Dom. Cien., ISSN: 2477-8818
Vol. 6, núm. 4, Octubre-Diciembre 2020, pp. 1550-1576

DOI: http://dx.doi.org/10.23857/dc.v6i4.1566

Ciencias técnicas y aplicadas

Artículo de investigación

Propuesta de guía rápida de un sistema de gestión de la seguridad de la información, para el Registro de la Propiedad del Cantón Cuenca

Proposal for a quick guide for an information security management system, for the Registro de la Propiedad del Cantón Cuenca

Proposta de guia rápido de sistema de gestão de segurança da informação para o Cadastro de Imóveis do Cantão de Cuenca

Edgar Alejandro Loja-Tepán [I]
edgar_loja_2006@hotmail.com
https://orcid.org/0000-0001-8151-2283

Juan Pablo Cuenca-Tapia [II]
jcuenca@ucacue.edu.ec
https://orcid.org/0000-0001-5982-634X

Correspondencia: edgar_loja_2006@hotmail.com

***Recibido:** 30 de septiembre de 2020 ***Aceptado:** 28 de octubre de 2020 * **Publicado:** 27 de noviembre de 2020

I. Egresado de la Maestría en Tecnologías de la Información, Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.

II. Magíster en Sistemas de Información Gerencial, Docente de la Unidad Académica de Tecnologías de la Información y Comunicación (TIC), Jefatura de Posgrados, Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

La información se ha convertido en un recurso invaluable para las empresas. Y dependerá de su estructura, contenido y calidad para ser considerada como fuente de consulta para generar más información. Anteriormente la seguridad estaba orientada a proteger objetos físicos que tenían un valor meramente económico. Con el avance tecnológico y la transformación de la información física a un formato digital, la seguridad ha tomado nuevos horizontes. Los departamentos de Tecnologías de la Información y Comunicación (TIC), están llamados a generar seguridad de la información.

En tal virtud, se propone una guía basada en MAGERIT e ISO/IEC 27001, para generar niveles aceptables de seguridad en el Registro de la Propiedad del Cantón Cuenca (RPCC), para mantener la confidencialidad, integridad y disponibilidad de la información que se procesa. Para esto, es necesario identificar los riesgos y amenazas; y proponer los mecanismos necesarios para impedir que un riesgo se materialice y en caso que suceda se pueda minimizar la probabilidad y el impacto. Debemos considerar que la información del RPCC, está contenida en documentos físicos y en repositorios digitales. Por lo tanto, es importante implementar políticas de seguridad y controles necesarios que ayuden a proteger la información; tanto, de usuarios internos, así también de usuarios externos, que pueden hacer uso de alguna vulnerabilidad existente en la seguridad y tener acceso no autorizado a los datos. Esta intrusión puede afectar a la prestación de los servicios que ofrece la institución, y su recuperación, puede consumir grandes cantidades de recursos económicos y humanos.

Es por esta razón, que la seguridad de la información debe ser asumida como un nuevo objetivo del RPCC.

Palabras clave: Seguridad de la información; confidencialidad; integridad; disponibilidad; ISO 27001.

Abstract

Information has become an invaluable resource for companies. And it will depend on its structure, content and quality to be considered as a source of consultation to generate more information. Previously, security was aimed at protecting physical objects that had a purely economic value.

With technological advancement and the transformation of physical information to a digital format, security has taken on new horizons. The Information and Communication Technologies (ICT) departments are called upon to generate information security.

As such, a guide based on MAGERIT and ISO / IEC 27001 is proposed, to generate acceptable levels of security in the Land Registry of the Canton Cuenca (RPCC), to maintain the confidentiality, integrity and availability of the information that is processed. . For this, it is necessary to identify risks and threats; and propose the necessary mechanisms to prevent a risk from materializing and, if it happens, the probability and impact can be minimized. We must consider that the information of the RPCC is contained in physical documents and in digital repositories. Therefore, it is important to implement security policies and necessary controls that help protect information; both internal users, as well as external users, who may make use of any existing vulnerability in security and have unauthorized access to data. This intrusion can affect the provision of the services offered by the institution, and its recovery can consume large amounts of economic and human resources.

It is for this reason that information security must be assumed as a new objective of the RPCC.

Keywords: Information security; confidentiality; integrity; availability; ISO 27001.

Resumo

A informação tornou-se um recurso inestimável para as empresas. E vai depender de sua estrutura, conteúdo e qualidade para ser considerada fonte de consulta para gerar mais informações. Anteriormente, a segurança visava proteger objetos físicos que tinham um valor puramente econômico. Com o avanço tecnológico e a transformação das informações físicas em formato digital, a segurança ganhou novos horizontes. Os departamentos de Tecnologias de Informação e Comunicação (TIC) são chamados para gerar segurança da informação.

Como tal, propõe-se um guia baseado no MAGERIT e ISO / IEC 27001, para gerar níveis aceitáveis de segurança no Registro Predial do Cantão de Cuenca (RPCC), para manter a confidencialidade, integridade e disponibilidade das informações que são processadas. . Para isso, é necessário identificar riscos e ameaças; e propor os mecanismos necessários para evitar que um risco se materialize e, caso isso aconteça, a probabilidade e o impacto podem ser minimizados.

Devemos considerar que as informações da RPCC estão contidas em documentos físicos e em repositórios digitais. Portanto, é importante implementar políticas de segurança e controles necessários que ajudem a proteger as informações; tanto usuários internos, quanto usuários externos, que podem fazer uso de qualquer vulnerabilidade existente na segurança e têm acesso não autorizado aos dados. Essa intrusão pode afetar a prestação dos serviços oferecidos pela instituição, e sua recuperação pode consumir grande quantidade de recursos econômicos e humanos.

É por isso que a segurança da informação deve ser assumida como um novo objetivo da RPCC.

Palavras-chave: Segurança da informação; confidencialidade; integridade; disponibilidade; ISO 27001.

Introducción

El RPCC es una entidad adscrita a la Ilustre Municipalidad del Cantón Cuenca, está ubicada en la ciudad de Cuenca y los servicios que ofrece esta estrictamente dirigida a todas aquellas personas que radican o tienen un bien inmueble en la ciudad de Cuenca, y su trabajo esta soportado en el uso de la tecnología para la generación y manejo de la información registral. El uso adecuado de las TICS ayudará en un futuro a constituirse en un ejemplo a nivel nacional; pues, se busca que los servicios sean de calidad y los tiempos de respuesta deben permitir a los usuarios realizar sus trámites en el menor tiempo.

El RPCC goza de una autonomía administrativa y financiera, lo que ha permitido a la entidad invertir recursos económicos en la adecuación de un Data Center (DC), que sirve para realizar el almacenamiento y procesamiento de la información.

Un aspecto que debe ser mencionado, es que el RPCC dentro de sus funciones principales está el de registrar documental y electrónicamente las propiedades que están localizadas dentro del cantón Cuenca, este registro servirá para la generación de nueva información o generación de nuevos documentos que requieren los usuarios. Todo este proceso de registro se desarrolla en apego con las disposiciones legales contenidas en la Ley del Sistema Nacional del Registro de Datos Públicos, la Ordenanza para la Organización, Administración y Funcionamiento del Registro de la Propiedad

del Cantón Cuenca y más leyes que regulan el funcionamiento de las instituciones públicas dentro del territorio ecuatoriano.

Las normas de control interno, emitidas por la Contraloría General del Estado (CGE), en sus numerales 400 y 410 hablan sobre la responsabilidad institucional de establecer políticas y procedimientos para proteger la infraestructura tecnológica, es decir, los equipos y la información existente en el RPCC, motivo por el cual, todos los directores y funcionarios deben formar parte de las tareas de protección. Además, señala que las entidades deben contar con un área de tecnología, misma que será la responsable de aplicar las normas con el objetivo de proteger la información (Viceministerio de Telecomunicaciones y Tecnologías de la Información y Comunicación, 2018).

La legislación ecuatoriana ha desarrollado algunas normas y leyes que intentan controlar el uso adecuado de la información, sin embargo, existen delitos que se han consumado, de acuerdo a una noticia publicada en el diario el universo: "*Los delitos informáticos van en aumento en Ecuador, según las denuncias presentadas en la Fiscalía, desde antes de la pandemia del COVID-19. En el 2017 se registraron 8421 casos; subieron a 9571 y 10 279 en 2018 y 2019. La tendencia se mantiene"* (Ramos, 2020).

La realidad del RPCC, no es ajena a otra institución pública o privada, inclusive se puede convertir en blanco de un ataque informático, poniendo en peligro la integridad, confidencialidad y disponibilidad de la información, en el peor escenario, ser víctima de daños en su infraestructura física o lógica de los servidores. Por esta razón, el presente trabajo propone la generación un plan para proteger los datos de la institución. En lo posterior, servir de modelo para implementar protocolos de seguridad que permitan controlar el acceso de los usuarios a los diferentes sistemas, generar políticas de seguridad en el manejo del DC, e implementar actividades para proteger la información del RPCC.

La propuesta, está basada en la revisión de MAGERT (Amutio Gómez, 2012) y normas ISO 27001 (Excellence, 2014).

Norma ISO 27001

Describe paso a paso los requerimientos necesarios para implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), durante este proceso se puede realizar la evaluación de los

riesgos y simultáneamente permite determinar los controles para mitigar y en lo posible eliminar estos riesgos (18001, 2003).

Norma ISO 27002

Esta norma proporciona un listado detallado de los controles necesarios que se debe aplicar para resguardar la información. En su versión del 2013 esta norma agrupa a los controles en 14 dominios, 39 objetivos de control y 133 controles (27002:2005., 2011; ISOTools Excellence, 2019).

Norma ISO 27005

Entrega recomendaciones para gestionar los riesgos, que se pueden presentar dentro de un sistema de gestión de seguridad de la información (EALDE, 2017).

Cuando se habla de seguridad de la información, se busca cumplir con 3 puntos claves: la confidencialidad, integridad y disponibilidad. Estos puntos son conocidos como la triada CIA (por sus siglas en inglés: Confidentiality, Integrity, Availability) (ISOTools Excellence, 2017).

Metodología

La revisión bibliográfica permitió consolidar esta propuesta de seguridad de la información para el RPCC, con el objetivo de determinar las mejores prácticas para enfrentar un riesgo, poder cuantificarlo, determinar su impacto, probabilidad y los controles necesarios para impedir que se materialice una amenaza, recordando que el RPCC tiene información de todos los bienes inmuebles localizados en el cantón Cuenca y es considerado confidencial.

Se realizó, un análisis cualitativo y cuantitativo de los activos de información, y de las seguridades del RPCC, así también de las amenazas a las que se encuentra expuesta, para ello se aplicó una investigación descriptiva, aplicada y bibliográfica.

1. Lectura y revisión de bibliografía relacionado con la seguridad de la información (Información., 2018; MINTEL, 2020).
2. Revisión de trabajos de investigación, similares a la presente propuesta (Security & Plan, 2020).
3. Conocimiento de estado actual del RPCC, aplicando entrevistas, cuestionarios y observaciones, para obtener información de su estructura organizativa, personal

responsable del manejo de la tecnología, infraestructura tecnológica, y los servicios que ofrece.

4. Análisis DAFO del RPCC, con una visión meramente tecnológica.
5. Determinación del alcance de la propuesta, considerando el tamaño del RPCC.
6. Realizar una identificación de las partes interesadas de la información que maneja el RPCC.
7. Revisión de la metodología MAGERIT y la norma ISO 27001 para aprender a reconocer, analizar y mitigar los riesgos a los que este expuesto el RPCC.
8. Determinación de activos de información críticos del RPCC, aplicando entrevistas y cuestionarios al personal responsable del área del Tecnologías de la Información y Comunicación del RPCC.
9. Evaluación de las seguridades de la información existentes.
10. Reconocimiento de posibles amenazas a los que puede estar expuesta el RPCC, considerando el giro de negocio.
11. Análisis de las amenazas, para determinar el nivel de impacto y la probabilidad de ocurrencia, aplicando métodos sugeridos en MAGERIT e ISO 27001.
12. Identificación y valoración de las vulnerabilidades, a fin de aplicar correctivos a corto, mediano y largo plazo.
13. Sugerencia de controles mínimos que ayudaran a mitigar algunas amenazas, esto como medida preventiva y de aplicación inmediata.
14. Elaboración de la propuesta, basado en MAGERIT y la Norma ISO 27001, misma que podrá ser utilizada como punto de partida en la generación de un SGSI para el RPCC.

Esta metodología, puede ser sujeto a un proceso de retroalimentación y mejoramiento continuo, para esto podemos hacer uso el ciclo de vida de Deming, conocido como PDCA (por sus siglas en inglés) o PHVA (por sus siglas en español) y consiste en: Planificar, Hacer, Verificar y Actuar.

Resultados

Aplicando conceptos y utilizando como guía la metodología MAGERIT y la ISO/IEC 27001. Iniciamos identificando las partes interesadas de la información registral: clientes, la alta dirección

y los empleados del RPCC. Seguidamente se realizó un análisis DAFO del RPCC, con una visión orientada a la tecnológica e información existente (ISOTools Excellence, 2015).

Tabla 1: Análisis DAFO del RPCC

Fortalezas	**Debilidades**
• Cuenta con un Data Center. • Dispone de un sitio alterno, para respaldo de información.	• Información crítica, disponible para usuarios internos, sin mayores restricciones.
Oportunidades	**Amenazas**
• Capacitar al personal de tecnologías en seguridad de la información. • Capacitar al personal para desarrollar software con mejor calidad y seguro.	• Inexistencia de un sistema de gestión de seguridad de la información.

Fuente: Elaboración propia

Aplicando la metodología MAGERIT V3 y la norma ISO/IEC 27001 (Antecedentes, 2015), se elaboró el inventario de los activos informáticos que posee el RPCC.

Tabla 2: Activos Informáticos

Tipo de Activo: Datos		
Código	**Activo Informático**	**Descripción de Contenido**
DT001	Backup de Bases de Datos	Bases de datos de todos los sistemas del RPCC, en formato sql o zip.
DT002	Archivos Digitales	Archivos digitalizados en diferentes procesos, en formatos de imágenes o documentos
DT003	Manuales	Documentos de configuraciones realizadas en los servidores o en equipos informáticos.
Tipo de Activo: Servicios		
Código	**Activo Informático**	**Descripción de Contenido**

SE001	Página Web	Información relevante del RPCC, publicada cumpliendo disposiciones legales. Es de acceso público.
SE002	Facturación electrónica	Medio por el cual un cliente puede obtener sus facturas electrónicas autorizadas por el SRI (Servicio de Rentas Internas).
SE003	Correo electrónico	Servicio que permite el intercambio de información con entidades públicas o privadas, dentro y fuera del RPCC.
Tipo de Activo: Software		
Código	**Activo Informático**	**Descripción de contenido**
SW001	Sistema Registral SR2	Permite manejar toda la información referente a los bienes inmuebles de los clientes.
SW002	Sistema de Facturación SIFAREG	Registra los cobros realizados, por los servicios que se entrega a los clientes.
SW003	Sistema de Contabilidad SIGAME	Ayuda al manejo financiero y administrativo del RPCC.
SW004	Herramientas Ofimáticas	Procesadores de texto y hojas de cálculo que permiten manipular cualquier información.
SW005	Software de digitalización	Permiten transformar archivos físico en digitales.
SW006	Antivirus	Dedicado a combatir las posibles intrusiones de programas maliciosos.
SW007	Gestores de Bases de Datos	Mantiene ordenada la información en un formato de tablas relacionadas.
SW008	Sistemas operativos	Programas básicos que generan interfaces para controlar las computadoras y facilitar el uso de los sistemas.
SW009	Sistema de Turnos	Permite emitir tickets para organizar la atención a los clientes, de acuerdo al servicio que solicitan.
SW010	Licencias	Software que garantiza el correcto funcionamiento de algunos equipos o programas.
Tipo de Activo: Hardware		
Código	**Activo Informático**	**Descripción de Contenido**
HW001	Servidores y Storage	Equipos que albergan a los sistemas en ambientes virtuales.

HW002	Computadores	Son las estaciones de trabajo que se conectan con los sistemas informáticos y están disponibles para uso de los funcionarios.
HW003	Impresoras	Materializan los archivos digitales en documentos físicos, que son utilizados en diferentes actividades.
HW004	Escáneres	Transforman documentos físicos en digitales, y que formaran parte de diferentes procesos.
HW005	Switches	Permiten interconectar los equipos informáticos a la intranet del RPCC.
HW006	Firewall	Equipo que ayuda a administrar el tráfico entre redes, contribuyendo a la seguridad actual.
HW007	Proyectores	Son dispositivos que proyectan señales de video en superficies amplias.
HW008	Centralita	Dispositivo que administra el tráfico de voz.
HW009	Teléfonos	Equipos utilizados para intercomunicarse interna o externamente
HW010	Access Point	Permiten la interconexión de equipos, usando las redes inalámbricas.
HW011	Periféricos	Utilizados para un interactuar con los computadores.
HW012	Router ONT	Equipo para conexión a internet utilizando tecnología de fibra óptica.
Tipo de Activo: Soporte de Información		
Código	**Activo Informático**	**Descripción de Contenido**
SI001	Discos Duros Externos	Dispositivos portátiles de gran capacidad, para almacenamiento de información.
SI002	NAS	Equipo de gran capacidad de almacenamiento, generalmente empotrado en un rack y compartido en la red.
SI003	Flash Memorys	Dispositivos portátiles de poca capacidad de almacenamiento.
SI004	Robot de cintas	Su funcionamiento es similar a un NAS.
Tipo de Activo: Equipamiento auxiliar		
Código	**Activo Informático**	**Descripción de Contenido**
EA001	Generador eléctrico	Ubicado al interior del RPCC y su función es generar electricidad, en el caso de existir una interrupción del servicio eléctrico.

EA002	UPS	Almacena energía eléctrica en baterías, para posteriormente entregarlo en el caso de existir cortes eléctricos.
EA003	Equipo de climatización	Mantiene una temperatura controlada en el Data Center, para que los equipos funcionen adecuadamente.
EA004	Cableado eléctrico	Existe un cableado para uso exclusivo de equipos informáticos y otro para uso general. Están claramente identificados.
EA005	Cableado de datos	Cableado para uso de voz y datos, concentrado en el data center.
EA006	Fibra óptica	Utilizado para recibir el servicio de internet.
EA007	Equipo de monitoreo de temperatura	Controla que la temperatura en el data center no sufra alteraciones.
EA008	Sistema de video vigilancia	Ayuda a mantener vigilada las instalaciones del RPCC.
EA009	Equipos biométricos para apertura de puertas	Controla el acceso de los servidores a ciertas áreas.
EA010	Puerta de data center con blindaje	Incrementa el nivel de seguridad, en lo referente al acceso no autorizado al data center.
Tipo de Activo: Redes de comunicación		
Código	**Activo Informático**	**Descripción**
RD001	Telefonía IP	Facilita la comunicación entre las oficinas, mediante el uso de teléfonos IP.
RD002	Red Wifi	Permite que los dispositivos móviles accedan a la red y puedan utilizar los sistemas informáticos.
RD003	Red LAN	Distribuidos puntos de red en todas las oficinas para conectar los equipos informáticos.
RD004	Red internet	Servicio utilizado para el acceso a la internet.
RD005	VPN	Funcionalidad usada para realizar teletrabajo.
RD006	Sistema de audio centralizado	Utilizado para una comunicación general a todo el personal.
Tipo de Activo: Instalaciones		
Código	**Activo Informático**	**Descripción**

IN001	Data Center	Espacio de uso exclusivo, destinado para ubicar los servidores.
IN002	Área de TICs	Oficina con adecuaciones para el personal técnico del RPCC.
IN003	Sitio Alterno	Espacio físico ubicado fuera del RPCC, para realizar backups.
Tipo de Activo: Personas		
Código	**Activo Informático**	**Descripción**
PE001	Técnicos Informáticos	Personal con conocimientos de TIC, para el manejo de la infraestructura tecnológica del RPCC.

Fuente: Elaboración propia

Se determinaron las razones, por las cuales, los activos deben formar parte de un plan de seguridad de la información, para ello, la valoración se realizó considerando la norma ISO/IEC 27001, que menciona los principios básicos para la seguridad de la información: (C) Confidencialidad, (I) Integridad y (D) Disponibilidad. Aplicando una escala de valores para calificar el daño, que va desde 1 (mínimo) a 5 (extremo). Seleccionamos los activos considerados más importantes.

Tabla 3: Valoración de los Activos

Valoración de activo: Datos			
Código de Activo	**Principio**	**Valoración**	**Justificación**
DT002	C	3	Los accesos deben ser restringidos para evitar fuga de información.
	I	5	Los archivos digitalizados no deben ser modificados, para garantizar la seguridad jurídica.
	D	4	Deben estar disponibles para ser consultados en los diferentes procesos.
Valoración de activo: Software			
Código de Activo	**Principio**	**Valoración**	**Justificación**

SW001	C	4	Información que solo deben tener acceso los usuarios autorizados. Utilizando perfiles de usuarios.
	I	5	Para realizar cambios se debe contar con una autorización, mantener un historial de cambios para procesos de auditorías y garantizar la seguridad jurídica.
	D	4	El acceso debe ser únicamente para usuarios del RPCC, en horas laborables y solo en la intranet.
SW002	C	3	Los datos deben venir de fuente conocida, para evitar errores e inconsistencia.
	I	5	Los datos no se pueden modificar, salvo autorización expresa.
	D	3	Los usuarios autorizados deben estar claramente identificados, estar disponible únicamente en horas laborables y solo en la intranet.
SW007	C	4	La información contenida debe ser de fuente verificable y estar protegida con el uso de contraseñas.
	I	5	Los registros de datos no se deben modificar, salvo autorización expresa. Realizar respaldos de los registros para procesos de auditorías.
	D	4	El acceso será únicamente para personal de TIC, en horario 24/7.
Valoración de activo: Hardware			
Código de Activo	**Principio**	**Valoración**	**Justificación**
HW001	C	4	Tendrán acceso a su configuración únicamente personal de TIC, o usuarios con autorización expresa, con la supervisión de un responsable.

	I	4	La manipulación, se lo realizara con criterio técnico, para evitar dañar la data.
	D	4	Deberá estar en funcionamiento permanente y tendrán acceso únicamente personal autorizado.
HW002	C	3	Las configuraciones y actualizaciones se deben realizar mediante el Directorio Activo o por personal autorizado.
	I	3	La información aquí contenida no impacta en los procesos, sin embargo los datos solo deben ser modificados por el usuario propietario.
	D	3	Disponible en horas laborables, para los funcionarios del RPCC.
HW005	C	4	Las configuraciones realizadas deben ser conocidas por personal autorizado.
	I	4	Las modificaciones en sus configuraciones serán realizadas por personal autorizado.
	D	4	Estar disponible todo el tiempo para garantizar el tráfico en la red.
HW006	C	4	Los datos de las configuraciones deben estar a buen recaudo.
	I	5	Las actualizaciones y configuraciones se realizaran únicamente con personal autorizado.
	D	5	Debe estar en funcionamiento permanente.
Valoración de activo: Soporte de información			
Código de Activo	**Principio**	**Valoración**	**Justificación**
SI002	C	4	Solo usuarios autorizados podrán revisar la información contenida.

	I	3	No deberá permitir ningún tipo de modificación. Pues se trata de un equipo utilizado para temas de respaldos.
	D	4	Disponible todo el tiempo, para usuarios autorizados.
Valoración de activo: Equipamiento auxiliar			
Código de Activo	**Principio**	**Valoración**	**Justificación**
EA002	C	3	Su instalación y claves serán conocidas únicamente por personal autorizado.
	I	3	Su configuración debe ser realizado por personal especializado.
	D	4	Estará operativo permanentemente, garantizando el fluido eléctrico del Data Center.
EA009	C	3	Los datos de configuración serán conocidos por el personal autorizado.
	I	4	Los cambios se realizaran únicamente con autorización.
	D	4	Disponibles todo el tiempo.
Valoración de activo: Redes de comunicación			
Código de Activo	**Principio**	**Valoración**	**Justificación**
RD003	C	4	Garantizar que todos los paquetes lleguen a su destino, evitando periodos de latencia.
	I	5	Impedir que los paquetes sean modificados o interceptados.
	D	4	Los accesos a la red serán controlados por el personal de TIC.
Valoración de activo: Instalaciones			
Código de Activo	**Principio**	**Valoración**	**Justificación**

IN001	C	4	Únicamente personal autorizado accederá a su ubicación y será de uso exclusivo para equipos informáticos de data center.
	I	4	Las adecuaciones serán realizadas por personal especializado, previa autorización.
	D	4	Deberá estar disponible todo el tiempo, y el acceso será restringido.
Valoración de activo: Personas			
Código de Activo	**Principio**	**Valoración**	**Justificación**
PE001	C	4	Personal capacitado y formación profesional con ética, para que realice las acciones necesarias para precautelar la información.
	I	5	Las actividades estarán orientadas a manejar transparentemente la información del RPCC.
	D	5	Personal comprometido con el RPCC, a fin de estar presente cuando la institución lo requiera.

Fuente: Elaboración Propia

El siguiente paso es, analizar la relación de los activos con las amenazas y vulnerabilidades (Escuela Europea de Excelencia, 2019). Para esto vamos a utilizar criterios de (R) Riesgo, (I) Impacto y (P) Probabilidad, mismos que van a contener un valor mínimo de 1 a un valor extremo de 5. De igual manera, se ha considerado el análisis de activos relevantes.

Tabla 4: Análisis de Amenazas y Vulnerabilidades

Activo	Código	Amenazas	Vulnerabilidades	R	I	P
Datos	DT002	Eliminación y modificación de archivos	Acceso a carpetas compartidas, sin niveles de acceso	4	3	4

		Cambios no autorizados de archivos	Usuarios con poco conocimiento en manejo de archivos	4	3	3
		Fuga masiva de información	Acceso a todas las carpetas con archivos digitales	5	4	3
Servicios	SE003	Acceso no autorizado	Uso de contraseñas débiles o genéricas	5	3	4
		Filtración de correos con spam	Políticas de seguridad inexistentes o ineficientes	5	4	4
		Servidor fuera de operación	Interrupción en la comunicación	4	3	3
Software	SW001	Modificación de información	Acceso no controlado a módulos	4	4	4
		Ingreso de información errónea	Usuarios no capacitados en el uso del sistema	5	4	4
		Almacenamiento de información incorrecta	Sistema con errores en programación	4	4	3
		Incompatibilidad de multiplataforma	Sistemas desarrollados solo para ambientes Windows	3	3	2
	SW002	Generación de datos inexactos	Pruebas insuficientes de módulos desarrollados	4	3	3
		Sistema almacena información innecesaria o insuficiente	Módulos desactualizados	3	3	3
	SW003	Incumplimiento con la legislación ecuatoriana	Imposibilidad de realizar modificaciones en los módulos de software adquirido a terceros	4	5	4
		Mal funcionamiento del sistema	Sistema requiere instalación y configuración especial.	4	5	3
Hardware	HW001	Apagón de los servidores	Fallo en el suministro eléctrico	3	5	3

		Cortocircuito	Mantenimientos deficientes de las instalaciones eléctricas	3	5	3
		Fallo de partes	Partes que han cumplido su vida útil y no han sido reemplazados	3	4	4
	HW002	Daño de periféricos	Mal uso por parte de los usuarios	4	3	3
		Perdida de equipos	Falta de control en el acceso a los oficinas	4	3	3
		Mal funcionamiento del computador	Provocado por usuarios que borran archivos del sistema	4	3	4
	HW006	Conexiones externas no autorizadas	Configuración de políticas inexistentes	4	4	3
		Equipo fuera de servicio	Aplicación de configuraciones incorrectas por falta de conocimiento	4	4	3
Soporte de Información	SI002	Mal funcionamiento del equipo	Instalación y configuración mal aplicada	3	4	3
		Acceso no controlado	Políticas mal aplicadas por el personal responsable	3	4	3
Equipamiento auxiliar	EA002	Deterior prematuro de las baterías	Mantenimiento de las baterías mal realizadas	4	5	3
		Carga de batería insuficiente para el Data Center	Equipos innecesarios conectados al ups	3	4	3
		Mal funcionamiento del equipo	Poca capacitación en la configuración de estos equipos	4	5	4
	EA009	Destrucción de los dispositivos	Imposibilidad de colocar protecciones a estos dispositivos delicados	4	3	3

		Mal funcionamiento	Requiere configuración especializada y mantenimiento constante	4	3	4
Redes de comunicación	RD003	Perdida de paquetes	Equipos de red mal configurados	4	4	3
		Interceptación de paquetes de información	Ubicación de puntos de red en lugares no controlados	4	3	4
		Colapso de la red	Inexistencia de segmentación de la red	3	5	3
		Errores en el funcionamiento	Equipos con fallas físicas o lógicas por falta de mantenimiento periódico	3	4	3
Instalaciones	IN001	Incendio	Instalaciones eléctricas defectuosas	3	5	3
		Sobrecalentamiento del Data Center	Fallo en los equipos en enfriamiento	4	4	4
Personal	PE001	Renuncia de personal clave	Oferta laborales más favorables	4	4	4
		Actividades incompletas	Sobrecarga de trabajo	4	4	3
		Poca iniciativa para tomar decisiones	Falta de autotomía en toma de decisiones	4	3	4

Fuente: Elaboración propia

A continuación, se realizó la evaluación de los riesgos, considerando niveles de criticidad referente a los activos de información del RPCC. Se consideró 3 niveles: bajo, medio y alto. Se emitió un criterio de aceptación del riesgo.(Romero Carranza, 2013)

Tabla 5: Evaluación de Riesgos

Código	Riesgo	Justificación	Criticidad	Criterio de aceptación
R001	Acceso indiscriminado a las	Inexistencia de usuarios y claves.	Medio	El riesgo es aceptable a mediano plazo. Se debe

	carpetas compartidas.			planificar la creación de usuarios.
R002	Robo de credenciales para acceder a los sistemas	Cuentas de usuario y contraseñas genéricas	Medio	El riesgo no es aceptable. Se planificaran tareas de cambio de contraseñas.
R003	Personal no autorizado ingrese al Data Center	Controles muy leves o inexistentes.	Alta	Es inaceptable el riesgo, pues ninguna persona debe ingresar al DC, sin previa autorización.
R004	Ingreso de información inservible en los sistemas	Personal con poca capacitación para uso de los sistemas	Medio	Es aceptable el riesgo, sin embargo se realizara un plan de capacitación al personal.
R005	Personal no capacitado en puestos claves	Rotación constante de puestos	Medio	A mediano plazo es aceptable, y se propone realizar evaluaciones al personal.
R006	Latencia excesiva en el uso de los sistemas.	Falta de control del tráfico en la red	Bajo	Riesgo aceptable, sin embargo a largo plazo se aplicaran tareas de control en la intranet.
R007	Perdida de información injustificada, en los sistemas	Sistemas en producción, sin pasar por etapas de prueba	Alta	El riesgo no es aceptable, se debe utilizar buenas prácticas para desarrollar sistemas.

R008	Robo de información en medios extraíbles	Falta de control de los puertos de las computadores	Medio	El riesgo es aceptable a mediano plazo. Se propone uso de políticas en el Directorio Activo para el control de los puertos E/S.
R009	Daños en la red eléctrica por sobrecarga	Conexión de dispositivos no autorizados.	Medio	Riesgo aceptable a mediano plazo. Se realizara una revisión de los equipos conectados.
R010	Inundación en el cuarto del generador eléctrico	Generador ubicado en el subsuelo	Alto	El riesgo no es aceptable, se debe dar un seguimiento permanente y desarrollar un plan de contingencia.
R010	Sabotaje en la red eléctrica o la red de datos	Acceso a los ductos, por donde pasan los cables.	Alta	Riesgo inaceptable, se deben reforzar las seguridades en los accesos.
R011	Imposibilidad de aplicar controles de seguridad de la información	Inexistencia de un plan de seguridad de la información.	Medio	Riesgo aceptable a corto y mediano plazo, a largo plazo se debe elaborar un plan de seguridad de la información.

Fuente: Elaboración propia

Una vez que se conoció el nivel de criticidad de los riesgos, se planteó algunos controles para los riesgos analizados, basándome en la revisión de la norma ISO/IEC 27002:2005. Estos controles ayudaran a minimizar la criticidad, a corto plazo; y en el futuro esto puede ser utilizado como guía para generar un plan de seguridad mucho más robusto.

Tabla 6: Controles para los Riesgos

Código	Controles / Salvaguardas
R001	Realizar un registro de los usuarios, para controlar el acceso a estos recursos.
	Asignar niveles de privilegios a los usuarios registrados.
	Planificar respaldos constantes de información crítica.
	Aplicación de políticas de seguridad a las carpetas compartidas.
R002	Eliminación de técnicas para generar contraseñas genéricas.
	Utilización de métodos de cifrado para almacenar contraseñas.
	Generar políticas que obliguen a renovar las contraseñas en cortos periodos de tiempo.
	Inactivar a usuarios que no están en uso.
R003	Generar un perímetro de seguridad para el DC.
	Mantener las puertas bloqueadas.
	Llevar un registro de los usuarios que ingresan al DC.
	Documentar las actividades realizadas en el interior del DC.
R004	Capacitación permanente a todo el personal, sobre el uso de los sistemas informáticos.
	Revisión periódica de la integridad de la información.
	Planificación de inducción al nuevo personal.
	Generación de políticas de responsabilidad, para que los usuarios generen conciencia en la manipulación de la información.
	Elaboración de manuales de usuario y manuales de procesos.
R005	Creación de perfiles de puesto.

	Identificación de competencias y responsabilidades de cada usuario.
	Generación de un plan de capacitación a todo el personal.
	Evaluación de cumplimiento de metas y objetivos.
R006	Revisión periódica de los equipos que manejan la red.
	Revisión de las configuraciones y características de los sistemas.
	Planificar la revisión periódica del tráfico en la red.
	Revisión de la topología implementada.
R007	Validación de datos de entrada y salida.
	Revisión de procesamiento interno.
	Creación de ambientes de prueba de los sistemas.
	Realizar planes de mantenimiento de los sistemas que están en ambientes de producción.
R008	Generación de políticas de confidencialidad de la información.
	Firmar acuerdos de confidencialidad con personal que maneja información crítica.
	Aplicación de políticas de seguridad en el Directorio Activo.
R009	Mantenimientos periódicos preventivos en la red electica.
	Planificación de estudios para ampliar la capacidad de la red eléctrica.
	Capacitación al personal sobre el uso correcto de las instalaciones.
R010	Revisión periódica del sistema de agua potable y el sistema de desagua.
	Planificación para intervenir y aislar el cuarto del generador eléctrico.
R010	Políticas para acceso controlado a los ductos.

	Planes para incrementar las seguridades en los accesos.
	Revisión de los planos para reubicar puntos eléctricos o de datos.
R011	Concientizar a los directivos, sobre la necesidad de contar con un plan de seguridad de la información.
	Diseño de un plan para implementar seguridad de la información.

Fuente: Elaboración propia

Adicionalmente, se propone un control a nivel institucional:

Elaborar una normativa disciplinaria, para el personal que no acate los controles antes mencionados. Aplicando lo dispuesto en las leyes y normativas de la legislación ecuatoriana.

La aplicación de estos controles, permitirá generar un ambiente más favorable para identificar, evaluar y prevenir la ocurrencia de un riesgo. Haciendo que nuestras empresas tengan una oportunidad de crecer de forma segura.

Conclusiones

Al finalizar la presente propuesta se logró la identificación de activos de información críticos del RPCC, y se realizó un análisis de las amenazas a las que está expuesta.

Se conoció la infraestructura tecnológica con la que cuenta la institución, y en la que se soportan los servicios registrales, además, las inversiones realizadas en el equipamiento de un Data Center seguro y otras que están orientadas directamente con la seguridad de la información.

En base a disposiciones contenidas en las normas de control interno en su numeral 410 y las disposiciones emitidas por el Ministerio de Telecomunicaciones, mediante una publicación en el Registro Oficial Edición Especial Nro. 228 de 2020 (MINTEL, 2020), se concluyó que en la actualidad no es indispensable la implementación de un Sistema de Gestión de Seguridad de la Información en el Registro de la Propiedad del Cantón Cuenca, pues la entidad presta sus servicios únicamente en sus instalaciones.

Además, la implementación de seguridad de la información, puede resultar en una tarea un poco compleja, pues el RPCC es una entidad pequeña y no cuenta con personal capacitado, ni certificado en este tipo de metodologías.

Como un punto favorable, se encontró que el RPCC, tiene implementado algunas actividades, como son el respaldo de las bases de datos y copia del archivo digital. A la finalización de la presente propuesta, ha considerado complementar con otras actividades, como son la revisión periódica del firewall y restringir el acceso del personal al Data Center.

Se espera que a corto plazo el RPCC, inicie con la documentación de su hardware y software, sus activos de información identificados como críticos, de sus políticas de seguridad existentes y sus respectivos controles. A mediano plazo se espera que cuente con personal capacitado en temas de seguridad de la información y se haya iniciado con un proceso de seguridad de la información más completo, dando cumplimiento a las disposiciones legales, tomando como guía las metodologías de MAGERIT, o estándares de buenas prácticas como ISO/IEC 27001. A largo plazo el RPCC deberá contar un SGSI más desarrollado. Esto en el caso de que el RPCC busque una certificación.

Referencias

1. 18001, O. (2003). La norma. La Norma ISO 27001;Aspectos Claves de Su Implementación, 21. https://www.isotools.org/pdfs-pro/ebook-ohsas-18001-gestion-seguridad-salud-ocupacional.pdf
2. 27002:2005., I. (2011). Iso/iec 27002:2005. 11, 27002. http://www.iso27000.es/download/ControlesISO27002-2005.pdf
3. Amutio Gómez, M. A. (2012). Ministerio de Hacienda y Administraciones Publicas. 127. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
4. Antecedentes, O. (2015). española.
5. EALDE. (2017). ISO 27005 para la Gestión de Riesgos de Tecnologías de la Información. https://www.ealde.es/iso-27005-gestion-de-riesgos/

6. Escuela Europea de Excelencia. (2019). Listado de amenazas y vulnerabilidades en ISO 27001. https://www.escuelaeuropeaexcelencia.com/2019/11/listado-de-amenazas-y-vulnerabilidades-en-iso-27001/
7. Excellence, Isot. (2014). Sistemas de Gestión de Riesgos y Seguridad. https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/
8. Información., M. de T. y de la sociedad de la. (2018). Guía Para La Implementación Del Esquema Gubernamental De Seguridad De La Información. 17.
9. ISOTools Excellence. (2015). La matriz DAFO aplicada a los riesgos corporativos. https://www.isotools.org/2015/11/02/la-matriz-dafo-aplicada-a-los-riesgos-corporativos/
10. ISOTools Excellence. (2017). ¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información? https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/
11. ISOTools Excellence. (2019). ISO 27002. La importancia de las buenas prácticas en los Sistemas de Seguridad de la Información. https://www.isotools.org/2019/06/11/iso-27002-la-importancia-de-las-buenas-practicas-en-los-sistemas-de-seguridad-de-la-informacion/
12. MINTEL. (2020). Guia Para La Implementación De L Esquema Gubernamental De Seguridad De La Información (Nte Inen Iso/Iec 27001:2017). Acuerdo Ministerial No. 025-2019.
13. Ramos, X. (2020). Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro. El Universo. https://www.eluniverso.com/noticias/2020/09/27/nota/7991905/delitos-informaticos-internet-casos-reales-redes-sociales-ecuador#:~:text=Los delitos informáticos van en,La tendencia se mantiene.
14. Romero Carranza, J. L. (2013). Analisis De Criticidad. 23. http://bibing.us.es/proyectos/abreproy/5311/fichero/5-+Analisis+de+criticidad.pdf

15. Security, I., & Plan, M. (2020). PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN , CASO DE ESTUDIO : GOBIERNO PROVINCIAL DEL CAÑAR INFORMATION SECURITY MANAGEMENT PLAN , CASE STUDY : 5, 62–75.
16. Viceministerio de Telecomunicaciones y Tecnologías de la Información y Comunicación. (2018). Normas De Control Interno De La Contraloria General Del Estado. Ultima, 16–2014. http://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf