		
[des_ONG] Desarrollador	[7]		[9]		
[ssw_ONG] Soporte de software	[7]		[9]		
[shw_ONG] Soporte de hardware	[7]		[9]		

Figura 2.10. Valoración del personal técnico
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

2.3. MAPA DE RIESGOS

Las amenazas son el resultado de las vulnerabilidades, en otras palabras si en una organización se detecta una amenaza es porque hay una vulnerabilidad que un atacante puede utilizar en cualquier momento. [7]

En el caso de que las amenazas se concreten se debe determinar el riesgo y el impacto de los daños, por lo que hay que identificar aquellos que afecten directamente a los activos de acuerdo al nivel de probabilidad de ocurrencia (P) y al nivel de degradación de la Disponibilidad (D), Integridad (I), Confidencialidad (C), Autenticidad (A) y Trazabilidad (T). Las escalas de valoración de la metodología MAGERIT se muestran en las tablas 6 y 7.

Tabla 6**.** Degradación del valor

VALOR	DETALLE
MA	Muy alta
CP	Casi posible
P	Posible
PP	Poco probable
MR	Muy rara vez

Fuente: Departamento de Sistemas ONG
Elaboración: Autor

Tabla 7**.** Probabilidad de ocurrencia

VALOR	DETALLE
T	Total
MA	Muy Alta
A	Alta
M	Media
B	Baja
MB	Muy Baja

Fuente: Departamento de Sistemas ONG
Elaboración: Autor

Utilizando la herramienta PILAR es factible identificar las amenazas que pueden influir sobre un activo, y mediante esta valoración se podrán determinar las salvaguardas que se activarán en el tratamiento de los riesgos. En la figura 2.11 se aprecian los resultados obtenidos en la valoración de las amenazas que afectan al servicio de internet:

activo	co..	probabilidad	[D]	[I]	[C]
ACTIVOS					
[B] Activos esenciales					
[S] Servicios internos					
[inter_ONG] Internet			A	A	A
[E.1] Errores de los usuarios		P	M	M	M
[E.2] Errores del administrador del sistema / de la seguridad		P	M	M	M
[E.15] Alteración de la información		P		B	
[E.18] Destrucción de la información		P	M		
[E.19] Fugas de información		P			M
[E.24] Caída del sistema por agotamiento de recursos		MA	A		
[A.5] Suplantación de la identidad		P		A	A
[A.6] Abuso de privilegios de acceso		P	B	M	M
[A.7] Uso no previsto		P	B	M	M
[A.11] Acceso no autorizado		P		M	A
[A.13] Repudio (negación de actuaciones)		MA			
[A.15] Modificación de la información		MA		A	
[A.18] Destrucción de la información		P	A		
[A.24] Denegación de servicio		MA	A		
[pweb_ONG] Portal Web ONG			A	A	A
[email_ONG] Servicio Correo Electrónico			A	A	A
[E] Equipamiento					
[SW] Aplicaciones					
[HW] Equipos					
[COM] Comunicaciones					
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
[L] Instalaciones					
[P] Personal					

Figura 2.11. Valoración de amenazas – Servicio de Internet
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

2.4. EVALUACIÓN DE SALVAGUARDAS

Las salvaguardas o contra medidas están definidas como los protocolos tecnológicos que producen un reducción de los riesgos. Algunas amenazas desaparecen sólo organizándose en forma adecuada, otras necesitan elementos técnicos (programas o equipos), otra requieren seguridad física y, por último, está la política de personal. [8]

Para hacer frente a la probabilidad de que se concrete una amenaza, hay que identificar y realizar una valoración de las posibles salvaguardas. En Pilar las salvaguardas se tratan en 4 áreas: Gestión (G), Técnico (T), Seguridad Física (F) y Gestión de Personal (P).

En la pantalla que despliega Pilar que corresponde a la eficacia de las salvaguardas observamos que la tercera columna de recomendación indica el nivel de criticidad considerando la clase de activos, que puede ir a partir del 0 hasta el 9 como lo indica la figura 2.12.

Figura 2.12. Niveles de criticidad
Fuente: Pilar
Elaboración: Autor

En las siguientes columnas se ingresan los niveles de las salvaguardas actuales, objetivo y por último la herramienta PILAR despliega los rangos de niveles que recomienda.

Como se observa en la figura 2.13, los niveles de salvaguardas actuales están entre 0 y 3 lo cual muestra que faltan definir procesos para mejorar la protección de los activos de la institución; el objetivo es realizar una mejora continua sobre estos procesos hasta que sean gestionables y medibles.

	asp..	tdp	rec..		salvaguarda	...	f...	...	...	current	target	PILAR
					SALVAGUARDAS							
☐	G	EL	8		[IA] Identificación y autenticación					L3	L5	L2-L5
☐	T	EL	7		[AC] Control de acceso lógico					L3	L4	L2-L4
☐	G	PR			[D] Protección de la Información					L3	L4	n.a.
☐	G	EL			[K] Protección de claves criptográficas					L0	L2	n.a.
☐	G	PR	6		[S] Protección de los Servicios					L2	L4	L2-L4
☐	G	PR	7		[SW] Protección de las Aplicaciones Informáticas (SW)					L3	L4	L2-L4
☐	G	PR	7		[HW] Protección de los Equipos Informáticos (HW)					L3	L4	L2-L4
☐	G	PR	8		[COM] Protección de las Comunicaciones					L3	L5	L2-L5
☐	G	PR			[IP] Sistema de protección de frontera lógica							n.a.
☐	G	PR			[MP] Protección de los Soportes de Información							n.a.
☐	G	PR	6		[AUX] Elementos Auxiliares					L3	L4	L2-L4
☐	F	EL	6		[PPE] Protección física de los equipos					L3	L4	L3-L4
☐	F	PR	7		[L] Protección de las Instalaciones					L2	L4	L2-L4
☐	F	EL			[PPS] Protección del perímetro físico							n.a.
☐	P	PR	6		[PS] Gestión del Personal					L2	L4	L2-L4
☐	G	PR			[PDS] Servicios potencialmente peligrosos							n.a.
☐	G	CR	6		[IR] Gestión de incidentes					L0	L4	L2-L4
☐	T	PR	9		[tools] Herramientas de seguridad					L2	L4	L2-L5
☐	G	CR	6		[V] Gestión de vulnerabilidades					L1	L4	L2-L4
☐	T	MN			[A] Registro y auditoria							n.a.
☐	G	RC	5		[BC] Continuidad del negocio					L1	L4	L2-L3
☐	G	AD	5		[G] Organización					L2	L3	L2-L3
☐	G	AD	6		[E] Relaciones Externas					L3	L4	L3-L4
☐	G	AD	5		[NEW] Adquisición / desarrollo					L2	L3	L2-L3

Figura 2.13. Identificación de salvaguardas
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

Las salvaguardas escogidas fueron:

Protecciones Generales

- Gestionar la identificación y la autenticación de los usuarios, comprobar su identidad y los privilegios requeridos.
- Definir el procedimiento para conceder, suspender, cancelar y reactivar privilegios.

- Identificar y controlar los perfiles de acceso y sus privilegios asociados.
- Realizar la implementación de un IDS/IPS: Herramienta de detección / prevención de intrusión.
- Tener actualizados los antivirus constantemente
- Estimar los riesgos que existen sobre los activos de la organización.

Protección de la Información

- Implementar el uso de firmas electrónicas
- Realizar copias de seguridad
- Normar el acceso a las copias de seguridad con previa autorización

Protección de las aplicaciones (software)

- Realizar un inventario del software de la organización
- Normar el uso autorizado de las aplicaciones
- Controlar la instalación de software con licencia
- Definir procedimientos para realizar copias de seguridad
- Almacenar las copias de seguridad en sitios alternos
- Aplicar perfiles de usuarios

- Mantener un control de versiones de las actualizaciones de las aplicaciones de la organización

Protección de los equipos (hardware)

- Inventario actualizado.
- Identificación de la persona responsable.
- Registro de traslados internos.
- Mantenimiento realizado por personal autorizado

Protección de las comunicaciones

- Sólo dispositivos autorizados pueden tener acceso a redes y servicios de la ONG.
- Control de conexiones remotas a las redes de la ONG.
- Normativa de uso de los servicios de Red.
- Normativa para el uso del servicio de Internet.

Protección de los soportes de información

- Disponer de un inventario para los soportes de información.
- Identificar a la persona responsable.
- Disponer de armarios de seguridad para los soportes de información.

Elementos Auxiliares

- Disponer de un inventario para el equipamiento auxiliar.
- Identificar a la persona responsable.
- Mantener una bitácora de las entradas y salidas del equipamiento auxiliar.
- Mantener una climatización adecuada.
- Activar respaldo eléctrico en caso de emergencia.
- Proteger los equipos ante fluctuaciones y sobrecargas eléctricas.
- Mantener un Sistema de alimentación ininterrumpida.

Seguridad física – Protección de las instalaciones

- Disponer de normativa de seguridad de las instalaciones
- Protección del perímetro y vigilancia en las instalaciones de la ONG.
- Plan de emergencia ante incendios.
- Equipos de protección ante incendios.
- Plan de emergencia ante movimientos telúricos.
- Simulacros periódicos para la prevención de desastres.
- Disponer de mecanismos de autenticación.
- Dispone de cámaras de vigilancia.
- Se requiere autorización para el acceso de personas externas a la ONG.

Gestión del Personal

- Normativa para la gestión del personal.
- Capacitación del personal técnico y administrativo.
- Supervisar las operaciones críticas.
- Revisar constantemente los incidentes de disponibilidad de personal.

2.5. ESTADO DE RIESGO

Es la caracterización de los activos por su riesgo residual; es decir lo que puede pasar tomando en consideración las salvaguardas desplegadas. [9]

2.5.1. Impacto acumulado

Pilar realiza la evaluación del impacto acumulado sobre los activos de la organización permitiendo comparar el impacto potencial, el impacto actual y el impacto objetivo es decir después de haber implementado las salvaguardas, obteniéndose bajos niveles de impacto los mismos que se consideran residuales.[10]

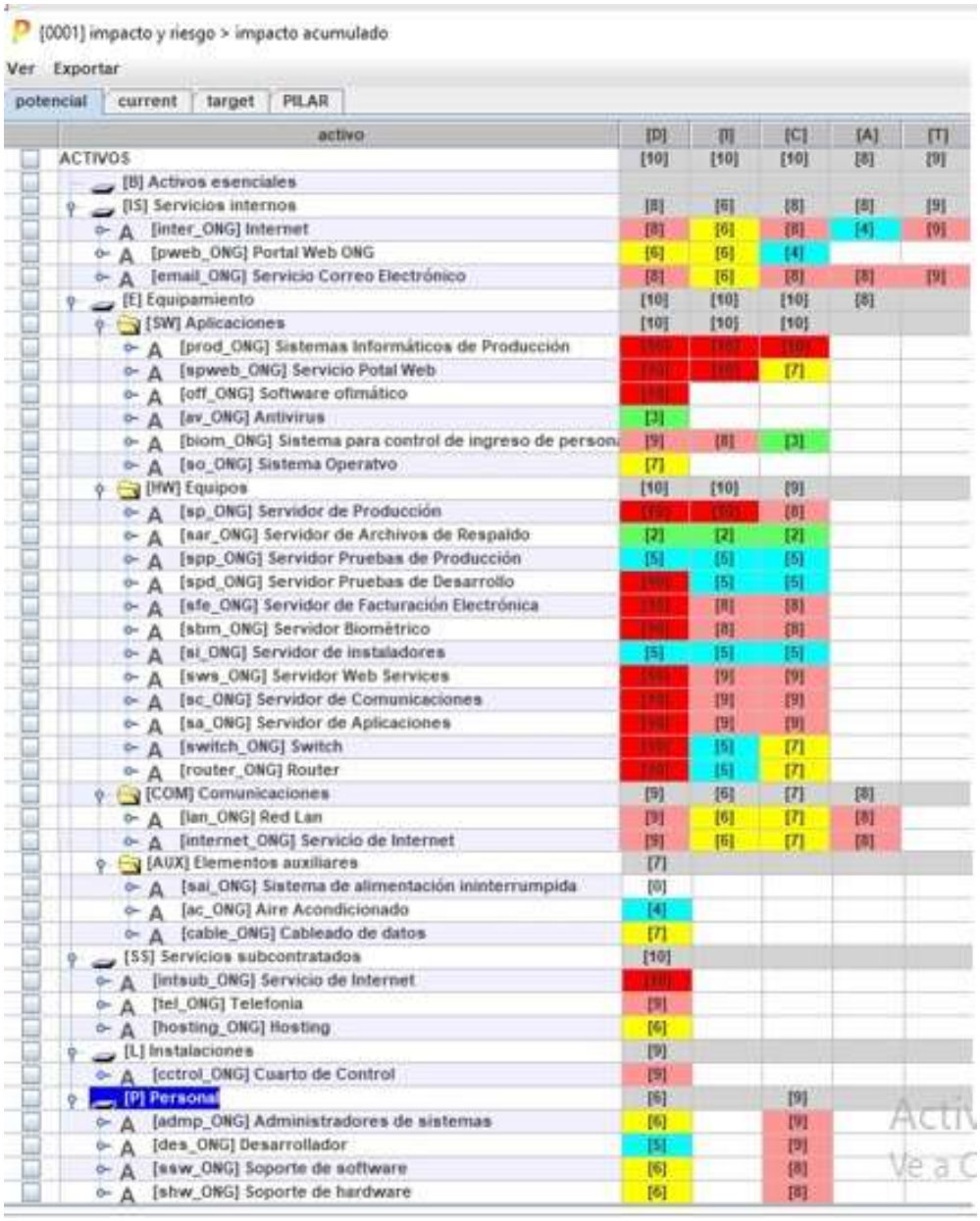
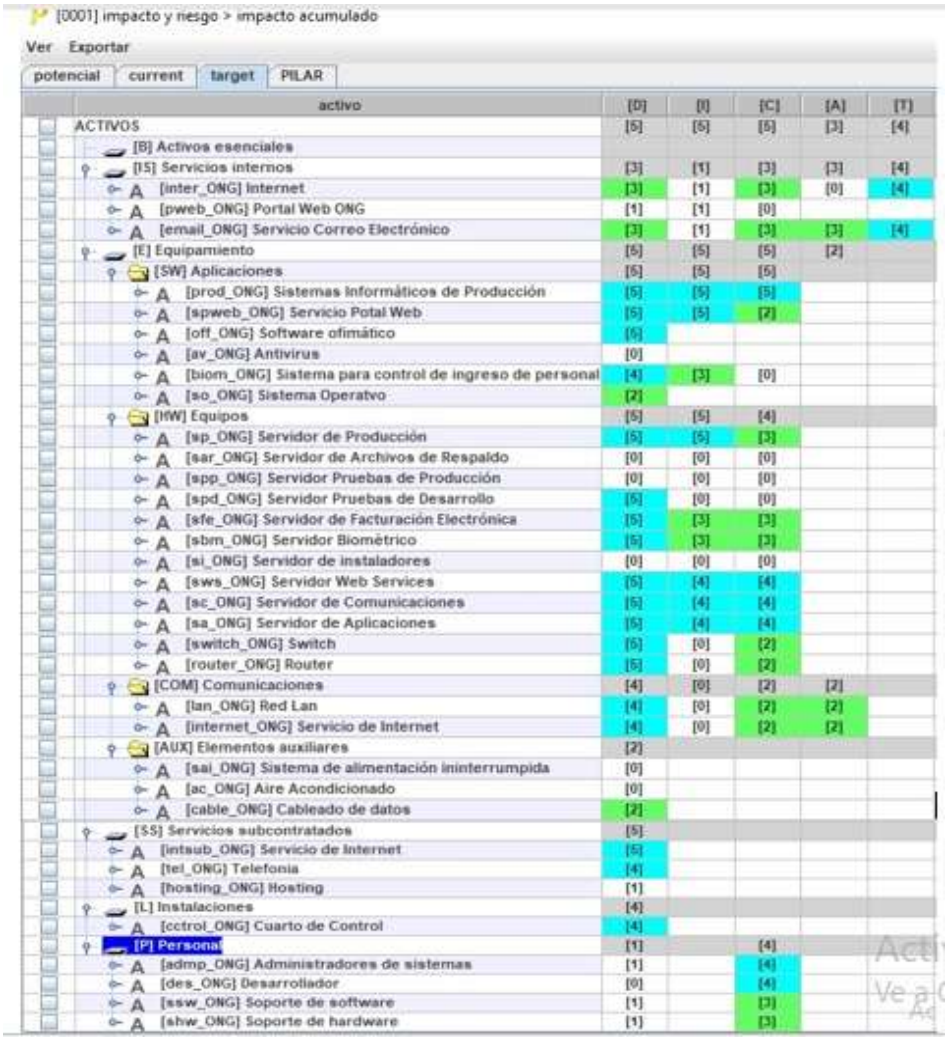


Figura 2.14. Impacto acumulado potencial
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

Figura 2.15. Impacto acumulado actual
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[5]	[5]	[5]	[3]	[4]
[B] Activos esenciales					
[IS] Servicios internos	[3]	[1]	[3]	[3]	[4]
[inter_ONG] Internet	[3]	[1]	[3]	[0]	[4]
[pweb_ONG] Portal Web ONG	[1]	[1]	[0]		
[email_ONG] Servicio Correo Electrónico	[3]	[1]	[3]	[3]	[4]
[E] Equipamiento	[5]	[5]	[5]	[2]	
[SW] Aplicaciones	[5]	[5]	[5]		
[prod_ONG] Sistemas Informáticos de Producción	[5]	[5]	[5]		
[spweb_ONG] Servicio Potal Web	[5]	[5]	[2]		
[off_ONG] Software ofimático	[5]				
[av_ONG] Antivirus	[0]				
[biom_ONG] Sistema para control de ingreso de personal	[4]	[3]	[0]		
[so_ONG] Sistema Operativo	[2]				
[HW] Equipos	[5]	[5]	[4]		
[sp_ONG] Servidor de Producción	[5]	[5]	[3]		
[sar_ONG] Servidor de Archivos de Respaldo	[0]	[0]	[0]		
[spp_ONG] Servidor Pruebas de Producción	[0]	[0]	[0]		
[spd_ONG] Servidor Pruebas de Desarrollo	[5]	[0]	[0]		
[sfe_ONG] Servidor de Facturación Electrónica	[5]	[3]	[3]		
[sbm_ONG] Servidor Biométrico	[5]	[3]	[3]		
[si_ONG] Servidor de instaladores	[0]	[0]	[0]		
[sws_ONG] Servidor Web Services	[5]	[4]	[4]		
[sc_ONG] Servidor de Comunicaciones	[5]	[4]	[4]		
[sa_ONG] Servidor de Aplicaciones	[5]	[4]	[4]		
[switch_ONG] Switch	[5]	[0]	[2]		
[router_ONG] Router	[5]	[0]	[2]		
[COM] Comunicaciones	[4]	[0]	[2]	[2]	
[lan_ONG] Red Lan	[4]	[0]	[2]	[2]	
[internet_ONG] Servicio de Internet	[4]	[0]	[2]	[2]	
[AUX] Elementos auxiliares	[2]				
[sai_ONG] Sistema de alimentación ininterrumpida	[0]				
[ac_ONG] Aire Acondicionado	[0]				
[cable_ONG] Cableado de datos	[2]				
[SS] Servicios subcontratados	[5]				
[intsub_ONG] Servicio de Internet	[5]				
[tel_ONG] Telefonia	[4]				
[hosting_ONG] Hosting	[1]				
[L] Instalaciones	[4]				
[cctrol_ONG] Cuarto de Control	[4]				
[P] Personal	[1]		[4]		
[admp_ONG] Administradores de sistemas	[1]		[4]		
[des_ONG] Desarrollador	[0]		[4]		
[ssw_ONG] Soporte de software	[1]		[3]		
[shw_ONG] Soporte de hardware	[1]		[3]		

Figura 2.16. Impacto acumulado objetivo
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

Las figuras 2.14 y 2.15 muestran cuán importante es aplicar salvaguardas para que se reduzcan los niveles del impacto, actualmente se encuentran en nivel medio, y el nivel objetivo es

lograr un bajo impacto en los activos de organización, ver la figura 2.16.

2.5.2. Riesgo acumulado

El riesgo acumulado se calcula que tomando en consideración el valor acumulado y el efecto directo de las amenazas sobre el activo. La herramienta PILAR realiza la valoración de los niveles de criticidad de los riesgos a los que se encuentran sometidos los activos de la organización. [11]

En la figura 2.17, se muestran los niveles de riesgo acumulado potencial que afectan a los activos, en el supuesto que no existiesen salvaguardas. La figura 2.18 muestra el nivel del riesgo acumulado actual, el cual está en nivel medio y en la figura 2.19 se obtiene el riesgo acumulado objetivo, el mismo que debe seguir analizándose para intentar que disminuya o si es posible que desaparezca.

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	(7,2)	(6,8)	(6,8)	(5,7)	(6,9)
[B] Activos esenciales					
[IS] Servicios internos	(6,6)	(5,4)	(5,7)	(5,7)	(6,9)
[inter_ONG] Internet	(6,6)	(5,4)	(5,7)	(3,3)	(6,9)
[pweb_ONG] Portal Web ONG	(5,4)	(5,4)	(3,4)		
[email_ONG] Servicio Correo Electrónico	(6,6)	(5,4)	(5,7)	(5,7)	(6,9)
[E] Equipamiento	(7,2)	(6,8)	(6,8)	(5,7)	
[SW] Aplicaciones	(6,8)	(6,8)	(6,8)		
[prod_ONG] Sistemas Informáticos de Producción	(6,8)	(6,8)	(6,8)		
[spweb_ONG] Servicio Potal Web	(6,6)	(6,6)	(5,1)		
[off_ONG] Software ofimático	(6,8)				
[av_ONG] Antivirus	(2,7)				
[biom_ONG] Sistema para control de ingreso de personal	(6,2)	(5,7)	(2,7)		
[so_ONG] Sistema Operativo	(5,1)				
[HW] Equipos	(7,2)	(6,8)	(6,2)		
[sp_ONG] Servidor de Producción	(7,2)	(6,8)	(5,7)		
[sar_ONG] Servidor de Archivos de Respaldo	(2,5)	(2,1)	(2,1)		
[spp_ONG] Servidor Pruebas de Producción	(4,2)	(3,9)	(3,9)		
[spd_ONG] Servidor Pruebas de Desarrollo	(7,2)	(3,9)	(3,9)		
[sfe_ONG] Servidor de Facturación Electrónica	(7,2)	(5,7)	(5,7)		
[sbm_ONG] Servidor Biométrico	(7,2)	(5,7)	(5,7)		
[si_ONG] Servidor de instaladores	(4,2)	(3,9)	(3,9)		
[sws_ONG] Servidor Web Services	(7,2)	(6,2)	(6,2)		
[ac_ONG] Servidor de Comunicaciones	(7,2)	(6,2)	(6,2)		
[sa_ONG] Servidor de Aplicaciones	(7,2)	(6,2)	(6,2)		
[switch_ONG] Switch	(7,2)	(3,9)	(5,1)		
[router_ONG] Router	(7,2)	(3,9)	(5,1)		
[COM] Comunicaciones	(7,2)	(4,4)	(5,1)	(5,7)	
[lan_ONG] Red Lan	(7,2)	(4,4)	(5,1)	(5,7)	
[internet_ONG] Servicio de Internet	(7,2)	(4,4)	(5,1)	(5,7)	
[AUX] Elementos auxiliares	(5,1)				
[sai_ONG] Sistema de alimentación ininterrumpida	(0,98)				
[ac_ONG] Aire Acondicionado	(3,3)				
[cable_ONG] Cableado de datos	(5,1)				
[SS] Servicios subcontratados	(6,8)				
[intsub_ONG] Servicio de Internet	(6,8)				
[tel_ONG] Telefonia	(6,1)				
[hosting_ONG] Hosting	(4,5)				
[L] Instalaciones	(6,2)				
[cctrol_ONG] Cuarto de Control	(6,2)				
[P] Persona	(4,5)		(6,6)		
[admp_ONG] Administradores de sistemas	(4,5)		(6,6)		
[des_ONG] Desarrollador	(3,6)		(6,6)		
[ssw_ONG] Soporte de software	(4,3)		(6,6)		
[shw_ONG] Soporte de hardware	(4,3)		(6,6)		

Figura 2.17. Riesgo acumulado potencial
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	(6,0)	(4,4)	(4,7)	(3,8)	(5,6)
[B] Activos esenciales					
[IS] Servicios internos	(5,4)	(2,4)	(3,2)	(3,8)	(5,6)
[inter_ONG] Internet	(5,4)	(2,4)	(3,2)	(1,5)	(5,6)
[pweb_ONG] Portal Web ONG	(4,2)	(2,4)	(0,96)		
[email_ONG] Servicio Correo Electrónico	(5,4)	(2,4)	(3,2)	(3,8)	(5,6)
[E] Equipamiento	(5,0)	(4,4)	(4,4)	(3,2)	
[SW] Aplicaciones	(4,4)	(4,4)	(4,4)		
[prod_ONG] Sistemas Informáticos de Producción	(4,4)	(4,4)	(4,4)		
[spweb_ONG] Servicio Potal Web	(4,4)	(4,4)	(2,6)		
[off_ONG] Software ofimático	(4,4)				
[av_ONG] Antivirus	(0,85)				
[biom_ONG] Sistema para control de ingreso de personal	(3,8)	(3,2)	(0,85)		
[so_ONG] Sistema Operativo	(2,6)				
[HW] Equipos	(5,0)	(4,3)	(3,9)		
[sp_ONG] Servidor de Producción	(5,0)	(4,3)	(3,3)		
[sar_ONG] Servidor de Archivos de Respaldo	(0,84)	(0,72)	(0,76)		
[spp_ONG] Servidor Pruebas de Producción	(2,0)	(1,4)	(1,6)		
[spd_ONG] Servidor Pruebas de Desarrollo	(5,0)	(1,4)	(1,6)		
[sfe_ONG] Servidor de Facturación Electrónica	(5,0)	(3,2)	(3,3)		
[sbm_ONG] Servidor Biométrico	(5,0)	(3,2)	(3,3)		
[si_ONG] Servidor de instaladores	(2,0)	(1,4)	(1,6)		
[swa_ONG] Servidor Web Services	(5,0)	(3,7)	(3,9)		
[sc_ONG] Servidor de Comunicaciones	(5,0)	(3,7)	(3,9)		
[sa_ONG] Servidor de Aplicaciones	(5,0)	(3,7)	(3,9)		
[switch_ONG] Switch	(5,0)	(1,3)	(2,8)		
[router_ONG] Router	(5,0)	(1,3)	(2,8)		
[COM] Comunicaciones	(4,6)	(1,5)	(2,7)	(3,2)	
[lan_ONG] Red Lan	(4,6)	(1,5)	(2,7)	(3,2)	
[internet_ONG] Servicio de Internet	(4,6)	(1,5)	(2,7)	(3,2)	
[AUX] Elementos auxiliares	(3,6)				
[sai_ONG] Sistema de alimentación ininterrumpida	(0,69)				
[ac_ONG] Aire Acondicionado	(1,9)				
[cable_ONG] Cableado de datos	(3,6)				
[SS] Servicios subcontratados	(6,0)				
[intsub_ONG] Servicio de Internet	(6,0)				
[tel_ONG] Telefonia	(5,6)				
[hosting_ONG] Hosting	(3,7)				
[L] Instalaciones	(4,6)				
[cctrol_ONG] Cuarto de Control	(4,6)				
[P] Personal	(3,0)		(4,7)		
[admp_ONG] Administradores de sistemas	(3,0)		(4,7)		
[des_ONG] Desarrollador	(2,0)		(4,7)		
[ssw_ONG] Soporte de software	(2,7)		(4,6)		
[shw_ONG] Soporte de hardware	(2,7)		(4,6)		

Figura 2.18. Riesgo acumulado actual
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	(2,6)	(2,2)	(2,1)	(1,2)	(2,4)
[B] Activos esenciales					
[IS] Servicios internos	(2,1)	(0,89)	(0,95)	(1,2)	(2,4)
[inter_ONG] Internet	(2,1)	(0,89)	(0,95)	(0,56)	(2,4)
[pweb_ONG] Portal Web ONG	(0,99)	(0,89)	(0,47)		
[email_ONG] Servicio Correo Electrónico	(2,1)	(0,89)	(0,95)	(1,2)	(2,4)
[E] Equipamiento	(2,6)	(2,2)	(2,0)	(0,94)	
[SW] Aplicaciones	(2,2)	(2,0)	(2,0)		
[prod_ONG] Sistemas Informáticos de Producción	(2,2)	(2,0)	(2,0)		
[spweb_ONG] Servicio Potal Web	(2,2)	(2,0)	(0,85)		
[off_ONG] Software ofimático	(2,2)				
[av_ONG] Antivirus	(0,41)				
[biom_ONG] Sistema para control de ingreso de personal	(1,6)	(0,96)	(0,38)		
[so_ONG] Sistema Operativo	(0,88)				
[HW] Equipos	(2,6)	(2,2)	(1,7)		
[sp_ONG] Servidor de Producción	(2,6)	(2,2)	(1,1)		
[sar_ONG] Servidor de Archivos de Respaldo	(0,38)	(0,30)	(0,31)		
[spp_ONG] Servidor Pruebas de Producción	(0,73)	(0,66)	(0,66)		
[spd_ONG] Servidor Pruebas de Desarrollo	(2,6)	(0,66)	(0,66)		
[sfe_ONG] Servidor de Facturación Electrónica	(2,6)	(1,1)	(1,1)		
[sbm_ONG] Servidor Biométrico	(2,6)	(1,1)	(1,1)		
[si_ONG] Servidor de instaladores	(0,73)	(0,66)	(0,66)		
[sws_ONG] Servidor Web Services	(2,6)	(1,7)	(1,7)		
[sc_ONG] Servidor de Comunicaciones	(2,6)	(1,7)	(1,7)		
[sa_ONG] Servidor de Aplicaciones	(2,6)	(1,7)	(1,7)		
[switch_ONG] Switch	(2,6)	(0,65)	(0,91)		
[router_ONG] Router	(2,6)	(0,65)	(0,91)		
[COM] Comunicaciones	(2,0)	(0,68)	(0,83)	(0,94)	
[lan_ONG] Red Lan	(2,0)	(0,68)	(0,83)	(0,94)	
[internet_ONG] Servicio de Internet	(2,0)	(0,68)	(0,83)	(0,94)	
[AUX] Elementos auxiliares	(0,90)				
[sai_ONG] Sistema de alimentación ininterrumpida	(0,08)				
[ac_ONG] Aire Acondicionado	(0,55)				
[cable_ONG] Cableado de datos	(0,90)				
[SS] Servicios subcontratados	(2,3)				
[intsub_ONG] Servicio de Internet	(2,3)				
[tel_ONG] Telefonia	(1,8)				
[hosting_ONG] Hosting	(0,81)				
[L] Instalaciones	(1,7)				
[cctrol_ONG] Cuarto de Control	(1,7)				
[P] Personal	(0,79)		(2,1)		
[admp_ONG] Administradores de sistemas	(0,79)		(2,1)		
[des_ONG] Desarrollador	(0,61)		(2,1)		
[ssw_ONG] Soporte de software	(0,75)		(2,1)		
[shw_ONG] Soporte de hardware	(0,75)		(2,1)		

Figura 2.19. Riesgo acumulado objetivo
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

2.5.3. Informes

Mediante el uso de la herramienta Pilar se han obtenido como resultado de las evaluaciones realizadas varios gráficos:

La figura 2.20 muestra los parámetros de seguridad que se afectan en cada activo, prevaleciendo la Disponibilidad en la mayoría de activos.

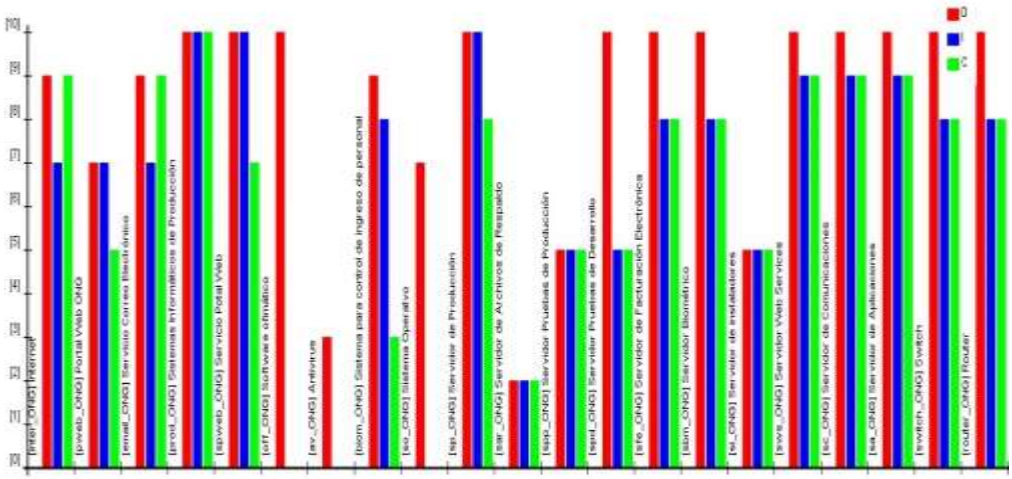


Figura 2.20. Valor de activo
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

En las figuras 2.21 y 2.22 se reflejan los valores del impacto y riesgos acumulados sobre cada uno de los activos definidos en las gráficas radiales, en el cual se consideran la implementación de las salvaguardas antes planteadas que permiten que estos valores disminuyan los parámetros de vulnerabilidad de los activos hasta el nivel objetivo.

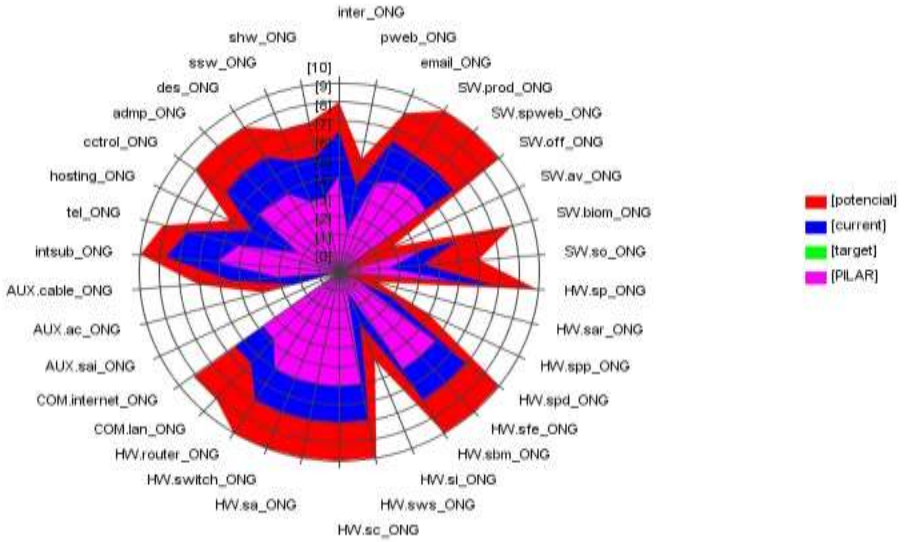


Figura 2.21. Impacto acumulado
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

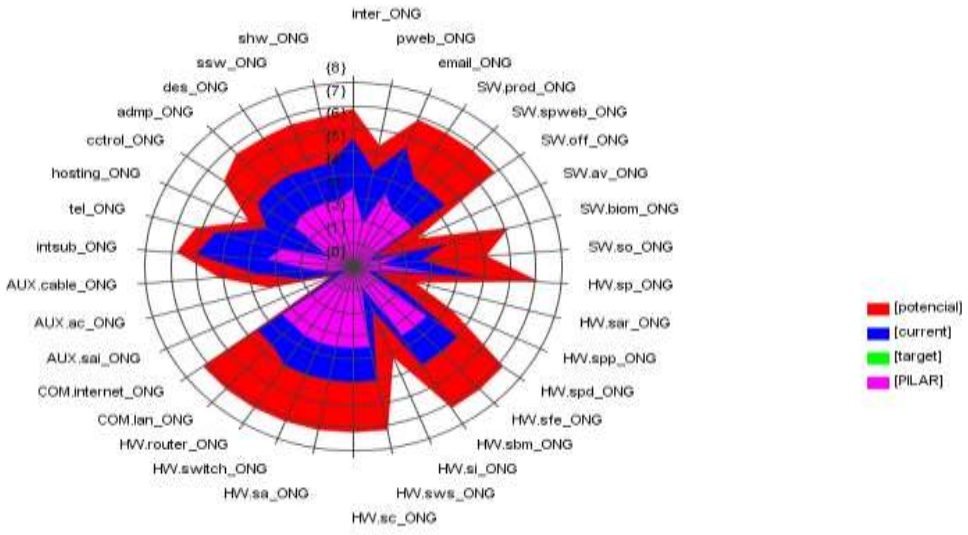


Figura 2.22. Riesgo acumulado
Fuente: Pilar - Departamento de Sistemas ONG
Elaboración: Autor

2.6. PLAN DE SEGURIDAD

Un plan de seguridad es una agrupación de tareas que se realiza por conveniencia, bien porque se trata de tareas que individualmente carecerían de eficacia, porque se trata de tareas con un objetivo común o porque se trata de tareas que competen a una única unidad de acción. [12]

2.6.1. Normativa de seguridad

Normativa sobre el uso autorizado de las aplicaciones informáticas

- El departamento de Sistemas es el responsable de la instalación y supervisión del software en los equipos informáticos y de telecomunicaciones de la ONG. Sólo se permitirá la instalación de programas con licenciamiento apropiado.
- No está permitido instalar ningún tipo de software, para fines personales o de recreación, en los equipos informáticos de la ONG.
- Para proteger los sistemas informáticos de la ONG, todos los equipos informáticos deben disponer de antivirus,

antimalware, privilegios de acceso, parches de seguridad, etc.

- Los empleados a los que se les asigna un equipo son los responsables de la protección lógica de los sistemas y son los encargados de informar al departamento de Sistemas sobre cualquier eventualidad.
- Las actualizaciones del software utilizado en la ONG se llevaran a cabo de acuerdo al plan de actualización desarrollado por el departamento de Sistemas.
- El departamento de Sistemas es el responsable de realizar revisiones periódicas para asegurar que sólo programas con licencia están instalados en los computadores de la organización.
- No está permitido almacenar en los equipos informáticos de la ONG información de tipo personal como fotos, música, videos, juegos o archivos informáticos que no correspondan al trabajo que desarrolla el empleado en la Organización.
- Es responsabilidad del departamento de Sistemas dictar las normas, procedimientos y calendarios de la auditoría.

- El departamento de Sistemas administrará las licencias de todo el software de la ONG y vigilará su vigencia de acuerdo a la normativa de organización.
- Todo software de propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades de la ONG.
- Los empleados tienen la obligación de verificar que la información y que los medios de almacenamiento que utilizan para la misma, estén libres de cualquier tipo de software dañino, por lo que siempre deben utilizar un antivirus.

Normativa sobre el uso de equipos informáticos

- Todo equipo informático que esté conectado a la red de la ONG debe sujetarse a las normas y procedimientos de instalación que estipule el departamento de Sistemas.
- El departamento de Sistemas deberá tener un registro actualizado de todos los equipos informáticos de la Organización.
- El cuidado de los equipos informáticos le corresponde a la persona a la cual se le asignó, y es su responsabilidad

notificar al departamento de Sistemas sobre cualquier anomalía.

- El departamento de Sistemas es el responsable de la instalación y del mantenimiento preventivo y correctivo de los equipos informáticos. Los responsables de los equipos informáticos no deberán moverlos, instalar o desinstalar dispositivos.
- No se podrá consumir alimentos o ni bebidas mientras se estén utilizando los equipos informáticos de la ONG.
- En el supuesto que existiera un daño en los equipos informáticos por negligencia del empleado responsable del mismo, éste deberá a cubrir el valor de la reparación o reposición del mismo.

Normativa sobre la protección de la información

- El servidor de almacenamiento compartido es exclusivo para respaldos de información de los usuarios finales.
- Los empleados de la ONG deberán hacer un respaldo periódico de la información que administran en sus equipos informáticos.

- El código fuente de las aplicaciones informáticas de la ONG se respaldan mensualmente en discos compactos y es responsabilidad del departamento de Sistemas.
- La información de la base de datos de la ONG se almacena diariamente en la Nube de la organización y es responsabilidad del departamento de Sistemas.

Normativa de uso de los servicios de Red

- El departamento de Sistema es el ente responsable de proporcionar a los usuarios el acceso a los recursos informáticos de la red de la organización.
- Según los lineamientos institucionales, le corresponde al departamento de Sistemas administrar, mantener y actualizar la infraestructura de la red de la ONG.
- Los recursos disponibles a través de la red serán de uso exclusivo para asuntos concernientes con las actividades de la organización.
- Todo equipo informático que esté o sea conectado a la red de la ONG, debe de sujetarse a los protocolos de acceso que emite el departamento de Sistemas.

Normativa sobre el uso del servicio de internet

- El acceso al servicio de internet es exclusivamente para actividades concernientes a la ONG.
- La información de los mensajes de correo electrónico y de los archivos adjuntos debe ser considerada como propiedad de la ONG.
- Está prohibido descargar cualquier tipo de software en los equipos informáticos de la organización.

Normativa sobre la protección de las instalaciones

- La Dirección General deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.
- El acceso del personal se llevará a cabo de acuerdo a las normas y procedimientos que disponga la Dirección General.
- Se llevará un registro permanente del acceso y salida de personal, invitados y visitantes sin excepción.

Normativa sobre la gestión del personal

- Establecer normas de conducta de los colaboradores de la ONG para formar un ambiente laboral adecuado y armonioso.
- Los contratos de trabajo de la ONG deberán contener cláusulas de confidencialidad para evitar fugas de información de la organización.
- Se deben realizar capacitaciones periódicas tanto para el personal técnico como para el personal administrativo.

2.6.2. Plan de capacitación

El coordinador del plan de tratamiento de riesgos tecnológicos, nombrado por el jefe de Sistemas; tendrá la función de estructurar, implementar y evaluar las actividades del plan, a través de capacitaciones y simulacros de situaciones extremas que permitan al personal del departamento de sistemas adquirir las destrezas para enfrentar exitosamente cualquier eventualidad crítica con éxito.

También se dará talleres y charlas al personal administrativo de la ONG, para explicar las directrices de cómo proceder ante una emergencia tecnológica.

La periodicidad de la capacitación debe ser cada seis meses o en forma extraordinaria cuando exista algún cambio en la infraestructura tecnológica de la ONG o se integre un nuevo miembro al departamento de Sistemas.

2.6.3. Plan de ejecución

El proceso para implementar el plan de tratamiento de los riesgos existentes en la ONG es el siguiente:

En primer lugar se aplicaron las salvaguardas con nivel L0 como medidas preventivas.

A continuación se aplicaron las salvaguardas que poseen niveles L1 y L2, estas son aquellas en las que se encuentran los procesos que necesitan mejoras en su gestión.

Por último se aplicaron las salvaguardas de nivel L3 y L4 a los procesos implementados que deben continuar y optimizarse.

CAPÍTULO 3

EVALUACIÓN DE RESULTADOS

3.1. CAPACITACIÓN

Las jornadas de capacitación para el presente Plan de tratamiento de riesgos tecnológicos duraron tres días y fueron organizadas por cada área del departamento de Sistemas:

El área de desarrollo dio prioridad al respaldo, recuperación y puesta en ejecución de los servidores, sistemas informáticos, bases de datos, portal web de facturación electrónica y sistema de control biométrico.

Se hizo énfasis en que se debe asegurar la disponibilidad del servicio y la integridad de los datos mediante la evaluación de las salvaguardas y los controles diarios.

El área de soporte de software priorizó el conocimiento de los procesos críticos que lleva a cabo cada departamento de la ONG, para poder dar una solución inmediata a cualquier eventualidad reportada por los usuarios, tomando como criterio principal la disponibilidad de los servicios que oferta la ONG.

El área de soporte de Hardware conoció las actividades a ejecutar para servir de apoyo al área de desarrollo y al área de soporte de software, servidores y equipos de desarrollo, y realizó un plan de mantenimiento de los equipos sin descuidar el soporte a los usuarios.

También se dictó una charla de concientización al personal administrativo acerca de las vulnerabilidades y amenazas informáticas a los que están expuestos y las buenas prácticas sobre la utilización de la tecnología.

En cada jornada de capacitación se realizó un registro del personal técnico o administrativo que fue sido capacitado y se elaboró un acta para evidenciar dicho proceso formativo.

3.2. EJECUCIÓN

A lo largo de la aplicación del Plan de Tratamiento de Riesgos Informáticos en la ONG se realizaron varias actividades:

- Se contrató a una empresa para la colocación y mantenimiento de cámaras de seguridad para controlar el ingreso y permanencia en el cuarto de control.
- Se realizó una auditoría a los computadores del personal administrativos para verificar si habían instalado software no autorizado en dichos equipos.
- Se realizó la recarga de los extintores del departamento de informática y del cuarto de control.
- Se realizó la compra de Switches y Routers que sirvan como reposición ante la eventualidad de fallo de alguno de los equipos de comunicación con el objetivo de mantener la disponibilidad de los servicios.
- Se implementó un servidor de Backup como medida de contingencia para el servidor de producción y los sistemas informáticos que almacena.
- Se realizó el mantenimiento de los UPS de los servidores y de los equipos del departamento de sistemas.

- Se respaldó la información de la base de datos de la ONG en la nube.
- Se presentó a la dirección financiera la necesidad de la construcción y equipamiento de un Centro de Datos alterno como medida de contingencia ante una eventualidad de gran magnitud.

3.3. PRUEBAS

Se sugirió a la dirección general que las pruebas del Plan de Tratamientos de Riesgos Tecnológicos se deberían realizar mayo y diciembre, al igual que las capacitaciones al personal del departamento de sistemas y administrativo.

Éstas estarían subordinadas a cambios por la implementación de soluciones informáticas o actualizaciones en el plan de tratamiento de riesgos informáticos.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La gestión de riesgos y sus metodologías mediante las cuales se hace frente a las amenazas de una organización, actualmente son procesos prioritarios en las empresas, ya que el su éxito o fracaso de la empresa depende en gran medida de ellos. [13]

2. Con el Plan de Tratamiento de Riesgos Tecnológicos se establecieron normativas y procesos que permiten al personal del departamento de Sistemas, mantener la disponibilidad, integridad y disponibilidad de los sistemas y servicios informáticos de la ONG.

3. La utilización de la metodología MAGERIT permitió la identificación y clasificación de los principales activos de información de la ONG, así como determinar las posibles amenazas a las que está expuesta la organización; las mismas que fueron controladas utilizando medidas preventivas y correctivas.

4. La herramienta PILAR se utilizó para identificar los activos de la ONG, evaluar las amenazas y definir salvaguardas para obtener los niveles de criticidad de riesgo e impacto; permitiendo determinar la necesidad de implementar normativas y procedimientos para proteger los bienes y la información de la organización.

Recomendaciones

1. Mantener actualizado el Plan de tratamiento de riesgos tecnológicos, para identificar riesgos que puedan afectar a los principales procesos de la organización, para lo cual se debe nombrar un responsable dentro del Departamento de Sistemas.

2. Capacitar al personal del departamento de Sistemas en temas relacionados al análisis y gestión de riesgos y en tópicos sobre seguridad informática, de tal manera que sea más eficiente la implementación y seguimiento de las medidas presentadas en el presente Plan.

3. Definir a MAGERIT como metodología institucional de la ONG, para continuar con el análisis y la gestión de riesgos, de tal manera que permita estar preparados para enfrentar y solventar cualquier amenaza futura a los activos tecnológicos de la organización.

4. Para continuar en la línea de trabajo de reducción de los riesgos tecnológicos a los que está expuesta la ONG, se recomienda desarrollar un análisis de riesgo cuantitativo donde se considere el costo económico para la organización si se materializan las amenazas, así como la inversión para implementar y mantener las salvaguardas.

BIBLIOGRAFÍA

[1] Gestión de Calidad Consulting, Riesgo y Gestión de Riesgos en el contexto ISO, http://gestion-calidad.com/riesgo-y-gestion-de-riesgos-en-el-contexto-iso , fecha de la consulta mayo de 2020

[2] Consejo Superior de Administración Electrónica, MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html, fecha de la consulta mayo de 2020

[3] Consejo Superior de Administración Electrónica, MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html, fecha de la consulta mayo de 2020

[4] Consejo Superior de Administración Electrónica, MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html, fecha de la consulta mayo de 2020

[5] Consejo Superior de Administración Electrónica, MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html, fecha de la consulta mayo de 2020

[6] A. Barco and J. Mañas, Eds., GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-470D) - MANUAL DE USUARIO PILAR Versión 5.1, 2011.

[7] Seguridad Informática BRM, Amenazas de seguridad, https://seguridadeinformaticabrm.wordpress.com/2017/02/03/amenazas-de-seguridad/, fecha de la consulta mayo de 2020

[8] Consejo Superior de Administración Electrónica, MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html, fecha de la consulta junio de 2020

[9] Consejo Superior de Administración Electrónica, MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html, fecha de la consulta mayo de 2020

[10] Consejo Superior de Administración Electrónica, PILAR – Glosario de términos, https://www.pilar-tools.com/es/glossary/index.html , fecha de la consulta mayo de 2020

[11] Consejo Superior de Administración Electrónica, MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html, fecha de la consulta mayo de 2020

[12] Consejo Superior de Administración Electrónica, MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html, fecha de la consulta mayo de 2020

[13] M. Raffino, *Concepto.de*, https://concepto.de/gestion-de-riesgos/, fecha de la consulta 03 de julio de 2020.