DOI: http://dx.doi.org/10.23857/dc.v7i6.2332

Ciencias Técnicas y Aplicadas
Artículo de investigación

Diseño de la estructura de un manual de políticas de seguridad de la información para la Unidad de Informática del Gobierno Autónomo Descentralizado Municipal del Cantón Camilo Ponce Enríquez

Design of the structure of a manual of information security policies for the Information Department of the Gobierno Autónomo Descentralizado Municipal of the Camilo Ponce Enríquez

Desenho da estrutura de um manual de política de segurança da informação para a Unidade de Informática da Prefeitura Municipal Autônoma Descentralizada do Cantão Camilo Ponce Enríquez

Ronald Javier Condoy Orellana [I]
condoyronald@hotmail.com
https://orcid.org/0000-0002-0295-0224

Jenny Karina Vizñay Durán [II]
jviznay@ucacue.edu.ec
https://orcid.org/0000-0001-7557-5034

Correspondencia: condoyronald@hotmail.com

***Recibido:** 30 de agosto de 2021 ***Aceptado:** 15 de septiembre de 2021 *** Publicado:** 12 de octubre de 2021

I. Estudiante de la Carrera de Ingeniería de Sistemas. Universidad Católica de Cuenca, Cuenca, Ecuador.

II. Ingeniera de Sistemas, Docente de la Unidad Académica de Informática, Ciencias de la Computación e Innovación Tecnológica, Grupo de Investigación Simulación, Modelado, Análisis y Accesibilidad (SMA2), Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

El masivo uso de la tecnología ha demostrado la necesidad imperiosa de la gestión de la seguridad de la información. En los GAD Municipales debido a la naturaleza de la información que manejan, el aspecto seguridad debe ser un aspecto prioritario; sin embargo, se conoce que no ha recibido la importancia requerida, motivo por el cual esta investigación se orienta al diseño de la estructura de un manual de políticas de seguridad basado en normativas y buenas prácticas internacionales y nacionales que sirvan al GAD objeto de estudio como una guía en la gestión de la confidencialidad, integridad y disponibilidad de los activos de información.

Se inicia con el análisis de la situación actual con enfoque ISO 27001, luego se realiza el análisis de riesgos en los activos de información, basado en la metodología Magerit; de los resultados obtenidos se eligen los activos de mayor incidencia y se realiza una alineación de éstos con los dominios y objetivos de control de la ISO/IEC 27002:2013, obteniendo así los dominios de Seguridad de la Información que en un futuro deben ser considerados para la elaboración de un manual de seguridad de la información.

Palabras clave: Políticas de seguridad; ISO/IEC 27002:2013; riesgos; vulnerabilidades.

Abstract

The massive use of technology has demonstrated an imperative need for information security management. In the Municipal GADs, due to the nature of the information they handle, the security should be a priority aspect; However, it is known that it has not received the required importance, so this research is oriented to the design of the structure of a security policy manual based on international and national regulations and good practices that serve the GAD under study as a guide in managing the confidentiality, integrity and availability of information assets.

The study begins with the analysis of the current situation with an ISO 27001 approach, then the risk analysis is carried out on the information assets, based on the Magerit methodology; From the results obtained, the assets with the greatest incidence are chosen and they are aligned with the domains and control objectives of ISO / IEC 27002: 2013, thus obtaining the Information Security domains that should be considered in the future. for the preparation of an information security manual.

Keywords: Security politics; ISO/IEC 27002:2013; risks; vulnerabilities.

Resumo

O uso massivo de tecnologia demonstrou a necessidade imperiosa de gerenciamento de segurança da informação. Nos GADs Municipais, pela natureza das informações que tratam, o aspecto da segurança deve ser prioritário; No entanto, sabe-se que não tem recebido a importância exigida, razão pela qual esta pesquisa se orienta para o desenho da estrutura de um manual de política de segurança baseado em normas e boas práticas internacionais e nacionais que servem como guia ao GAD em estudo. na gestão da confidencialidade, integridade e disponibilidade dos ativos de informação.

Inicia-se com a análise da situação atual com uma abordagem ISO 27001, em seguida é realizada a análise de risco sobre os ativos de informação, com base na metodologia Magerit; A partir dos resultados obtidos, são escolhidos os ativos com maior incidência e alinhados aos domínios e objetivos de controle da ISO / IEC 27002: 2013, obtendo-se assim os domínios de Segurança da Informação que deverão ser considerados no futuro. manual de segurança da informação.

Palavras-chave: Políticas de segurança; ISO / IEC 27002: 2013; riscos; vulnerabilidades.

Introducción

Las empresas, organizaciones, instituciones a nivel mundial han fundamentado mayoritariamente sus procesos en el uso de las tecnologías de información, dejando así observar que es una necesidad inminente la gestión de la seguridad de la información. A pesar de ello, se ha observado que no existe un aprovechamiento o rendimiento óptimo a nivel de hardware o software, debido principalmente al débil control, o peor aún a la inexistencia de políticas de seguridad de la información, trayendo como consecuencia el uso no apropiado de los activos de información que pueden desencadenar en la presencia de riesgos que provoquen inseguridad en los datos que podrían causar pérdidas, daños o ataques que perjudiquen a la institución.

En las Normas de Control Interno de la Contraloría General de Estado (Contraloría General del Estado, 2019), dispuesto para las entidades y los organismos del sector público, en el código Nro. 400 Actividades de Control, señala que, “La máxima autoridad de la entidad y las servidoras y servidores responsables del control interno de acuerdo a sus competencias, establecerán políticas y procedimientos para manejar los riesgos en la consecución de los objetivos institucionales, proteger y conservar los activos y establecer los controles de acceso a los sistemas de información”.

De acuerdo a (Presidencia de la República del Ecuador, 2021), el Código Orgánico de Organización Territorial y Autonomía Descentralizada menciona que: "los Gobiernos Autónomos Descentralizados Municipales son personas jurídicas de derecho público de autonomía política, administrativa y financiera que se centra en brindar servicios y principios a la ciudadanía en competencia de obras y servicio de calidad, control territorial y participación ciudadana, respetando los ámbitos sociales, económicos y culturales".

El GAD Municipal del Cantón Camilo Ponce Enríquez gestiona información confidencial procesada y almacenada en los activos de información que abarcan la situación territorial, ocupacional y financiera en competencia del cantón, convirtiéndole en información altamente vulnerable. Por lo tanto, se requiere de políticas de seguridad de la información que mitiguen la manipulación, suplantación y pérdida, ante la presencia de amenazas, que podría provocar complicaciones a la funcionalidad de la institución, por ello, se plantea el objetivo: Diseñar la estructura de un manual de políticas de seguridad de la información para la gestión apropiada de los recursos informáticos de la Unidad de Informática del GAD Municipal del Cantón Camilo Ponce Enríquez promoviendo la disponibilidad, confidencialidad e integridad de los recursos informáticos. Esta estructura se ampara en lineamientos basados en normativas y metodologías que permitan la correcta gestión de seguridad de la información.

Desarrollo

Conceptos relacionados

Amenazas. - Eventos que se pueden suscitar en la institución para causar daños a los recursos informáticos que cuenten con información importante, violando la seguridad con accesos no autorizados generando grandes pérdidas (Baca Urbina, 2016).

Vulnerabilidad. - Debilidad que se puede presentar en algún recurso tecnológico, que facilite la presencia de eventos intencionales o no intencionales y que pongan en riesgos a la información (Ortiz, 2021).

Políticas de seguridad. - Conjunto de reglas que el personal de una organización debe respetar para poder acceder a los recursos informáticos y a los datos. Son desarrolladas para salvaguardar la información de la organización, brindando a los datos su integridad, disponibilidad y confidencialidad (Vega Velasco, 2008).

Seguridad de la información. - Disciplina basada en un conjunto de medidas preventivas que se encarga de diseñar métodos, técnicas o normativas confiables para salvaguardar y proteger la información que contienen los recursos informáticos (Figueroa Suárez, Rodríguez Andrade, Bone Obando, & Saltos Gómez, 2017).

Manual de políticas de Seguridad de la Información. – Es un conjunto de lineamientos, reglas, leyes y normas establecidas por la gerencia con ámbito legal, las cuales deben ser acatadas por todo el personal que utilice las tecnologías de la información y comunicación, con la finalidad de gestionar, controlar y salvaguardar la información.

Confidencialidad. - Tiene como objetivo impedir que la información sea divulgada a personal no autorizado.

Integridad. - Mantiene los datos sin modificaciones o alteraciones por personas no autorizadas. Teniendo la información tal como fue generada por la persona encargada.

Disponibilidad. – Refiere a la disposición de la información en el momento que sea requerido acceder a ella.

Riesgo. - Evento no esperado que impide el cumplimiento de alguna tarea, mismo que contraer numerosas pérdidas en relación a la información que se cuenta en recursos informáticos (Sena & Tenzer, 2004).

Impacto. – Es la forma de poder encontrar el deterioro producido sobre el activo derivado de materialización de una amenaza

Salvaguardas. – Son conocidas también como contra medidas, aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo en un activo.

Riesgo acumulado. – Es el cálculo que tomando en consideración el valor propio de un activo y el valor de los activos que depende de él, este valor se concatena con el deterioro causado por una amenaza y la estimación de la frecuencia con la que se realiza la misma (Magerit, 2012).

Riesgo potencial. – Son aquellos supuestos riesgos de los activos en caso de que no existiera salvaguardas presentes.

Riesgo repercutido. – Es el cálculo tomando en cuenta únicamente el valor propio que tiene un activo, este valor se ajusta con la degradación causada por una amenaza y la estimación de la frecuencia de la misma (Magerit, 2012).

Riesgo residual. – Es aquel riesgo que se permanece en el activo después del tratamiento del riesgo y la aplicación de las salvaguardas determinadas (Deloitte, 2015).

ISO 27001. – Esta es una norma Internacional dirigida para los Sistemas de Gestión de la Seguridad de la Información que permite evaluar riesgos para así mediante óptimos controles poder disminuir o eliminar riesgos y fortalecer la confidencialidad e integridad de los datos (La Universidad en Internet, 2019).

Análisis de riesgos. - Evaluación por medio de los activos existentes en una organización permita determinar su estado, su valor, eventos inesperados, daños y consecuencias que se pueden presentar; facilitando la elaboración de un plan de seguridad que permita cumplir con los objetivos de seguridad de la organización, para la mitigación de riesgos y amenazas en los activos (Magerit, 2012).

Magerit. - Metodología de análisis y gestión de riesgos de los sistemas de información que implementa el Proceso de Gestión de Riesgos dentro de un marco de una organización, para que las altas gerencias tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información (Magerit, 2012).

Herramienta P.I.L.A.R. – Su significado "Procedimiento Informático - Lógico utilizado para el análisis de riesgos", esta es una herramienta basada en la metodología Magerit, desarrollada en el Centro Nacional de Inteligencia de España, orientado para brindar soporte al análisis de riesgos de sistemas de información, PILAR está dirigida para organizaciones que hacen uso de las TIC y que requieran gestionar eficientemente sus activos (Centro Nacional de Inteligencia de España, 2014).

Norma ISO /IEC 27002:2013. - Norma Internacional entre la ISO (Organización Internacional de Normalización) y la IEC (Comisión Electrotécnica Internacional) proporciona pautas para los estándares de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluida la selección, implementación y gestión de la organización (Organización Internacional de Normalización, 2013).

Norma NTE INEN-ISO/IEC 27002. - Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002 es una traducción idéntica de la Norma Internacional ISO/IEC 27002:2013 (Servicio Ecuatoriano de Normalización INEN, 2017).

Trabajos Relacionados

En el año 2015, se realizó un proyecto titulado "Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato", con la finalidad de brindar seguridad a la información usando la norma ISO 27002:2013. En primer lugar, se analizó la situación actual de la dirección, mediante

entrevistas y estudios a la red inalámbrica. A partir de los resultados, se elaboraron políticas de seguridad basado en los dominios de ISO 27002:2013, considerando los más óptimos para mejorar el control y prevención de vulnerabilidades en la información y mantener la continuidad del negocio de la dirección (Torres Núñez, 2015).

En el año 2019, el trabajo de investigación titulado "Políticas de seguridad para las tecnologías de la información y comunicación en la empresa Borja Inborja S.A.", propuso una estructura de políticas de seguridad, misma que identificó inicialmente el nivel de seguridad que existía utilizando la ISO 27001. Luego, con la finalidad de establecer los riesgos a los cuales las TICs están mayormente expuestas, se realizó un análisis de riesgos a través de la metodología Magerit y la herramienta Pilar. Posteriormente, con los riesgos identificados, se elabora una propuesta que consta de la alineación con los dominios y controles de la ISO 27002, mismos que deberían ser considerados para la elaboración de las políticas de seguridad. Finalmente, el autor resalta los beneficios de su trabajo, en la medida que permite mejorar los procesos tecnológicos de la empresa en un futuro (Pulla Vásquez, 2019).

En el año 2020, se publicó un artículo denominado "Políticas de seguridad de la información bajo la norma ISO 27002:2013 para el Gobierno Autónomo Descentralizado del Cantón Biblián", en el que resalta la importancia de las políticas de seguridad, puesto que mitigan los riesgos en los sistemas, en el uso de la información y en las redes. Los autores parten de un análisis de la situación actual del proceso de la seguridad de la información, luego utilizan la metodología cuantitativa (entrevistas) en la que identifican los riesgos informáticos en los activos, mismos que permiten plantear la propuesta de políticas de seguridad de la información para resguardar y proteger la información. Los actores concluyen que para la implementación de políticas de seguridad se deben seguir lineamientos de normas vigentes y procesos metodológicos. Además, destaca que es importante la implementación de políticas puesto que ayuda a mantener segura a la información del GAD y permite a los funcionarios el uso correcto de los activos de información (Álvarez Lozano & Andrade López, 2020).

Metodología

El presente proyecto inicia con el análisis de la situación actual de la institución en relación a temas de seguridad de la información con la elaboración y aplicación de un cuestionario basado en los

controles de la Norma ISO 27001, estos resultados se retroalimentan con la respuesta obtenida de una entrevista aplicada al jefe de Tecnología.

En segunda instancia, luego de haber conocido la situación inicial, se realiza el análisis de riesgos con la herramienta Pilar (basada en la metodología MAGERIT), que permita observar el grado de seguridad en los activos de información y seleccionar los riesgos que requieran mayor atención en conjunto con la recomendación de salvaguardas.

Posteriormente, se desarrolla la alineación de los activos prioritarios y sus salvaguardas con los dominios y controles de la norma ISO/IEC 27002 que permita determinar los enfoques que deben tener las normas de seguridad, de acuerdo a la materialización de los posibles riesgos.

Finalmente, en base al resultado de la alineación se propone pautas para las políticas de seguridad, y; se hace las recomendaciones pertinentes para la elaboración del manual de políticas de seguridad para la Unidad de Informática del GAD Municipal del Cantón Camilo Ponce Enríquez.

Resultados

Análisis de la situación actual

Se inicia con la elaboración de un cuestionario basado en la ISO 27001 en donde se abordan los diferentes dominios y controles de seguridad, el formulario contiene una lista de controles agrupados en 11 secciones, mismos que son marcados por el jefe de informática a través del checklist.

Por su parte, los resultados se representan a través de tres rangos de valoración en función del cumplimiento de los controles (ver tabla 1):

Tabla 1: Diagnóstico de la ISO 27001

DIAGNÓSTICO (ISO 27001)	
CONTROLES AGRUPADOS POR ÁREAS	**RANGO DE VALORACIÓN**
POLÍTICAS DE SEGURIDAD	0% a 33%
DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
ORGANIZACIÓN DE LA SEGURIDAD	34% a 66%
SEGURIDAD DE LOS RRHH	
GESTIÓN DE COMUNICACIONES Y OPERACIONES	
CONTROL DE ACCESOS	
SEGURIDAD FÍSICA Y DEL AMBIENTE	
ADMINISTRACIÓN DE INCIDENTES	
CUMPLIMIENTO	
ADMINISTRACIÓN DE ACTIVOS	67% a 100%

Fuente: Autoría Propia

Los resultados obtenidos en la encuesta se resumen en:

- Áreas que requieren mayor atención: políticas de seguridad, desarrollo y mantenimiento de los sistemas y continuidad del negocio.
- Áreas de mediana atención: organización de la seguridad, seguridad de los RRHH, gestión de comunicaciones y operaciones, control de accesos, seguridad física y del ambiente, administración de incidentes, cumplimiento.
- Área que requiere menor atención: administración de activos.

Inicialmente se tiene que son dos áreas las que requieren mayor atención. Sin embargo, al proponer la gestión de seguridad de la información por primera vez, es necesario delimitar más su alcance para tratar un área como prioridad, es así que se realiza la aplicación de una entrevista al jefe de Informática sobre aspectos de prioridad y los riesgos observables en la gestión diaria de los procesos concernientes a los activos, se decide que el área prioritaria para este caso de estudio es: Políticas de Seguridad.

Análisis de Riesgos

Una vez determinado que "Políticas de Seguridad" es el área prioritaria a ser tratada, se procede con el análisis de riesgos basado en la metodología Magerit, soportada con la herramienta Pilar. Los pasos que considera la metodología son: identificación y valoración de los activos, determinación de las amenazas expuestas a los activos, determinación de las salvaguardas, determinación del impacto y riesgo y selección de los activos prioritarios.

Identificación y valoración de activos. - Se realiza un levantamiento de activos, donde se determina un total de 24 activos, mismos que para un mejor manejo se han agrupado por criterios de similitud de uso, grado de importancia y categoría, siendo estos clasificados por:

- Aplicaciones (Sistemas informáticos).
- Equipos (Servidores, laptops, router, switch).
- Comunicaciones (Internet, red LAN).
- Datos (Gestores de base de datos).
- Personal (Personal encargado en la Unidad).

Para realizar la valoración de los activos se considera los criterios de valoración que proporciona Magerit (ver tabla 2).

Tabla 2: Criterios de valoración

NIVEL	CRITERIO
10	Muy Alto (+)
9	Muy Alto (-)
8	Alto (+)
7	Alto (-)
6	Medio (+)
5	Medio (-)
4	Bajo (+)
3	Bajo (-)
2	Muy Bajo (+)
1	Muy Bajo (-)
0	Depreciable

Fuente: Magerit

En base a las consideraciones anteriores, se obtiene la siguiente valoración en función a la importancia de cada activo en las dimensiones de seguridad de Magerit: disponibilidad, integridad y confidencialidad en los activos de la Unidad de Informática (ver ilustración 1).

Ilustración 1: Valoración de los Activos

activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
[IS] Servicios internos			
[E] Equipamiento			
[SW] Aplicaciones			
[SW-001-SIGAME] SISTEMA CONTABLE SIG-AME	[8]	[9]	[8]
[SW-002-SII] SIIM Sistema Integral de Información Multi-Finalitario	[8]	[9]	[8]
[SW-003-SIRP] SIRP Sistema Informático para Automatización del Registro de la Propi	[7]	[9]	[8]
[SW-004-AM] Attendance management	[4]	[5]	[6]
[SW-005-HO] HERRAMIENTAS OFIMATICAS	[3]	[n.a.]	[2]
[SW-006-SO] SISTEMA OPERATIVO	[5]	[4]	[5]
[SW-007-AV] ANTIVIRUS	[6]	[3]	[2]
[HW-007-PW] PAGINA WEB	[5]	[2]	[n.a.]
[HW-009-CE] CORREO ELECTRONICO	[5]	[4]	[5]
[HW] Equipos			
[HW-001-SERV] SERVIDORES	[7]	[n.a.]	[5]
[HW-002-PC] COMPUTADORAS PORTATIL	[6]	[n.a.]	[n.a.]
[HW-003-IMP] IMPRESORA	[4]	[n.a.]	[n.a.]
[HW-004-M] MONITOR	[2]	[n.a.]	[n.a.]
[HW-005-UPS] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	[2]	[n.a.]	[n.a.]
[HW-006-ST] SWITCH	[6]	[n.a.]	[n.a.]
[HW-007-RT] ROUTER	[6]	[3]	[4]
[HW-008-HDD] DISCO DURO	[3]	[n.a.]	[5]
[COM] Comunicaciones			
[COM-001-NET] INTERNET	[7]	[6]	[6]
[COM-002-LAN] RED LAN	[6]	[5]	[7]
[COM-003-RI] RED INALAMBRICA	[2]	[3]	[4]
[AUX] Elementos auxiliares			
[D] DATOS			
[D-001-GBD] GESTOR DE BASE DE DATOS	[7]	[8]	[8]
[SS] Servicios subcontratados			
[L] Instalaciones			
[P] Personal			
[PGAD] PERSONAL GAD			
[PGAD-001-JEFE] JEFE DE UNIDAD DE INFORMÁTICA	[6]	[2]	[7]
[PGAD-002-ANALIST] ANALISTA DE INFORMATICA	[6]	[2]	[7]
[PGAD-003-ASIST] ASISTENTE INFORMÁTICO	[2]	[2]	[4]

Fuente: Herramienta Pilar

Determinación de las amenazas. – Con el uso de la herramienta PILAR y el apoyo del jefe de Tecnología se determina las amenazas que podrían materializar el riesgo en los activos como consecuencia de no realizar un tratamiento correcto, estas amenazas se presentan a continuación por categoría de activos (ver tabla 3).

Tabla 3: Determinación de las amenazas

AMENAZAS				
APLICACIONES	**EQUIPOS**	**COMUNICACIONES**	**DATOS**	**PERSONAL**
[I.5] Avería de origen físico o lógico [E.8] Difusión de software dañino [E.20] Vulnerabilidades de los programas [E.21]Errores de mantenimiento / actualizaciones de programas [E.24] Caída del sistema por agotamiento de recursos [A.8] Difusión de software dañino. [A.11] Acceso no autorizado [A.22] Manipulación de programas.	[N.1] Fuego [I.2] Daños por agua. [I.3] Contaminación medioambiental [I.4] Contaminación electromagnética [I.5] Avería de origen físico y lógico [I.6] Corte de suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.11] Emanaciones electromagnéticas [E.23] Errores de mantenimiento [E.24] Caída del sistema por agotamiento de recursos. [E.25] Perdida de equipos [A.7] Uso no previsto [A.11] Acceso no autorizado. [A.23] Manipulación de hardware [A.24] Denegación del servicio [A.25] Robo de equipos [A.26] Ataque destructivo	[I.8] Fallo de servicio de comunicaciones [E.2] Errores del administrador del sistema/ de la seguridad [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.15] Alteración de la información [E.19] Fugas de información [E.24] Caída del sistema por agotamiento de recursos [A.5] Suplantación de identidad [A.7] Uso no previsto [A.9] [Re-]encaminamiento de mensajes [A.11] Acceso no autorizado [A.12] Análisis de trafico [A.14] Interceptación de información [A.15] Modificación de información [A.18] Destrucción de la información [A.24] Denegación de servicio	[I.5] Avería de origen físico [E.8] Difusión de software dañino [E.15] Alteración de la información [E.18] Destrucción de la Información [E.19] Fugas de la Información [E.20] Vulnerabilidades de los programas [E.21]Errores de mantenimiento / actualizaciones de programas [A.5] Suplantación de identidad [A.6] Abuso de privilegios de acceso. [A.8] Difusión de software dañino. [A.11] Acceso no autorizado [A.22] Manipulación de programas	[E.15] Alteración de la información [E.18] Destrucción de la Información [E.19] Fugas de la Información. [E.28] Indisponibilidad del personal [A.15] Modificación de la Información. [A.18] Destrucción de la información [A.19] Revelación de la información [A.28] Indisponibilidad del Personal [A.29] Extorsión [A.30] Ingeniería social (picaresca)

Fuente: Herramienta Pilar

Identificación de las salvaguardas. – Una vez determinadas las amenazas, la herramienta PILAR presenta un listado de posibles salvaguardas generales basadas en aspectos de gestión, técnicas, para seguridad física y de gestión del personal. Sin embargo, debido a aspectos legislativos, políticos y otros se han seleccionado del listado que la herramienta ha presentado como alternativa solo aquellos aplicables prioritariamente, y para complementar de mejor manera se ha tomado algunas otras salvaguardas mencionadas en el libro de MAGERIT y que la herramienta no la ha considerado prioritarias, pero que aportan notablemente en la mitigación de los riesgos. Es decir que, las salvaguardas que se enlistan a continuación son aquellas más significativas que aportan a la realidad del GAD. (Ver tabla 4).

Tabla 4: Salvaguardas propuestas

SALVAGUARDAS				
APLICACIONES	**EQUIPOS**	**COMUNICACIONES**	**DATOS**	**PERSONAL**
Identificación y autentificación - Control de acceso lógico - Protección de los servicios - Protección de aplicaciones informáticas - Gestión de incidentes - Herramientas de seguridad - Gestión de vulnerabilidades - Gestión de mantenimiento y actualizaciones. - Copias de Seguridad de los datos (backup).	- Protección de equipos informáticos - Protección física de los equipos - Aseguramiento de la disponibilidad - Protección de las instalaciones - Gestión de incidentes - Protección del perímetro físico - Herramientas de seguridad - Continuidad del negocio - Cambio (actualizaciones y mantenimiento) - Climatización. - Suministro eléctrico.	- Control de acceso lógico - Protección de servicios - Aseguramiento de la disponibilidad - Protección de comunicaciones - Protección de las instalaciones - Gestión de incidentes - Protección del perímetro físico - Herramientas de seguridad - Herramienta de monitorización de tráfico. - Herramienta de detección / prevención de instrucción. - Continuidad del negocio	- Identificación y autentificación - Control de acceso lógico - Protección de la información - Protección de servicios - Herramientas de seguridad - Continuidad del negocio - Copias de Seguridad de los datos (backup). - Aseguramiento de la integridad.	- Gestión del personal - Gestión de incidentes - Organización - Formación y concienciación - Relaciones externas. - Aseguramiento de la disponibilidad

Fuente: Herramienta Pilar

Identificación del impacto y riesgo - Todos los activos de información se encuentran expuestos a riesgos, por lo cual es de importancia seleccionar los más relevantes, proponer la aplicación de salvaguardas para la mitigación del riesgo, es por ello que se realiza el cálculo del riesgo potencial y repercutido agrupados por su categoría.

El cálculo para el riesgo inherente se lo realiza en base al impacto y a la probabilidad de ocurrencia de las amenazas que han sido presentadas por la gestión diaria inherente a los activos sin contar con salvaguardas, o con salvaguardas mínimas; mientras que, el cálculo del riesgo residual se lo realiza en base al impacto y a la probabilidad de ocurrencia de las amenazas luego de la aplicación de las salvaguardas determinadas luego del análisis de riesgos. Para la representación de los riesgos se toma en cuenta las categorías de los activos siendo estos representados por códigos de R1 hasta R5 (ver tabla 5).

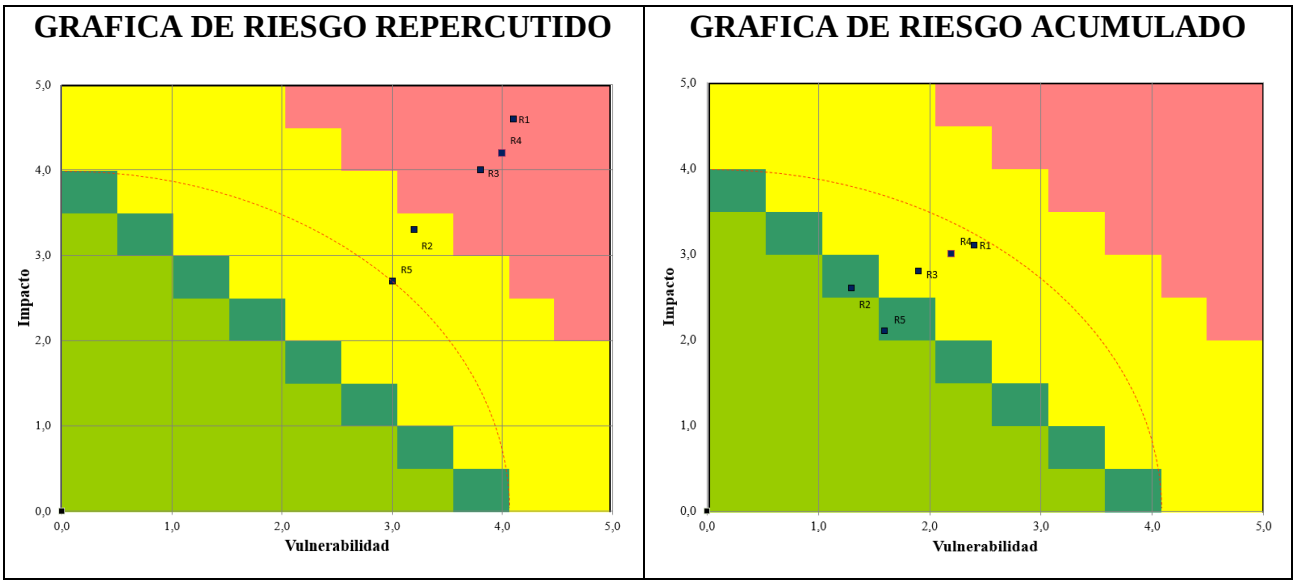
Tabla 5: Identificación de riesgo repercutido y acumulado

RIESGO REPERCUTIDO				RIESGO ACUMULADO		
CÓD	**ACTIVO POR CATEGORÍA**	**AMENAZAS**	**NIVEL DE CRITICIDAD**	**CÓD**	**SALVAGUARDA**	**NIVEL DE CRITICIDAD**
R1	Aplicaciones	Avería de origen físico o lógico. Difusión de software dañino. Vulnerabilidades de los programas. Errores de mantenimiento / actualizaciones de programas. Caída del sistema por agotamiento de recursos	Alto	R1	Identificación y autentificación Control de acceso lógico Protección de los servicios Protección de aplicaciones informáticas Gestión de incidentes Herramientas de seguridad Gestión de vulnerabilidades Gestión de mantenimiento y actualizaciones. Copias de Seguridad de los datos (backup).	Medio
R2	Equipos	Fuego Daños por agua. Contaminación medioambiental Contaminación electromagnética Avería de origen físico y lógico Corte de suministro eléctrico Condiciones inadecuadas de temperatura o humedad Emanaciones electromagnéticas Errores de mantenimiento Caída del sistema por agotamiento de recursos. Perdida de equipos Uso no previsto Acceso no autorizado. Manipulación de hardware Denegación del servicio Robo de equipos Ataque destructivo	Medio	R2	Protección de equipos informáticos Protección física de los equipos Aseguramiento de la disponibilidad Protección de las instalaciones Gestión de incidentes Protección del perímetro físico Herramientas de seguridad Continuidad del negocio Cambio (actualizaciones y mantenimiento) Climatización. Suministro eléctrico.	Bajo
R3	Comunicaciones	Fallo de servicio de comunicaciones Errores del administrador del sistema/ de la seguridad Errores de [re-]encaminamiento Errores de secuencia Alteración de la información Fugas de información Caída del sistema por agotamiento de recursos Suplantación de identidad Uso no previsto [Re-]encaminamiento de mensajes Acceso no autorizado Análisis de trafico Interceptación de información Modificación de información Destrucción de la información Denegación de servicio	Medio	R3	Control de acceso lógico Protección de servicios Aseguramiento de la disponibilidad Protección de comunicaciones Protección de las instalaciones Gestión de incidentes Protección del perímetro físico Herramientas de seguridad Herramienta de monitorización de tráfico. Herramienta de detección / prevención de instrucción. Continuidad del negocio	Medio
R4	Datos	Avería de origen físico Difusión de software dañino Alteración de la información Destrucción de la Información Fugas de la Información Vulnerabilidades de los programas Errores de mantenimiento / actualizaciones de programas Suplantación de identidad Abuso de privilegios de acceso. Difusión de software dañino. Acceso no autorizado Manipulación de programas	Alto	R4	Identificación y autentificación Control de acceso lógico Protección de la información Protección de servicios Herramientas de seguridad Continuidad del negocio Copias de Seguridad de los datos (backup). Aseguramiento de la integridad.	Medio
R5	Personal	Alteración de la información Destrucción de la Información Fugas de la Información. Indisponibilidad del personal Modificación de la Información. Destrucción de la información Revelación de la información Indisponibilidad del Personal Extorsión Ingeniería social (picaresca)	Medio	R5	Gestión del personal Gestión de incidentes Organización Formación y concienciación Relaciones externas. Aseguramiento de la disponibilidad	Bajo

Fuente: Autoría propia

En la siguiente ilustración, el gráfico de la izquierda expone el mapa de riesgo repercutido que deja ver los riesgos ubicados en niveles altos y medio altos por la falta de salvaguardas; en la parte derecha el gráfico de riesgo acumulado permite observar como el nivel de criticidad de riesgos disminuiría notablemente con a la aplicación de salvaguardas. (Ver ilustración 2).

Ilustración 2: Matriz de riesgo repercutido y acumulado



Fuente: Autoría propia

En el riesgo repercutido se puede observar que en la categoría aplicaciones cuenta con un nivel de criticidad alto, sus activos son de gran importancia para la institución debido a que son sistemas de uso financiero y administrativo, al materializarse algún tipo de riesgo se afectaría notablemente el desempeño de las labores diarias y la situación económica de la institución; sin embargo, el tratamiento que se ha dado para la gestión de estos activos es escasa. Otra de las categorías críticas son los Datos, estos se enfocan a información confidencial administrativa y financiera. Las demás categorías cuentan con un nivel de criticidad medio, debido a que se han aplicado controles básicos que aportan con la mitigación de riegos; sin embargo, por su importancia requieren ser mejoradas (ver ilustración 2).

En el riesgo acumulado se puede observar que la aplicación adecuada de las salvaguardas propuestas para cada activo permitiría la disminución notable de los niveles de criticidad, permitiendo mitigar las amenazas y brindar mayor protección y seguridad de estos activos que permitan el correcto

funcionamiento; esta valoración se ha realizado con la evaluación desde las perspectivas: gerencial, tecnológica informática y usuario. (Ver ilustración 2).

Determinación de activos prioritarios. –Para identificar aquellos activos prioritarios a ser considerados para la determinación de políticas, se identifica mediante el nivel de riesgo de cada activo basados en los siguientes niveles de criticidad (ver tabla 6).

Tabla 6: Niveles de criticidad

NIVELES DE CRITICIDAD	
{9}	Catástrofe
{8}	Desastre
{7}	Extremadamente crítico
{6}	Muy crítico
{5}	Crítico
{4}	Muy alto
{3}	Alto
{2}	Medio
{1}	Bajo
{0}	Despreciable

Fuente: Magerit

En base a las consideraciones anteriores, se obtiene la siguiente valoración en función a la importancia de cada activo en las dimensiones de seguridad de Magerit: disponibilidad, integridad y confidencialidad en los activos de la Unidad de Informática (ver ilustración 3).

Ilustración 3: Criticidad de riesgos de los activos de información

activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
[IS] Servicios internos			
[E] Equipamiento			
[SW] Aplicaciones			
[SW-001-SIGAME] SISTEMA CONTABLE SIG-AME	[8]	[9]	[8]
[SW-002-SII] SIIM Sistema Integral de Información Multi-Finalitario	[8]	[9]	[8]
[SW-003-SIRP] SIRP Sistema Informático para Automatización del Registro de la Propi	[7]	[9]	[8]
[SW-004-AM] Attendance management	[4]	[5]	[6]
[SW-005-HO] HERRAMIENTAS OFIMATICAS	[3]	[n.a.]	[2]
[SW-006-SO] SISTEMA OPERATIVO	[5]	[4]	[5]
[SW-007-AV] ANTIVIRUS	[6]	[3]	[2]
[HW-007-PW] PAGINA WEB	[5]	[2]	[n.a.]
[HW-009-CE] CORREO ELECTRONICO	[5]	[4]	[5]
[HW] Equipos			
[HW-001-SERV] SERVIDORES	[7]	[n.a.]	[5]
[HW-002-PC] COMPUTADORAS PORTATIL	[6]	[n.a.]	[n.a.]
[HW-003-IMP] IMPRESORA	[4]	[n.a.]	[n.a.]
[HW-004-M] MONITOR	[2]	[n.a.]	[n.a.]
[HW-005-UPS] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	[2]	[n.a.]	[n.a.]
[HW-006-ST] SWITCH	[6]	[n.a.]	[n.a.]
[HW-007-RT] ROUTER	[6]	[3]	[4]
[HW-008-HDD] DISCO DURO	[3]	[n.a.]	[5]
[COM] Comunicaciones			
[COM-001-NET] INTERNET	[7]	[6]	[6]
[COM-002-LAN] RED LAN	[6]	[5]	[7]
[COM-003-RI] RED INALAMBRICA	[2]	[3]	[4]
[AUX] Elementos auxiliares			
[D] DATOS			
[D-001-GBD] GESTOR DE BASE DE DATOS	[7]	[8]	[8]
[SS] Servicios subcontratados			
[L] Instalaciones			
[P] Personal			
[PGAD] PERSONAL GAD			
[PGAD-001-JEFE] JEFE DE UNIDAD DE INFORMÁTICA	[6]	[2]	[7]
[PGAD-002-ANALIST] ANALISTA DE INFORMATICA	[6]	[2]	[7]
[PGAD-003-ASIST] ASISTENTE INFORMÁTICO	[2]	[2]	[4]

Fuente: Herramienta Pilar

Selección de activos prioritarios. – Se seleccionan aquellos activos que poseen un nivel de criticidad de riesgo de 3 (alto) hasta 9 (catástrofe), en las dimensiones de seguridad (ver tabla 7).

Tabla 7: Activos Prioritarios

CATEGORÍA	ACTIVOS	[D]	[I]	[C]
APLICACIONES	SISTEMA CONTABLE SIG-AME	5.7	6.2	5.7
	SIIM SISTEMA INTEGRAL DE INFORMACIÓN MULTI - FINALITARIO	5.7	6.2	5.7
	SIRP SISTEMA INFORMÁTICO PARA AUTOMATIZACIÓN DEL REGISTRO DE PROPIEDAD.	5.1	6.2	5.7
	ATTENDANCE MANAGEMENT	3.3	3.9	4.5
	SISTEMA OPERATIVO	3.9	3.3	3.9
	CORREO ELECTRÓNICO	3.9	3.3	3.9
EQUIPOS	SERVIDORES	5.4		3.9
	COMPUTADORAS PORTÁTIL	4.8		
	SWTICH	4.8		
	ROUTER	4.8	0.98	2.8
COMUNICACIONES	INTERNET	5.4	3.2	3.9
	RED LAN	4.8	2.7	4.5
DATOS	GESTOR DE BASE DE DATOS	5.1	5.7	6.9
PERSONAL	JEFE DE UNIDAD DE INFORMÁTICA	3.9	2.1	5.4
	ANALISTA DE INFORMÁTICA	3.9	2.1	5.4

Fuente: Autoría propia

Alineación con la ISO/IEC 27002:2013

Con el análisis de riesgos se ha podido conocer la realidad de los activos de la Unidad de Informática del GADM del Cantón Camilo Ponce Enríquez. Las debilidades encontradas en la gestión seguridad de varios activos puede observarse con detalle en la Tabla 8, que es el resultado del análisis de riesgos realizado con la herramienta Pilar, misma que detalla los activos de información que requieren incrementar el nivel de protección, las posibles amenazas con cada dominio a que corresponda, y las salvaguardas que permitirán mitigar las amenazas.

Las salvaguardas han sido seleccionadas en base a un análisis comparativo entre los resultados que recomienda la herramienta Pilar y alimentado con las salvaguardas que contiene el Libro II de Magerit. La elaboración de la Tabla 8 expone de manera clara la alineación de los activos con los dominios, objetivos de control y controles de la ISO/IEC 27002:2013, éstos constituyen los criterios de los dominios que deberían ser considerados para la elaboración del manual de políticas de seguridad.

Tabla 8: Alineación con la ISO/IEC 27002

CAT	ACTIVOS	AMENAZAS	DOMINIOS			SALVAGUARDAS	CONTROLES ISO/IEC 27002
			D	I	C		
APLICACIONES	- [SW-001-SIGAME] SISTEMA CONTABLE SIG-AME - [SW-002-SII] SIIM Sistema Integral de Información Multi – Finalitario - [SW-003-SIRP] SIRP Sistema Informático para Automatización del Registro de Propiedad. - [SW-004-AM] Attendance Management - [SW-006-SO] Sistema Operativo - [HW-009-CE] Correo Electrónico	[I.5] Avería de origen físico o lógico	X			- Identificación y autentificación - Control de acceso lógico - Protección de los servicios - Protección de aplicaciones informáticas - Gestión de incidentes - Herramientas de seguridad - Gestión de vulnerabilidades - Gestión de mantenimiento y actualizaciones. - Copias de Seguridad de los datos (backup).	9.4 Control de acceso a sistemas y aplicaciones. 12.2. Protección contra malware. 12.3. Copias de Seguridad 12.6. Gestión de la Vulnerabilidad técnica 14.1 Requisitos de seguridad de los sistemas de información. 16.1 Gestión de incidentes de seguridad de la información y mejoras. 17.1 Continuidad de la seguridad de la información.
		[E.8] Difusión de software dañino	X	X	X		
		[E.20] Vulnerabilidades de los programas	X	X	X		
		[E.21]Errores de mantenimiento / actualizaciones de programas	X	X			
		[E.24] Caída del sistema por agotamiento de recursos	X				
		[A.8] Difusión de software dañino.	X	X	X		
		[A.11] Acceso no autorizado		X	X		
		[A.22] Manipulación de programas.	X	X	X		
EQUIPOS	- [HW-001-SERV] Servidores - [HW-002-PC] Computadoras Portátil - [HW-006-ST] Swtich - [HW-007-RT] Router	[N.1] Fuego	X			- Protección de equipos informáticos - Protección física de los equipos - Aseguramiento de la disponibilidad - Protección de las instalaciones - Gestión de incidentes - Protección del perímetro físico - Herramientas de seguridad - Continuidad del negocio - Cambio (actualizaciones y mantenimiento) - Climatización. - Suministro eléctrico.	6.2 Dispositivos para movilidad y teletrabajo. 8.1. Responsabilidad sobre los activos 8.3 Manejo de los medios 9.2 Gestión de acceso de los usuarios 11.2. Seguridad de los equipos 16.1 Gestión de incidentes de seguridad de la información y mejoras.
		[I.2] Daños por agua.	X				
		[I.3] Contaminación medioambiental	X				
		[I.4] Contaminación electromagnética	X				
		[I.5] Avería de origen físico y lógico	X				
		[I.6] Corte de suministro eléctrico	X				
		[I.7] Condiciones inadecuadas de temperatura o humedad	X				
		[I.11] Emanaciones electromagnéticas			X		
		[E.23] Errores de mantenimiento	X				
		[E.24] Caída del sistema por agotamiento de recursos.	X				
		[E.25] Perdida de equipos	X		X		
		[A.7] Uso no previsto	X		X		
		[A.11] Acceso no autorizado.	X		X		
		[A.23] Manipulación de hardware	X		X		
		[A.24] Denegación del servicio	X				
		[A.25] Robo de equipos	X		X		
		[A.26] Ataque destructivo	X				
COMUNICACIONES	- [COM-001-NET] Internet - [COM-002-LAN] Red LAN	[I.8] Fallo de servicio de comunicaciones	X			- Control de acceso lógico - Protección de servicios - Aseguramiento de la disponibilidad - Protección de comunicaciones - Protección de las instalaciones - Gestión de incidentes - Protección del perímetro físico - Herramientas de seguridad - Herramienta de monitorización de tráfico. - Herramienta de detección / prevención de instrucción. - Continuidad del negocio	9.1 Requisitos de negocio para el control de accesos: 9.2 Gestión de acceso de los usuarios 12.6. Gestión de la Vulnerabilidad técnica 13.1 Gestión en la seguridad en las redes 16.1 Gestión de incidentes de seguridad de la información y mejoras. 17.1 Continuidad de la seguridad de la información.
		[E.2] Errores del administrador del sistema/ de la seguridad	X	X	X		
		[E.9] Errores de [re-]encaminamiento			X		
		[E.10] Errores de secuencia		X			
		[E.15] Alteración de la información		X			
		[E.19] Fugas de información			X		
		[E.24] Caída del sistema por agotamiento de recursos	X				
		[A.5] Suplantación de identidad		X	X		
		[A.7] Uso no previsto	X	X	X		
		[A.9] [Re-]encaminamiento de mensajes			X		
		[A.11] Acceso no autorizado		X	X		
		[A.12] Análisis de trafico			X		
		[A.14] Interceptación de información			X		
		[A.15] Modificación de información		X			
		[A.18] Destrucción de la información	X				
		[A.24] Denegación de servicio	X				
DATOS	- [D-001-GBD] Gestor de Base de Datos	[I.5] Avería de origen físico	X			- Identificación y autentificación - Control de acceso lógico - Protección de la información - Protección de servicios - Herramientas de seguridad - Continuidad del negocio - Copias de Seguridad de los datos (backup). - Aseguramiento de la integridad.	9.1 Requisitos de negocio para el control de accesos: 9.2 Gestión de acceso de los usuarios 9.3 Responsabilidades del usuario 9.4 Control de acceso a sistemas y aplicaciones: 12. Seguridad en la operativa. 12.2 Protección contra un malware 12.3 Copias de seguridad 12.6 Gestión de la vulnerabilidad técnica
		[E.8] Difusión de software dañino	X	X	X		
		[E.15] Alteración de la información		X			
		[E.18] Destrucción de la Información	X				
		[E.19] Fugas de la Información			X		
		[E.20] Vulnerabilidades de los programas	X	X	X		
		[E.21]Errores de mantenimiento / actualizaciones de programas	X	X			
		[A.5] Suplantación de identidad		X	X		
		[A.6] Abuso de privilegios de acceso.	X	X	X		
		[A.8] Difusión de software dañino.	X	X	X		
		[A.11] Acceso no autorizado		X	X		
		[A.22] Manipulación de programas	X	X	X		
PERS	- [PGAD-001-JEFE] Jefe de Unidad de Informática	[E.15] Alteración de la información		X		- Gestión del personal - Gestión de incidentes	6.1 Organización Interna
		[E.18] Destrucción de la Información	X				

	- [PGAD-002-ANALIST] Analista de Informática	[E.19] Fugas de la Información.			X	- Organización - Formación y concienciación - Relaciones externas. - Aseguramiento de la disponibilidad	9.2 Gestión de acceso de los usuarios 9.3 Responsabilidades del usuario 18.1 Cumplimiento de los requisitos legales y contractuales.
		[E.28] Indisponibilidad del personal	X				
		[A.15] Modificación de la Información.		X			
		[A.18] Destrucción de la información	X				
		[A.19] Revelación de la información			X		
		[A.28] Indisponibilidad del Personal	X				
		[A.29] Extorsión	X	X	X		
		[A.30] Ingeniería social (picaresca)	X	X	X		

Fuente: Autoría propia

Columna 1 (CAT). - El nombre de la categoría a la que corresponden los activos.

Columna 2 (Activos). - Visualiza el listado de activos que corresponden a cada categoría.

Columna 3 (Amenazas). - Posibles amenazas que pueden materializar los riesgos en cada uno de los activos.

Columna 4 (Dominios). - Dominios considerados para el análisis de riesgos.

Columna 5 (Salvaguardas). - Controles recomendados para la aplicación sobre los activos de modo para mitigar los riesgos.

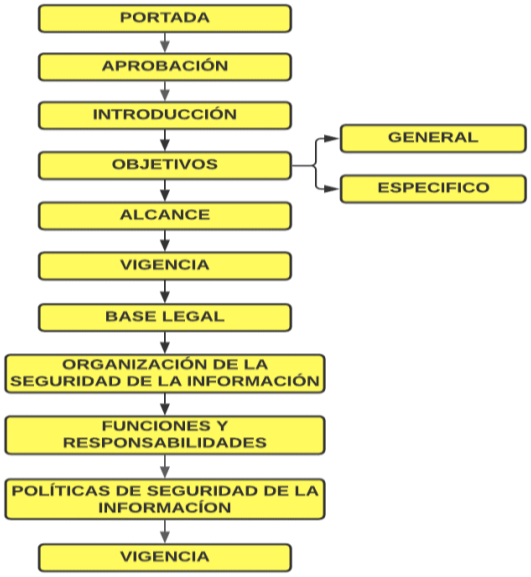
Columna 6 (Controles ISO/IEC 27002). - Controles correspondientes a la ISO 27002 (Políticas de Seguridad) que se relacionan directamente (como equivalencia) con las salvaguardas obtenidas con la herramienta Pilar.

Recomendación para la Estructura del Manual de Políticas de Seguridad de la Información

Con la información resultante del análisis de riesgos realizado y la alineación con la ISO/IEC 27002, se ha obtenido un listado de controles como guía para una futura creación del manual de políticas de seguridad de la información que facilite la implementación de políticas de seguridad a la Unidad de Informática del GADM del Cantón Camilo Ponce Enríquez.

A continuación, se podrá observar un conjunto de lineamientos que deberían ser observados para la elaboración de un Manual de Políticas de Seguridad de la Información. Se empieza con la estructura que debería tener el manual, mismo que se observa gráficamente en la ilustración 4.

Ilustración 4: Estructura del documento del manual de políticas de seguridad



Fuente: Autoría Propia

La estructura propuesta expone de manera clara y sencilla los principales elementos que deben ser considerados de un manual de políticas. Sin embargo, queda a consideración de quienes desarrollen el mismo realizar los ajustes que consideren pertinentes.

Recomendaciones para la elaboración de las políticas de seguridad.

En la tabla de alineación se ha utilizado numerales que al parecer no tienen un orden establecido, esto es debido a que se considera la misma nomenclatura original de la norma ISO/IEC 27002:2013. Se realiza la tabla 9 para aclarar la nomenclatura utilizada para la recomendación de los dominios y controles que se expone posteriormente, ya que se presentan con la misma numeración de la norma ISO/IEC 27002

Tabla 9: Nomenclatura de la ISO 27002

NOMENCLATURA	SIGNIFICADO
6.	Dominio
6.2	Objetivo de control
-	Controles propuestos

Fuente: Autoría Propia

A continuación, se enlista los dominios y objetivos de control de la ISO/IEC 27002:2013 a considerar y, los controles expuestos en la NTE INEN-ISO/IEC 27002 para la elaboración el manual de políticas de seguridad de la información.

6. Aspectos organizativos de la seguridad de la información.

6.1 Organización Interna. – Estimar los siguientes controles:

- Asignar y definir responsabilidades de seguridad de la información.
- Mantener los contactos apropiados con las autoridades pertinentes, grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.

6.2. Dispositivos para movilidad y teletrabajo. - Considerar los siguientes controles:

- Adoptar una política de soporte y medidas de seguridad para gestionar los riesgos introducidos por el uso de dispositivos móviles.
- Implementar una política y medida de soporte de seguridad para proteger la información a la que se accede, procesa o almacenada en los sitios de teletrabajo.

8. Gestión de Activos.

8.1 Responsabilidad sobre los activos. - Apreciar los siguientes controles:

- Identificar, elaborar y mantener un inventario de los activos asociados con la información y las instalaciones para el procesamiento de la información asignando un propietario.
- Identificar, documentar e implementar las reglas para el uso aceptable de la información, los activos asociados con la información y las instalaciones de procesamiento de información.
- Todos los empleados y terceras partes deberían devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.

8.3 Manejo de los medios. - Evaluar los siguientes controles:

- Implementar procedimientos para la gestión de los medios extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.
- Proteger los medios que contengan información contra accesos no autorizados, usos indebidos o deterioro durante el transporte fuera de los límites físicos de la organización.

9. Control de Accesos

9.1 Requisitos de negocio para el control de accesos. - Tomar en cuenta los siguientes controles:

- Establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.

- Únicamente se debería proporcionar a los usuarios el acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente autorizados.

9.2 Gestión de acceso de los usuarios. - Analizar los siguientes controles:

- Implementar un procedimiento formal de registro, control, restricción y retirada de usuarios de todos los sistemas y servicios.
- Retirar a la finalización del empleo, del contrato o del acuerdo, o ajustados en caso de cambio la asignación y el uso de privilegios de acceso deberían estar restringidos y controlados.

9.3 Responsabilidades del usuario. – Tener en consideración los siguientes controles:

- Requerir que los usuarios sigan las prácticas de la organización en el uso de la información secreta de autenticación.

9.4 Control de acceso a sistemas y aplicaciones. – Utilizar los siguientes controles:

- Restringir el acceso a la información y a las funciones de las aplicaciones del sistema mediante una política de control de acceso.
- Controlar por medio de un procedimiento seguro de inicio de sesión el acceso a los sistemas y a las aplicaciones.
- Asegurar la calidad y sistema gestión de contraseñas.

11. Seguridad Física y Ambiental

11.1 Áreas seguras. - Valorar los siguientes controles:

- Definir los parámetros de seguridad para proteger las áreas que contienen información crítica y sensible, así como las instalaciones de procesamiento de la información.
- Proteger las áreas seguras mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.
- Diseñar y aplicar la las áreas seguras y la protección física contra desastres naturales, ataques maliciosos o accidentes.

11.2 Seguridad de los equipos. – Contemplar los siguientes controles:

- Situar y proteger los equipos de forma que se reduzcan los riesgos de las amenazas y accesos no autorizados.
- Proteger los equipos contra fallos de alimentación y otras alteraciones causadas por fallos en las instalaciones de suministro.
- Proteger contra interceptaciones, interferencias o daños el cableado eléctrico y de telecomunicaciones que transmite datos o que da soporte a los servicios de información.

- Brindar a los equipos un mantenimiento correcto que asegure su disponibilidad y su integridad continuas.
- Aplicar medidas de seguridad a los equipos situados fuera las instalaciones de la organización, teniendo en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones.
- Comprobar los medios de almacenamiento para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos o reutilizarlos

12. Seguridad en la operativa.

12.2 Protección contra un malware. - Tomar en consideración los siguientes controles:

- Implementar los controles de detección, prevención y recuperación que sirvan como protección contra un malware, así como procedimientos adecuados de concienciación al usuario.

12.3 Copias de seguridad. – Apreciar el siguiente control.

- Realizar copias de seguridad de la información, del software y del sistema y verificar periódicamente de acuerdo con la política de copias de seguridad acordada.

12.6 Gestión de la vulnerabilidad técnica. - Tener presente el siguiente control.

- Obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, evaluar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas adecuadas para afrontar el riesgo asociado.

13. Seguridad en las Telecomunicaciones.

13.1 Gestión en la seguridad en las redes. – Examinar los siguientes controles:

- Gestionar y controlar las redes y proteger la información en los sistemas y aplicaciones.
- Identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red e incluir acuerdos de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan

14. Adquisición, desarrollo y mantenimiento de los sistemas de información.

14.1 Requisitos de seguridad de los sistemas de información. - Valorar los siguientes controles:

- Incluir en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información requisitos relacionados con la seguridad de la información.
- Proteger de cualquier actividad fraudulenta, disputa de contrato, difusión y modificaciones no autorizadas la información involucrada en aplicaciones que pasan a través de redes públicas.

16. Gestión de incidentes en la seguridad de la información.

16.1 Gestión de incidentes de seguridad de la información y mejoras. – Estimar los siguientes controles:

- Establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.
- Notificarse lo antes posible, a través de los canales de gestión adecuados los eventos de seguridad de la información.
- Todos los empleados, contratistas, terceras partes usuarias de los sistemas y servicios de información deberían ser obligados a anotar y notificar cualquier punto débil que observen o que sospechen que exista, en los sistemas o servicios.
- Responder los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
- Definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como evidencia.

17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

17.1 Continuidad de la seguridad de la información. – Considerar los siguientes controles:

- Determinar las necesidades de seguridad de la información y de continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
- Establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.
- Verificar los controles de continuidad de seguridad de la información establecidos e implementados en intervalos regulares.

18. Cumplimiento

18.1 Cumplimiento de los requisitos legales y contractuales. - Se debe tener en cuenta el siguiente control:

- Definir de forma explícita, documentar y mantener actualizados para cada sistema de información de la organización todos los requisitos pertinentes, tanto legales como reglamentarios, contractuales.

Recomendaciones Finales para el Manual de Políticas

Un Manual de Políticas de Seguridad de la Información, es un documento normativo que llevará a los usuarios de los activos a entender la obligatoriedad de la aplicación de ciertas normas o reglas, así como por el contrario la prohibición de algunas acciones. Al ser un documento normativo también incluirá la responsabilidad sobre el actuar de cada usuario y la reglamentación punitiva en caso de incumplimiento, es por ello que debe redactarse de la manera más clara posible, se debe definir una estructura particular para redactar las normas de modo que el usuario se encuentre familiarizado con su lectura y no se preste para interpretaciones ambiguas.

Por poner un ejemplo, la estructura podría ser: [sujeto] [verbo imperativo que indica obligación o prohibición] [verbo principal] [asunto] [detalles].

El sujeto. - será la persona, el grupo, la empresa, etc., que debe procurar el cumplimiento u observar la no ejecución de una acción. Ejemplo: "El usuario" **Verbo Imperativo. -** indica obligación o prohibición. Ejemplo: Debe ó No Debe. **Verbo principal. -** La acción misma, ejemplo: "cambiar" **Asunto. -** la redacción que aclara la idea. Ejemplo: su contraseña de acceso al sistema principal. **Detalles. -** cualquier particularidad que aclare el enunciado. Ejemplo: "cada tres meses".

Conclusiones

Mediante el análisis de situación actual se identificaron aspectos de seguridad que no han sido atendidos apropiadamente, como: políticas de seguridad, desarrollo y mantenimiento de sistemas y continuidad del negocio, demostrando que estos pueden efectuar falencias en la gestión de los activos, la presencia de riesgos y amenazas en la información.

Se han determinado activos de información de prioridad alta para la institución, que se encuentran altamente vulnerables ante la presencia de riesgos que requieren de mayor atención. Sin embargo, el enfoque en cuanto al aspecto de seguridad que se le da a estos activos es bastante bajo a pesar de su importancia.

Se observó que la herramienta P.I.L.A.R en primera instancia ha sugerido salvaguardas afines a los riesgos determinados. Sin embargo, de acuerdo a la situación de la institución no son del todo aplicables, es por ello que se ha procedido a realizar una retroalimentación manual con el apoyo del jefe de la Unidad de Informática para dar validez y aprobación.

Los actuales lineamientos que se proponen para la elaboración de un Manuel de Políticas de Seguridad de la Información, satisfacen las necesidades actuales, siendo estos aplicables en un tiempo cercano, ya que, si se lo aplica durante un tiempo largo, estos requerirán de actualizaciones en el análisis de riesgos para satisfacer las nuevas necesidades que se presenten en dicho tiempo.

Referencias

1. Álvarez Lozano, L. G., & Andrade López, M. S. (25 de Noviembre de 2020). Políticas de Seguridad de la Información bajo la Norma ISO 27002:2013 para el Gobierno Autónomo Descentralizado del Cantón Biblián. Polo del Conocimiento, 5(11), 591-621.
2. Baca Urbina, G. (2016). Introducción a la Seguridad Informatica (1 ed.). Mexico D. F: Grupo Editorial Patria. Obtenido de https://acortar.link/LR1hr
3. Centro Nacional de Inteligencia de España. (2014). Pilar. Recuperado el 23 de Agosto de 2021, de ¿Qué es Pilar?: https://n9.cl/eszvn
4. Contraloría General del Estado. (2019). Normas de Control Interno de la Contraloria General del Estado. Quito: Lexis Finder. Obtenido de https://acortar.link/PGJyJP
5. Deloitte. (Noviembre de 2015). Deloitte. Obtenido de COSO Evaluación de Riesgos - Enterprise Risk Services: https://n9.cl/fre78
6. Figueroa Suárez, J., Rodríguez Andrade, R., Bone Obando, C., & Saltos Gómez, J. (2017). La seguridad informática y la seguridad de la información. Polo del Conocimiento, 2(12), 145-155. Obtenido de https://n9.cl/4tzta
7. La Universidad en Internet. (11 de Diciembre de 2019). La Universidad en Internet. Obtenido de Qué es la certificación ISO 27001 y para qué sirve?: https://n9.cl/ibx3j
8. Magerit. (2012). Libro I - Guía Técnicas MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (Tercera ed., Vol. I). Madrid: Ministerio de Hacienda y Administraciones Públicas.
9. Magerit. (2012). Libro III - Guía Técnicas MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (Tercera ed., Vol. III). Madrid: Ministerio de Hacienda y Administracion Pública.
10. Organización Internacional de Normalización. (Octubre de 2013). Iso.org. (ISO, Editor, & ISO/IEC 27002:2013 Tecnologías de la información — Técnicas de seguridad — Código de prácticas para los controles de seguridad de la información) Recuperado el 2021 de Abril de

14, de ISO/IEC 27002:2013 Tecnologías de la información — Técnicas de seguridad — Código de prácticas para los controles de seguridad de la información: https://n9.cl/drg51

11. Ortiz, A. (22 de Julio de 2021). Blog HostDime Perú, Servidores dedicados. (¿Qué es una vulnerabilidad en seguridad informática?) Recuperado el 10 de Mayo de 2021, de https://n9.cl/ry12m
12. Presidencia de la República del Ecuador. (2021). Código Orgánico Organización Territorial Autonomía Descentralización (COOTAD). Quito, Ecuador: Lexis. Obtenido de https://www.oas.org/juridico/pdfs/mesicic4_ecu_org.pdf
13. Pulla Vásquez, T. E. (2019). Políticas de Seguridad para las tecnologías de la información y comunicación en la empresa Industrias Borja Inborja S.A. Cuenca: Universidad Católica de Cuenca.
14. Sena, L., & Tenzer, S. M. (2004). Introducción a Riesgo Informático. Universidad de la República de Uruguay, 1(1).
15. Servicio Ecuatoriano de Normalización INEN. (2017). Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002 Tecnologías de la Información — Técnicas de Seguridad — Códico de Práctica para los Controles de Seguridad de la Información (ISO/IEC 27002:2013+Cor. 1:2014+Cor. 2: 2015, IDT) (2 ed.). Quito, Ecuador: Servicio Ecuatoriano de Normalización INEN.
16. Torres Núñez, E. M. (2015). "Políticas de Seguridad de la información basado en la Norma ISO/ICE 27002:2013 para la Dirección de Tecnologías de Información y Comunicación de la Universidad Técnica de Ambato". Ambato, Ecuador: Universidad Técnica de Ambato. Obtenido de https://n9.cl/qsz2w
17. Vega Velasco, W. (Septiembre de 2008). Políticas y Seguridad de la Información. SciELO, 2(2), 63-69. Obtenido de https://n9.cl/pbe7v