Revista Innovación y Software
Vol. 2, No. 2, Mes Septiembre-Febrero, 2021
ISSN: 2708-0935
Pág. 27-43
https://revistas.ulasalle.edu.pe/innosoft

Tipo de artículo: Artículos originales
Temática: Redes y seguridad informática
Recibido: 12/05/2021 | Aceptado: 24/06/2021 | Publicado: 30/09/2021

Identificadores persistentes:
ARK: ark:/42411/s6/a39
PURL: 42411/s6/a39

Propuesta de un plan de seguridad de la información para incrementar la fiabilidad de datos en una financiera

Proposal of an information security plan to increase the reliability of data in a financial company

Wilmer Aufredy Apaza Chávez[1*]

[1] Universidad Nacional de Trujillo. Trujillo-Perú. wapazac@unitru.edu.pe

[*] Autor para correspondencia: wilfre500@gmail.com

Resumen
La entidad financiera tiene como función principal ofrecer sus servicios de colocación de tarjetas, préstamos, etc., hacia los clientes que soliciten en sus diferentes establecimientos. Ante ello se identificó que en el banco existen actividades que están generando mal manejo de la información por parte del personal hacia los clientes lo cual está ocasionando reclamos de los mismos por inconsistencia de los datos que trae como consecuencia la desafiliación de sus servicios. Por ese motivo se desarrolló una propuesta de un plan de seguridad de la información en los procesos y áreas del banco Ripley, teniendo como objetivo el incremento de la fiabilidad de sus datos, logrando los tres principios para un SGSI como son disponibilidad, integridad y confidencialidad. Para lograr dicho objetivo se seleccionó las normas ISO/IEC 27001 y 27002 para aplicar los controles de la propuesta del plan de seguridad de la información en el banco Ripley, quedando claramente establecidos los responsables y la información que se maneja en cada una de los procesos y áreas. Como resultado se realizó el alcance del plan, así como definir las políticas, análisis de gestión de riesgos, se dio prioridad al manejo de la información por áreas, además se analizó los activos del banco donde se garantice la fiabilidad de los datos, luego se definió el plan aplicando los controles de la ISO/IEC 27002. Se concluyó en definir los indicadores para evaluar la propuesta del plan de seguridad de la información para incrementar la fiabilidad de sus datos.

Palabras clave: Datos, Gestión, Información, ISO/IEC 27002, Plan ,SGSI

Abstract
The main function of financial entity is to offer its services for the placement of cards, loans, etc., to customers who request in their different establishments. Given this, it was identified that in the bank there are activities that are generating mishandling of information by the staff towards the clients, which is causing complaints from them due to the inconsistency of the data that results in the disaffiliation of their services.
For this reason, a proposal for an information security plan was developed in the processes and areas of Ripley Bank, with the objective of increasing the reliability of its data, achieving the three principles for an ISMS such as availability, integrity and confidentiality. To achieve this objective, the ISO / IEC 27001 and 27002 standards were selected to apply the controls of the proposal for the information security plan in the Ripley bank, with the responsible parties and the

information handled in each of the processes being clearly established. and areas. As a result, the scope of the plan was carried out, as well as defining the policies, risk management analysis, priority was given to the management of the information by areas, and the assets of the bank were analyzed where the reliability of the data is guaranteed, then defined the plan applying the controls of ISO / IEC 27002
It was concluded in defining the indicators to evaluate the proposal of the information security plan to increase the reliability of its data.
Keywords: *Data, Management, Information, ISO / IEC 27002, Plan,SGSI*

Introducción

En el Perú, en la actualidad en las organizaciones financieras es incuestionable que la gran mayoría de los procesos del negocio son soportados, automatizados y gestionados por sistemas informáticos, así como los sistemas de información apoyan la actividad gerencial y la toma de decisiones; incluso muchas veces, es la propia información y el acceso a la misma, el producto o servicio que se intercambia como el principal objeto del negocio. La seguridad de la información ya no puede ser considerada como el resultado de un accionar defensivo y reactivo para preservar los activos del negocio, ya que muchas veces, es un activo del mismo, una condición para operar y/o competir con el sector financiero, un generador de valor. Requiere un accionar proactivo y su incorporación como elemento estratégico. A modo de ejemplo, un banco que gestione adecuadamente la seguridad de la información, por un lado, da cumplimiento a sus obligaciones y regulaciones y a su vez genera confianza entre sus clientes.

la información es el principal activo de toda organización según los más modernos paradigmas de la administración empresarial pudiendo hacer su aparición de muchas formas, impresa o escrita en el papel, almacenada electrónicamente, transmitida por correo, ilustrada en películas o hablada en conversaciones. En el ambiente de negocios financieros de hoy, esa información está constantemente bajo la amenaza de muchas fuentes, que pueden ser internas o externas, accidentales o maliciosas para con el banco. Con el incremento del uso de nueva tecnología para almacenar, transmitir y recobrar información se han abierto canales para un mayor número y variedad de amenazas. Es por ello que se requiere establecer, un planeamiento de seguridad de la información dentro de cualquier tipo de organización. Es necesario asegurar la confidencialidad, integridad y disponibilidad de la información vital para el banco y de sus clientes [1].

Una estrategia de gestión de información es esencial para sobrevivir en el mercado financiero actual, un ejemplo es ver un escenario donde los activos de información de la organización están rodeados por un complejo ambiente de objetos y amenazas que van desde simples virus de una computadora hasta robos de la propiedad intelectual del negocio [2].

Por lo tanto, cada vez hay más conciencia y consenso en la importancia de la seguridad de la información en las empresas y organizaciones cualquiera sea el sector de la economía o rol en la sociedad que desempeñen, en lo particular

en las empresas medianas y grandes. Sin embargo, existen diversas industrias y estructuras empresariales que hacen que algunos temas deban ser analizados y estudiados con una estrategia diferente, ya sea por criticidad de la información que manejan, su dimensión o estructura empresarial [3].

A modo de ejemplo, pequeñas empresas, con una infraestructura limitada y sistemas informáticos de gestión que no requieren almacenamiento y procesamiento de información confidencial o critica ni están sujetos a estrictas normas regulatorias, normalmente van a enfrentar riesgos menores, deben considerar aspectos diferentes a la de una gran corporación o grupo empresarial financiero, y también una dimensión del problema diferente, tanto en la problemática como en la del capacidad de gestión de la solución. Por lo tanto, su estrategia y decisiones responderán a estas diferencias estructurales.

Por otra parte, organizaciones más grandes como pueden ser: empresas del sector financiero, salud, operadores de telefonía, gubernamentales, etc., deben afrontar la seguridad de la información de forma metodológica y planificada y con planes concretos, con un enfoque de continuidad del negocio y mejora continua. Además de parámetros y dimensiones diferentes en su relación costo-beneficio, existen motivos legales, regulaciones y contratos que requieren de la protección de información personal y sensible además de la crítica y estrategia del negocio.

De acuerdo a algunas encuestas internacionales, el mayor riesgo a la seguridad de la información está dado por el factor humano, específicamente errores, conductas inapropiadas y/o negligencias generadas internamente. también existen referencias donde se asegura que la inversión en la gestión de la seguridad (de T.I.) es más efectiva que la inversión tecnológica para mejorar los niveles de seguridad [4][5].

El desafío es entonces lograr el desarrollo del plan de seguridad de la información que conduzca en una solución eficaz y eficiente, desde el punto de vista técnico y económico que provea los niveles de seguridad requeridos y brinde la confianza necesaria en la entidad financiera, los socios del negocio y los clientes y bajo este enfoque es necesario considerar lo siguiente: las necesidades de los procesos del negocio con respecto a la información, aplicaciones. El uso eficaz y eficiente de los recursos tecnológicos como soporte de estos procesos de negocio. Un enfoque predictivo, estratégico y económicamente raciona en la evaluación y tratamiento de riesgos. La confiabilidad de las soluciones con particular atención en la continuidad del negocio y de los procesos estratégicos (críticos y de mayor valor)

Para alinear todo lo dicho anteriormente en cuanto a la seguridad de la información se utilizará la norma ISO/IEC 27001, controles de la ISO 27002, esta norma ha sido preparada para proporcionar los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información. Esta debe conservar la confidencialidad, integridad y disponibilidad de la información al aplicar un proceso de gestión de riesgo y la entrega confianza a las partes interesadas cuyos riesgos son gestionados de manera adecuada.

Revista Innovación y Software
Vol. 2, No. 2, Mes Septiembre-Febrero, 2021
ISSN: 2708-0935
Pág. 27-43
https://revistas.ulasalle.edu.pe/innosoft

La Información

Es un activo del negocio, tiene una función importante en la organización y por consecuencia debe estar protegido adecuadamente (ISO/IEC, 2014). La información puede ser clasificada de diversas formas, pero por la manera de comunicarse tenemos: Hablada en reuniones, impresa o escrita en papel, almacenada electrónicamente, transmitida por correo convencional o electrónicamente, Exhibido por videos corporativos. Los activos de la información son todo lo que tiene valor para la organización como: Software, servicios, intangibles como la reputación e imagen, personas y sus habilidades, certificaciones, Computadora, servidor etc.

Figura 1: Activos de la Información. Fuente Bendermacher.

Seguridad de la Información

La Seguridad de la información es mucho más que establecer firewalls, aplicar parches para corregir nuevas vulnerabilidades de un sistema de software o guardar copias de seguridad.

“Seguridad de información es determinar que requiere ser protegido y por qué, de que debe ser protegido y cómo protegerlo”, es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad y disponibilidad, disminuyendo el rendimiento de los equipos o bloquear el acceso a usuarios autorizados al sistema.

Dependiendo del tipo de información manejada y de los procesos realizados por una organización, esta podrá destinar más o menos recursos a garantizar la confidencialidad, la integridad o autenticidad y la disponibilidad de sus activos de información. Para toda organización, es fundamental contar con un SGSI. Muchas empresas creen tener sistemas eficientes y eficaces para proteger y asegurar la información, tienen controles e inclusive software para aplicar los controles, pero los aplican solo cuando hay incidente de seguridad; de manera que actúan de forma reactiva, sin tener

un enfoque claro y bien estructurado para un SGSI. Es por ello que las organizaciones requieren de un sistema que permita asegurar la información de manera proactiva, no obstante, hay organizaciones que han diseñado verdaderos SGSI, pero al momento de la puesta en marcha resultan caducos o incluso no aplican los controles.

La seguridad de la información involucra la tecnología, las personas y la estructura organizacional (procesos), las normativas, lo cual hace necesario un amplio conocimiento sobre la gestión de estos recursos. Sin embargo, esta gestión puede servir parcialmente, poco o nada si existen fallas de hardware, de software, fallas humanas, desastres naturales, ataques terroristas, entre otros, sin que la organización haya estado preparada para estos eventos

Es importante que, en todo este proceso, saber de qué proteger, de quien proteger y cómo proteger, esta es la palabra clave para poder direccionar el diseño y el mejoramiento continuo del SGSI. Dada la competencia de la globalización y las nuevas formas de comercio internacional, las empresas, sin importar su tamaño, su actividad o ubicación, deben estar preparadas para asegurar su información.

Calidad de la Información

Se caracteriza por la preservación de los siguientes aspectos:

- Confidencialidad: Se asegura que la información sea accesible solo para aquellos que estén autorizados
- Integridad: Salvaguardando la exactitud de la información en su procesamiento, así como su modificación autorizada
- Disponibilidad: Asegurando que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando sea necesario

La sensibilización de los directivos y responsables de la organización, que deben ser conscientes de la necesidad de destinar recursos a esta función.

Los conocimientos, las capacidades e implicación de los responsables del sistema informático: dominio de la tecnología utilizada en el sistema y conocimiento sobre posibles amenazas y los tipos de ataque. La mentalización, formación de responsabilidades de todos los involucrados en el sistema. Instalación, configuración y mantenimiento correcto de los equipos. Soporte de los fabricantes de hardware y software que permitan realizar actualizaciones y mejoras para cubrir fallos y problemas relacionados con la seguridad. Considerar que hay amenazas internas como externas en la seguridad de la información.

Revista Innovación y Software
Vol. 2, No. 2, Mes Septiembre-Febrero, 2021
ISSN: 2708-0935
Pág. 27-43
https://revistas.ulasalle.edu.pe/innosoft

Seguridad Informática

Entre los conceptos que más resalta la seguridad informática es la física que cubre todo lo referido a los equipos informáticos, computadores, servidores y equipamiento de la red. La seguridad lógica se refiere a las distintas aplicaciones que se ejecutan en cada uno de estos equipos. Los desastres naturales (Incendios, inundaciones, terremotos, etc.), los tenemos en cuenta a la hora de ubicar los emplazamientos del centro de proceso de datos donde alojamos los principales servidores de la empresa; pero, aunque tengamos el mejor sistema de extinción de incendios o la sala esté perfectamente sellada, siempre deberíamos tener un segundo CPD (centro de procesamiento de datos) para que la actividad no pare. Robos nuestros equipos, y sobre todo la información que contienen, resultan valiosos para otros individuos u organizaciones. Debemos proteger el acceso a la sala del CPD mediante múltiples medidas de seguridad: vigilantes, tarjetas de acceso, identificación mediante usuario y contraseña, etc. Fallas de suministro Los ordenadores utilizan corriente eléctrica para funcionar y necesitan redes externas para comunicarse con otras empresas y con los clientes. Estos servicios los contrataremos con determinados suministradores, pero debemos estar preparados para las ocasiones en que no puedan proporcionarlo: unas baterías o un grupo electrógeno por si falla la corriente eléctrica, una segunda conexión a Internet como línea de backup, incluso podemos optar por una solución inalámbrica para estar protegidos ante un corte del servicio. Las amenazas lógicas: Virus troyanos o malwares, en general. Como ocurre con el spam en el correo electrónico, el malware es software no deseado y que debemos eliminar, perdida de datos en general. Como ocurre con el spam en el correo electrónico, el malware es software no deseado y que debemos eliminar, ataque a las aplicaciones de los servidores en general. Como ocurre con el spam en el correo electrónico, el malware es software no deseado y que debemos eliminar.

Tabla 1: Consecuencia de la seguridad de la Información. Fuente Elaboración propia

Imagen	Volumen del Negocio	Productividad y Presentación del Servicio
Pérdida de imagen respecto al cliente Pérdida de imagen respecto a los proveedores Pérdida de imagen a otras partes	Pérdida de ingresos/facturación Posibles indemnizaciones a terceros Posibles sanciones Pérdida de oportunidades del negocio Pérdida de contratos/caída de	Disminución rendimiento laboral Interrupción de procesos productivos Retraso de entregas Cese de transacciones Enfado de

Ventaja de los competidores, etc.	acciones	empleados

Sistema de Gestión de Seguridad de la Información

El manejo de la seguridad de información es como un proceso, requiere de conocimientos, habilidades y capacidades de las áreas técnicas, legal, humana y organizacional. Un sistema en la que se puedan integrar todos los factores con todos los requerimientos y consideraciones organizacionales, recibe el nombre de sistema de gestión de seguridad de la información, conocido por las siglas como SGSI. La parte del sistema general de gestión, que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información en una organización se denomina SGSI. Para implementar un sistema de gestión de seguridad de información en una organización, debe considerar lo siguiente: Formalizar la gestión de seguridad de información, Analizar y gestionar los riesgos. Establecer los procesos de gestión de seguridad en base a la metodología, Certificar la gestión de la seguridad. Para esto debe tenerse en cuenta el marco legal, los estándares, las metodologías, los requerimientos, entre otros aspectos fundamentales.

Por su trascendencia, es importante mencionar algunos de los enfoques más relevantes al tema de la gestión para la continuidad de las operaciones: Plan para recuperación ante desastres *(Disaster recovery planning RDP)*, se enfoca en la recuperación de los servicios de TI y los recursos, dados un evento que ocasionara una interrupción mayor en su funcionamiento. Plan para reanudación del negocio *(Business resumption planning BRP)*, se centraliza en la reanudación de los procesos de los negocios afectados por una falla en las aplicaciones de TI. Se enfoca en la utilización de procedimientos relacionados con el área de trabajo.Plan para la continuidad de las operaciones *(Continuity or operation planning COOP)*, busca la recuperación de las funciones estratégicas de una organización que se desempeñan en sus instalaciones corporativas. Plan de contingencia *(contingency planning CP)*, se enfoca en las recuperaciones de los servicios y recursos de TI, después de un desastre de dimensiones mayores o de una interrupción menor. Especifica procedimientos lineamientos para la recuperación, tanto en áreas de la empresa como las alternas. Plan de respuesta ante emergencias *(Emergency response planning)*, su objetivo es salvaguardar a los empleados, el público, el ambiente y los activos de la empresa.

Últimamente se busca de inmediato llevar la situación de crisis a un estado de control. Todos los enfoques tienen como denominador común, el cual, es un limitado alcance. Cada una de estas ópticas de planeación se centra en proyección de aspectos específicos de la organización, ignorando otras áreas críticas. Para atender esta limitación, se requiere un enfoque de planeación integrado, que permita proteger todas las áreas críticas de la organización. Plan de continuidad

del negocio PNC (o sus siglas en inglés *BCP-Businnes continuity plan*), integra el alcance y los objetivos de todos estos enfoques [6].

Figura 2: Proyectos que constituyen un SGSI. Fuente Gómez.

La norma ISO/27001

La norma ISO 27001, es un estándar desarrollado como modelo para el establecimiento, implantación, operación, monitorización, revisión, mantenimiento y mejora de un SGSI para cualquier tipo de organización. Permite diseñar e implementar un SGSI, se encuentra influenciado por las necesidades, objetivos, requisitos de seguridad, los procesos, los empleados. Los sistemas de soporte y la estructura de la organización. Su origen es británico se creó en el año 2005, pero tiene su versión más reciente que data del año 2013, la Organización Internacional para la Normalización (ISO) la oficializo como norma.

El ISO 27001:2013 es el único estándar certificable, aceptado internacionalmente de manera global para la gestión de la seguridad de información; aplica a todo tipo de organizaciones, tanto por su tamaño como su actividad. La norma ISO 27001, actúa bajo el enfoque de procesos. La aplicación de unos sistemas de procesos, dentro de la organización, junto con la identificación y las intersecciones de estos procesos, así como su gestión, puede denominarse como enfoque basado en procesos. El enfoque basado en procesos para la gestión de la seguridad de información presentada en esta norma, enfatiza a los usuarios, la importancia de: La comprensión de los requisitos de la seguridad de una organización y la necesidad de establecer políticas y objetivos para la seguridad de información, Implementar y operar controles para dirigir los riesgos de la seguridad de información de una organización con el contexto de los riesgos globales del negocio de la organización, Realizar seguimiento y revisar el desempeño y la eficiencia del SGSI, Mejora continua con base en

mediciones objetivos. Es una forma sistemática de administrar la información sostenible de una institución, para que permanezca segura. Abarca a las personas, los procesos y las tecnologías de información. La forma total de la seguridad de la información, y a la integración de las diferentes iniciativas de seguridad necesitan ser administradas para cada elemento sea completamente efectivo. Aquí en donde entra el SGSI, que permite coordinar esfuerzos de seguridad con mayor efectividad.

Órganos gubernamentales regulatorias para entidades financieras

La Superintendencia de Banca, Seguros y AFP es el organismo encargado de la regulación y supervisión de los Sistemas Financiero, de Seguros y del Sistema Privado de Pensiones, así como de prevenir y detectar el lavado de activos y financiamiento del terrorismo. Su objetivo primordial es preservar los intereses de los depositantes, de los asegurados y de los afiliados al SPP.

La SBS es una institución de derecho público cuya autonomía funcional está reconocida por la Constitución Política del Perú. Sus objetivos, funciones y atribuciones están establecidos en la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca, Seguros y AFP (Ley 26702)[7].

La oficina Nacional de Gobierno Electrónico e Informática ,la Presidencia del Consejo de Ministros – PCM a través de la ONGEI, se encarga de normar, coordinar, integrar y promover el desarrollo de la actividad informática en la Administración Pública (DS Nº 066-2003-PCM, DS Nº 067-2003-PCM).Impulsa y fomenta el uso de las TICs para la modernización y descentralización del estado.Actúa como ente rector del Sistema Nacional de Informática, dirige y supervisa la política nacional de informática y gobierno electrónico. (Oficina Nacional de Gobierno Eléctronico e Informática, 2018).

Materiales y métodos

Poblacion y muestra

La población (N) está compuesta por los directivos de las diferentes áreas del negocio como operaciones y gerencia de sistemas de la sucursal del Banco Ripley -Trujillo, Es de tipo poblacional ya que lo conforman los usuarios de los departamentos del banco de operaciones y gerencia de sistemas. De ello, se estima la muestra (n), la cual al ser menor o igual que 30, se calcula directamente como sigue:

N=29 personas

Instrumentación

A continuación, se procede a citar las técnicas e instrumentos que se utilizarán para la recolección de datos en el desarrollo de la presente investigación.

Para definir el alcance a nivel estratégico de seguridad de la información en el banco se procederá a identificar el organigrama y su plan estratégico de la entidad bancaria en el aspecto de seguridad de la información

Para diseñar las políticas y controles del diseño del plan de seguridad de la información basado en la norma ISO/IEC 27002 se procederá a recolectar la información de los controles de acuerdo a la ISO/IEC 27002 y se elaborará un plan de seguridad de la información que contenga: cuadro de niveles de control, en sus diferentes capítulos como: política de seguridad, aspectos organizativos de la seguridad de la información, gestión de activos, seguridad ligada a los recursos humanos, seguridad física y del entorno, gestión de comunicaciones y operaciones, control de acceso, adquisición desarrollo y mantenimiento de los sistemas de información, gestión de incidentes de la seguridad de la información y mejoras, gestión de la continuidad del negocio y cumplimiento arquitectura del programa de indicadores, de la metodología ISO/IEC 27002 , la técnica de Entrevistas a los directivos y como instrumento a las guías de entrevistas.

Para analizar la matriz de gestión de riesgos de acuerdo a la planificación. Se procederá con recolectar la información de los activos y se procederá a evaluar en cuanto a la gestión de riesgo, para ello tomamos en cuenta los activos como son personas, procesos y tecnología

Para el análisis de los datos recolectados, se utilizará el Método Deductivo, pues se va de lo general a lo específico. Este comienza dando paso a los datos en cierta forma válidos, para llegar a una deducción a partir de un razonamiento de forma lógica o suposiciones; o sea se refiere a un proceso donde existen determinadas reglas y procesos donde gracias a su asistencia, se llegan a conclusiones finales partiendo de ciertos enunciados o premisas. Ver figura 3

La validación y confiabilidad fue presentado por los docentes Ing. Nelson Ángeles Quiñones con CIP: 185097, Ing. Edward Vega Gavidia CIP:130533 y el Ing. David Agreda Gamboa CIP:86691, todos colegiados para que puedan dar sus observaciones y luego de ella procedieron a firmar las constancias de validez.

Revista Innovación y Software
Vol. 2, No. 2, Mes Septiembre-Febrero, 2021
ISSN: 2708-0935
Pág. 27-43
https://revistas.ulasalle.edu.pe/innosoft

Figura 3: Plan de seguridad de la información. Fuente Elaboración propia.

Resultados y discusión

Realizamos el análisis FODA a nivel de TI y estratégico, como el de los procesos que maneja el banco, luego de ello elaboramos el documento final que conforma el alcance del plan de seguridad de la información.

Tabla 2: Matriz RAM de micropocesos y áreas del banco.

	Operaciones	Comercial	Finanzas	Riesgos	Cobranzas	CRM	RRHH
MP1	RAM	RAM		RA	A	RA	
MP2		RAM		RA			A
MP3	RA	RAM		RA	RA	RA	A
MP4	A	A	RAM	A	A	A	A
MP5	RAM		RAM				RA
MP6	RA	RA	RA	RA	RA	RA	RAM
MP7	RA	RA	A	RAM	A	RA	
MP8	RAM		RA	RA	RA		
MP9		A	A	A	RAM	A	
MP10	A	RA			A	RAM	

Nota: M. Ejecuta el Proceso | R: Recibe información | A: Brinda información

MP1: Tarjetas de crédito: Administrar las tarjetas de crédito

MP2. Captaciones: Administrar las captaciones de nuevos clientes

MP3: Atención al cliente: Administrar los servicios de atención y contacto directo con el cliente

MP4. Soporte financiero: Administrar presupuesto y contabilidad

MP5: Soporte Operativo Administrativo: Todas las transacciones financieras del banco deben estar respaldadas y su gestión debe ser continua y de soporte a los demás macroprocesos

MP6.Recursos Humanos: Selección de nuevo personal y administración de personal, control de tiempos y compensaciones

MP7.Gestion de Riesgos: Riesgo de crédito, de mercado, de operación de liquidez

MP8. Control de cumplimiento: Soporte al directorio, que involucra la auditoría interna y el cumplimiento normativo

MP9.Cobranzas: Recuperar temprana o tardíamente las cuotas atrasadas de compromisos de pago de los clientes

MP10: Fidelización: Administración de clientes, perfil de uso y fidelización

Identificamos que macroprocesos son estratégicos, tácticos y operativos, de acuerdo a la participación de cada proceso en los objetivos de negocio.

Para empezar con el diseño del plan de Seguridad de Información para el banco Ripley tendremos en cuenta los siguientes puntos a desarrollar: Ver figura 4

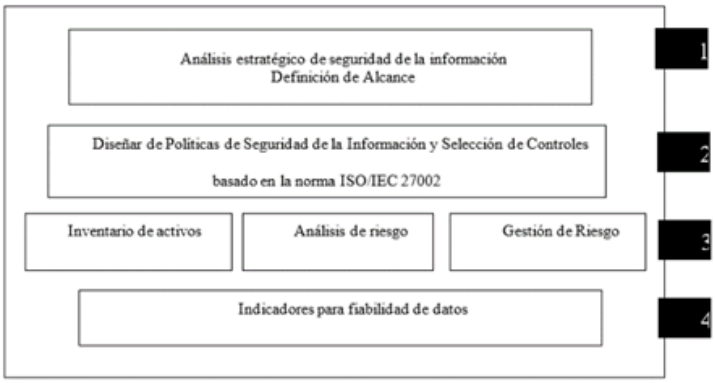

Figura 4: Esquema de diseño del plan SGSI ISO-27002. Fuente Elaboración propia

Se diseñará las políticas de seguridad de la información con el propósito de proteger la información del banco, estas servirán como una guía para una futura implementación de medidas de seguridad que ayuden a cumplir con la integridad, confidencialidad y la disponibilidad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales. Este documento de políticas de seguridad se realizó tomando como base la siguiente documentación. Normas internas del banco referidas a la seguridad de la información. Requerimientos de la

superintendencia de banca y seguros (SBS) sobre riesgo de la tecnología de la información. Estándar de la seguridad de la información ISO/IEC 27002.

El inventario de activos es la recopilación de todos aquellos elementos indispensables para que la administración electrónica pueda prestarse con todas las garantías, de manera que los ciudadanos tengas confianza en ella. Metodología para analizar, evaluar y gestionar los riesgos.

Figura 5: Pasos para aplicar la metodología en la gestión de riesgos. Fuente Elaboración Propia

El nivel de riesgo vendrá dado por el valor más alto para cada activo. Tanto el nivel de vulnerabilidad como el nivel (o probabilidad) de amenaza se valoran de 0 a 3 (no aplicado, bajo, medio y alto).

Nivel de riesgo = Nivel de amenaza x Nivel de vulnerabilidad x Nivel de impacto.

Luego de aplicar los controles a los activos, procedemos a establecer los indicadores los cuales se usarán en la implementación para medir el impacto de la planificación y por consiguiente una implementación futura, cabe señalar que el objetivo de esta investigación es estipular los indicadores en este planeamiento de la seguridad de la información en la fiabilidad de datos, lo que quiere decir que se enfoca en los tres pilares de un SGSI que son:

Tabla 3: Cálculo del riesgo para aplicaciones comerciales. Fuente elaboración propia

Amenaza	Impacto (valor del activo)	Nivel de amenaza	Vulnerabilidad	Nivel de Riesgo
Fuego	7	1	0	0
Robo	7	1	1	7
Error de mantenimiento	7	1	3	21
Fallo de software	7	3	2	42
Fallo de comunicaciones	7	2	1	14
Errores de usuario	7	2	2	28

Confidencialidad: el cual previene el acceso no autorizado a la información, de manera intencional o no.

Integridad: Evita modificaciones de la información por parte de personal no autorizado

Disponibilidad: Proporciona acceso seguro a la información en el momento en que se precisa.

Luego de "Definir los indicadores para evaluar el plan de seguridad de la información", podemos apreciar que solo se contemplan 10 indicadores que ayudarán en la implementación de controles de un SGSI, de acuerdo a estos parámetros se debe realizar una evaluación en la cual se determinará el impacto que generará la planificación en el banco.

Elección de los indicadores a través de la evaluación de expertos en la aplicación del método V de Aiken. En qué medida los indicadores de la prueba son una muestra representativa del constructo. Medida para cuantificar el acuerdo de los jueces (expertos) A continuación, presentamos los resultados al aplicar el método de Aiken para la elección y fiabilidad de los datos de acuerdo a la evaluación de los expertos.

De la figura 4, como podemos apreciar los coeficientes de Aiken (A_k) para ambas representatividades y luego de la evaluación de los jueces, los puntos de cortes aceptables del método de Aiken nos dicen que estamos en la métrica permitida la cual da validez de nuestros indicadores para aplicarse y garantizar el incremento de la fiabilidad de los datos. $0.6<=A_k<=1.0$, el intervalo de resultado obtenido: $A_k=0.96$ y $A_k=0.98$

Tabla 4: Análisis del método V de Aiken mediante expertos para la elección de indicadores. Fuente elaboración propia

Indicadores	Fiabilidad de datos A_k por indicador	Elección de indicadores A_k por indicador
ID 1	0,92	0,92
ID 2	1,00	1,00
ID 3	0,92	1,00
ID 4	1,00	1,00
ID 5	0,92	1,00
ID 6	1,00	1,00
ID 7	1,00	0,92
ID 8	0,92	1,00
ID 9	1,00	1,00
ID 10	0,92	1,00
Ak Total	0,96	0,98

Se realizó un análisis del método V de Aiken para determinar la elección de indicadores mediante expertos, el cual nos dio como resultado un coeficiente que está en el margen de corte como aceptable en la escala de Aiken y el cual garantiza la valides de los indicadores para lograr el incremento de la fiabilidad de los datos.

Conclusiones

Se logró realizar el documento oficial del alcance para la aplicación del plan de seguridad de la información basado en la norma ISO/IEC 27001 y sus controles contemplados en la ISO/IEC 27002.

Se logró desarrollar el documento de las políticas de seguridad de la información, el cual representa una herramienta muy importante para la aplicación de los controles en los procesos que se determinó en el alcance.

Se logró evaluar la matriz de gestión de riesgos de acuerdo a los activos (personal, procesos y tecnología) al cual se les determinó un valor de acuerdo a la vulnerabilidad que ocasionaría este en caso de alguna eventualidad, y de acuerdo a ello se determinó los controles a aplicar en los procesos donde se manipulan estos activos.

Se logró definir los indicadores para evaluar el plan de la seguridad de la información, donde se aprecian los indicadores, garantizan la confiabilidad de los datos y está lista para ser aplicadas en una futura implementación.

Agradecimientos

A la universidad Nacional de Trujillo por ser mi alma mater y a todo el personal docente y administrativo que labora en la Escuela de Postgrado Sección de Ingeniería, por sus enseñanzas y apoyo durante el tiempo que curse la maestría.

Referencias

[1] Moreira, M. (2015). Auditoría del sistema informático del ministerio de transporte y obras públicas. España: Escuela politécnica nacional.

[2] Mega, G. (2014). Metodología de Implementación de un SGSI en un grupo Empresarial Jerarquico. Montevideo-Uruguay: Universidad de la República.

[3] Pressman, R. (2013). Ingeniería del Software. McGraw Hill, 10-15.

[4] Security, F. O. (5 de Mayo de 2017). Federal Office for Information Security – Germany. Obtenido de "The IT Security Situation in Germany in 2017: http://www.bsi.bund.de/english/publications/securitysituation/Lagebericht_2017_englisch.pdf

[5] Grundschutz, G. (8 de Junio de 2017). Federal Office for Information Security – Germany. Obtenido de http://www.bsi.bund.de/

[6] Guerra, A., & Mantilla, R. (2009). Diseño de un Sistema de Gestión de Seguridad de la Información para Cooperativas de Ahorro y Credito en Base a la norma ISO 27001.

[7] SBS. (15 de Enero de 2017). Superintendecia de Banca , Seguros y AFP. Obtenido de https://www.sbs.gob.pe/

[8] Aguilar, M., & Villena, A. (2015). Sistema de Gestión de Seguridad de la Información en una Institución Financiera. TESIS PUCP, 6-9.

[9] BCRP. (15 de Enero de 2017). Banco de Reserva del Perú. Obtenido de http://www.bcrp.gob.pe/sitios-de-interes/entidades-financieras.html.

[10] Bendermacher, J. (s.f.). Auditoría interna y auditoría externa. Obtenido de https://global.theiia.org/translations/PublicDocuments/GPI-Distinctive-Roles-in-Organizational-Governance-Spanish.pdf

[11] Betarte, G. (2014). Information Security – Security conscious. Uruguay. Obtenido de https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

[12] Munoz, G. Wastewater treatment for the U.C. Davis Arboretum. Recuperado de: http://lda.ucdavis.edu/people/2013/GMunoz.pdf Tomado el 04/01/2015.

[13] Córdova, L., & Muñoz, R. (2014). Planeamiento Estratégico de Tecnología de Información de Banco Ripley Perú. Tesis - UPC, 20-30.

[14] Franco, D., & Guerrero, C. (2013). Sistemas de Controles de la Seguridad Informática basado en ISO/IEC 27002. 5-8.

[15] Gomez, G. (2016). Interpretación de la Norma ISO/IEC 27001:2013. Informe de investiagacion, Universidad ESAN, Lima.

[16] Indacochea, A. (2012). Una Propuesta para mejorar las prácticas de Gobierno Corporativo en el Perú. CENTRUM,Pontificia Universidad Catolica del Perú, 12-15.

[17] Mantilla, A. (junio de 2009). Diseño de un sistema de seguridad de la información para cooperativas de ahorro y crédito en base a la norma ISO 27001. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/8108/1/CD-2254.pdf

[18] Muñoz, R. (2017). Planeamiento Estratégico de Tecnología de la Información de Banco Ripley Perú. Lima: Repositorio UPC.

[19] NCh-ISO. (2013). Tecnología de Información-Técnicas de Seguridad -Sistema de Gestión de Seguridad de la Información. Norma Chilena - 27001, 1-2.

[20] SBS. (15 de Enero de 2017). Superintendecia de Banca , Seguros y AFP. Obtenido de https://www.sbs.gob.pe/