Polo del Conocimiento

Pol. Con. (Edición núm. 52) Vol. 5, No 11
Noviembre 2020, pp. 591-621
ISSN: 2550 - 682X
DOI: 10.23857/pc.v5i11.2011

Políticas de Seguridad de la Información bajo la Norma ISO 27002:2013 para el Gobierno Autónomo Descentralizado del Cantón Biblián

Information Security Politics under ISO 27002: 2013 standard for the Decentralized Autonomous Government of the Canton Biblián

Políticas de Segurança da Informação segundo a norma ISO 27002: 2013 para o Governo Autônomo Descentralizado do Cantão Biblián

Lourdes Gabriela Álvarez-Lozano [I]
lourdes.alvarez @est.ucacue.edu.ec
https://orcid.org/0000-0003-2665-8997

Miguel Santiago Andrade-López [II]
msandradel@ucacue.edu.ec
https://orcid.org/0000-0002-6882-4204

Correspondencia: dlojam@ucacue.edu.ec

Ciencias Técnicas y Aplicadas
Artículo de investigación

*Recibido: 20 de septiembre de 2020 *Aceptado: 29 de octubre de 2020 * Publicado: 25 de Noviembre de 2020

I. Ingeniera de Sistemas, Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.

II. Magíster en Evaluación y Auditoría de Sistemas Tecnológicos, Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

El uso de las Tecnologías de la Información y Comunicación (TICS), como parte de la modernización, es vital para el éxito de una empresa u organización del estado, gracias a las facilidades que brindan. Dentro de esta realidad se observa que los recursos humanos desconocen los riesgos y situaciones de vulnerabilidad a los que pueden estar sujetas ciertas entidades en áreas relacionadas al manejo, la protección de activos y de la información; debido a los ataques informáticos o desastres físicos. Este artículo aborda la importancia del conocimiento de las políticas de seguridad que debe tener el Gobierno Autónomo Descentralizado Municipal del Cantón Biblián (GADMCB), para mitigar los riesgos en sus sistemas, redes y acceso a la información, partiendo desde el análisis de la situación actual de la organización y en base de la norma ISO 27002:2013 se plantea una propuesta de políticas de seguridad de información para resguardar, proteger y respaldar información de usuarios internos y externos que dispone la entidad.

Palabras claves: Políticas de seguridad; ataques informáticos; norma ISO 27002:2013; riesgo; vulnerabilidad del sistema.

Abstract

The use of Information and Communication Technologies (ICT), as part of modernization, is vital for the success of a company or state organization, thanks to the facilities they provide. Within this reality, it is observed that human resources are unaware of the risks and situations of vulnerability to which certain entities may be subject in areas related to the management, protection of assets and information; due to computer attacks or physical disasters. This article addresses the importance of knowledge of the security policies that the Autonomous Decentralized Municipal Government of the Cantón Biblián (GADMCB) must have, to mitigate risks in their systems, networks and access to information, starting from the analysis of the current situation of the organization and based on the ISO 27002: 2013 standard, a proposal for information security policies is proposed to safeguard, protect and support information of internal and external users that the entity has.

Keywords: Security policies; computer attacks; ISO 27002:2013 standard; system risk; vulnerability.

Resumo

A utilização das Tecnologias de Informação e Comunicação (TIC), no âmbito da modernização, é vital para o sucesso de uma empresa ou organismo estatal, graças às facilidades que disponibilizam. Dentro desta realidade, verifica-se que os recursos humanos desconhecem os riscos e as situações de vulnerabilidade a que certas entidades podem estar sujeitas nas áreas relacionadas com a gestão, protecção de bens e informação; devido a ataques de computador ou desastres físicos. Este artigo aborda a importância do conhecimento das políticas de segurança que a Prefeitura Municipal Autônoma Descentralizada de Cantón Biblián (GADMCB) deve ter para mitigar riscos em seus sistemas, redes e acesso à informação, a partir da análise da situação atual da organização e com base na norma ISO 27002: 2013, é proposta uma proposta de políticas de segurança da informação para salvaguardar, proteger e apoiar as informações de usuários internos e externos que a entidade possui.

Palavras-chave: Políticas de segurança; ataques a computadores; norma ISO 27002: 2013; risco; vulnerabilidade do sistema.

Introducción

El GADMCB, es un organismo de gobierno local y público dentro de sus funciones es el encargado de promover el desarrollo sustentable del cantón utilizando adecuadamente la planificación como parte de su gestión administrativa y financiera, impulsando procesos y distintas formas de desarrollo emitiendo políticas públicas; además, tiene la facultad de la organización y de la gestión de talentos, recursos materiales conforme a lo previsto en la constitución, dentro de su autonomía financiera tiene la función de recibir, generar y administrar de manera directa, predecible y oportuna los recursos económicos correspondientes en el Presupuesto General de Estado. (Constitución de la República del Ecuador, 2008, págs. 88-93)

Las funciones que desempeña el GADMCB no le excluyen de los mecanismos de control y supervisión establecidos por las bases constitucionales y legales del país. (Presidencia de la República del Ecuador, 2015, págs. 40-43). Uno de las normativas de control interno de contraloría es el COOTAD, que en su apartado 405 señala:

> "La máxima autoridad, las servidores y servidoras responsables del control interno de acuerdo a sus competencias, establecerán políticas y procedimientos para manejar los

> riesgos en la consecuencia de los objetivos institucionales, proteger y conservar los activos y establecer los controles de acceso a la información" (Acuerdo de la Contraloría General del Estado, 16 Diciembre del 2014).

Es así que este organismo público cuenta con recursos humanos, tecnológicos y activos siendo menester utilizar sistemas operativos para almacenar, transportar y procesar información, quedando expuesta a los diferentes tipos de amenazas tanto físicas y virtuales como la manipulación de información, suplantación, o perdida afectando el normal funcionamiento de la organización.

Como datos preliminares para el desarrollo del presente trabajo se debe manifestar que en los años 2011 y 2012 la institución sufrió ataques internos y externos, ocasionando alteración de la información en los siguientes sistemas informáticos:

- Sistema Catastro Predial
- Sistemas de Agua Potable

En el año 2015 nuevamente fue expuesto a un ataque externo mediante el acceso no autorizado a la red privada a través de la central telefónica, causando un perjuicio económico para la entidad.

Como un mecanismo de evitar las amenazas y riesgos en los sistemas y aplicaciones informáticas del GABMCB se planteó como objetivo principal: Proponer políticas y controles de seguridad basadas en la Norma ISO 27002:2013 mediante la evaluación financiera y gestión de riesgo para la correcta administración de los accesos y gestión de activos.

En la actualidad, la incorporación y funcionamiento de las tecnologías informáticas es ilimitada en todos los ámbitos y procesos, generando un cambio en los aspectos sociales, culturales, políticos y económicos como un recurso clave en los procesos de modernización. Para el GADMCB el uso de las TICS se encuentra en todos los medios y mecanismos permitiendo que el ser humano interactúe, realice transacciones internas y externas, procese datos, gestione información, para estar a la altura de la era moderna, las TICS ha permitido automatizar procesos, como manifiesta Naser (2016).

> La utilización de estas tecnologías en la gestión pública constituye un pilar fundamental para la modernización y eficacia del Estado, ayuda al control interno y externo, aporta transparencia al sector público, disminuye sus costos al compartir recursos y ayuda a la descentralización, al acercar el gobierno a los ciudadanos, quienes son libres para

> consultar sobre información de los actos públicos del Estado que sean de su interés. (p.35).

La facilidad de acceso a la información tanto de los usuarios internos y externos de una organización representa un aumento en el riesgo de que la información y los recursos sean vulnerados, comprometiendo la seguridad de la entidad así como la privacidad de los datos almacenados como sus recursos entre estos los financieros y administrativos.

Con estos antecedentes, es imperativo la implementación de políticas de seguridad y normas para proteger los datos que posee esta organización del estado, tomando como marco de referencia la Norma Internacional ISO 27002:2013. Esta edición cuenta con 114 controles en 14 categorías, las mismas que permiten:

> "Orientar, establecer, implementar, operar, monitorear, analizar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información, SGSI y está alineada con la norma ISO 9001 con el fin de apoyar la implementación y operación, consistente e integrada con sistemas de gestión relacionados. Es decir, consolidar diversos sistemas de gestión de las organizaciones en uno sólo sistema integrado, optimizando sus procesos y facilitando el tránsito de información entre ellos". (Escuela Superior de Redes RED CEDIA, 2014, pág. 21).

Esta norma estándar en su última versión, proporciona servicios para salvaguardar información, con el objetivo de mantener confiabilidad, integridad y disponibilidad de los recursos a fin de cumplir los requerimientos legales estatales. Estas normas permiten definir, implementar, monitorear, evaluar la seguridad de información que manejan los organismos mediante una planificación basada en el análisis de los niveles de riesgos y midiendo el impacto que sufre con frecuencia; con todos estos insumos, se pretender generar políticas, normas y procedimientos para la aplicación de los controles de protección de los diferentes procesos y activos que gestiona en la actualidad el GADMCB dando prioridad a los ingresos de los tributos municipales.Para crear políticas de seguridad se debe entender en primera instancia, las amenazas comunes que puede sufrir una empresa u organismo, como lo señala Silvia (2020, pp. 1-3).

En la actualidad los riesgos de ser víctimas de un incidente informático aumentan por las ilimitadas utilizaciones de ordenadores u aplicaciones conectadas a internet, generando mayores posibilidades de ataques informáticos, existiendo amenazas internas y externas. Al hablar de seguridad de la información se refiere a las características y condiciones de sistemas de procesos de datos y su

almacenamiento, que permita garantizar su confidencialidad, integridad y disponibilidad según (Erb, 2009, pp.9-10).

Según las investigaciones obtenidas por el Departament for Digital, Culture, Media y Sport (2018), las amenazas internas suelen ser más dañinas y entre los incidentes de red aproximadamente el 60% y 80% suelen ser causados dentro de la misma institución por usuarios o personal técnico; porque los sistemas de prevención de intrusos o IPS, y firewalls no son mecanismos efectivos siendo estas amenazas maliciosas o simples descuidos.

Mientras que las amenazas externas se originan fuera de la red local por personas ajenas a la organización y por las vulnerabilidades que permiten acceder a los sistemas informáticos como: Base de datos, software, equipos , servidores, dispositivos de red porque se encuentran desprotegidos, sin vigilancia, dando problemas como ataques de denegación de servicio, robo de información o fuga y la obtención de un acceso no autorizado a la información a cualquier elemento que tenga valor para la organización, estas situaciones puede darse por personas, proceso y servicios que no estén con las debidas seguridades. (pp.35-38).

Se debe considerar también las vulnerabilidades informáticas para posibles ataques, como los que transgreden sobre aplicaciones o sistemas instalados, otras suceden sobre aplicaciones no instaladas por la empresa u organización y finalmente las aún no conocidas por la empresa u organización que desarrolla el programa, siendo primordial que en todo ámbito los sistemas y redes operen con seguridad.

Metodología

Para el presente estudio se utilizó la metodología cuantitativa en base a la aplicación de una encuesta tomando como referencia las políticas de seguridad de la información de acuerdo a la norma ISO 27002:2013. Este instrumento se aplicó a 20 funcionarios del GADMCB que utilizan los sistemas informáticos con la finalidad de identificar los riesgos y activos expuestos.

De los resultados obtenidos de la aplicación de las encuestas, se identificó el Valor del Activo (VA), Expectativa de pérdida individual (SLE), Factor de exposición (FE); como otro proceso, la determinación del ARO (Taza de Ocurrencia Anualizada) de cada amenaza que puede materializar el riesgo. Posteriormente se calculó el ALE (Expectativa de Pérdida Anual) de los Activos si la amenaza se efectuara, como siguiente paso se definió las acciones que se considere necesarias para

mitigar los riesgos; con este proceso, se obtuvo el valor del costo operacional y el índice de mitigación de las acciones de controles en base a los riesgos (Areitio J. , 2008, págs. 99-106)

Con los procesos indicados en los párrafos preliminares, se obtuvo el ROSI (Retorno sobre la inversión en la seguridad) mediante los procesos de ALE y índice de mitigación con el objetivo de identificar el retorno de la inversión puntualizando en el riesgo de mayor porcentaje. Una vez, obtenidos los resultados del ROSI se determinó el índice de la capacidad de protección considerando el riesgo residual y el riesgo inherente en base al costo operacional y las probabilidades de ocurrencia.

Como último proceso del presente trabajo, se evalúa el riesgo en base a la ocurrencia x el impacto para el establecimiento de sus categorías. En base a estos resultados se determinará las políticas y controles de seguridad a proponer, basadas en la Norma ISO 27002:2013 mediante la evaluación financiera de seguridad y gestión de riesgo para la correcta administración de los accesos y gestión de activos como alternativa para contrarrestar las amenazas, que cuando se materializan causan daños al computador o al organismo público siendo el objetivo principal.

Resultados

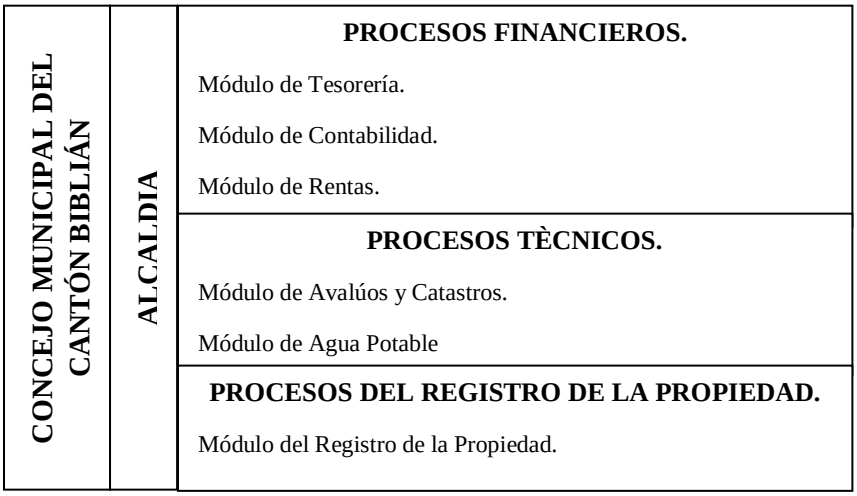
Para la presentación de los resultados obtenidos es importante dar conocer datos sobresalientes del GADMCB, como también la distribución de los diferentes procesos automatizados para el uso del personal de las áreas administrativas y financiera que posee dicha organización.

Datos del Municipio del Cantón Biblián

El GADMCB pertenece a uno los cantones de la provincia del Cañar, ocupa una superficie de 205,30Km². Biblián fue elevado a la categoría de Cantón el 01 de agosto de 1944, está ubicado en la zona septentrional de la hoya del Paute, a una altura media de 2608 msnm, el clima es frío y húmedo con una temperatura media de 14°C.

Con respecto a esta organización pública, en la figura 1, se observa la distribución del uso de los sistemas informáticos a través de los diferentes módulos

Figura 1: Procesos que soporta TIC (2020).



Autoría: Propia

Identificación de los activos

La seguridad de la información involucra la implementación de estrategias y planes que cubran los procesos, donde la información es considerada el activo principal. Esta estrategia debe considerara como punto principal el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos, con el objetivo de detectar amenazas que puedan generar vulnerabilidades y que pongan en riesgo dicho activo, es decir; que ayuden a proteger y salvaguardar tanto información, sistemas y equipos informáticos que procesa y administra el GADMCB.

En la tabla 1 se visualiza el inventario tecnológico, en donde se observa los servicios de los Sistemas Informáticos, Aplicaciones y Equipos Informáticos que actualmente cuenta el GADMCB.

Tabla 1: Inventario tecnológico

Infraestructura	Cantidad
Servidores de producción	4
Sistemas y servicios informáticos	Sistema informáticos SIM_B(Cobros de tributos Municipales) Sistema informático SIGAME(Sistema contable) Servicio WEB, consulta en línea Servicio Mail

Pol. Con. (Edición núm. 52) Vol. 5, No 11, Noviembre 2020, pp. 591-621, ISSN: 2550 - 682X

Base de datos	Sql Server Postgres
Equipos de red de LAN interna	9 swicht 4 antenas ubiquiti
Computadoras de escritorio	54
Laptops	32
Impresoras	42
Escáner	8
Telefonía	38
Cámaras de vigilancia	6

Fuente: Sistema del AME. Módulo Bodega GADMCB (2020)

Elaboración: Autoría: Propia

Identificación de los riesgos

El principal objetivo de este proceso es identificar los riesgos a los que se encuentran expuestos los principales activos del GADMCB.

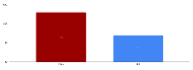
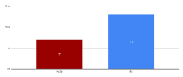
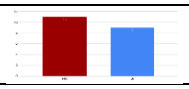
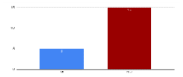
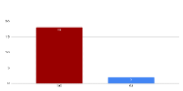
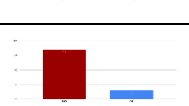
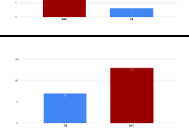
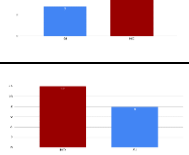
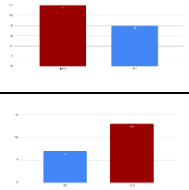
En este apartado se muestra la división poblacional de los encuestados (funcionarios) con sus respectivos departamentos, como se observa en la tabla 2, en la tabla 3, se ubicará los resultados con sus respectivos porcentajes; y, finalmente en tabla 4, se presenta los riesgos identificados en base al análisis e interpretación de las encuestas aplicadas.

Tabla 2: Distribución de los encuestados

DEPARTAMENTOS	**FUNCIONARIOS**
Administrativo	8
Financiero	5
Obras Públicas	2
Registro de la Propiedad	2
Planificación	3
Total	20

Fuente: Autoría Propia

Tabla 4: Resultados de encuestas aplicadas.

PREGUNTA	RESULTADOS	*%NO*	*%SI*
1.- ¿Existe establecido políticas de seguridad de la información?		65%	35%
2.- ¿Existen políticas, lineamientos y/o directrices para el uso y control de acceso a los sistemas informáticos municipal?		*35%*	*65%*
3.- ¿Existe una norma y/o directrices emitidas, para la creación y uso de contraseñas para el acceso a los sistemas informáticos municipal?		*55%*	*45%*
4.- ¿Existe alguna exigencia para el cambio de su contraseña para el respectivo acceso a los sistemas informáticos, cada cierto periodo de tiempo?		75%	25%
5.- ¿Ha facilitado a otra persona dentro o fuera de la institución contraseña de acceso a los sistemas informáticos, para realizar procesos a su responsabilidad?		90%	10%
6.- ¿Existe alguna exigencia para el cambio de su contraseña en su computador cada cierto periodo de tiempo?		85%	15%
7.- ¿Existe alguna exigencia o control para la asignación y uso de privilegios de acceso de usuario a los sistemas informáticos?		65%	35%
8.- ¿Existe alguna exigencia o control para la buena práctica en el uso de la información secreta de autenticación?		60%	40%
9.- ¿Existe alguna exigencia y control respecto al respaldo y almacenamiento de información crítica y/o sensible en lugares externos a la organización?		65%	35%
10.- ¿Existen políticas, lineamientos y/o directrices, que indique en qué periodo, tiempo se debe respaldar la información de su equipo?		80%	20%
11.- ¿Existe en su departamento procedimientos a seguir en el caso de ocurrir algún problema con su computador o los sistemas informáticos?		80%	20%
12.- ¿Existe alguna exigencia o control para el acceso a sitios WEB permitidos, para el cumplimiento de sus funciones?		30%	70%
13.- ¿Controla ud quien y cuando utiliza dispositivos de almacenamiento en su computador?		45%	55%
14.- ¿Ha existido suspensión de algún servicio que usted necesita para realizar su trabajo diario en la oficina?		55%	45%
15.- ¿Existen políticas, lineamientos y/o directrices para el correcto y buen uso de los equipos informáticos?		50%	50%
16.- ¿Conoce ud algunas políticas de seguridad de la información?		80%	20%

Fuente: Autoría Propia

Tabla 5: Análisis e interpretación de los riesgos detectados

DESCRIPCIÓN	RIESGO
R1	Vulnerabilidad y alteraciones de las configuraciones y puertos de acceso a las terminales de los servidor (Proxy MikroTik, WEB, Correos) ante cualquier amenaza interna o externa.
R2	Fuga y pérdida de la disponibilidad de la información, al no existir los controles adecuados para el acceso y autenticación de los usuario no autorizados a los sistemas y aplicaciones informáticas del GADMCB.
R3	Pérdida de información crítica y/o sensible que se genera por falta de servidores de respaldos (réplicas) internos/externos del GADMCB.
R4	Perdida de información, recursos económicos, servicios paralizados ocasionado como resultado de daño físico de los activos del GADBMCB originados ya sea por desastres naturales, daños accidentales o ataque maliciosos.

Fuente: Autoría Propia

Determinación del ROSI (Retorno sobre la inversión en la seguridad)

En este apartado se presenta los procesos para la respectiva evaluación financiera de seguridad y gestión de riesgo para el GADMCB. Para la determinación del ROSI como primer proceso se debe calcular la expectativa de pérdida individual (SLE), para este proceso se debe establecer los servicios considerados en cada riesgo y de cada servicio considerar el valor del activo, configuraciones, licencias y soporte técnico (sin considerar las pérdidas de ingresos por no tener al activo en funcionamiento), además es importante identificar el porcentaje de factor de exposición de los servicios.

a) *SLE (Determinación de la expectativa de pérdida individual).* Para este cálculo se aplicó la siguiente formula:

SLE= *Expectativa de pérdida individual*

VA= *Valor del activo*

FE= *Factor de exposición*

Formula: SLE*=VA X FE*

El resultado de este proceso se expone en la tabla 6 en cada uno de los riesgos relacionado a cada servicio informático del GADMCB y el valor del activo.

Tabla 6: SLE (Determinación de la expectativa de pérdida individual)

Riesgo	Servicio	Activo	Valor activo (VA)	FE (Factor de exposición)	FE%	SLE
R1	Servidores(Proxy, BDD, WEB, Correos Institucionales, Virtuales)	Servidores Soporte Técnico Licencias	$ 12,471.09	Cuenta con un Proxy de control. Cuenta con controles de accesos básicos a la información. Cuenta con Swich administrables de acceso a la red interna.	20%	$ 2,494.22
R2	Sistema Informáticos.	Configuración e instalación de los sistema de Informáticos Municipales Soporte Técnico	$ 9,200.00	Existe un control de acceso a datos confidenciales del GAD Municipal. Los sistemas informáticos cuentan con controles de accesos básicos a la información.	70%	$ 6,440.00
R3	Servidor de respaldos(réplicas)	Servidor Configuración Licencias	$ 5,200.00	Cuenta con servidores donde se almacena respaldos(réplicas) de la información, periódicamente. Cuentan con algún proceso para generar o salvaguardar la información crítica y/o sensible. Existe algún control para proteger la información.	60%	$ 3,120.00
R4	Activos(equipos informáticos)	Equipos de red y comunicaciones Equipos informáticos Configuraciones Licencias	$ 205,000.00	Existe un plan de contingencia para salvaguardar los activos. Cuenta con pólizas de seguro vigentes Cuenta con los inventaros de los equipos informáticos actualizados. Existe algún control sobre el buen uso de los equipos informáticos.	30%	$ 61,500.00

Fuente: Autoría: Propia

En la tabla 7 se detalla los ingresos generados por los sistemas de recaudación de los tributos municipales y servidores al GADMCB, por horas y al año.

Tabla 7: Ingresos generados por los Sistemas de recaudación de los tributos municipales/servidores

Activo	Hora	8 horas laborables	Al año
Sistemas de recaudación de los tributos municipales/servidores	$ 587,73	$ 4.701,83	$ 2.072.839,30

Fuente: Autoría: Propia

b) *ARO (Taza de Ocurrencia Anualizada).* Sirve para conocer la frecuencia de la amenaza al año, como se presenta en la **tabla 8** se está representada a continuación.

Tabla 8: ARO (Taza de Ocurrencia Anualizada)

Riesgo	Amenazas	Estadísticas	ARO
R1	Ataque Man In The Middle (MITM)	1 vez cada 2 años	50%
R2	Acceso de personal no autorizado.	1 vez cada 2 años	50%
R3	Infección por virus	2 vez cada año	50%
	Falla eléctrica	1 vez cada 4 años	25%
R4	Infección por virus	1 vez cada 2 años	50%
	Falla eléctrica	1 vez cada 4 años	25%
	Amenaza natural	1 vez cada 4años	25%

Fuente: Autoría: Propia

Interpretación: donde se define el ARO que se presenta las amenazas determinando que el R4, tiene más probabilidades que la amenazas ocurran con mayor frecuencia.

c) ALE *(Expectativa de pérdida anual).* A continuación, en la tabla 9 se determinará la pérdida monetaria que se puede esperar para un activo debido a la materialización de las amenazas detectadas anualmente.

Fórmula: ***ALE*** **=** *SLE x ARO*

ALE= Expectativa de pérdida anual

ARO= Tasa de ocurrencia anualizada

Tabla 9: Expectativa de pérdida anual

Activo	Amenaza	VA	FE	ARO	ALE
Servidores (Proxy, BDD, Correos institucionales, Servidor hosting)	Ataque Man In The Middle (MITM)	$ 12,471.09	0.2	0.5	$ 1,247.11
Sistemas informáticos (Recaudación de los tributos municipales, Sistema de Avalúos y Catastros, Sistema Contable)	Acceso de personal no autorizado.	$ 9,200.00	0.7	0.5	$ 3,220.00
Servidor de respaldos(réplicas)	Infección por virus	$ 5,200.00	0.6	0.5	$ 1,560.00
	Falla eléctrica	$ 5,200.00	0.6	0.25	$ 780.00
Activos(equipos informáticos)	Infección por virus	$205,000.00	0.3	0.5	$33,300.00
	Falla eléctrica	$205,000.00	0.3	0.25	$15,375.00
	Amenaza natural	$205,000.00	0.3	0.25	$15,375.00

Fuente: Autoría: Propia

d) *Acciones para mitigar el riesgo*. En esta etapa se analizó los distintos controles para salvaguardas los activos que posee el GADMCB de los posibles riesgos como se muestra en la tabla 10.

Tabla 10: Índice de mitigación y costo de solución

Riesgos	Acciones Controles	Costo	Costo total Acciones	Índice de mitigación
R1	Políticas de seguridad de control de acceso.			
	Adquirir sistemas de control de acceso(firewall)	$ 6,500.00		
	Adquirir licencias de certificación SSL	$ 1,500.00		
	Capacitación a los usuarios.	$ 1,000.00	$ 9,000.00	85%
R2	Políticas de seguridad de control de acceso.			
	Implementación de sistema informático que cumpla y controla los log de acceso a los sistemas informáticos, que permita la asignación de usuarios con privilegios de acceso según las actividades establecidas a cada funcionario.	$35,000.00		
	Soporte técnico	$ 5,000.00		
	Capacitación a los usuarios.	$ 2,000.00	$42,000.00	90%
R3	Políticas de seguridad			
	Adquisición servidores de respaldos(réplicas)	$ 4,500.00		
	Adquisición de licencias	$ 1,500.00		
	Configuración de servidor	$ 1,200.00		
	Capacitación técnica.	$ 1,200.00	$ 8,400.00	90%
R4	Políticas de seguridad			
	Póliza de seguro	$ 40,000.00		
	Adecuación del data center	$ 8,000.00		
	Mantenimiento del cableado eléctrico	$ 80,000.00	$128,000.00	85%

Fuente: Autoría: Propia

Una vez considerado las acciones propuestas en la sección anterior nos da un índice de mitigación, y el costo de solución; mismo que será considerado para el cálculo del ROSI en el siguiente apartado.

Se detalla las acciones necesarias para mitigar los riesgos identificados se realizó un análisis financiero (costo) para la implementación de cada control.

e) Calcular el ROSI *del riesgo*

A continuación, en la tabla 11, se determinará el Porcentaje de retorno de inversión en Seguridad de la Información, considerando el ALE (ver tabla 9) por el índice de mitigación y costo de solución (ver tabla 10).

Formula:

ROSI= (ALE x índice de mitigación – Costo de solución) / Costo de solución

Tabla 11: Cálculo del ROSI (Retorno de la inversión en la Seguridad de la Información)

Riesgo	ALE	Índice de Mitigación	ROSI	%
R1	$ 1,247.11	0.85	0.12	12%
R2	$ 3,220.00	0.90	0.07	7%
R3	$ 2,340.00	0.85	0.24	24%
R4	$ 61,500.00	0.80	0.38	38%

Fuente: Autoría: Propia

Como resultado se debe indicar que el ROSI de mayor porcentaje es de 66% para el retorno de inversión con respecto a la expectativa de pérdida anual valor de $ 99,99.00 en relación del 0.85 porcentaje de índice de mitigación, menor porcentaje es de 3% para el retorno de la inversión con respecto a la expectativa de pérdida anual valor de $ 3,220.00 en relación al 0.90% con el mayor índice de mitigación

Índice de Capacidad de Protección. Para el establecimiento del índice de capacidad de protección, se aplicará la siguiente formula.

CP= (RI-RR)/RI

CP=Capacidad de protección

RR=Riesgo residual

RI=Riesgo inherentes

Capacidad de Protección es igual al Riesgo Inherente (costo de incidente x la probabilidad de ocurrencia), para obtener este valor se debe considerar el cálculo del ALE menos; y finalmente; el Riesgo Residual (costo de incidente x Nueva probabilidad de ocurrencia). Se debe considerar que el factor de mitigación afectara la probabilidad de ocurrencia.

Tabla 12: Índice de Capacidad de Protección.

Riesgo	Costo Operacional	RI	Probabilidad de ocurrencia	Nueva probabilidad de ocurrencia	Diferencia de % de probabilidad de ocurrencia	Nueva probabilidad de ocurrencia del incidente	RR	CP
R1	$ 9,000.00	$ 1,247.11	0.50	0.85	15	0.07	$ 93.53	0.93
R2	$ 42,000.00	$ 3,220.00	0.50	0.90	10	0.05	$ 161.000	0.95
R3	$ 8,400.00	$ 2,340.00	0.75	0.85	15	0.11	$ 263.2000	0.89
R4	$ 128,000.00	$61,500.00	0.75	0.80	20	0.15	$ 9,225.75	0.85

Figura 2: Gráfica de protección

Fuente: Autoría: Propia.

Evaluar el riesgo

A continuación, en las tablas: 13 y 14 se observa el valor de la probabilidad y el impacto para evaluar el riesgo.

Tabla 13: Ocurrencia del riesgo

PROBABILIDAD	DESCRIPCIÓN	VALOR
Muy Alta	Es casi seguro que el riego ocurra. Ocurre cada mes, o cada año	5
Alta	Es muy factible que el riesgo ocurra. Ha ocurrido en el pasado, en el último año y volverá a ocurrir	4
Media	Es factible que el riesgo ocurra Ha ocurrido al menos una vez en el GADMCB	3
Baja	Es muy poco factible que el riesgo ocurra Nunca ha ocurrido en el GADMCB	2
Muy Baja	Es casi imposible que el riesgo ocurra Es posible que ocurra, pero a la fecha nunca ha pasado en el GADMCB	1

Fuente: Autoría: Propia

Tabla 14: Impacto de riesgo

IMPACTO	DESCRIPCIÓN	VALOR
Extremo / Muy grave	Si el riesgo llegara a ocurrir, tendría muy alto impacto o efecto sobre el GADMCB	5
Mayor / Grave	Si el riesgo llegara a ocurrir, tendría alto impacto o efecto sobre el GADMCB	4
Moderado	Si el riesgo llegara a ocurrir, tendría medio impacto o efecto sobre el GADMCB	3
Menor / Leve	Si el riesgo llegara a ocurrir, tendría bajo impacto o efecto sobre el GADMCB	2
Bajo	Si el riesgo llegara a ocurrir, tendría muy bajo impacto o efecto sobre el GADMCB	1

Fuente: Autoría: Propia

En la tabla 15 y 16 se refleja los valores de la probabilidad de ocurrencia por el impacto.

Probabilidad x Impacto.

Tabla 15: Valoración de los Riesgos

RIESGO	PROBABILIDAD	IMPACTO	VALOR	CATEGORÍA
R1	4	5	20	Riesgo muy alto
R2	5	5	25	Riesgo muy alto
R3	3	5	15	Riesgo muy alto
R4	3	4	12	Riesgo alto

Fuente: Autoría: Propia

Tabla 16: Índice de Riesgo de cada uno de los Riesgos

RIESGO	VALOR	ÍNDICE
R1	20	0.28
R2	25	0.35
R3	15	0.21
R4	12	0.17

Fuente: Autoría: Propia

En la tabla 17 se refleja la obtención de la matriz de evaluación de riesgo con sus categorías considerando los valores y los índices de riesgo.

Tabla 17: Matriz de evaluación y categoría de Riesgo

Probabilidad	**Muy Alta**	5	5	10	15	20	R2 25
	Alta	4	4	8	12	16	R1 20
	Media	3	3	6	9	R4 12	R3 15
	Baja	2	2	4	6	8	10
	Muy Baja	1	1	2	3	4	5
			1	2	3	4	5
			Bajo	**Menor / Leve**	**Moderado**	**Mayor / Grave**	**Extremo / Muy grave**
			Impacto				

CATEGORÍA	VALOR
Riesgo bajo	1 a 3
Riesgo moderado	4 a 6
Riesgo alto	8 a 12
Riesgo muy alto	15 a 25

Fuente: Autoría: Propia

Implementar controles

De acuerdo al cuadro de resultados donde de identificó los riesgos como resultado de la investigación mediante una valoración cuantitativa aplicado a los 20 funcionarios que son usuarios claves para el uso de los sistemas y aplicativos informáticos, se realizó una valoración de cada riesgo en que probabilidad de ocurrencia y el impacto que genera ante la presentación de los riesgos (ver Tabla 15. Matriz de evaluación y categoría de Riesgo), mismo que pueden afectar el desempeño o producir pérdidas financieras, de servicio, de reputación, etc.

Se realice el proceso de aplicación de controles de seguridad en base a la norma ISO 27002:2013, agrupa un total de 114 controles o salvaguardas sobre buenas prácticas para la gestión de seguridad de la información organizada en 14 dominios y 35 objetivos de control, para ello se realizó un análisis relevante en base a los resultados obtenidos de la investigación para la aplicabilidad en base a ciertos controles enfocados en la realidad del GADMCB, permitiendo mitigar los riesgos encontrados en la etapa de análisis de riesgos.

Se incluye la justificación de la selección de algunos controles de la norma ISO 27002:2013, estas razones pueden ser:

L: Requerimientos legales: Requisitos legales, Reglamentos

C: Obligaciones Contractuales: Con la prestación de servicio

N: Requerimiento del negocio: Necesidad de seguridad de la entidad

R: Análisis de riesgos: Resultado de análisis de riesgo

Tabla 18: Políticas de Seguridad de la información basada en la norma ISO 27002:2013

A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN					
A.5.1 Dirección de gestión de seguridad de la información					
Objetivo: Proporcionar dirección y soporte de la gestión de la seguridad de la información, aplicables al GAD Municipal del Cantón Biblián alineados a las leyes, reglamentos vigentes.					
Dominios	**Control**	**Razones**			
		L	**C**	**N**	**R**

Pol. Con. (Edición núm. 52) Vol. 5, No 11, Noviembre 2020, pp. 591-621, ISSN: 2550 - 682X

A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas de seguridad de la información debe ser definido, aprobado por la máxima autoridad, publicado y comunicado a los empleados y partes externas relevantes.	X		X	
A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas de seguridad de la información deben ser revisadas planificados o siempre que se produzcan cambio significativo, con el objetivo de mantener su idoneidad, adecuación y eficacia.			X	
A.6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN						
A.6.1 Organización interna						
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la organización						
A.6.1.1	Asignación de responsabilidades para la seguridad de la información	Todas las responsabilidades de seguridad de la información crítica y/o sensible deben ser bien definidas y asignadas al personal según las funciones o tareas que lo realizan, la unidad de talento humano se debe encargar de asegurar que todos los funcionarios conozcan sus responsabilidades con respecto al uso de los recursos informáticos y la información.			X	
A.6.1.2	Separación de funciones	Deben existir controles y políticas que se establezca identificando las funciones en conflicto y áreas de responsabilidades, mismas que deben estar separadas para reducir las oportunidades de modificación no autorizada o no intencional o el mal uso de los activos del GAD Municipal.			X	X
A.6.1.3	Contacto con las autoridades	N/A				
A.6.1.4	Contacto con grupos de interés especial	N/A				
A.6.1.5	Seguridad de la información	N/A				
A.6.2 Dispositivos para movilidad y teletrabajo						
A.7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS						
A.7.1	Antes de la Contratación	N/A				

A.7.2	Durante la Contratación	N/A				
A.7.3	Cese o cambio de puesto de trabajo	N/A				
A.8 GESTIÓN DE ACTIVOS						
A.8.1 Responsabilidades sobre los activos						
Objetivo: Identificar los activos de la organización y definir las responsabilidades de actividad						
A.8.1.1	Inventario de activos	La información, otros activos asociados con la información y las instalaciones para el procesamiento de la información deben ser identificados y tener actualizado e inventario de los activos.			X	
A.8.1.2	Propiedad de los activos	Debe existir control sobre los activos, mismos que deben estar etiquetados y bien inventariados, y debe tener un responsable.			X	
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de la información, los activos asociados con la información y las instalaciones de procesamiento de información.			X	
A.8.1.4	Devolución de activos	Todos los empleados y terceras partes deben devolver todos los activos de entregados que estén en su poder al finalizar su empleo, contrato o acuerdo.			X	
A.8.2 Clasificación de la información						
Objetivo: Asegurar que la información reciba un nivel apropiado de protección de acuerdo con su importancia para el GAD Municipal del Cantón Biblián.						
A.8.2.1	Clasificación de la información	La información debe ser clasificada en términos de la importancia de su relevancia frente a requisitos legales, valor, sensibilidad, y criticidad ante revelación o modificación no autorizadas.			X	X
A.8.2.2	Etiquetado de la información	Debe desarrollarse e implementarse un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por el GAD Municipal.			X	
A.8.2.3	Manejo de las activos	Los procedimientos para el manejo de los activos deben ser desarrollados e implementados de acuerdo con el esquema de clasificación de la información adoptada por el GAD Municipal.			X	
A.8.3 Manejo de los soporte de almacenamiento						

8.3.1	Gestión de soporte extraíbles	N/A				
8.3.2	Eliminación de soportes	N/A				
8.3.3	Soporte físico de tránsito	N/A				
A.9 CONTROL DE ACCESO						
A.9.1 Requisitos de negocio para el Control de Acceso						
Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.						
A.9.1.1	Políticas de control de accesos	Se debe establecer, documentar y revisar una política de control de acceso basado en los requisitos y exigencias establecidos según la norma vigente del sector público y de seguridad de la información.			X	X
A.9.1.2	Acceso de redes y servicios	Únicamente se debe proporcionar a los usuarios a los accesos a los sistemas, servicios de red para cuyo uso hayan sido específicamente autorizados.			X	X
A.9.2 Gestión de Acceso de los usuarios						
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.						
A.9.2.1	Registro y retiro de usuario	Se debe implementar un procesamiento formal de registro y retirada de usuarios que hagan posible la asignación de los derechos de acceso.			X	X
A.9.2.2	Provisión de acceso a usuarios	Se debe implementar un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.			X	X
A.9.2.3	Gestión de privilegios de derechos de acceso	La asignación y el uso de privilegios de acceso deben restringida y controlada.			X	X
A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	Debe existir un control para la asignación de la información secreta de autenticación sea controlada a través de un proceso formal de gestión			X	X
A.9.2.5	Revisión de los derechos de acceso a usuarios	Los responsables de los activos y los sistemas deben revisar el derecho de acceso de usuarios en determinado periodo definido.			X	X

A.9.2.6	Retirada y ajustes de los derechos de acceso	Los derechos de acceso de todos los funcionarios, a la información y a las instalaciones de procesamiento de la información deben existir controles para el retiro de los respectivos accesos a la finalización del empleo, del contrato o del acuerdo, o ajustarlo en caso de cambio.			X	X
A.9.3 Responsabilidades del usuario						
Objetivo: Hacer que los usuarios sean responsables de salvaguardar la información de autenticación.						
A.9.3.1	Uso de la información secreta de autenticación	Debe existir un control para el uso de la información secreta de autenticación de los sistemas informáticos.			X	X
A.9.4 Control de acceso a sistemas y aplicaciones						
Objetivo: Prevenir el acceso no autorizado a los sistemas informáticos y aplicaciones						
A.9.4.1	Restricción del acceso a la información	El acceso a la información y a las aplicaciones de los sistemas debe ser restringido, mediante políticas establecidas en el GAD Municipal.			X	X
A.9.4.2	Procedimientos seguros de inicio de sesión	Debe existir un control mediante una política existente, para el procedimiento seguro de inicio de sesión.			X	
A.9.4.3	Sistema de gestión de contraseña	Los sistemas y controles para la respectiva gestión de contraseñas deben ser interactivos y asegurar la calidad de contraseñas.			X	X
A.9.4.4	Uso de programas utilitarios privilegiados	El uso de programas que pueden ser capaces de invalidar los controles de seguridad de los sistemas y aplicaciones, deben ser restringidos y controlados.			X	
A.9.4.5	Controles de acceso al código fuente del programa	Debe existir controles que restringa el acceso al código fuente.			X	
A.10 CIFRADO						
A. 10.1	Controles Criptográficos	N/A				
A.11 SEGURIDAD FÍSICA Y DE ENTORNO						

Pol. Con. (Edición núm. 52) Vol. 5, No 11, Noviembre 2020, pp. 591-621, ISSN: 2550 - 682X

A.11.1 Áreas Seguras						
Objetivo: Prevenir el acceso físico no autorizado, los daños e interferencias a la información del GAD Municipal, y a las instalaciones de procesamiento de la información.						
A.11.1.1	Perímetro de seguridad física	Los perímetros de seguridad deben ser definidos y usados correctamente, para el uso y protección de las áreas que contienen información crítica y/o sensible, así como las estaciones de procesamiento de la información.			X	X
A.11.1.2	Controles físicos de entrada	Deben existir controles de seguridad adecuadas, aplicadas en las áreas seguras, para asegurar y garantizar únicamente el acceso al personal autorizado.			X	
A.11.1.3	Seguridad de oficinas instalaciones	Para garantizar la seguridad física de las oficinas e instalaciones, deben existir controles que exija realizar diseño de los mismos y ser aplicado.			X	
A.11.1.4	Protección contra amenazas externas y ambientales	Debe existir un control que garantice la protección física contra desastres naturales, ataques naturales, ataques maliciosos o accidentes.			X	X
A.11.1.5	Trabajo en áreas seguras	Debe existir procedimientos para trabajar en áreas seguras, mismos que deben ser diseñados y aplicados.			X	X
A.11.1.6	Áreas de carga y entrega	Debe existir un control en los puntos de acceso tales como las áreas de cargas y entrega y otros puntos donde pueda acceder personal no autorizado a las instalaciones, y si fuera posible, aislar dichos puntos de las instalaciones de procesamiento de la información para evitar accesos no adecuados.			X	
A.11.2 Seguridad de los Equipos						
Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones en el GAD Municipal.						
A.11.2.1	Ubicación y protección de equipos	Debe existir controles que proteja y garantice que los equipos informáticos deben estar situados y protegidos de tal forma que se reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados.			X	X
A.11.2.2	Instalaciones de suministros	Deben existir controles de protección a los equipos informáticos contra fallos eléctricos y otras alteraciones.			X	X
A.11.2.3	Seguridad de cableado	Debe existir control de seguridad para el cableado eléctrico y de telecomunicaciones que trasmite datos o que da soporte a los servicios de información.			X	X
A.11.2.4	Mantenimiento de los equipos	Debe existir un plan de mantenimiento preventivo y correctivo de los equipos que asegure la disponibilidad y la integridad continúa.			X	

A.11.2.5	Eliminación de los activos	Si no existe autorización previa, los equipos la información o el software no deben sacarse de las instalaciones.			X	
A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones	Debe existir medidas de seguridad de los equipos informáticos fuera de las instalaciones del GAD Municipal, considerando los riesgos que conlleva trabajar fuera de las instalaciones de la entidad.			X	
A.11.2.7	Reutilización o eliminación segura de equipos	N/A				
A.11.2.8	Equipo de usuarios desatendido	N/A				
A.11.2.9	Política depuesto de trabajo despejado y pantalla limpia	N/A				
A.12 SEGURIDAD DE LAS OPERACIONES						
A.12.1 Procedimientos y responsabilidades operacionales		N/A				
A.12.2 Protección contra código malicioso						
Objetivo: Asegurar que las estaciones de procesamiento de la información y la información delicada del GAD Municipalidad estén protegidas contra código malicioso						
A.12.2.1	Controles contra código malicioso	Se debe implementar controles de detección, prevención y recuperación que sirvan como protección contra código malicioso, así como procedimientos adecuados de concienciación de usuarios.			X	X
A.12.3 Copias de Seguridad						
Objetivo: Evitar pérdida de datos						
A.12.3.1	Copias de seguridad de la Información	Debe existir controles y políticas para resguardad la seguridad de la información, como realizar copias de seguridad de la información de manera periódica en las estaciones del GAD Municipal, como con proveedores externos.			X	X

A.12.4 Registro de actividad y supervisión	N/A				
A.12.5 Control de software en explotación	N/A				
A.12.6 Gestión de la vulnerabilidad técnica	N/A				
A.12.7 Consideraciones de las auditorías de los sistemas informáticos	N/A				
A. 13 SEGURIDAD EN LAS TELECOMUNICACIONES					
A.13.1 Gestión de la seguridad en las redes	N/A				
A.13.2 Intercambio de información con parte externas	N/A				
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN					
A.14.1 Requisitos de seguridad de los sistemas de información	N/A				
A.14.2 Seguridad en los procesos de desarrollo y soporte	N/A				
A.14.3 Datos de prueba	N/A				
15 RELACIONES CON SUMINISTRADORES					
A.15.1 Seguridad de la información en las relaciones con suministradores	N/A				
A.15.2 Gestión de la presentación del servicio por suministradores	N/A				
16 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN					

A.16.1 Gestión de incidentes de seguridad de la información y mejoras	N/A				
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO					
A.17.1 Continuidad de la seguridad de la información	N/A				
A.17.2 Redundancias	N/A				
18. CUMPLIMIENTO					
A.18.1 Cumplimiento de los requisitos legales y contractuales	N/A				
A.18.2 Revisiones de la seguridad de la información	N/A				

Fuente: https://www.efectus.cl/wp-content/uploads/2018/12/Controles_ISO27002-2013.pdf

Elaboración: Propia.

Discusión

El presente artículo evidencia la necesidad de aplicar controles y políticas de seguridad de la información bajo los lineamientos de los controles y objetivos enmarcados dentro la norma ISO 27002:2013, para llegar a este análisis se realizó un estudio realizado en un análisis preliminar en base a la situación actual del GADMCB, donde se pudo analizar los procesos y tratamiento de la información más crítico y sensibles realizando una evaluación de amenazas que al explorar las vulnerabilidades pueden ocasionar el riesgo. Un riesgo que afecta las operaciones y las puede paralizar se define como “desastre”. Un desastre es “un evento que altera los procesos críticos de la organización que afecta su misión y degrada su servicio a un punto donde el impacto financiero y operacional se convierte en inaceptable” (Hiles & Banes, 2010)

Con el objetivo de definir los procesos y controles aplicarse para salvaguardar la información y los activos y de esta forma garantizar la integridad, confiabilidad, disponibilidad y trazabilidad de la información.

Para la aplicabilidad del análisis se procedió a realizar el presente proyecto bajo el pleno conocimiento y autorización de la máxima autoridad del GAD Municipal del Cantón Biblián (GADMB), de manera principal nos enfocamos con los funcionarios de los departamentos administrativos y financiero que usan los sistemas y aplicaciones informáticos para determinar la situación actual e identificar los riesgos, el levantamiento de información se realizó en el sitio mediante entrevistas aplicados a 20 funcionarios, en base a los resultados obtenidos se realizó la evaluación financiera de Seguridad y Gestión de Riesgo , para determinar el índice de capacidad de protección costo/beneficio.

Conclusiones

Se determinó la necesidad de implementar políticas de seguridad de información para mitigar el riesgo basada en la norma ISO 27002:2013 en el marco de referencia para gestionar la seguridad de la organización, proponer diferentes controles y políticas de seguridad con el objetivo de salvaguardar los activos, proteger, respaldar información y planear estrategias de cambio y mejora continua.

A través de esta investigación se pudo comprobar que la implementación de políticas de seguridad de información, no es una tarea fácil implica considerar factores como lineamientos de la norma vigente, procesos metodológicos que sean ajustables y perfectibles que requiere el involucramiento del personal humano y consideraciones sobre aspectos tecnológicos, pero es importante implementar para mantener segura la información con la que cuenta el GADMCB, al tener establecido políticas, normas y procedimientos, los funcionarios van a conocer cómo manejar los activos de información de forma que estén menos expuestos a riesgos de seguridad y si estos se presentan saber la manera en que deben proceder para minimizar.

Referencias

1. Acuerdo de la Contraloría General del Estado. (16 Diciembre del 2014). NORMAS DE CONTROL INTERNO DE LA CONTRALORIA. Quito.
2. Altamirano, J., & Bayona, S. (2017). Políticas de Seguridad de la Información: Revisión Sistemática de las Teorías que Explican su Cumplimiento. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 117-126.

3. Areitio, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. Madrid-España, S.A: LEARNING PARANINFO,.
4. Areitio, J. (s.f.). Seguridad de la Información.
5. Cárdenas, F. (2015). Sistematización del Presupuesto Participativo del Cantón Biblián. Biblián: The Game Comunicación Estratégica.
6. Constitución de la República del Ecuador. (20 de 10 de 2008). Decreto Legislativo. 87-92. Quito, Pichincha, Ecuador: Lexis. Recuperado el 20 de 08 de 2020, de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf
7. Contreras, L. (17 de 04 de 2017). Diseño de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27001 para la Dirección de Sistemas de la Gobernación de Boyacá. Universidad de Boyacá. Tunja, Boyacá, Colombia.
8. Cortes, Y. (24 de Abril de 2018). Apoyo al área de seguridad de la información de la corporación de alta tecnología para la defensa de Codaltec para concluir la implementación y operación del sistema de gestión de seguridad de la información SGSI según la norma técnica colombiana ISO-IEC . Universidad Cooperativa de Colombia. Villavicencio, Bogotá, Colombia: UCC.
9. Del Rio, M. (24 de Agosto de 2011). Deficiencias más comunes en los SGSI basados en la ISO 27001. Obtenido de SEGURITYBYDEFAULT.COM: http://www.securitybydefault.com/2011/08/deficiencias-mas-comunes-en-los-sgsi.html
10. Deparment for Digital, Culture, Media y Sport. (2018). Cyber Security Breaches Survey 2018. San Francisco: Social Research Institute.
11. Erb, M. (2009). Gestion de riesgos en la segurida informática. Gestion de riesgos, 1-20.
12. Escuela Superior de Redes RED CEDIA. (2014). Gestión de la Seguridad de Información . Bogota : CEDIA.
13. Hangbae, C. (2013). Is ISMS for financial organizations effective on their business? Mathematical and Computer Modelling, 79-84.
14. Hiles, A., & Banes, P. (2010). El manual definitivo de gestión de la continuidad empresarial . . Wiley.
15. ISOTools EXCELLENCE. (05 de Marzo de 2018). Plataforma Tecnológica para la Gestión de la Excelencia. Obtenido de Calidad y excelencia: https://www.isotools.org/2018/03/05/la-norma-iso-iec-27000-va-a-ser-revisada/
16. Ladino, M. y. (2011). Fundamentos de ISO 27001 y su Aplicación en las Empresas . Scientia Et Technica, 334-339.

17. Ledesma, D. (02 de 02 de 2015). Desarrollo de Políticas de Seguridad de la Información basadas en la Norma ISO 27002 para una Coordinación zonal del INEC. Repositorio de la Pontífece Universidad Católica del Ecuador sede Ambato. Ambato, Tunguragua, Ecuador. Obtenido de Repositorio de la Universidad Católica del Ecuador sede Ambato: http://repositorio.pucesa.edu.ec/bitstream/123456789/1555/1/76092.pdf
18. Mifsud, E. (2012). Políticas de seguridad. ¿Cómo podemos proteger el sistema informático? Observatorio Tecnologíco, 1-17.
19. Naser, A. (2016). La nueva era digital. Tecnológico de Costa Rica. Pensis, 35.
20. Pilla, J. (14 de Septiembre de 2019). Diseño de una política de Seguridad de Información Área de Tecnología de la Información de la Cooperativa de Ahorro y Crédito Chibuleo LTDA., Basado en la Norma ISO/IEC 27002:2013. Repositorio de la Universidad Internacional SEK. Quito, Pichincha, Ecuador.
21. Presidencia de la República del Ecuador. (2015). Código Órganico Organización Territorial Autónomia Descentralización. Quito: Lexis.
22. Quiroz, S. (2017). Seguridad en Informática: Consideraciones. Revista Científica: Dominio de las Ciencias, 677-688.
23. Ramos, Y., Urrutia, O., & Ordoñez, D. y. (2017). Adoptar una política de seguridad de la información basadosen un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca. 4to Congreso Internacional AmITIC 2017 (págs. 88-95). Popayán: S/N.
24. Rincón, D. (19 de Mayo de 2014). Viabilidad de la implementación de la norma ISO 27001 en la empresa transportes Colombia S.A. Universidad Cooperativa de Colombia. Cundinamarca, Bogotá, Colombia: UCC.
25. Silva, J. (2020). Seguridad Infórmatica: Amenazas Comunes. Corredura de Seguros, 23-25