INSTITUTO TECNOLÓGICO DE COSTA RICA

Área Académica de Administración de Tecnologías de Información

Propuesta de mejora para las Políticas de Seguridad de la Información del Banco Central de Costa Rica, basado en el estándar ISO/IEC 27002:2005

Proyecto final de graduación para optar por el grado de Licenciatura en Administración de Tecnologías de Información.

Estudiante: Manfred Sierra Montoya

Cartago, Costa Rica, 2014

INSTITUTO TECNOLÓGICO DE COSTA RICA

ÁREA DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

GRADO ACADÉMICO: LICENCIATURA

Los miembros del Tribunal Examinador del Área de Administración de Tecnologías de Información recomendamos que el presente Informe Final del Proyecto de Graduación del estudiante *Manfred Sierra Montoya*, sea aceptado como requisito parcial para obtener el grado académico de *Licenciatura en Administración de Tecnologías de Información.*

_____

Rodrigo Bogarín
Miembro Tribunal Examinador

_____

Yarima Sandoval
Miembro Tribunal Examinador

_____

Jorge Carmona
Miembro Tribunal Examinador

_____

Sonia Mora
Coordinadora del Proyecto de Graduación de la Licenciatura en Administración de Tecnologías de Información

Noviembre 2014

Dedicatoria

A mis abuelitos, Ángel Montoya Coto, quien hoy ya no está conmigo y María de los Ángeles Avendaño Solano por ser mi apoyo por tanto tiempo y siempre motivarme a seguir adelante.

A mis padres y hermano, por ayudarme a cumplir mis metas en la vida, pero principalmente a mi madre por todos sus sacrificios y palabras de aliento que me ayudaron a continuar y superar todos los obstáculos que se me presentaron.

Agradecimientos

A Dios por darme salud, sabiduría y las capacidades suficientes para cumplir esta meta.

A mi familia, en general, por siempre apoyarme y darme fuerzas cuando hacían falta. A Melissa por ser una gran compañera, amiga y mi apoyo incondicional. A mis compañeros de trabajo y amigos, Pablo e Ignacio, con los cuales trabajé en la mayor parte de este proceso. También quiero agradecer a mis amigos María de Jesús, Mónica, Roberto y Máximo, quienes fueron parte fundamental en mi desarrollo por su apoyo y amistad. A William le agradezco por el apoyo durante esta última etapa.

A la profesora Lorena Zúñiga por darme la oportunidad de trabajar con ella y poner su confianza en mí. Al profesor Alfredo Solano por sus enseñanzas que fueron fundamentales para el desarrollo de mi proyecto. También agradezco a mi profesor asesor Rodrigo Bogarín por su disposición a ayudarme y ser un guía en esta última etapa y en general, a todos aquellos profesores por su ayuda en mi formación.

Al Banco Central de Costa Rica, principalmente a Franklin Giralt Amador por abrirme la puerta y guiarme en el desarrollo de mi proyecto final de graduación y a la División Gestión y Desarrollo por acogerme en esta última etapa y enseñarme tantas cosas, tanto a nivel profesional como personal.

Por último, pero no menos importante, al Instituto Tecnológico de Costa Rica por ser mi segundo hogar durante estos últimos años.

Resumen

El presente proyecto consiste en un análisis de las Políticas de Seguridad de la Información del Banco Central de Costa Rica y documentación complementaria, en el área de la Seguridad de la Información con respecto a la cobertura de los controles del estándar ISO/IEC 27002:2005. Lo anterior permite desarrollar un conjunto de propuestas de políticas, controles y lineamientos adaptables a las Políticas Específicas de la Seguridad de la Información, con el fin de mejorarlas en esta Entidad.

Lo primero que se logra identificar durante el desarrollo del proyecto es que las Políticas Específicas de Seguridad de la Información son la base del Sistema de Gestión de Seguridad de la Información del Banco, pues determinan la intención y el compromiso de la gerencia al trato y gestión de la Seguridad de la Información dentro de este. Además, estas funcionan como fuente primaria de conocimiento para el resto de la organización sobre cómo actuar en concordancia con los requisitos organizacionales de seguridad.

Específicamente sobre el planteamiento del documento de Políticas Específicas de Seguridad de la Información, se logra identificar que se encuentra estructurado según algunos de los dominios del estándar ISO/IEC 27002:2005, donde se identifica una sección introductoria del documento, posterior a ello se establecen los aspectos organizativos de Seguridad de la Información, para luego dirigirse directamente a la definición de políticas, controles y lineamientos de seguridad, los cuales se plantean para cuatro áreas: seguridad física y del entorno, gestión de comunicaciones y operaciones, control de accesos y el área de adquisición y por último, desarrollo y mantenimiento de sistemas. Según lo anterior, quedan fuera de las Políticas Específicas de Seguridad de la Información, los dominios de seguridad de los recursos humanos, gestión de incidentes de Seguridad de la Información, continuidad del negocio y el dominio de cumplimiento; sin embargo, algunas de las políticas de Seguridad de la Información cubren algunos de los controles considerados en dichos dominios.

Basado en los resultados de la valoración, se logra identificar que el dominio para el cual hay un mayor número de controles cubiertos totalmente es el de gestión de incidentes de Seguridad de la Información y continuidad del negocio y por otro lado, el más desatendido por la documentación del Sistema de Gestión de Seguridad de la Información es el de seguridad de los recursos humanos. En general, se obtuvo como resultado que del total de 133 controles del estándar ISO/IEC 27002:2005, un porcentaje de 24,81% está cubierto totalmente por la documentación evaluada, un 39,85% en forma parcial y un 35,34%% de los controles no se cubre del todo y todos estos fueron aplicables a la organización.

Las propuestas de mejora consistieron en un conjunto de posibles políticas, controles y lineamientos que podrían ser adoptados por el Banco para cerrar la brecha existente con el estándar ISO/IEC 27002:2005, siempre y cuando se evalúe que efectivamente puedan ser adoptados por la organización, según el proceso de gestión de riesgos y los recursos organizacionales para implementar dichas medidas; aunque bien, se logró también identificar que existen buenas prácticas adoptadas por el Banco, pero que no se encuentran documentadas y por tal razón, se consideraron como parte de la brecha.

Palabras claves: Seguridad de la Información, Política de la Seguridad de la Información, ISO/IEC 27002

Abstract

This project consists of an analysis of the Information Security Policy of the Banco Central de Costa Rica and additional documents in the area of Information Security, regarding the coverage of standard ISO / IEC 27002: 2005 controls. This allows developing a set of proposed policies, controls and guidelines adaptable to the “Políticas específicas de la Seguridad de la Información” document, to improve the treatment of Information Security in the Bank.

The first aspect identified during the project development is that the Políticas específicas de la Seguridad de la Información are the base of the Information Security Management System of the Bank because they determine the intent and commitment of management to the treatment of Information Security within the Bank. Besides these Políticas específcas de la Seguridad de la Información are the primary sources of knowledge for the rest of the organization on how to act in accordance with organizational security requirements.

Specifically on the approach of the Políticas específicas de la Seguridad de la Información document, it is identified as structured according to some of the domains of the ISO/IEC 27002:2005 standard, because there are an introductory section of the document, after that it is identified the organizational aspects of Information Security, and then it is found the definition of policies, controls and safety guidelines, which are group by four areas: physical and environmental security, communications and operations management, access control and the area of acquisition, development and maintenance of systems. The Information Security domains of human resources, Information Security incident management, business continuity and the compliance domain are excluded from the Políticas específicas de la Seguridad de la Información; however, some other documents cover the controls in those domains.

Based on the results of the assessment is identified that Information Security incident management and business continuity domains are the ones with greater number of fully covered controls, and secondly that the most unattended domain by the Information Security Management System documentation is the human resources domain. The overall result obtained is that from the 133 controls of ISO/IEC 27002:2005 standard, are fully covered by the assessed documentation a percentage of 24.81%, a 39.85% are partially covered and a 35.34% of controls are not covered at all, considering that all controls were applicable to the organization.

The proposed improvements consisted of a set of possible policies, controls and guidelines that could be adopted by the Bank to close the gap with the ISO / IEC 27002: 2005 standard, considering to evaluate the possible implementation of those policies, controls and guidelines but well, it was also possible to identify existing good practices adopted by the Bank. Also it should be considered to evaluate if Information Security good practices are implemented in the Bank but not documented as policies, controls or guidelines yet.

Keywords: Information Security, Information Security Policy, ISO/IEC 27002.

Índice general

Índice de figuras

Índice de tablas

Índice de gráficas

Capítulo I: Introducción

El presente documento responde al proyecto para optar por el grado de Licenciatura en Administración de Tecnologías de Información; el cual consiste en la identificación, valoración y propuesta de mejora a las políticas y los documentos complementarios, asociados al Sistema de Gestión de la Seguridad de Información (SGSI) del Banco Central de Costa Rica (BCCR), tomando como base el estándar ISO/IEC 27002:2005. La valoración permitirá verificar qué controles propuestos por el estándar están contemplados en las Políticas de Seguridad de la Información asociadas a la estructura del SGSI del Banco; así como determinar cuáles otros no se han tomado en consideración y a partir de ello, junto con la opinión de los principales interesados, hacer una priorización y realizar las recomendaciones correspondientes para mejorar la completitud del marco normativo interno que sustenta la Seguridad de la Información de la Entidad.

La información es un activo valioso de la Institución, por lo cual, su seguridad debe ser gestionada. En una institución bancaria, la información adquiere un nivel de valor superior que en otras organizaciones, pues posee datos financieros, tanto suyos como de otras entidades. La Seguridad de la Información en el Banco Central de Costa Rica requiere atención especial, porque sus funciones afectan la economía del país. Para atender las necesidades de resguardo de la información del Banco Central de Costa Rica, se ha planteado un Sistema de Gestión de Seguridad de Información, el cual está a cargo del Departamento de Gestión de Gestión de Calidad, perteneciente a la División Gestión y Desarrollo del Banco. La Institución desea que se evalúe, a partir de ISO/IEC 27002:2005, las Políticas de Seguridad de la Información y los documentos complementarios que componen la estructura de su SGSI e identificar oportunidades de mejora para ellos.

Los resultados finales de este proyecto son de interés para el Departamento de Gestión Calidad del Banco, pues van a ser los insumos para mejorar las políticas y documentos asociados a la Seguridad de la Información, de acuerdo con lo planteado por ISO/IEC 27002:2005; estos van a ser presentados como recomendaciones que nacen de la valoración realizada. Es de importancia, para el resguardo de la información bancaria, realizar esta evaluación, ya que va a permitir mejorar la calidad del Sistema de Gestión de Seguridad de la Información y reducir vulnerabilidades. Las recomendaciones se van a desarrollar a partir de los controles definidos en el estándar ISO/IEC 27002:2005, pero además, se van a plantear a partir de la opinión de los principales interesados del Sistema de Gestión de Seguridad de Información, de manera tal que el resultado se encuentre alineado con los esfuerzos institucionales.

1.1. Descripción general

1.1.1. Antecedentes

Se describe en esta sección, a nivel general, el contexto del Banco Central de Costa Rica.

1.1.1.1. Descripción de la organización

El Banco Central de Costa Rica (2014a) es una organización cuyo principal objetivo es controlar la inflación, realizar labores conjuntamente con el Consejo Nacional de Supervisión de Sistema Financiero para cumplir con sus objetivos. Se encarga también de la emisión y administración de los billetes y monedas, entre otras tareas. Sus principales funciones se destacan a continuación:

- El mantenimiento del valor externo y de la conversión de la moneda nacional.
- La custodia y la administración de las Reservas Monetarias Internacionales de la Nación.
- La definición y el manejo de la política monetaria y cambiaria.
- La gestión como consejero y banco-cajero del Estado.
- La promoción de condiciones favorables al robustecimiento, la liquidez, la solvencia y el buen funcionamiento del Sistema Financiero Nacional.

1.1.1.1.1. Historia

El Banco Central de Costa Rica (2014a) describe la historia de la entidad a continuación:

Al intensificarse la actividad económica y bancaria del país, surgió la necesidad de crear un Banco Central que actuara como mayor autoridad que el simple Departamento Emisor que hasta ese momento (1945) estaba adscrito al Banco Nacional de Costa Rica; este último establecido a fines de 1936 al reorganizarse el antiguo Banco Internacional.

En 1948, al decretarse la nacionalización de la banca privada -recepción de depósitos del público - y dada la necesidad de dotar al nuevo Sistema Bancario Nacional de una integración orgánica adecuada y una orientación eficiente por parte del Estado, se hizo más urgente la necesidad de establecer el Banco Central como órgano independiente y rector de la política económica, monetaria y crediticia del país. Con este propósito se promulgó la Ley 1130, del 28 de enero de 1950, que estableció el Banco Central de Costa Rica con características definidas y propias, que le permitieron, en lo sucesivo, actuar como Órgano Central de la economía del país.

Por la importancia que tuvo para la historia bancaria de Costa Rica la fundación del Banco Central de Costa Rica, el respectivo proyecto, que derivó en la Ley 1130, incluye varios razonamientos para sustentar la decisión de los Poderes Legislativo y Ejecutivo de dictar y sancionar esa ley, la cual, en un principio, tuvo un carácter transitorio, por cuanto el Banco Central de Costa Rica tendría las mismas funciones y facultades del Departamento Emisor del Banco Nacional de Costa Rica, hasta la desaparición de este último. Entonces el Banco Central de Costa Rica operó con sujeción a las disposiciones de ambas leyes: la de su fundación y la que regía al Departamento Emisor.

El 23 de abril, 1953 fue promulgada la Ley 1552, denominada Ley Orgánica del Banco Central de Costa Rica, la cual, fue sustituida por la Ley 7558 del 3 de noviembre de 1995.

1.1.1.1.2. Misión

“Mantener la estabilidad interna y externa de la moneda nacional y asegurar su conversión a otras monedas.” (Banco Central de Costa Rica, 2014a).

1.1.1.1.3. Visión

“Ser un banco central reconocido por la sociedad costarricense y la comunidad internacional por su eficiencia, transparencia y credibilidad en mantener una inflación baja y estable.” (Banco Central de Costa Rica, 2014a).

1.1.1.1.4. Objetivos estratégicos

Los objetivos estratégicos del Banco Central de Costa Rica (2014a), son:

- Mantener la estabilidad interna de la moneda nacional, procurando a su vez la ocupación plena de los recursos productivos.
- Mantener la estabilidad externa de la moneda nacional y asegurar su libre conversión a otras monedas.
- Promover un sistema de intermediación financiera estable, eficiente y competitivo.
- Promover la eficiencia del sistema de pagos interno y mantener su normal funcionamiento.
- Garantizar la excelencia operacional de la Institución, entendida como la ejecución de las funciones esenciales para el cumplimiento de los objetivos institucionales al menor costo posible y bajo condiciones de riesgo aceptables.

1.1.1.1.5. Organigrama

Se muestra en la Figura 1. Organigrama del Banco Central de Costa Rica, el organigrama institucional de la organización.

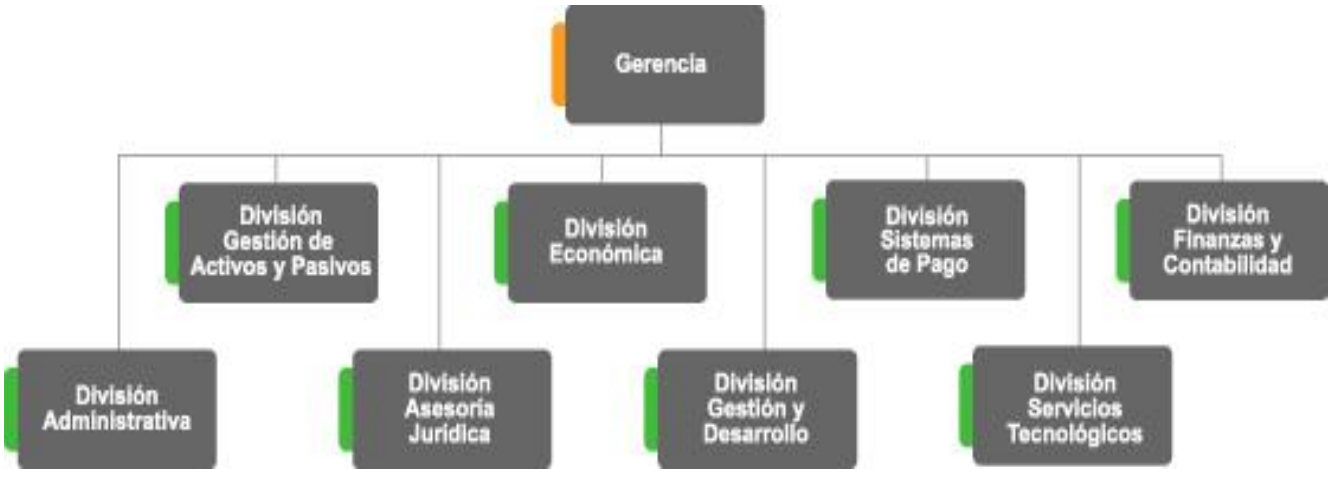


Figura 1. Organigrama del Banco Central de Costa Rica
Fuente: (Banco Central de Costa Rica, 2014a)

1.1.1.2. Departamento de Gestión de Calidad

Se hace en esta sección, una descripción del Departamento de Gestión de Calidad de la Institución.

1.1.1.2.1. Objetivo general

El objetivo del Departamento de Gestión de Calidad, según el Banco Central de Costa Rica,es el siguiente:

> Administrar el proceso de gestión institucional de procesos, servicios, información, comunicación, gobierno corporativo, control interno, Seguridad de la Información, continuidad de negocios y reorganizaciones administrativas; dotándolo de metodologías, herramientas y promoviendo los cambios culturales necesarios que permitan a la entidad alcanzar sus objetivos estratégicos.

1.1.1.2.2. Funciones principales

Las funciones principales del Departamento de Gestión de Calidad son las siguientes:

1. Promover y apoyar el cambio tecnológico a nivel institucional, ajustando los procesos sujetos de automatización, de manera que esta se realice sobre procesos eficientemente diseñados, para garantizar el uso racional y eficiente de los recursos requeridos para su operación regular.
2. Desarrollar las metodologías relacionadas con la gestión de procesos, servicios, control interno, Seguridad de la Información, continuidad de negocios, gobierno corporativo, información, comunicación y reorganizaciones administrativas, así como con los cambios asociados a su implementación; que permitan un mejor desempeño institucional.
3. Desarrollar la gestión de la información, como medio para mejorar el desempeño en la ejecución de los procesos y en el cumplimiento de los objetivos institucionales.

4. Ejecutar programas de sensibilización para atender los cambios culturales producto de las innovaciones tecnológicas y metodológicas propuestas en la gestión de procesos, servicios, control interno, Seguridad de la Información, continuidad de negocios, gobierno corporativo, información, comunicación y reorganizaciones administrativas.
5. Recomendar implementar buenas prácticas de Gobierno Corporativo en el Banco Central, con el fin de transparentar la relación entre los diferentes niveles gerenciales y la ciudadanía.
6. Promover y velar por el mejoramiento continuo en la prestación de los servicios que ofrece el banco, con el objetivo de mejorar la calidad del servicio y simplificar los trámites que el ciudadano debe realizar en la Institución.
7. Asesorar al Comité de Continuidad de Negocios del Banco en la planificación y mejora de la estrategia de continuidad, con base en normas y buenas prácticas internacionales, facultando que los servicios críticos se continúen brindando en caso de una interrupción.
8. Monitorizar y actualizar el estado de las recomendaciones producto de las revisiones realizadas por la auditoría interna y de las evaluaciones del Sistema de Control Interno en cada una de las dependencias del banco, con la finalidad de mantener el control sobre las fechas de cumplimiento de las recomendaciones.
9. Diseñar, implementar, mantener, evaluar y mejorar del Sistema de Control Interno del banco, con el propósito de procurar la eficiencia en las operaciones, el logro de los objetivos estratégicos y la protección del patrimonio con un grado razonable de seguridad.
10. Diseñar, implementar, mantener, evaluar y mejorar el Sistema de Gestión de Calidad y el Sistema de Gestión de Seguridad de la Información, esto como parte del Sistema de Control Interno del banco, con el propósito de mejorar continuamente los servicios que ofrece el banco de una forma segura.

11. Diseñar y desarrollar los proyectos de mejora institucional a través de procesos de acciones de mejora, reordenamientos funcionales y reorganizaciones administrativas, con la finalidad de promover la mejora de la eficiencia y calidad en la institución.
12. Administrar los sistemas de comunicación, imagen Institucional y relaciones públicas, con el objetivo de brindar información clara, segura y oportuna.

1.1.1.2.3. Organigrama de la División Gestión y Desarrollo

El Departamento de Gestión de Calidad del Banco, junto con los departamentos de Riesgos y Planeación y Control de Gestión, conforma la División Gestión y Desarrollo, tal como se puede observar en la Figura 2. Organigrama de la División Gestión y Desarrollo del Banco Central de Costa Rica.

Figura 2. Organigrama de la División Gestión y Desarrollo del Banco Central de Costa Rica
Fuente: (Banco Central de Costa Rica, s.f.)

1.1.2. Planteamiento del problema.

Se describe a continuación, el conjunto de variables que afectan a la institución, son base y dan origen al presente proyecto.

1.1.2.1. Situación problemática

El Sistema de Gestión de Seguridad de la Información es administrado por el Departamento de Gestión de Calidad, perteneciente a la División Gestión y Desarrollo del Banco Central de Costa Rica. Como base de este SGSI, se planteó un documento denominado “Políticas específicas para la Seguridad de la Información", el cual posee el conjunto de políticas, controles y lineamientos a nivel de la Institución, que definen la manera de gestionar la Seguridad de la Información.

Este conjunto de políticas buscan que la información dentro del Banco se gestione de manera que se cumplan los requisitos de disponibilidad, confidencialidad e integridad de los datos bancarios.

La Institución busca adaptarse a los estándares ISO/IEC 27000, en el sentido de implementar los controles planteados en ellos, específicamente por el estándar ISO/IEC 27002:2005. Para ello el Departamento de Gestión de Calidad busca mejorar la documentación de su Sistema de Gestión de Seguridad de la Información, principalmente el documento de Políticas Específicas de Seguridad de la Información de la Entidad. Cabe mencionar que el Banco Central de Costa Rica, a pesar de su deseo apegarse al estándar, no busca certificarse.

En febrero del presente año se realizó un trabajo similar dentro del Banco Central de Costa Rica. Este fue realizado por Ricardo Morales, colaborador del Departamento de Gestión de Calidad de la División Gestión y Desarrollo. El objetivo fue identificar qué controles del estándar ISO/IEC 27001 se contemplaban dentro del documento de Políticas Específicas de Seguridad de la Información, lo cual dio como resultado una actualización del documento, aprobada por la Junta Directiva del Banco, para mayo de 2014.

La lectura del informe de dicha evaluación, permite identificar una serie de documentos que complementan en general la Política de Seguridad de la Información del BCCR, los cuales no fueron evaluados en ese momento.

Ahora bien, aunque en el proyecto ejecutado por Ricardo Morales, se evaluó el documento de Políticas Específicas de Seguridad de la Información, no se valoraron otros documentos de alto impacto para la Seguridad de la Información. Además, un Sistema de Gestión de Seguridad de la Información debe basarse en la mejora continua, por tal razón, se requiere evaluar de nuevo el documento de Políticas Específicas de Seguridad de la Información, así como los documentos de mayor impacto excluidos en la última valoración.

El Banco requiere que los documentos principales que componen su Sistema de Gestión de Seguridad de la Información se evalúen con respecto al estándar ISO/IEC 27002:2005. Esto da pie a otra característica de la necesidad de la Institución, ya que se requiere que en caso de existir; por cada dominio de la Norma se identifiquen los principales documentos que regulen cómo se debe gestionar la Seguridad de la Información. Estos documentos pueden ser políticas, manuales, procesos o procedimientos. El objetivo de esta valoración es identificar la brecha existente entre estos documentos y la norma, lo cual brinda una perspectiva de la situación actual del Sistema Gestión de Seguridad de la Información de la Entidad.

La necesidad no radica simplemente en identificar la brecha entre la documentación actual y el estándar. Además, se requieren recomendaciones para mejorar dicha documentación. Estas propuestas de mejora deben enfocarse en los dominios de Seguridad de la Información, planteados por el estándar, de mayor interés para la Institución. Esto obedece a que el Departamento de Gestión de Calidad piensa considerar dichas recomendaciones en el plan de trabajo del próximo año y se razona enfocar los esfuerzos en las principales prioridades de Seguridad de la Información, según su criterio.

Analizando la situación problemática se identifican las siguientes interrogantes:

- ¿Pueden catalogarse las Políticas Específicas de Seguridad de la Información del Banco, como la base de la estructura de su SGSI?
- ¿Cuál es el nivel de cobertura del estándar ISO/IEC 27002:2005 por parte de las Políticas Específicas de Seguridad de la Información y los documentos complementarios?
- ¿Cómo puede mejorar el marco normativo interno del Banco Central con respecto a Seguridad de la Información en el ámbito de los dominios prioritarios del estándar ISO/IEC 27002:2005?

1.1.2.2. Beneficios esperados

Se esperan los siguientes beneficios a partir de la valoración a las Políticas de Seguridad de la Información del Banco Central de Costa Rica:

- Mejorar la metodología de valoración de las Políticas Específicas de Seguridad de la Información del Banco, a través de una herramienta que soporte dicho proceso.
- Mejorar la calidad y completitud de la documentación que soporta el Sistema de Gestión de Seguridad de la Información del BCCR a partir de una normativa reconocida internacionalmente.

1.1.3. Objetivos

Se detalla en esta sección, el objetivo general y los objetivos específicos del presente proyecto.

Objetivo general

Proponer mejoras para las Políticas de Seguridad de la Información del Banco Central de Costa Rica, sobre los dominios de seguridad prioritarios, tomando como referencia el estándar ISO/IEC 27002:2005, para el mes de noviembre del año 2014.

Objetivos específicos

1. Desarrollar una herramienta a partir del estándar ISO/IEC 27002:2005 que permita valorar las Políticas de Seguridad de la Información del Banco Central de Costa Rica.
2. Identificar documentación complementaria al documento de Políticas Específicas de Seguridad de la Información que se encuentre dentro del alcance de los dominios del estándar ISO/IEC 27002:2005.
3. Identificar la brecha existente entre las Políticas Específicas de Seguridad de la Información y los documentos complementarios valorados, con respecto al estándar ISO/IEC 27002:2005.

4. En relación con cuatro dominios del estándar ISO/IEC 27002:2005, desarrollar propuestas de mejora, considerando la opinión de los principales interesados en el Sistema de Gestión de Seguridad de la Información de la Entidad.

1.1.4. Alcance, entregables, supuestos y limitaciones del proyecto

1.1.4.1. Alcance

El actual proyecto se define como la propuesta de mejora de las políticas de Seguridad de la Información del Banco Central de Costa Rica, donde se identifica el documento denominado “Políticas Específicas de Seguridad de la Información” como principal componente. Para hacer la valoración y la propuesta de mejora, se va a tomar como referencia el estándar ISO/IEC 27002:2005.

Se evaluará el documento de Políticas Específicas de Seguridad de la Información de la Institución, además de los principales documentos que complementen el anterior en la cobertura de los 11 dominios planteados por el estándar ISO/IEC 27002:2005, los cuales se enumeran a continuación:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de activos.
4. Seguridad ligada a los recursos humanos.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Adquisición, desarrollo y mantenimiento de sistemas de información.
9. Gestión de incidentes de Seguridad de la Información.
10. Gestión de continuidad del negocio.
11. Conformidad.

Para realizar la evaluación de los documentos se elaborará una herramienta basada en los controles propuestos por ISO/IEC 27002:2005. La cual estará compuesta por los controles establecidos en la norma, de manera tal que se identifiquen cuáles controles se abarcan en la documentación que compone el Sistema de Gestión de Seguridad de la Información del Banco Central de Costa Rica.

La valoración realizada debe dar como resultado un conjunto de oportunidades de mejora las cuales consistirán en un conjunto de políticas, controles y lineamientos que permitan mejorar el alineamiento del Banco al estándar ISO/IEC 27002:2005; sin embargo, el Departamento de Gestión de Calidad desea que las recomendaciones para mejorar las Políticas Específicas de Seguridad de la Información y demás documentos valorados, sean enfocadas en los cuatro dominios de mayor interés (Ver Anexo 1.), para la Seguridad de la Información de la entidad. Además, las recomendaciones planteadas deben estar alineadas a la opinión de colaboradores de la institución que estén a cargo de los documentos valorados. Los dominios para los cuales se plantearán mejoras, son los siguientes:

- Organización de la Seguridad de la Información.
- Gestión de activos.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Gestión de incidentes de la Seguridad de la Información.

Este proyecto excluye la evaluación de la implementación y eficiencia de los controles y demás contenido planteado en los documentos evaluados.

Dado lo anterior, se debe mencionar que el estándar ISO/IEC 27002:2005 va a ser utilizado como un marco de referencia meramente.

1.1.4.2. Entregables

Los entregables de este proyecto son:

- Herramienta para evaluar los principales documentos que conforman la estructura del SGSI basado en la norma ISO/IEC 27002:2005.
- Informe de la brecha identificada en la valoración realizada.

- Recomendaciones para la mejora de la documentación que compone el Sistema de Gestión de Seguridad de Información del BCCR, con respecto a los cuatro dominios del estándar.

1.1.4.3. Supuestos

Los supuestos del proyecto son los siguientes:

1. El BCCR proveerá el documento ISO/IEC 27002:2005.
2. Se tendrá acceso a las políticas y demás documentos que compongan la estructura del SGSI del Banco.
3. Se contará con asesoramiento del Departamento de Gestión de Calidad del BCCR cuando se requiera evacuar dudas.

1.1.4.4. Limitaciones

Las limitaciones para el presente proyecto se describen a continuación:

1. No se implementarán las propuestas de mejora planteadas.
2. Las propuestas de mejora serán desarrolladas sólo sobre los cuatro dominios de Seguridad de la Información, prioritarios para el Banco.
3. La herramienta de valoración debe estar basada en el estándar ISO/IEC 27002:2005.
4. La herramienta de valoración debe desarrollarse en una hoja de cálculo, donde se pueda documentar el cumplimiento o no de los aspectos de los controles del estándar ISO/IEC 27002:2005 por parte de las Políticas específicas de la Seguridad de la Información y demás documentación valorada.
5. El informe de la brecha debe documentar sólo aquellos aspectos no contemplados por las Políticas específicas de la Seguridad de la Información y demás documentación valorada.
6. Las propuestas de mejora deben consistir en políticas, controles y lineamientos u otros enunciados alineados al estándar ISO/IEC 27002:2005; que se adapten al formato de las Políticas específicas de la Seguridad de la Información del BCCR.

Capítulo II: Marco teórico

Se ha identificado un conjunto de temas que alimentan el desarrollo de este proyecto, los cuales serán detallados más adelante, pero cabe resaltar a continuación los conceptos más significativos, los cuales son:

- Seguridad de la Información.
- Sistema de Gestión de Seguridad de la Información.
- Estándar ISO/IEC 27000.

La información en una organización es un activo más, el cual le permite mantener la operativa del negocio. Según lo anterior, se puede decir que proteger la información es un tema crítico y por tal razón, requiere de una gestión adecuada. Una correcta administración de la Seguridad de la Información se puede abordar a través de un Sistema de Gestión de la Seguridad de la Información, el cual está sustentado por una serie de documentos que consisten en políticas, controles, lineamientos, procesos, manuales y procedimientos que tengan por objetivo cubrir los requerimientos de Seguridad de la Información de la entidad. Dado lo anterior, se puede decir que existe una relación directa entre la completitud de la documentación y el cumplimiento de los requisitos de seguridad de información de la organización, es por tal razón que es necesario evaluar constantemente dichos documentos.

En la actualidad existe una serie de normas, metodologías, buenas prácticas y demás, que proveen un marco de referencia a las organizaciones para atender sus necesidades de Seguridad de la Información, en este proyecto se hará uso del estándar ISO/IEC 27002:2005. El objetivo del uso del estándar en este proyecto es brindar un conjunto de buenas prácticas que permitan identificar oportunidades de mejora a la documentación que sustenta la Seguridad de la Información dentro del Banco Central de Costa Rica. A continuación se detallan los conceptos que sustentan este proyecto.

2.1. Seguridad de la Información

Entiéndase el término de información, como todos aquellos datos de valor para una organización. (Montuschi, s.f.). Según ISO/IEC (2005b) la información es un activo que es esencial para alcanzar los objetivos de una organización, por lo tanto, necesita ser protegido adecuadamente. Además, el estándar ISO/IEC 27002:2005, menciona que la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades; por tal razón, las organizaciones deben identificar y satisfacer los requerimientos de la Seguridad de su Información, así como de todos sus activos. (IT Governance Institute, 2007). Según Chardon y González (2002), se define el concepto de amenaza como "un fenómeno de origen natural, socio-natural, tecnológico o antrópico en general, definido por su naturaleza, ubicación, recurrencia, probabilidad de ocurrencia, magnitud e intensidad (capacidad destructora)" y el concepto de vulnerabilidad como "la probabilidad que una comunidad, expuesta a una amenaza natural, tecnológica o antrópica más generalmente, según el grado de fragilidad de sus elementos (infraestructura, vivienda, actividades productivas, grado de organización, sistemas de alerta, desarrollo político institucional entre otros), pueda sufrir daños humanos y materiales en el momento del impacto del fenómeno". Si bien se define el término de vulnerabilidad en función de una comunidad, este podría ser también asociado a una determinada organización.

Para definir los requerimientos de Seguridad de la Información es fundamental identificar cuán importante es, ya que cuanto mayor es su valor, mayor es el impacto de los riesgos que la amenazan. (Asociación Española para la Calidad , 2013).

Las operaciones del negocio son alimentadas por la información y debería dársele la protección necesaria. Ligado a lo anterior, en 2000, Arribas señala lo siguiente: “La información interna es inherente a las organizaciones. Y es que, una empresa es, al fin y al cabo, un conjunto de personas que interaccionan intercambiando información.” De lo expuesto se puede extraer que una organización sin información no podría existir. Por tal razón, una empresa debe buscar maneras de almacenar y transferir la información considerando que, según ISO (2005b) sin importar los medios utilizados, los datos deben ser protegidos. La defensa de la información es una tarea esencial para asegurar la continuidad y el desarrollo del negocio. (AENOR, 2010).

Según ISO (2005a), la Seguridad de la Información es la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento. Por otro lado, el estándar ISO/IEC 27002:2005 complementa la definición dando un enfoque más comercial, al denominar la Seguridad de la Información como su protección ante amenazas para asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

De las definiciones brindadas de Seguridad de Información, se puede inferir que un atentado contra ella podría provocar pérdidas económicas en una entidad.

La necesidad de protección de los datos nace de la probabilidad que los riesgos que los rodean se materialicen. Podría decirse que la Seguridad de la Información se relaciona con la certeza y la falta de riesgo o contingencia, por lo tanto, Seguridad de la Información radica en minimizar esa incertidumbre que existe de que un riesgo se materialice. Se puede entender como seguridad un estado de cualquier sistema o tipo de información que indica que ese sistema o información está libre de riesgo. (Asociación Española para la Calidad , 2013).

La Asociación Española para la Calidad (2013), también aclara que la seguridad absoluta no es posible, no existe un sistema 100% seguro, de forma que el elemento de riesgo está siempre presente, independiente de las medidas que se tomen, por lo que se debe hablar de niveles de seguridad. Otro aspecto a considerar, es que la Seguridad de la Información cubre a la organización tanto interna como externamente. Es por ello que incluso la Seguridad de la Información puede ser un factor de imagen para la empresa, donde una certificación podría ser un factor importante de confianza para mantener y establecer relaciones comerciales. (Saint-Germain, 2005).

La Seguridad de la Información busca preservar tres características de esta, las cuales son: disponibilidad, integridad y confidencialidad, cuyos conceptos se describen a continuación, según ISO/IEC (2005a):

- Confidencialidad: La confidencialidad se define como el hecho que la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: El concepto de integridad, con respecto al tema de Seguridad de la Información como mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. En algunas referencias se suele utilizar la palabra exactitud como sinónimo de integridad en el contexto de Seguridad de la Información.
- Disponibilidad: En términos de Seguridad de la Información, se define disponibilidad como el acceso y utilización de la información y los sistemas de tratamiento de la misma por aquellos que lo requieran, siempre y cuando posean la debida autorización.

Bajo estas definiciones se plantea la idea de que la Seguridad de la Información debe garantizar la continuidad del negocio, asegurarse de mantener su operativa y permitir que las personas, sistemas y procesos tengan acceso a la información requerida, de acuerdo con sus roles y responsabilidades. Los conceptos de confiabilidad, integridad y disponibilidad son complementarios para poder caracterizar la información como segura.

Según ISO/IEC (2005b) “para lograr la Seguridad de la Información se debe implementar un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de *software* y *hardware*”. Además, se necesita establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario, para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

Existe una serie de factores críticos de éxito para la adecuada Gestión de la Seguridad de la Información. ISO/IEC (2005b) indica los siguientes:

- Política, objetivos y actividades de Seguridad de Información que reflejan los objetivos comerciales.
- Un enfoque y marco referencial para implementar, mantener, monitorear y mejorar la Seguridad de la Información que sea consistente con la cultura organizacional.
- Soporte visible y compromiso de todos los niveles de gestión.
- Un buen entendimiento de los requerimientos de Seguridad de la Información, evaluación del riesgo y gestión del riesgo.
- Mercadeo efectivo de la Seguridad de la Información con todos los gerentes, empleados y otras partes para lograr conciencia sobre el tema.
- Distribución de lineamientos sobre la política y los estándares de Seguridad de la Información para todos los gerentes, empleados y otras partes involucradas.
- Provisión para el financiamiento de las actividades de gestión de la Seguridad de la Información.
- Proveer el conocimiento, capacitación y educación apropiados.
- Establecer un proceso de gestión de incidentes de Seguridad de la Información.
- Implementación de un sistema de medición que se utiliza para evaluar el desempeño en la gestión de la Seguridad de la Información y retroalimentación de sugerencias para el mejoramiento.

2.1.1. Identificación de requerimientos de Seguridad de la Información

La Seguridad de la Información dentro de la empresa debe plantearse según su contexto, por lo cual, tomar un estándar, norma o metodología y adaptarlo a la organización no basta. Según ISO/IEC (2005b), existen tres fuentes de requerimientos organizacionales con respecto al tema de Seguridad de la Información, a continuación se describen estas fuentes:

- Riesgos organizacionales: La evaluación de riesgos permite identificar amenazas para los activos, se evalúa el impacto y probabilidad, esto se toma como insumo para definir requerimientos de Seguridad de la Información. También se requiere tomar en cuenta la estrategia y objetivos organizacionales.
- Otras fuentes son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio.
- Finalmente, la otra fuente definida por el estándar es el conjunto particular de principios, objetivos y requerimientos comerciales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

La Seguridad de la Información se basa principalmente en el proceso de administración del riesgo.

2.1.2. Administración de riesgos

El riesgo se define como la posibilidad que un evento ocurra y sea capaz de poner en peligro el cumplimiento de los objetivos de la organización. La organización debe establecer un sistema para minimizar el riesgo y no comprometer sus objetivos. (Mejía, 2004).

Este sistema organizacional para controlar el riesgo se conoce como *Administración de riesgos;* Mejía (2004) define el concepto como la coordinación de las acciones en una empresa, que permite manejar la incertidumbre a través del establecimiento de medidas para identificar, valorar y manejar los eventos potenciales que puedan presentarse y afectar el logro de sus objetivos.

La administración de riesgos es vital para el proceso de gestión de Seguridad de la Información, pues cada día existen más riesgos que amenazan, tanto a la información como a los medios de procesamiento de la misma; algunas amenazas son: ataques terroristas, fuego, inundaciones y terremotos, entre otros. (Saint-Germain, 2005).

Minimizar el riesgo y mantener la información crítica de manera confidencial, disponible y además íntegra, no es una tarea fácil dentro de la organización, por lo cual es recomendable establecer un Sistema de Gestión de Seguridad de la Información.

2.2. Sistema de Gestión de Seguridad de la Información

Un Sistema de Gestión de Seguridad de la Información, según ISO/IEC (2005b), está basado en el riesgo y tiene por objetivo establecer, implementar, operar, monitorear, mantener, revisar y mejorar la Seguridad de la Información.

2.2.1. Implementación de un Sistema de Gestión de Seguridad de la Información

El estándar ISO/IEC 27001:2005 propone adaptar el Sistema de Gestión de Seguridad de la Información al modelo de mejora continua PDCA o círculo de Deming, por lo que plantea cuatro fases por las que el SGSI debe ser sometido para mantener este modelo. En la Figura 3. Ciclo PDCA adaptado a un Sistema de Gestión de la Seguridad de la Información, se representa el modelo de mejora continua PDCA aplicado a un SGSI. Según Harrington, la mejora continua es “una metodología sistemática desarrollada para ayudar a una organización a tener avances significativos en la manera que operan sus procesos” (citado en Suárez y Ramis, 2008).

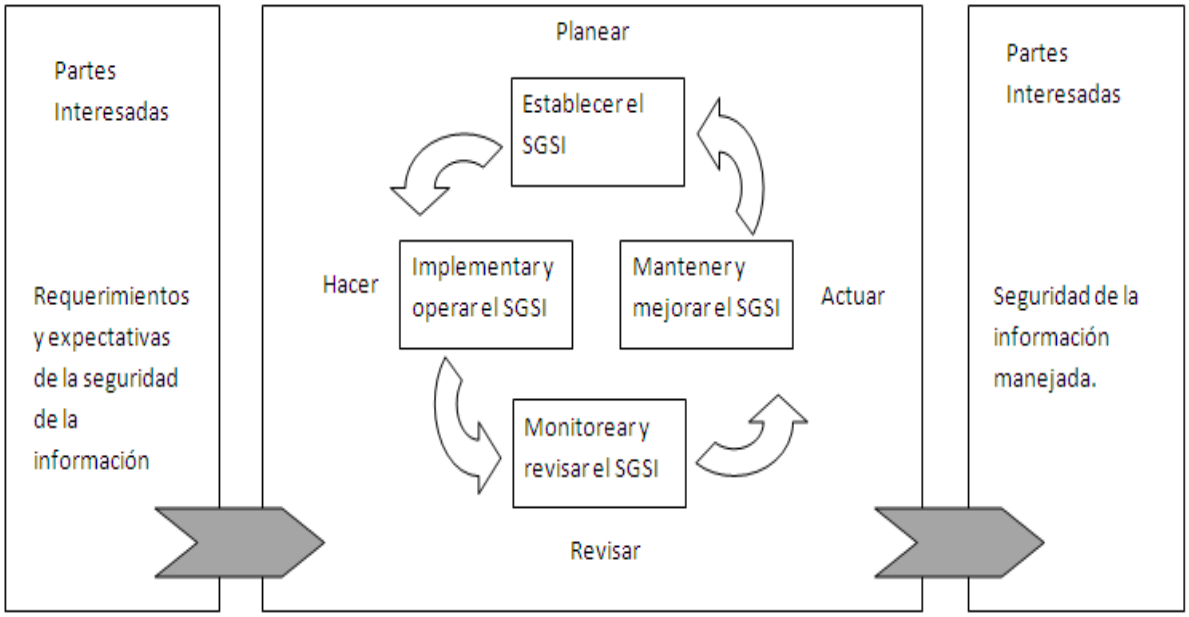


Figura 3. Ciclo PDCA adaptado a un Sistema de Gestión de la Seguridad de la Información
Fuente: (ISO/IEC, 2005a)

ISO (2005b) establece una serie de actividades para cada una de las fases requeridas en la adaptación del SGSI bajo el modelo PDCA. A continuación se enumeran algunas de estas:

2.2.1.1. Planear: Establecer el SGSI

La organización debe hacer lo siguiente en esta fase:

a) Definir el alcance y los límites del SGSI en términos de las características del negocio, la organización, su ubicación, activos, tecnología y además, definir qué aspectos se excluyen del alcance y su justificación.
b) Definir una política para el SGSI en términos de las características de la organización, su ubicación, activos y tecnología. Esta debe:
    1. Incluir un marco referencial para establecer sus objetivos y instaure un sentido de dirección general y principios para la acción en relación con la Seguridad de la Información.
    2. Tomar en cuenta los requerimientos comerciales y legales o reguladores y las obligaciones de la seguridad contractual.

3. Estar alineada con el contexto de gestión de riesgo estratégico de la organización en el cual se dará establecimiento y mantenimiento al SGSI.
4. Establecer el criterio con el que se evaluará el riesgo.
5. Ser aprobada por la gerencia.

c) Definir el enfoque de evaluación del riesgo de la organización. Esto implica:
   1. Identificar una metodología de cálculo del riesgo adecuado para el SGSI y los requerimientos identificados de seguridad, legales y reguladores de la información comercial.
   2. Desarrollar los criterios para aceptar los riesgos e identificar los niveles de riesgo aceptables.

d) Identificar los riesgos. Esta actividad requiere identificar lo siguiente:
   1. Los activos dentro del alcance del SGSI y los propietarios de estos activos.
   2. Las amenazas para aquellos activos.
   3. Las vulnerabilidades que podrían ser explotadas por las amenazas.
   4. Los impactos que pueden tener la pérdida de integridad, disponibilidad y confidencialidad de los activos.

e) Analizar y evaluar el riesgo, lo cual incluye calcular:
   1. El impacto comercial sobre la organización que podría resultar de una falla en la seguridad, tomando en cuenta una pérdida de integridad, disponibilidad o confidencialidad de los activos.
   2. La probabilidad realista de que ocurra dicha falla a la luz de las amenazas y probabilidades prevalecientes y los impactos asociados con estos activos y los controles implementados actualmente.
   3. Los niveles de riesgo.
   4. Y por último, determinar si el riesgo es aceptable o requiere tratamiento, utilizando el criterio de aceptación del riesgo definido dentro del SGSI.

f) Identificar y evaluar las opciones de tratamiento de riesgos. El estándar recomienda las siguientes opciones:
   1. Aplicar los controles apropiados.

2. Aceptar los riesgos consciente y objetivamente, siempre que satisfagan las políticas y criterios establecidos de aceptación del riesgo.
3. Evitar los riesgos.
4. Transferir los riesgos a otras entidades.

g) Seleccionar los objetivos de control y controles para el tratamiento de riesgos. El estándar ISO/IEC 27001:2005 recomienda una serie de objetivos de control y controles; sin embargo, es el estándar ISO/IEC 27002:2005 el que profundiza en ellos.
h) Obtener la aprobación de la gerencia para los riesgos residuales propuestos.
i) Obtener la autorización de la gerencia para la implementación y operación del SGSI.
j) Preparar un enunciado de aplicabilidad. Este debe contener lo siguiente:
   1. Los objetivos de control y controles seleccionados y la justificación de su selección.
   2. Los objetivos de control y controles implementados actualmente.
   3. La exclusión de objetivos de control y controles propuestos por el estándar y la justificación.

2.2.1.2. Hacer: Implementar y operar el SGSI

La organización debe hacer lo siguiente en esta fase:

a) Formular un plan de tratamiento de riesgo que identifique la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la Seguridad de la Información.
b) Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, los cuales incluyen tener en cuenta el financiamiento y asignación de roles y responsabilidades.
c) Implementar los controles seleccionados para satisfacer los objetivos de control.
d) Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo se van a utilizar dichas mediciones para evaluar la efectividad del control con el fin de producir resultados comparables y reproducibles.

e) Implementar los programas de capacitación y conocimiento.
f) Manejar las operaciones del SGSI.
g) Manejar los recursos del SGSI.
h) Implementar los procedimientos y otros controles capaces de permitir una pronta detección y respuesta a incidentes de seguridad.

2.2.1.3. Revisar: Monitorear y revisar el SGSI

La organización debe llevar a cabo en esta fase, las siguientes actividades:

a) Ejecutar procedimientos de monitoreo y revisión, además, controles con el objetivo de:
    1. Detectar prontamente los errores en los resultados de procesamiento.
    2. Identificar rápidamente los incidentes y violaciones de seguridad fallidas y exitosas.
    3. Permitir a la gerencia determinar si las actividades de seguridad, delegadas a las personas o implementadas, mediante la tecnología de información, se estén realizando como se esperaba.
    4. Ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad, mediante el uso de indicadores.
    5. Determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.
b) Realizar revisiones regulares de la efectividad del SGSI.
c) Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.
d) Revisar las evaluaciones del riesgo en los intervalos planeados y revisar el nivel de riesgo residual y aceptable identificados, tomando en cuenta los cambios en:

    1. La organización.
    2. Tecnología.
    3. Objetivos y procesos comerciales.
    4. Amenazas identificadas.

5. Efectividad de los controles implementados.
6. Eventos externos.

e) Realizar auditorías internas sobre el SGSI en los intervalos planeados.
f) Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso del SGSI.
g) Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.
h) Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI.

2.2.1.4. Actuar: Mantener y mejorar el SGSI

Aquí la organización debe realizar lo siguiente:

a) Implementar las mejoras identificadas para el SGSI.
b) Llevar a cabo las acciones preventivas y correctivas requeridas.
c) Comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo con las circunstancias y cuando sea relevante, acordar cómo proceder.
d) Asegurar que las mejoras cumplan con los objetivos planteados.

2.2.2. Requerimientos de documentación del Sistema de Gestión de Seguridad de la Información

La documentación de un Sistema de Gestión de la Seguridad de la Información, según ISO/IEC (2005a), debe incluir los registros de las decisiones gerenciales, asegurar que las acciones puedan ser asociadas a las decisiones políticas y tomadas por la gerencia y que los resultados registrados puedan ser reproducibles.

En el estándar ISO/IEC 27001:2005 se plantea que la documentación que debe incluir un SGSI sea la siguiente:

- Enunciados de la política de Seguridad de la Información y los objetivos del SGSI. La política de Seguridad de la Información se compone de un conjunto de políticas específicas, la cuales consisten en una intención y dirección general expresada formalmente por la gerencia.
- El alcance del SGSI.
- Procedimientos y controles de soporte del SGSI.
- Una descripción de la metodología de evaluación del riesgo.
- Reporte de la evaluación del riesgo.
- Plan de tratamiento del riesgo.
- Los procedimientos documentados necesarios para asegurar la planeación, operación y control de sus procesos de Seguridad de la Información y describir cómo medir la efectividad de sus controles.
- Registros requeridos por el estándar ISO/IEC 27001:2005.

2.3. Estándar ISO/IEC 27000

El concepto de estándar es definido como un documento establecido por consenso, aprobado por un cuerpo reconocido el cual ofrece reglas, guías o características para que se use repetidamente. (Project Management Institute, 2014). El conjunto de estándares ISO/IEC 27000, desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), proveen un marco de referencia para la gestión de Seguridad de la Información. (ISO 27000 Directory, 2013).

2.3.1. Conjunto de estándares que conforman la serie de normas ISO/IEC 27000

ISO/IEC 27000 está constituido por otros estándares cuya área de enfoque se mantiene dentro del alcance de la Seguridad de la Información. A continuación, basado en ISO 27000 Directory (2013), se hace una breve descripción de seis de los miembros de esta familia de estándares:

ISO/IEC 27001: El estándar fue publicado en octubre del 2005, como remplazo del estándar BS7799-2. Su contenido consiste en la especificación para un Sistema de Gestión de la Seguridad de la Información. Cabe mencionar que este estándar es certificable. El objetivo del estándar es proveer los requerimientos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información. La implementación de un SGSI basado en este estándar, debe ser una decisión estratégica; se deben considerar las necesidades y objetivos organizacionales, los requerimientos de seguridad, los procesos del negocio y además, el tamaño y estructura de la organización.

La versión 2005 del estándar toma como base el ciclo PDCA para estructurar el Sistema de Gestión de Seguridad de la Información. La versión del 2013 del estándar establece un énfasis especial en medir y evaluar el desempeño del Sistema de Gestión de Seguridad de la Información, además se agrega una sección sobre *outsourcing* y se le brinda atención especial al contexto organizacional de la Seguridad de la Información.

Para optar por una certificación, la organización debe pasar por todo un proceso de adaptación de su Sistema de Gestión de Seguridad de la Información basado en el estándar ISO/IEC 27001:2005. Este se puede observar en la Figura 4. Proceso de preparación para optar por una certificación ISO/IEC 27001 para un SGSI.

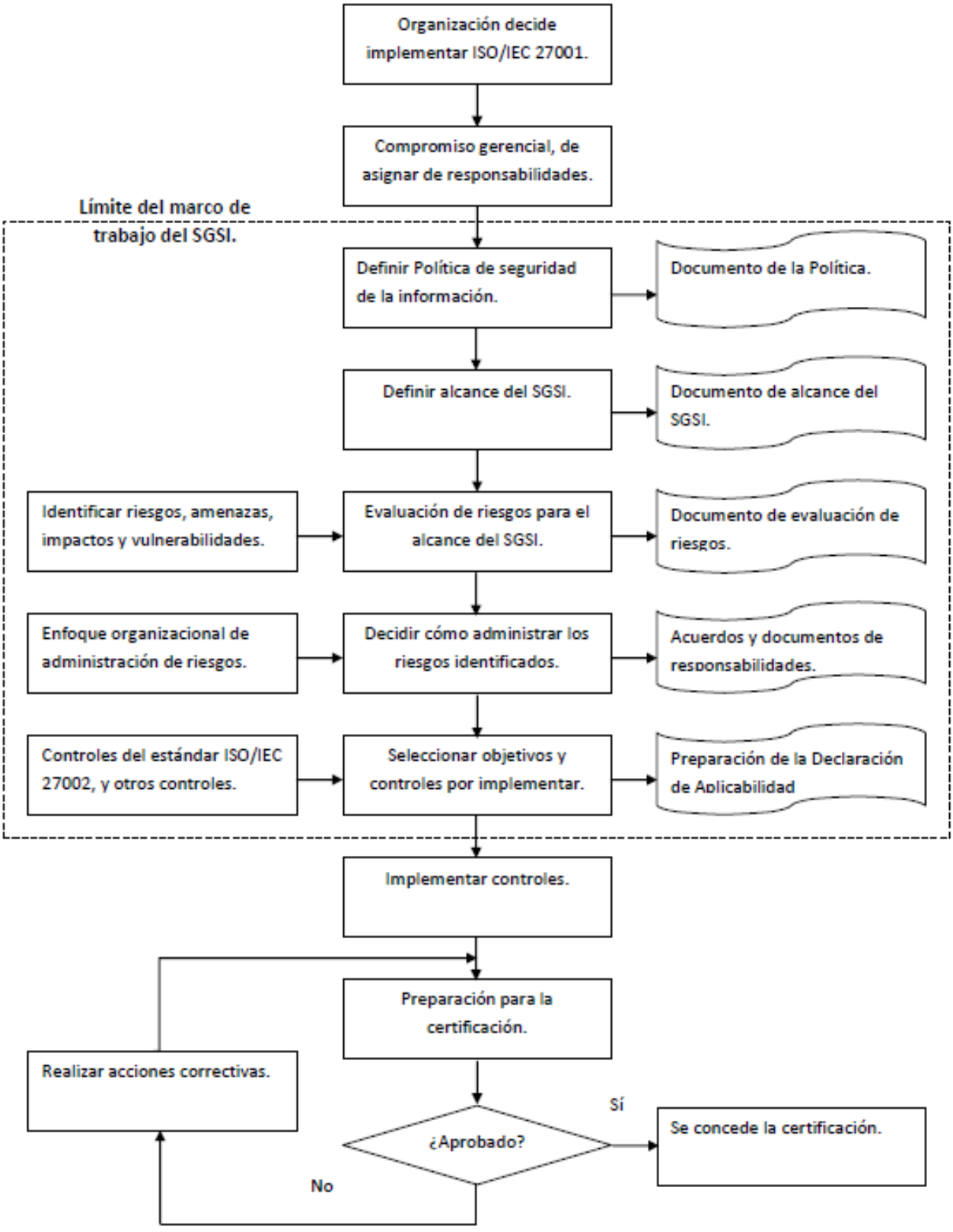


Figura 4. Proceso de preparación para optar por una certificación ISO/IEC 27001 para un SGSI
Fuente: (ISO 27000 Directory, 2013)

ISO/IEC 27002: El estándar ISO/IEC 27002 nace del renombramiento del antiguo ISO 17799. Su contenido radica principalmente en una serie de objetivos de control y controles que complementan lo establecido por el estándar ISO/IEC 27001.

La base de ISO 27002 fue un documento planteado por el gobierno del Reino Unido, hasta que en 1995 fue publicado como estándar por el BSI (British Standard Institute) bajo el nombre de BS7799. Para el año 2000, al estándar se le cambia nuevamente el nombre; sin embargo, no por el BSI, sino por ISO, el nombre asignado en ese momento fue ISO 17799. En el 2005 se lanza una nueva versión del estándar y posteriormente, se le cambio el nombre por ISO 27002. En el año 2013 se lanza la última versión del estándar. ISO/IEC 27002:2013 contiene 114 controles, a diferencia de la versión del 2005, el cual contiene 133. Otra diferencia es que la versión 2013 se estructura en 14 dominios, mientras que la versión anterior posee 11.

ISO/IEC 27003: El objetivo de ISO/IEC 27003 es proveer una ayuda y guía en la implementación de un Sistema de Gestión de Seguridad de la Información. Está enfocado en el ciclo PDCA, con respecto a establecer, implementar, revisar y mejorar el SGSI.

ISO/IEC 27004: Publicado en el 2009, ISO/IEC 27004 provee una guía en el desarrollo y uso de métricas para la valoración de la efectividad de los controles aplicados en el SGSI de una organización, en conformidad con ISO/IEC 27001. También posee un apéndice que contiene métricas, las cuales se pueden alinear al estándar ISO/IEC 27002.

ISO/IEC 27005: ISO/IEC 27005 está basado en la administración de riesgos de Seguridad de la Información. Este estándar provee una guía para administrar los riesgos de Seguridad de la Información, haciendo énfasis en el cumplimiento de los requerimientos del estándar ISO/IEC 27001.

ISO/IEC 27006: Este estándar ofrece una guía para la acreditación de entidades certificadoras de Sistemas de Gestión de Seguridad de la Información.

2.3.2. Costos y beneficios de la implementación de un SGSI basado en estándares ISO/IEC 27000

Se requiere implementar un sistema documentado que se enfoque en alcanzar los objetivos de seguridad, según ISOTools (2013), para la adecuada gestión de la Seguridad de la Información; este sistema puede plantearse, tomando como referencia los estándares ISO/IEC 27000. ISOTools indica que a pesar de los beneficios de este sistema basado en ISO/IEC 27000, existen actividades que generan una serie de costos. En la Tabla 1. Costos y beneficios de la implementación de un SGSI basado en ISO/IEC 27001:2005, se indican cuáles son las fuentes de costos y los beneficios de la implementación de un SGSI basado en ISO/IEC 27001.

Fuentes de costo	Beneficios
✓ Realización de inventarios, para conocer el valor de los activos totales de una empresa. Para ello, es necesario llevar a cabo la identificación, definición, descripción y valoración de los activos, lo que conlleva tiempo y costos. ✓ Implantar una mejora continua del sistema, requerida por la propia norma. ✓ Analizar los riesgos a los que se encuentran sometidas las empresas. ✓ Desarrollo de un plan de continuidad del negocio. ✓ Integrar diversos controles de seguridad y control de riesgos. ✓ Mantenimiento a largo plazo del sistema.	✓ Aumento de la competitividad en el mercado, proporciona diferenciación. ✓ La seguridad como un sistema metódico y controlado. ✓ Reducción de riesgos. ✓ Mayor compromiso de mantenimiento y mejora de la seguridad. ✓ Adaptación a la legislación vigente. ✓ Realización de auditorías externas, otorgan una visión diferente que se traduce en actividades de mejora interna. ✓ Acceso a un mayor número de clientes que exigen la acreditación en ISO 27001. ✓ Mayor efectividad y eficiencia en la resolución de incidencias.

Tabla 1. Costos y beneficios de la implementación de un SGSI basado en ISO/IEC 27001:2005
Fuente: (ISOTools, 2014)

2.3.3. Descripción detallada del estándar ISO/IEC 27002:2005

El estándar ISO/IEC 27002 fue inicialmente denominado ISO 17799. Este estándar provee una serie de controles y objetivos de control que se encuentran sujetos al estándar ISO/IEC 27000. (ISO 27000 Directory, 2013).

2.3.3.1. Alcance

ISO/IEC (2005b) define que el alcance del estándar ISO/IEC 27002:2005 es establecer los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la Seguridad de la Información en una organización. Los objetivos definidos en el estándar proporcionan un lineamiento general sobre los objetivos de gestión de Seguridad de la Información, generalmente aceptados. Los objetivos de control y los controles de este estándar internacional son diseñados para ser implementados y así, satisfacer los requerimientos identificados por una evaluación del riesgo.

2.3.3.2. Estructura del estándar

Es fundamental, para entender la estructura de este estándar, comprender los conceptos de dominio, objetivo de control, control y lineamiento de implementación. Los dominios se podrían definir como las áreas en las que se puede segmentar la Seguridad de la Información. Según ISO/IEC (2005b), en el estándar ISO/IEC 27002:2005, un objetivo de control es el establecimiento de lo que se debiera lograr con respecto a la Seguridad de la Información; un control define el enunciado de control específico para satisfacer el objetivo de control al cual está asociado; un lineamiento de implementación proporciona información más detallada para apoyar la implementación de un determinado control. A diferencia de la definición de un control del estándar, un control en general es un mecanismo utilizado para el tratamiento de los riesgos.

Cabe mencionar que un dominio se compone de uno o más objetivos de control, el cual se compone de uno o más controles y cada uno de ellos posee un lineamiento de implementación.

La estructura el estándar ISO/IEC 27002:2005 se divide en 11 dominios, los cuales se componen de 39 objetivos de control y estos a su vez en 133 controles. En la Figura 5. Ejemplo genérico de la estructura de un dominio del estándar ISO/IEC 27002:2005, se presenta un ejemplo sobre cómo se estructura un dominio del estándar ISO/IEC 27002:2005.

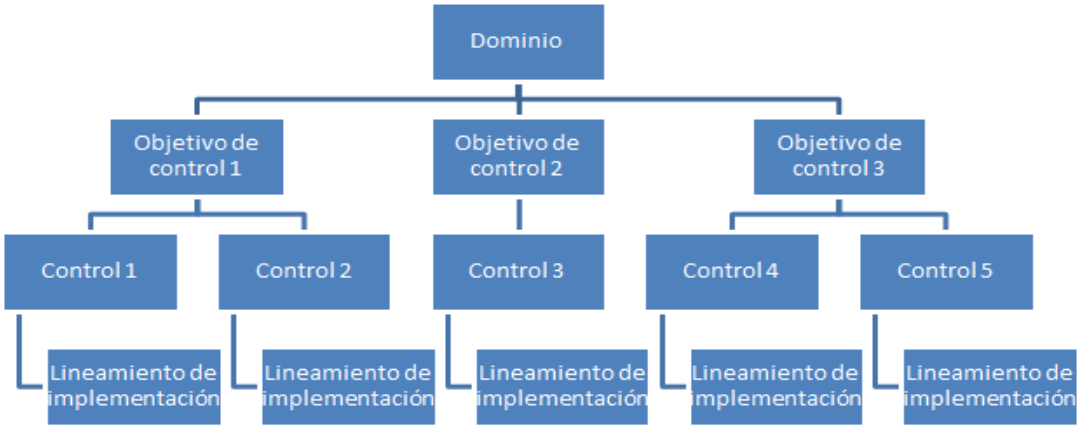


Figura 5. Ejemplo genérico de la estructura de un dominio del estándar ISO/IEC 27002:2005
Fuente: Elaboración propia

A continuación se hace una descripción de cada uno de los dominios del estándar ISO/IEC 27002:2005 y sus respectivos controles.

2.3.3.2.1. Política de seguridad

El objetivo de este dominio es garantizar a la organización el soporte y gestión necesarios para la Seguridad de la Información, según los requisitos institucionales y normativos. En este dominio se plantea una política que determina el compromiso organizacional con la gestión de la Seguridad de la Información. (ISOTools, 2013).

Según ISO/IEC (2005b), a continuación se enlistan los controles asociados al presente dominio, además de su correspondiente enunciado:

- **Documento de la política de Seguridad de la Información:** Este control indica que el documento de la política de Seguridad de la Información debiera ser aprobado por la gerencia y publicado y comunicado a todos los empleados y las partes externas relevantes.

- **Revisión de la política de Seguridad de la Información:** Este control indica que la política de Seguridad de la Información debiera ser revisada a intervalos planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

2.3.3.2.2. Organización de la Seguridad de la Información

El objetivo de este dominio es establecer un marco de referencia para definir el camino para la implementación y control de la Seguridad de la Información dentro de la organización. (ISOTools, 2013). Cabe mencionar que este es uno de los dominios de Seguridad de la Información para los cuales se plantearán las propuestas de mejora.

Según ISO/IEC (2005b), a continuación se enlistan los controles asociados al presente dominio, además de su correspondiente enunciado:

- **Compromiso de la gerencia con la Seguridad de la Información:** Apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la Seguridad de la Información.
- **Coordinación de la Seguridad de la Información:** Las actividades de la Seguridad de la Información debieran ser coordinadas por representantes de diferentes partes de la organización con roles y funciones laborales relevantes.
- **Asignación de las responsabilidades de la Seguridad de la Información:** Las responsabilidades de la Seguridad de la Información debieran estar claramente definidas.
- **Proceso de autorización para facilidades procesadoras de información:** Definir e implementar un proceso de la gerencia para la autorización de nuevas facilidades de procesamiento de información.
- **Acuerdos de confidencialidad:** Identificar y revisar regularmente que los requerimientos de confidencialidad o acuerdos de no-divulgación, reflejen las necesidades de la organización para proteger la información.

- **Contacto con las autoridades:** Mantener los contactos apropiados con las autoridades relevantes, esto en caso que se presente un incidente de Seguridad de la Información.
- **Contacto con grupos de interés especial:** Con el fin de mantener a la organización actualizada en el tema de Seguridad de la Información, se debieran mantener contactos apropiados con grupos de interés especial u otros foros especializados y asociaciones profesionales de seguridad.
- **Revisión independiente de la Seguridad de la Información:** Revisar el enfoque de la organización para manejar la Seguridad de la Información, así como la implementación de los distintos mecanismos para la Seguridad de la Información, de manera independiente a intervalos planeados o cuando ocurran cambios significativos en la implementación de la seguridad.
- **Identificación de los riesgos relacionados con los grupos externos:** Identificar los riesgos originarios de procesos comerciales que involucran a grupos externos y que pudiesen afectar a la información o a los medios de procesamiento.
- **Tratamiento de la seguridad cuando se lidia con clientes:** Tratar todos los requerimientos de seguridad identificados antes de proporcionar a los clientes el acceso a la información o a otros activos de la organización.
- **Tratamiento de la seguridad en acuerdos con terceros:** Los acuerdos o contratos con terceros que involucran el acceso, procesamiento, comunicación o manejo de la información o de los medios de procesamiento de información de la compañía, debieran abarcar todos los requerimientos de seguridad relevantes.

2.3.3.2.3. Gestión de activos

El objetivo de este dominio es realizar una protección adecuada de los activos de la organización. (ISOTools, 2013). Este es el segundo de ellos para los cuales se plantearán propuestas de mejora.

Según ISO/IEC (2005b), a continuación se enlistan los controles asociados al presente dominio, además de su correspondiente enunciado:

- **Inventario de los activos:** Identificar todos los activos y además, elaborar y mantener un inventario de todos los activos importantes.
- **Propiedad de los activos:** La información y los activos asociados con los medios de procesamiento de información debieran ser propiedad de una parte designada de la organización.
- **Uso aceptable de los activos:** Identificar, documentar e implementar reglas para el uso aceptable de la información y los medios del procesamiento de la información.
- **Lineamientos de clasificación:** Clasificar la información en términos de su valor, requerimientos legales, sensibilidad y grado crítico para la organización.
- **Etiquetado y manejo de la información:** Desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado y manejo de la información en concordancia con el esquema de clasificación adoptado por la organización.

2.3.3.2.4. Seguridad de recursos humanos

El objetivo de este dominio es fijar las medidas necesarias para controlar la Seguridad de la Información, que sea manejada por los recursos humanos de la organización.

Según ISO/IEC (2005b), a continuación se enlistan los controles asociados al presente dominio, además de su correspondiente enunciado:

- **Roles y responsabilidades:** Definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de Seguridad de la Información de la organización.

- **Investigación de antecedentes:** Que los chequeos de verificación de antecedentes de todos los candidatos para empleo, contratistas y terceros debieran llevarse a cabo en concordancia con las leyes, regulaciones y ética relevantes y convinieran ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
- **Términos y condiciones del empleo:** Como parte de su obligación contractual; los usuarios empleados, contratistas y terceros, debieran aceptar y firmar un contrato con los términos y condiciones de su empleo, el cual debiera establecer sus responsabilidades y las de la organización para la Seguridad de la Información.
- **Responsabilidades de la gerencia:** Que la misma debiera requerir a los usuarios empleados, contratistas y terceras personas que apliquen la seguridad en concordancia con políticas y procedimientos bien establecidos por la organización.
- **Conocimiento, educación y capacitación en Seguridad de la Información:** Implica que todos los empleados de la organización y cuando sea relevante, los contratistas y terceras personas debieran recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales, conforme sea relevante para su función laboral.
- **Proceso disciplinario:** Debe existir un proceso disciplinario para los empleados que han cometido un incumplimiento de la seguridad.
- **Responsabilidades de terminación:** Definir y asignar claramente las responsabilidades en caso de la terminación del empleo o el cambio de empleo.
- **Devolución de los activos:** Que todos los usuarios empleados, contratistas y terceras personas debieran devolver todos los activos de la organización que tengan en su posesión a la terminación de su empleo, contrato o acuerdo.

- **Retiro de los derechos de acceso:** Que los derechos de acceso de todos los usuarios empleados, contratistas y terceras personas a la información y los medios de procesamiento de información debieran ser retirados a la terminación de su empleo, contrato o acuerdo; o debieran ser reajustados en caso de ser un cambio empleo.

2.3.3.2.5. Seguridad física y ambiental

El objetivo de este dominio es proteger a las instalaciones de la organización y a toda la información que maneja. (ISOTools, 2013).

Según ISO/IEC (2005b), a continuación se enlistan los controles asociados al presente dominio, además de su correspondiente enunciado:

- **Perímetro de seguridad física:** Utilizar perímetros de seguridad para proteger las áreas que contienen información y medios de procesamiento de información.
- **Controles de ingreso físico:** Las áreas seguras debieran protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.
- **Asegurar las oficinas, habitaciones y medios:** Diseñar y aplicar seguridad física a oficinas, habitaciones y medios.
- **Protección contra amenazas externas e internas:** Asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.
- **Trabajo en áreas seguras:** Diseñar y aplicar la protección física y los lineamientos adecuados para trabajar en áreas aseguradas.
- **Áreas de acceso público, entrega y carga:** Controlar los puntos de acceso como las áreas de entrega y carga y otros puntos por donde personas no-autorizadas puedan ingresar al local y si fuese posible, aislarse de los medios de procesamiento de información para evitar el acceso no autorizado.

- **Ubicación y protección del equipo:** Ubicar o proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no-autorizado.
- **Servicios públicos de soporte:** Proteger el equipo de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte.
- **Seguridad del cableado:** El cableado de la energía y las telecomunicaciones que transportan datos o dan soporte a los servicios de información debieran protegerse contra la intercepción o daño.
- **Mantenimiento de equipo:** Mantener correctamente el equipo para asegurar su continua disponibilidad e integridad.
- **Seguridad del equipo fuera del local:** Aplicar controles de seguridad al equipo fuera del local, tomando en cuenta los diferentes riesgos de trabajar fuera las instalaciones físicas de la organización.
- **Seguridad de la eliminación o re-uso del equipo:** Chequear los ítems del equipo que contiene medios de almacenaje para asegurar que se haya retirado o sobre-escrito cualquier información confidencial o licencia de *software* antes de su eliminación.
- **Retiro de propiedad:** Que el equipo, información o *software* no debieran retirarse sin autorización previa.

2.3.3.2.6. Gestión de las comunicaciones y operaciones

El objetivo de este dominio es determinar los procedimientos y responsabilidades de las operaciones que realiza la organización, asegurándose que todos los procesos que estén relacionados con la información, se ejecuten adecuadamente. (ISOTools, 2013).

Según ISO/IEC (2005b), a continuación se enlistan los controles asociados al presente dominio, además de su correspondiente enunciado:

- **Procedimientos de operación documentados:** Los procedimientos de operación se debieran documentar, mantener y poner a disposición de todos los usuarios que los necesiten.
- **Gestión del cambio:** Controlar los cambios en los medios y sistemas de procesamiento de la información.
- **Segregación de los deberes:** Los deberes y áreas de responsabilidad debieran estar segregados para reducir las oportunidades de una modificación no-autorizada o mal uso no-intencional o mal uso de los activos de la organización.
- **Separación de los medios de desarrollo, prueba y operación:** Los medios de desarrollo, prueba y operación debieran estar separados para reducir los riesgos de acceso no-autorizado o cambios en el sistema operacional.
- **Entrega del servicio:** Asegurar que los controles de seguridad, definiciones del servicio y niveles de entrega incluidos en el acuerdo de entrega del servicio de terceros se implementen, operen y mantengan.
- **Monitoreo y revisión de los servicios de terceros:** Los servicios, reportes y registros provistos por terceros debieran ser monitoreados y revisados regularmente y se debieran llevar a cabo auditorías con regularidad.
- **Manejo de cambios en los servicios de terceros:** Manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de Seguridad de la Información existentes, teniendo en cuenta el grado crítico de los sistemas y procesos del negocio involucrados y la re-evaluación de los riesgos.
- **Gestión de la capacidad:** Monitorear, afinar el uso de los recursos y se debieran realizar proyecciones de los requerimientos de capacidad futura para asegurar el desempeño requerido del sistema.

- **Aceptación del sistema:** Establecer el criterio de aceptación de los sistemas de información nuevos, actualizaciones o versiones nuevas y se realizar pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación.
- **Controles contra códigos maliciosos:** Instaurar medidas de detección, prevención y recuperación para la protección contra códigos maliciosos y e implementar procedimientos para el apropiado conocimiento del usuario.
- **Controles contra códigos móviles:** Que donde se autorice el uso del código móvil, la configuración debiera asegurar que el autorizado opere de acuerdo con una política de seguridad definida y se debiera evitar la ejecución del código móvil no-autorizado.
- **Respaldos:** Hacer copias de respaldo de la información y *software* y se probar regularmente en concordancia con la política acordada de copias de respaldo.
- **Controles de redes:** Las redes debieran ser manejadas adecuadamente y controladas para proteger la información en ellas y mantener la seguridad de los sistemas y aplicaciones que hacen uso de la red.
- **Seguridad de los servicios de la red:** En todo contrato de redes se debieran identificar e incluir las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de red, ya sea que los servicios sean provistos interna o externamente.
- **Gestión de medios removibles:** Debieran existir procedimientos para la gestión de los medios removibles.
- **Procedimientos para el manejo de información:** Establecer los procedimientos para el manejo y almacenaje de información para protegerla de una divulgación no-autorizada o de un mal uso.
- **Seguridad de la documentación del sistema:** Proteger la documentación del sistema de accesos no-autorizados.
- **Políticas y procedimientos de intercambio de información:** Establecer políticas, procedimientos y controles de intercambio de información formales para su protección.

- **Acuerdos de intercambio:** Indica una serie de consideraciones a tomar en cuenta para la definición de acuerdos de intercambio.
- **Medios físicos en tránsito:** Que los medios que contienen información debieran ser protegidos contra accesos no-autorizados, mal uso o corrupción, durante el transporte más allá de los límites físicos de una organización.
- **Mensajes electrónicos:** Proteger adecuadamente la información involucrada en mensajes electrónicos.
- **Sistemas de información comercial:** Desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.
- **Comercio electrónico:** La información involucrada en el comercio electrónico que pasa a través de redes públicas debiera protegerse de la actividad fraudulenta, disputas de contratos, divulgación no-autorizada y modificación.
- **Transacciones en-línea:** Proteger la información involucrada en las transacciones en-línea para evitar una transmisión incompleta, *routing* equivocado, alteración no-autorizada del mensaje, divulgación no-autorizada, duplicación o repetición no-autorizada del mensaje.
- **Información públicamente disponible:** Resguardar la integridad de la información puesta a disposición en un sistema públicamente disponible para evitar una modificación no-autorizada.
- **Registro de auditoría:** Producir y mantener registros de auditoría de las actividades, excepciones y eventos de Seguridad de la Información, durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
- **Uso del sistema de monitoreo:** Establecer procedimientos para el monitoreo del uso de los medios de procesamiento de la información y se revisar regularmente los resultados de las actividades de monitoreo.
- **Protección del registro de información:** Proteger los medios y la información del registro para evitar la alteración y el acceso no autorizado.

- **Registros del administrador y operador:** Registrar las actividades del administrador del sistema y el operador del sistema.
- **Registro de fallas:** Registrar y analizar las fallas y tomar las acciones necesarias.
- **Sincronización de relojes:** Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización se debieran sincronizar con una fuente que proporcione la hora exacta acordada.

2.3.3.2.7. Control de acceso

El objetivo de este dominio es asegurar que sólo se permita el acceso autorizado a los sistemas de información de la organización. (ISOTools, 2013).

Según ISO/IEC (2005b), a continuación se enlistan los controles asociados al presente dominio, además de su correspondiente enunciado:

- **Política de control del acceso:** Establecer, documentar y revisar la política de control de acceso con base en los requerimientos comerciales y de seguridad para el acceso.
- **Registro del usuario:** Debiera existir un procedimiento formal para el registro y des-registro del usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información.
- **Gestión de privilegios:** Restringir y controlar la asignación y uso de privilegios.
- **Gestión de las claves secretas de los usuarios:** La asignación de claves secretas se debiera controlar a través de un proceso de gestión formal.
- **Revisión de los derechos de acceso del usuario:** La gerencia debiera revisar los derechos de acceso de los usuarios en intervalos regulares y utilizando un proceso formal.
- **Uso de claves secretas:** Se debiera requerir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de claves secretas.

- **Equipo del usuario desatendido:** Asegurar que el equipo desatendido tenga la protección apropiada.
- **Política de escritorio y pantalla limpios:** Adoptar una política de escritorio limpio para papeles y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
- **Política sobre el uso de los servicios de la red:** Los usuarios sólo debieran tener acceso a los servicios para los cuales hayan sido específicamente autorizados.
- **Autenticación del usuario para las conexiones externas**: Utilizar métodos de autenticación apropiados para controlar el acceso de usuarios remotos.
- **Identificación del equipo en las redes:** La identificación automática del equipo se debiera considerar como un medio para autenticar las conexiones de ubicaciones y equipos específicos.
- **Protección del puerto de diagnóstico y configuración remota:** Controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
- **Segregación en redes:** Los grupos de servicios de información, usuarios y sistemas de información debieran ser segregados en redes.
- **Control de conexión a la red:** Para las redes compartidas, especialmente aquellas que se extienden a través de las fronteras de la organización, se debiera restringir la capacidad de los usuarios para conectarse a la red, en línea con la política de control de acceso y los requerimientos de las aplicaciones comerciales.
- **Control de *routing* de la red:** Implementar controles de *routing* en las redes para asegurar que las conexiones de la computadora y los flujos de información no violen la política de control de acceso de las aplicaciones comerciales.
- **Procedimientos para un registro seguro:** El acceso a los sistemas operativos debiera ser controlado mediante un procedimiento de registro seguro.

- **Identificación y autenticación del usuario:** Todos los usuarios tienen un identificador único (ID de usuario) para su uso personal y acceso a sistemas operativos y se debiera escoger una técnica de autenticación adecuada para sustanciar la identidad de un usuario.
- **Sistema de gestión de claves secretas:** Los sistemas para el manejo de claves secretas para acceso a sistemas operativos debieran ser interactivos y asegurar que se establezcan claves secretas adecuadas.
- **Uso de las utilidades del sistema:** Restringir y controlar estrechamente el uso de los programas de utilidad que podrían ser capaces de superar los controles del sistema y la aplicación.
- **Cierre de una sesión por inactividad:** Las sesiones inactivas debieran ser cerradas después de un período de inactividad definido.
- **Limitación del tiempo de conexión:** Utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional para las aplicaciones de alto riesgo.
- **Restricción del acceso a la información:** El acceso de los usuarios y el personal de soporte a la información y las funciones del sistema de la aplicación debiera limitarse en concordancia con la política de control de acceso definida.
- **Aislar el sistema confidencial:** Los sistemas confidenciales debieran tener un ambiente de cómputo aislado.
- **Computación y comunicaciones móviles:** Establecer una política y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móvil.
- **Teletrabajo:** Desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de teletrabajo.

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

El objetivo de este dominio es establecer los requisitos en la etapa de implementación o desarrollo del *software* para que este sea seguro. (ISOTools, 2013).

Según ISO/IEC (2005b), a continuación se enlistan los controles asociados al presente dominio, además de su correspondiente enunciado:

- **Análisis y especificación de los requerimientos de seguridad:** Los enunciados de los requerimientos comerciales para los sistemas de información nuevos o las mejoras a los sistemas de información existentes, debieran especificar los requerimientos de los controles de seguridad.
- **Validación de los datos de entrada:** Validar los datos de entrada para las aplicaciones.
- **Control del procesamiento interno:** Los chequeos de validación se debieran incorporar en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.
- **Integridad del mensaje:** Identificar los requerimientos para asegurar la autenticidad y proteger la integridad de los mensajes en las aplicaciones e identificar e implementar los controles apropiados.
- **Validación de los datos de salida:** Este control indica que se debieran validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada sea el correcto y el apropiado para las circunstancias.
- **Política sobre el uso de controles criptográficos:** Desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.
- **Gestión de claves:** Establecer la gestión de claves para dar soporte al uso de técnicas criptográficas en la organización.
- **Control del *software* operacional:** Implantar procedimientos para el control de la instalación del *software* en ambientes operacionales.

- **Protección de la data del sistema:** Los datos de prueba se debieran seleccionar cuidadosamente y se debieran proteger y controlar.
- **Control de acceso al código fuente del programa:** Restringir el acceso al código fuente del programa.
- **Procedimientos del control del cambio:** Controlar la implementación de los cambios, mediante el uso de procedimientos formales para el control del cambio.
- **Revisión técnica de la aplicación después de cambios en el sistema:** Cuando se cambian los sistemas de operación, se debieran revisar y probar las aplicaciones comerciales críticas para asegurar que no exista un impacto adverso sobre las operaciones organizacionales o en la seguridad.
- **Restricciones sobre los cambios en los paquetes de *software*:** No se debiera fomentar modificaciones a los paquetes de *software*, limitarse a los cambios necesarios y ser estrictamente controlados.
- **Filtración de información:** Evitar las oportunidades para la filtración de información.
- **Desarrollo de *software* abastecido externamente:** El desarrollo del *software* abastecido externamente debiera ser supervisado y monitoreado por la organización.
- **Control de las vulnerabilidades técnicas:** Obtener oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando, evitar la exposición de la organización a dichas vulnerabilidades y adoptar las medidas apropiadas tomadas para tratar los riesgos asociados.

2.3.3.2.9. Gestión de incidentes de la Seguridad de la Información

El objetivo de este dominio es aplicar un proceso de mejora continua en la gestión de incidentes de Seguridad de la Información. (ISOTools, 2013).

Según ISO/IEC (2005b), a continuación se enlistan los controles asociados al presente dominio, además de su correspondiente enunciado:

- **Reporte de eventos en la Seguridad de la Información:** Indica que los eventos de Seguridad de la Información debieran ser reportados a través de los canales gerenciales apropiados lo más pronto posible.
- **Reporte de las debilidades en la seguridad:** Se debiera requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información, tomen nota y reporten cualquier debilidad de seguridad observada o sospechosa en el sistema o los servicios.
- **Responsabilidades y procedimientos:** La gerencia debiera establecer las responsabilidades y los procedimientos para asegurar una respuesta rápida, efectiva y metódica ante los incidentes de Seguridad de la Información.
- **Aprendizaje de los incidentes en la Seguridad de la Información:** Establecer mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la Seguridad de la Información.
- **Recolección de evidencia:** Cuando una acción de seguimiento contra una persona u organización después de un incidente en la Seguridad de la Información involucra una acción legal (ya sea civil o criminal), se debiera recolectar, mantener y presentar la certeza para cumplir con las reglas de evidencia establecidas en la jurisdicción relevante.

2.3.3.2.10. Gestión de la continuidad del negocio

El objetivo de este dominio es asegurar la continuidad operativa de la organización. (ISOTools, 2013).

Según ISO/IEC (2005b), a continuación se enlistan los controles asociados al presente dominio, además de su correspondiente enunciado:

- **Incluir la Seguridad de la Información en el proceso de gestión de continuidad del negocio:** Desarrollar y mantener un proceso gerencial para la continuidad del negocio en toda la organización para tratar los requerimientos de Seguridad de la Información necesarios para la continuidad comercial de la organización.

- **Continuidad del negocio y evaluación del riesgo:** Identificar los eventos que pueden causar interrupciones a los procesos comerciales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la Seguridad de la Información.
- **Desarrollar e implementar los planes de continuidad, incluyendo la Seguridad de la Información:** Desarrollar e implementar planes para mantener restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla de los procesos comerciales críticos.
- **Marco referencial de la planeación de la continuidad del negocio:** Mantener un solo marco referencial de los planes de continuidad del negocio para asegurar que todos los planes sean consistentes, tratar consistentemente los requerimientos de Seguridad de la Información e identificar las prioridades para la prueba y el mantenimiento.
- **Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio:** Los planes de continuidad del negocio debieran ser probados y actualizados regularmente para asegurar que sean efectivos.

2.3.3.2.11. Cumplimiento

El objetivo de este dominio es asegurar que los requisitos legales de seguridad referidos al diseño, operación, uso y gestión de los sistemas de información se cumplan. (ISOTools, 2013).

Según ISO/IEC (2005b), a continuación se enlistan los controles asociados al presente dominio, además de su correspondiente enunciado:

- **Identificación de la legislación aplicable:** Definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales relevantes y el enfoque de la organización para satisfacer esos requerimientos, para cada sistema de información y la organización.
- **Protección de registros organizacionales:** Proteger los registros importantes de pérdida, destrucción, falsificación; en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.

- **Protección de la *data* y privacidad de la información personal:** Asegurar la protección y privacidad de los datos conforme lo requiera la legislación, regulaciones y si fuesen aplicables, las cláusulas contractuales relevantes.
- **Prevención del mal uso de los medios de procesamiento de la información:** Disuadir a los usuarios de utilizar los medios de procesamiento de la información para propósitos no autorizados.
- **Regulación de controles criptográficos:** Los controles criptográficos se debieran utilizar en cumplimiento con todos los acuerdos, leyes y regulaciones relevantes.
- **Cumplimiento con las políticas y estándares de seguridad:** Los gerentes debieran asegurar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para asegurar el cumplimiento de las políticas y estándares de seguridad.
- **Chequeo del cumplimiento técnico:** Los sistemas de información debieran chequearse regularmente para ver el cumplimiento de los estándares de implementación de la seguridad.
- **Controles de auditoría de los sistemas de información:** Las actividades y requerimientos de auditoría que involucran chequeos de los sistemas operacionales debieran ser planeados y acordados cuidadosamente para minimizar el riesgo de interrupciones en los procesos comerciales.
- **Protección de las herramientas de auditoría de los sistemas de información:** Proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o trasgresión posible.

El estándar ISO/IEC 27002:2005 es el marco de referencia que va a ser utilizado en el presente proyecto; sin embargo, existen otros marcos de referencia que indican cómo gestionar la Seguridad de la Información en una organización. Estos marcos de referencia no se enfocan por completo en la Seguridad de la Información, pero sí pueden ser utilizados como una base para ciertos criterios.

Capítulo III: Marco metodológico

Se hace una descripción del marco metodológico aplicado en el presente proyecto en esta sección del documento. Se concibe una descripción de la investigación realizada, se detalla la metodología aplicada, así como las fuentes y técnicas para obtener la información utilizada en el proyecto.

3.1. Investigación

Se documenta en esta sección, el tipo de investigación así como su diseño.

3.1.1. Tipo de investigación

Se utilizó un tipo de investigación cualitativa para el presente proyecto. Se identifica como cualitativo, basándose en la descripción, según Vera (2008), donde indica que un estudio cualitativo es aquel donde se estudia la calidad de las actividades, relaciones, asuntos, medios, materiales o instrumentos en una determinada situación o problema.

Según Hernández, Fernández y Baptista (2010), un enfoque cualitativo se selecciona cuando se busca comprender la perspectiva de los participantes acerca de los fenómenos que los rodean, profundizar en sus experiencias, perspectivas, opiniones y significados, es decir, la forma en que los participantes perciben subjetivamente su realidad. Además, los autores indican que la investigación cualitativa utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación; también definen el concepto de datos cualitativos como “descripciones detalladas de situaciones, eventos, personas, interacciones, conductas observadas y sus manifestaciones.” Del mismo modo, una de las características de una investigación cualitativa es que “el investigador cualitativo utiliza técnicas para recolectar datos, como la observación no estructurada, entrevistas abiertas, revisión de documentos, discusión en grupo, evaluación de experiencias personales, registro de historias de vida, e interacción e introspección con grupos o comunidades.”

Se selecciona el tipo de estudio cualitativo, pues en este proyecto se busca valorar la completitud de las políticas de Seguridad de la Información del Banco Central de Costa Rica con respecto al estándar ISO/IEC 27002:2005. La recolección de datos no va a depender de mediciones numéricas, sino más bien del estudio de documentación, complementado con entrevistas, las cuales son técnicas de recolección de datos cualitativos.

3.1.2. Diseño de la investigación

El diseño de la investigación de este proyecto se cataloga como investigación acción.

La investigación-acción se enfoca en resolver problemas cotidianos y su propósito fundamental es brindar información que soporte la toma de decisiones para programas, procesos y reformas estructurales. Según Stringer, “las tres fases esenciales de los diseños de investigación-acción son: *observar* (construir un bosquejo del problema y recolectar datos), *pensar* (analizar e interpretar) y *actuar* (resolver problemas e implementar mejoras), las cuales se dan de manera cíclica, una y otra vez, hasta que el problema es resuelto, el cambio se logra o la mejora se introduce satisfactoriamente”. (Citado en Hernández, Fernández y Baptista, 2010).

El diseño de la investigación se identifica como investigación acción, pues los resultados van a ser utilizados por el Departamento de Calidad del Banco Central de Costa Rica para tomar decisiones y mejorar en el siguiente periodo las políticas de Seguridad de la Información de la entidad. Asimismo, el proyecto se pudo resumir en las tres fases de una investigación-acción de la siguiente manera:

- Observar: Se estudió documentación y se recolectaron datos
- Pensar: Se analizaron los datos de la valoración realizada y se interpretaron.
- Actuar: Se propusieron recomendaciones para la mejora de las Políticas específicas de la Seguridad de la Información de la Institución.

3.2. Descripción de la metodología utilizada

Se planteó una metodología que tuviese como fin identificar su brecha con los controles propuestos por el estándar ISO/IEC 27002:2005, para realizar la valoración de las Políticas Específicas de Seguridad de la Información y documentos complementarios.

El objetivo es diagnosticar la brecha entre la documentación que sustenta la Seguridad de la Información en el Banco con respecto al estándar ISO/IEC 27002:2005, generar propuestas de mejora y alinearlas a los intereses de la institución a partir de reuniones de revisión y aceptación.

A continuación se describen los pasos requeridos para llevar a cabo el proyecto:

1. **Identificar y definir el problema del Banco Central a de Costa Rica:**
   En esta fase se identificó, especificó y documentó el problema que la institución deseaba resolver. Fue primordial definir el alcance del problema para posteriormente llevar a cabo actividades que lo pudieron resolver. Estas se plantearon a partir de los objetivos del proyecto, lo cual permitiría que fueran alcanzados. Para cumplir el objetivo de esta fase se realizaron reuniones con Franklin Giralt Amador, Director del Departamento de Calidad del banco, además, patrocinador del proyecto y con Ricardo Morales Rojas, colaborador del departamento.

   En esta fase se hizo una selección de los dominios del estándar ISO/IEC 27002:2005, bajo los cuales se deseaba que se plantearan mejoras para las políticas de Seguridad de la Información de la Institución.

2. **Estudiar el documento ISO/IEC 27002:2005 y otras referencias:**
   Conociendo el problema que se deseaba resolver, fue necesario investigar y adquirir el conocimiento para brindar una posible solución. En esta fase del proyecto se adquirió dicho conocimiento, base para el desarrollo del mismo.

Se consideró fundamental el estudio del estándar ISO/IEC 27002:2005, pues era el documento referencia para la evaluación de las Políticas Específicas de Seguridad de la Información y los documentos complementarios del Banco Central de Costa Rica. Además, se investigaron otras fuentes y marcos de referencia que brindaran datos relevantes sobre Seguridad de la Información, con el fin de generar una base integral sobre el tema, fundamentada en diversas visiones y enfoques.

3. **Identificar controles del estándar ISO/IEC 27002:2005 no contemplados en el documento de Políticas Específicas de Seguridad de la Información del Banco Central de Costa Rica:**

   La Política de Seguridad de la Información del Banco Central de Costa Rica, en general, está dada por un documento denominado “Políticas Específicas de Seguridad de la Información”. En la última evaluación de las Políticas Específicas de Seguridad de la Información, previa a este proyecto, se identificaron controles del estándar ISO/IEC 27002:2005 que no pudieron asociarse a ninguna política, control o lineamiento de dicho documento, pero sí a otros instrumentos de la institución.

   En este paso se realizó un listado de dichos controles no cubiertos por las Políticas Específicas de Seguridad de la Información y se logró, haciendo lectura y análisis del informe de la evaluación realizada a inicios del presente año sobre este documento.

4. **Identificar documentos complementarios a las Políticas Específicas de Seguridad de la Información, según los dominios del estándar ISO/IEC 27002:2005.**

   Se identificaron otros documentos que los cubrieran a partir del listado de controles no cubiertos por las Políticas Específicas de Seguridad de la Información. La identificación de estos se realizó a partir de reuniones con Ricardo Morales, colaborador del Departamento de Gestión de Calidad, quien ejecutó la última evaluación de Políticas Específicas de Seguridad de la Información del banco.

5. **Desarrollo de herramienta de evaluación:**

   Esta herramienta permitió determinar cuáles controles del estándar ISO/IEC 27002:2005 no se contemplan en la documentación del Banco Central de Costa Rica. Para realizarla, se hizo lectura y estudio del estándar. Además, se hicieron revisiones de dicha herramienta con don Franklin Giralt, Director del Departamento de Gestión de Calidad del Banco, para validar su estructura y funcionamiento.

6. **Valoración de las Políticas Específicas de Seguridad de la Información y documentos complementarios:**

   Se aplicó en esta fase, la herramienta de evaluación desarrollada. El objetivo era identificar y documentar cuáles controles del estándar ISO/IEC 27002:2005 se contemplaban, ya fuera parcial o totalmente y cuáles no se abarcaban en los documentos evaluados. Además, se documentaba, dentro de la herramienta, las observaciones relevantes que pudieran incidir posteriormente en el proyecto, así como la evidencia que permitiera definir que un control se contemplaba parcial o totalmente. En esta fase se identificó la brecha entre las Políticas Específicas de Seguridad de la Información del Banco y el estándar ISO/IEC 27002:2005.

7. **Documentación de brecha:**

   Se procedió a documentar la brecha identificada cuando se aplicó la herramienta de evaluación. Este informe indicó por cada dominio del estándar, qué porcentaje de controles se cubrían en las políticas de Seguridad de la Información del banco. Se hizo uso de gráficos que reflejaran esta brecha. Además, por cada control cubierto parcialmente o no cubierto, se documentaba cuáles aspectos hicieron falta para alcanzar una cobertura total.

8. **Desarrollo de propuestas de mejora.**

   Se realizaron las propuestas de mejora para los dominios del estándar catalogados como prioritarios para el Banco Central de Costa Rica. Estas propuestas se desarrollaron a partir de los resultados obtenidos de la valoración de las Políticas Específicas de Seguridad de la Información del banco y los documentos complementarios y su objetivo fue establecer mejoras específicas para la gestión de la Seguridad de la Información a través de los dominios prioritarios.

9. **Reuniones para la validación de las propuestas de mejora:**

   Se realizaron reuniones con Franklin Giralt Amador, Director del Departamento de Gestión de Calidad, y con Carolina Jiménez Chacón, colaboradora del mismo departamento, para filtrar las propuestas de mejora planteadas para las Políticas específicas de la Seguridad de la Información y alinearlas a los esfuerzos institucionales.

10. **Depuración y documentación final de propuestas de mejora para las políticas de Seguridad de la Información**:

    Se depuraron las propuestas de mejora y se documentaron. La priorización y ajustes se realizaron a partir del análisis de los resultados obtenidos de las revisiones realizadas.

La Figura 6. Metodología utilizada en el desarrollo del proyecto, describe a alto nivel el modelo de la metodología aplicada:

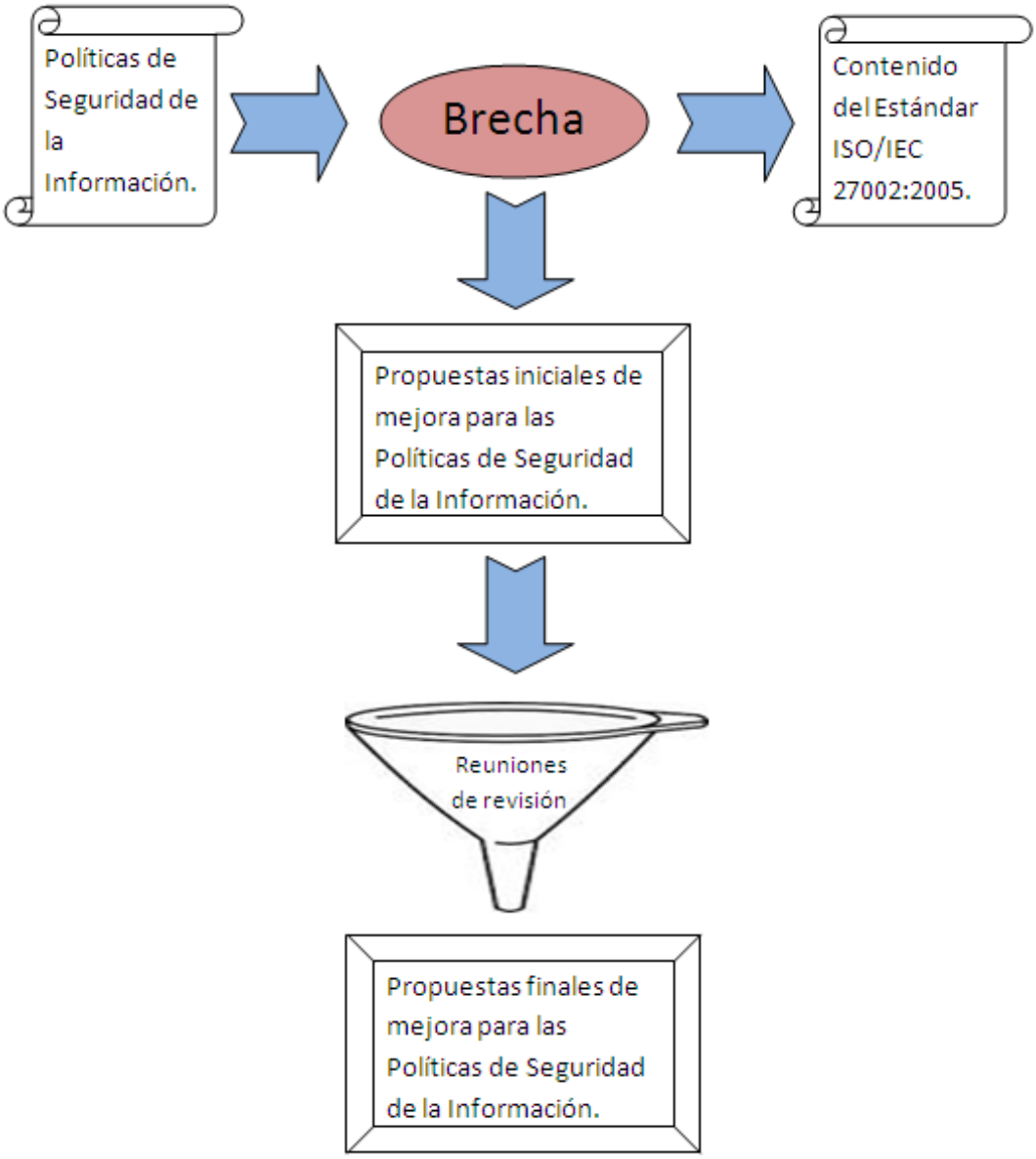


Figura 6. Metodología utilizada en el desarrollo del proyecto
Fuente: Elaboración propia.

3.3. Fuentes de información

Se enumeran a continuación, las fuentes de información utilizadas para la elaboración del proyecto:

- Reuniones iniciales con Franklin Giralt, Director del Departamento de Gestión de Calidad y Ricardo Morales, colaborador del mismo departamento, para identificar la necesidad de la institución y plantear el proyecto.
- Estándar ISO/IEC 27002:2005, estándares relacionados al anterior como ISO/IEC 27001 y otras referencias como los sitios Web, libros y artículos, entre otros.
- Documento de Políticas Específicas de Seguridad de la Información y documentos complementarios evaluados.
- Informe con la documentación de la brecha entre las Políticas Específicas de Seguridad de la Información del BCCR y el estándar ISO/IEC 27002:2005.
- Información obtenida de las diferentes reuniones a través del desarrollo del proyecto.

3.4. Técnicas de recolección de información

Las entrevistas, la observación y la revisión de documentos son técnicas indispensables para localizar información. (Hernández, Fernández y Baptista, 2010).

Las técnicas de recolección de información para el presente proyecto fueron las siguientes:

- Análisis documental: Es la principal técnica utilizada. El análisis documental fue aplicado para estudiar el contenido del estándar ISO/IEC 27002:2005, donde se obtuvo información de los dominios que lo componen y fueron la base para la evaluación llevada a cabo. Por otro lado, se estudiaron otras referencias bibliográficas que complementaron el estándar para generar el conocimiento requerido para llevar a cabo la ejecución del proyecto.

También se realizó un análisis a documentación interna del Banco Central de Costa Rica. Esta técnica se aplicó sobre el documento de políticas específicas de Seguridad de la Información y los otros documentos que fueron evaluados.

- Reuniones: Posterior a la evaluación de las Políticas Específicas de Seguridad de la Información y demás documentos, se realizaron reuniones de revisión con el fin de filtrar las propuestas planteadas y alinearlas a las necesidades del negocio. Estas se realizaron con Franklin Giralt Amador. Además, se realizaron otras con Ricardo Morales, para identificar el conjunto de documentos a valorar adicionales a las Políticas de Seguridad de la Información.

3.5. Técnicas de análisis de información

Existe según Hernández, Fernández y Baptista (2010), una serie de técnicas que pueden ser utilizadas para el análisis de datos cualitativos.

Para el análisis de la información recolectada en este proyecto se utilizaron las siguientes técnicas:

- Lectura y análisis de documentación: Esta técnica consiste en la lectura y análisis de documentos y fue aplicada al estudio de las Políticas Específicas de Seguridad de la Información, así como los demás documentos evaluados.
- Visualizaciones: Las visualizaciones utilizadas fueron los gráficos que mostraran los resultados obtenidos de la valoración de las Políticas Específicas de Seguridad de la Información y demás documentos.
- Describir e interpretar: Se ha hecho una interpretación del estándar ISO/IEC 27002:2005 con el fin de diseñar una herramienta para valorar las Políticas Específicas de Seguridad de la Información del Banco Central de Costa Rica. Así mismo se debió hacer una interpretación de los resultados de la valoración realizada con el fin de describirlos en un informe y además, plantear las propuestas de mejora.

- Aplicación de la herramienta de valoración: Esta va a ser aplicada sobre las Políticas de Seguridad de la Información y documentación complementaria, y tendrá como fin, indicar la brecha existente entre la documentación valorada y el estándar ISO/IEC 27002:2005. En la sección 3.5.1. se describe a profundidad dicha herramienta.

3.5.1. Descripción de la herramienta de valoración

La herramienta de valoración desarrollada tiene por objetivo evaluar el contenido de los documentos que plantean políticas, controles, lineamientos, procesos o procedimientos cuya área de aplicación se puede asociar a los dominios del estándar ISO/IEC 27002:2005 y determinan cómo gestionar la Seguridad de la Información dentro del Banco Central de Costa Rica.

Esta define una serie de aspectos por cada control del estándar que permite definir si está cubierto por el marco normativo interno del Banco con respecto a la Seguridad de la Información. Con el fin de mantener un orden en la herramienta y alinearla al estándar, esta se estructuró de manera similar, de manera tal que los aspectos que deben ser cubiertos se clasificaron por cada control, cada uno se agrupó por objetivo de control y los objetivos de control, según los dominios del estándar. Así, según lo anterior, podrían verse los resultados de una manera ordenada y segmentada de acuerdo con los dominios del estándar.

3.5.1.1. Estructura de la herramienta de valoración

La herramienta consiste en un documento de Excel compuesto de tres hojas de cálculo, las cuales serán descritas a continuación:

3.5.1.1.1. Hoja de valoración

La descripción de la estructura de la hoja de valoración se hará tomando como base la Figura 7. Muestra de la herramienta de valoración.

Dominio		5. Política de seguridad				
Documentos evaluados		Políticas específicas de Seguridad de la Información				
Objetivo de control	Control	Aspectos que políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir	¿Se cumple el aspecto?	Evidencia	Cobertura del control	Observaciones
5.1. Política de seguridad de la información	5.1.1. Documento de la política de seguridad de la información	Aprobación de la política de seguridad.				
		La política define el término de seguridad de la información.				
		La política define objetivos de la seguridad de la información.				
		La política establece el alcance de la seguridad de la información				
		La política establece la intención de la gerenecia, alineada a la estrategia de la institución.				
		La política identifica el marco referencial para definir controles				
		La política define responsabilidades de la seguridad.				
		La política referencia a documentos que la sustentan.				
	5.1.2. Revisión de la política de seguridad de la información	Está identificado el dueño de la política				
		Se definen intervalos planeados de revisión.				
		Se define que se debe llevar un registro de la revisión gerencial				
Dominio		6.Organización de la seguridad de la información				
Documentos evaluados		Políticas específicas de Seguridad de la Información, Código de ética, Políticas especícas Gestión de riesgos.				
Objetivo de control	Control	Aspectos que políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir	¿Se cumple el aspecto?	Evidencia	Cobertura del control	Observaciones
		La gerencia debe asegurarse de que los objetivos de seguridad se identifiquen y se alinien al negocio.				
		Obligatoriedad de la gerencia de revisar y aproabar las políticas.				
		Obligatoriedad de la gerencia de revisar la efectividad de las políticas.				

Figura 7. Muestra de la herramienta de valoración
Fuente: Elaboración propia.

La hoja de valoración, según la Figura 7, consiste en la plantilla que permite realizar la valoración. Esta se divide en 11 secciones, según la cantidad de dominios del estándar ISO/IEC 27002:2005. Cada sección inicia con un espacio donde se indica el dominio correspondiente y además, hay un espacio en blanco para que la persona que aplique la herramienta indique los documentos valorados por dominio. Para cada dominio se definió una serie de columnas que proveen información suficiente para realizar la valoración y además, que permita documentar los resultados obtenidos. Estas columnas pueden visualizarse en la Figura 7 y su descripción se encuentra en la Tabla 2. Descripción de las columnas de la herramienta de valoración. Ver Anexo 2 para observar la hoja de valoración completa.

Columna	Descripción
Objetivo de control	Se indican los objetivos de control por cada dominio del estándar.
Control	Se indica cada control asociado con los distintos objetivos de control de un dominio.
Aspectos que políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir	Se detallan los aspectos que se debieran cubrir para determinar si un control del estándar ISO/IEC 27002 se cubre total o parcialmente, si no se cubre o bien, si no aplica dentro de la organización.
¿Se cumple el aspecto?	Esta columna sirve para definir si un aspecto descrito anteriormente se cubre o no.

Columna	Descripción
	Tiene tres valores predeterminados los cuales son “Sí”, “No” y “N/A”, este último significa no aplica. Las celdas de esta columna deben llenarse estrictamente por evaluador con alguno de los valores predeterminados, ya que de esto depende la funcionalidad del resto de la columna “Cobertura del control” y por ende, de los resultados de la valoración.
Evidencia	Sirve para documentar la evidencia que indica que sí se cumple un determinado aspecto. Las celdas de esta columna deben llenarse por el evaluador y debiera ser lo más explícito posible. Se debe indicar el documento y sección específica que evidencia el cumplimiento de un determinado aspecto.
Cobertura del control	Determina por cada control si se encuentra cubierto dentro de la documentación valorada. Las celdas de esta columna adquieren el valor automáticamente, según el cumplimiento de los aspectos asociados a un determinado control. Los valores posibles para una celda de esta columna son:

Columna	Descripción
	• Total: La celda adquiere este valor cuando todos los aspectos de un determinado control se cumplen o si uno o más aspectos se cumplen y el resto no aplica. • Parcial: La celda adquiere este valor cuando uno o más aspectos de un control se cumplen y cuando uno o más aspectos del control se incumplen. • Nula: La celda adquiere este valor cuando todos los aspectos de un determinado control se incumplen o si uno o más aspectos se incumplen y el resto no aplica. • N/A: Significa no aplica. La celda adquiere este valor cuando todos los aspectos de un determinado control no aplican dentro de la organización.
Observaciones	Sirve para que el evaluador indique observaciones que considere relevantes y complementen la valoración.

Tabla 2. Descripción de las columnas de la herramienta de valoración
Fuente: Elaboración propia.

Si bien es cierto, esta plantilla de valoración ayuda a determinar la cobertura del estándar ISO/IEC 27002: 2005 por las políticas y demás documentos valorados de Seguridad de la Información; sin embargo, para determinar explícitamente propuestas de mejora a la documentación valorada, es recomendable plantearlas haciendo uso de la plantilla en conjunto del estándar ISO/IEC 27002, pues este último posee información complementaria que pudiese ser de utilidad.

3.5.1.1.2. Hoja de resultados

La hoja de resultados consiste en una tabla que resume los resultados obtenidos de la aplicación de la plantilla de valoración. Como se puede ver en la Figura 8. Tabla de resultados de la herramienta de valoración, la tabla de resultados se encuentra categorizada por dominios, según el estándar ISO/IEC 27002:2005, de manera tal que se conozcan los porcentajes de controles cubiertos totalmente, controles cubiertos parcialmente, controles no cubiertos y controles no aplicables dentro de la documentación valorada.

Al final de la tabla se consolida la suma de resultados por dominio y se brinda los resultados finales en general de la valoración.

Dominio	Resultados obtenidos			
	Controles cubiertos totalmente	Controles cubiertos parcialmente	Controles no cubiertos	Controles no aplicables
5.Política de seguridad	0,00%	100,00%	0,00%	0,00%
6.Organización de la Seguridad de la Información	9,09%	27,27%	63,64%	0,00%
7. Gestión de activos	20,00%	40,00%	40,00%	0,00%
8. Seguridad de recursos humanos	22,22%	11,11%	66,67%	0,00%
9. Seguridad física y ambiental	0,00%	23,08%	76,92%	0,00%
10. Gestión de las comunicaciones y operaciones	18,75%	40,63%	34,38%	6,25%
11. Control de acceso	32,00%	28,00%	40,00%	0,00%
12. Adquisición, desarrollo y mantenimiento de los sistemas de información	18,75%	31,25%	50,00%	0,00%
13. Gestión de incidentes de la Seguridad de la Información	0,00%	0,00%	100,00%	0,00%
14. Gestión de la continuidad del negocio	0,00%	0,00%	100,00%	0,00%
15. Cumplimiento	0,00%	0,00%	100,00%	0,00%
TOTAL	15,79%	27,07%	55,64%	1,50%

Figura 8. Tabla de resultados de la herramienta de valoración
Fuente: Elaboración propia.

Cabe mencionar que los datos mostrados en la Figura 8, no reflejan los resultados reales de la valoración aplicada a la documentación del Sistema de Gestión de Seguridad de la Información del Banco Central de Costa Rica.

3.5.1.1.3. Hoja de gráficas

La hoja de gráficas viene a ser una herramienta auxiliar de la hoja de resultados, ya que como se puede observar en la Figura 9. Hoja de gráficas de la herramienta de valoración, esta representa a manera de gráficos los resultados de la valoración aplicada.

Figura 9. Hoja de gráficas de la herramienta de valoración
Fuente: Elaboración propia.

Los datos mostrados en la en la Figura 9, no reflejan los resultados reales de la valoración aplicada a la documentación del Sistema de Gestión de Seguridad de la Información del Banco Central de Costa Rica.

3.5.2. ¿Cómo utilizar la herramienta de valoración?

Se requiere seguir los siguientes pasos para usar la plantilla de valoración:

- Identificar los documentos que se van a evaluar por cada dominio y registrarlos dentro de la herramienta.
- Verificar que cada aspecto que se indica en la plantilla se cumpla o no dentro la documentación; si se cumple, se debe registrar la evidencia.
- Anotar las observaciones relevantes a lo identificado en la documentación valorada.
- Observar los resultados obtenidos de la valoración en la hoja de resultados o bien, en la hoja de gráficas.

Capítulo IV: Análisis de resultados

4.1. Listado de documentos evaluados

Adicional a las Políticas Específicas de Seguridad de la Información se evaluaron otros documentos complementarios, según los dominios y controles del estándar ISO/IEC 27002:2005.

El objetivo principal fue valorar las Políticas específicas de la Seguridad de la Información para luego proponer mejoras, pero dentro del Banco existen otros instrumentos para la gestión de la Seguridad de la Información que atienden los controles no contemplados por las políticas. En ese caso, aunque no fueran políticas, se consideró que estos documentos podrían contemplarse en el alcance de la valoración, pues definían la manera en que el Banco Central de Costa Rica aborda el tema de la Seguridad de la Información.

A continuación se enlistan los documentos contemplados en la valoración:

- Políticas específicas de la Seguridad de la Información.
- Código de ética.
- Políticas específicas de Gestión de Riesgos.
- Planes de continuidad del negocio.
- Regulaciones con clientes en los negocios del Banco.
- Reglamento para el trámite de denuncias e investigaciones preliminares en el Banco Central de Costa Rica y sus Órganos de Desconcentración Máxima.
- Ley de Administración Pública (Proceso administrativo).
- Proceso de contratación de personal del Banco.
- Operaciones de seguridad.
- Lineamientos de acceso al código fuente.
- Proceso de Gestión de Cambios al *Software*.
- Proceso de Gestión de cambios de infraestructura de TI.
- Servicios de Soporte al BCCR: Procedimientos.
- Políticas específicas del Sistema Interno de Gestión.

- Proceso Atención de Incidentes de Seguridad Tecnológica.
- Proceso de continuidad del negocio.
- Marco legal externo ubicado en la intranet.
- Marco legal interno ubicado en la intranet.
- Proceso Ejecución de Auditorías.
- Proceso Estudios de Mercado para Soluciones Tecnológicas.
- Ley N° 8968 - Protección de la Persona frente al tratamiento de sus datos personales.
- Proceso de Evaluaciones Internas de Cumplimiento de TI.

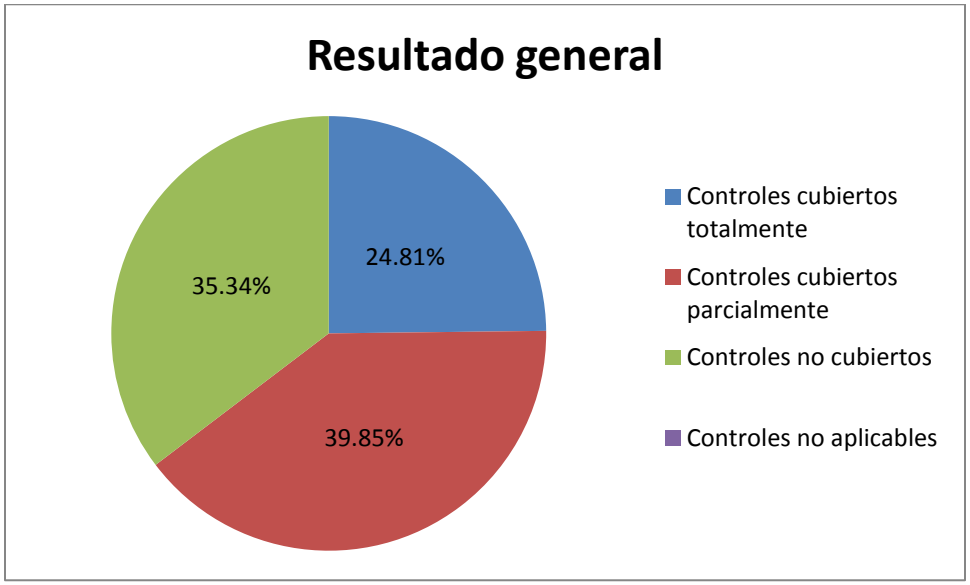
4.2. Resultados obtenidos de la valoración aplicada

Se hace en esta sección, una descripción de los resultados obtenidos de la valoración aplicada.

4.2.1. Resultados generales de la valoración

Se puede observar, en la sección 4.2.1, Documentación de brecha, en los resultados obtenidos por dominio que todos los controles fueron aplicables al Banco. Además, se puede ver en la Gráfica 1. Cobertura de los controles del estándar ISO/IEC 27002:2005, que apenas un 24,81% de los controles fue cubierto totalmente por la documentación valorada. Este resultado se genera a partir de que existen políticas que en general se pueden asociar a un determinado control del estándar ISO/IEC 27002:2005; sin embargo, cuando se inició el proceso de descomposición de los controles del estándar para verificar que en realidad las políticas, controles y lineamientos del Banco cubrieran a cabalidad sus lineamientos de implementación, se logró identificar leves brechas que hacían que la cobertura de dichos controles no fueran totales, sino más bien parciales. Es por lo anterior que el porcentaje de controles cubiertos parcialmente es alto, llegando al 39,85%.

Al analizar ese fenómeno de leves brechas, se identifica que una posible solución para la mejora de las Políticas Específicas de Seguridad de la Información es plantear nuevas políticas y complementar las actuales, ya que algunas de las identificadas pueden plantearse más bien como controles y lineamientos asociados con las políticas ya existentes. Por otro lado, se identificó un porcentaje de 35,34% de controles no cubiertos. Este tema es de cuidado, porque se logró determinar que algunas prácticas del estándar ISO/IEC 27002:2005 se realizaban, pero no estaban documentadas y por ello, se consideró su cobertura como nula; uno de los dominios donde más se evidenció lo mencionado fue el de recursos humanos. Así que debería revisarse a nivel organizacional cuáles buenas prácticas se siguen con respecto a la Seguridad de la Información y documentarlas, ya sea a nivel de política, control, lineamiento, procesos, procedimientos u otros mecanismos.



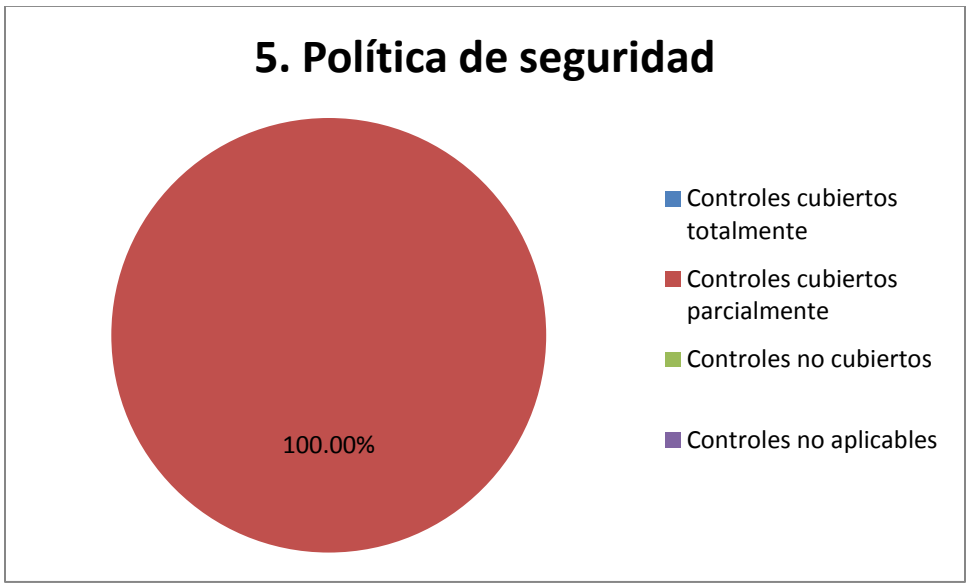
Gráfica 1. Cobertura de los controles del estándar ISO/IEC 27002:2005
Fuente: Elaboración propia.

4.2.1.1. Resumen de resultados por dominio

Se presentan en esta sección los resultados generales de la valoración realizada por cada dominio.

4.2.1.1.1. Política de seguridad

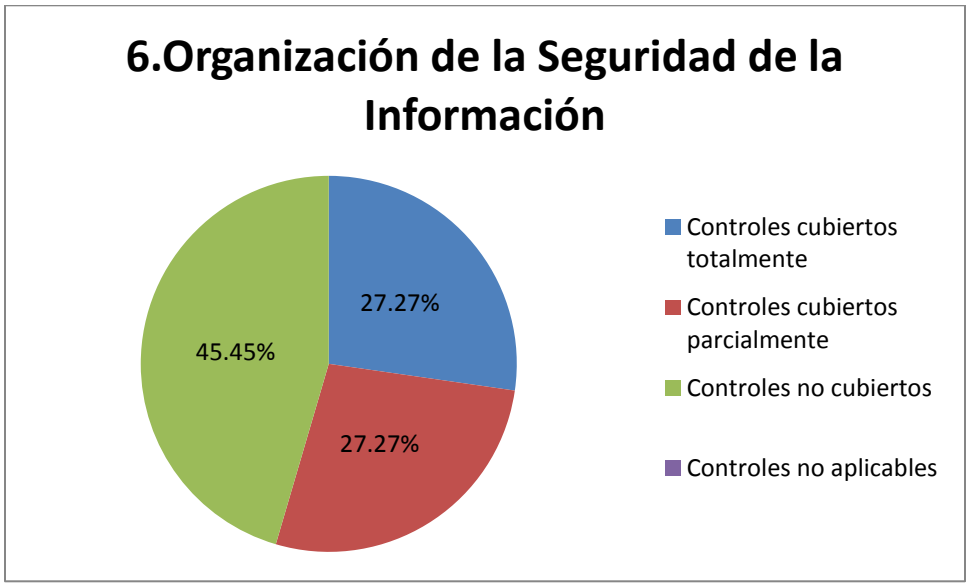
Se identificó para dicho dominio, según lo que se puede observar en la Gráfica 2. Cobertura de los controles del dominio de política de seguridad, que todos son aplicables al Banco y que el 100% de ellos se encuentra parcialmente cubierto. Es importante cerrar la brecha identificada, pues los controles de este dominio colaboran con el planteamiento estratégico de la Seguridad de la Información. Por otro lado, es importante que se definan los periodos de revisión de la Seguridad de la Información, ya que la importancia de las políticas, controles y lineamientos radica en su cumplimiento y efectividad en el tratamiento de los riesgos, lo cual implica que sea un requerimiento organizacional revisar ambos aspectos.



Gráfica 2. Cobertura de los controles del dominio de política de seguridad
Fuente: Elaboración propia

4.2.1.1.2. Organización de la Seguridad de la Información

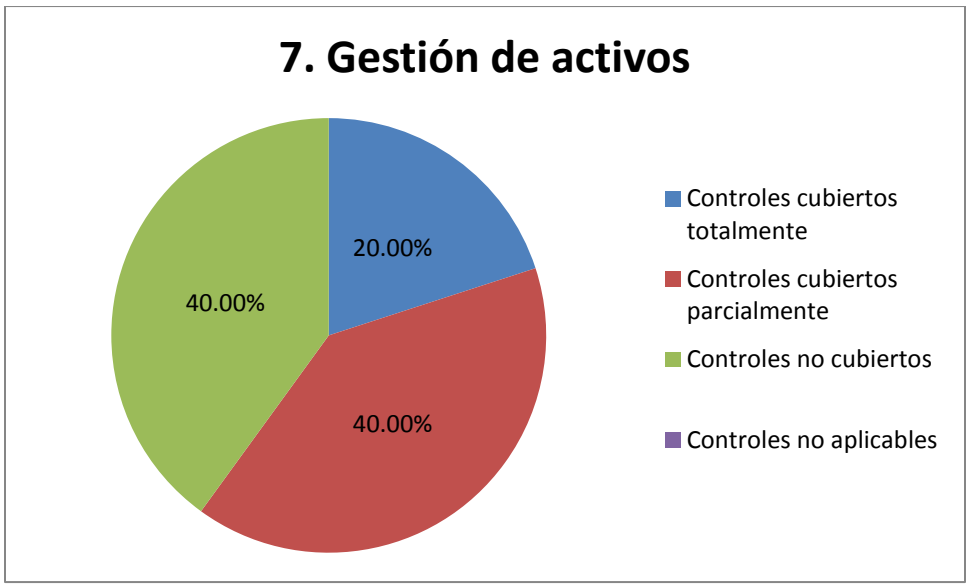
Todos los controles del presente dominio son aplicables al Banco y se identificaron los porcentajes de cobertura mostrados en la Gráfica 3. Cobertura de los controles del dominio de organización de la Seguridad de la Información. Con respecto a la brecha, es importante mencionar que debiera cerrarse, pues el actuar de los empleados, contratistas y terceros, es un factor clave para lograr los objetivos de la Seguridad de la Información organizacional, por lo tanto, se debieran establecer políticas que regulen cómo gestionar la interacción con dichos grupos.



Gráfica 3. Cobertura de los controles del dominio de organización de la Seguridad de la Información
Fuente: Elaboración propia.

4.2.1.1.3. Gestión de activos

Existen varios aspectos no cubiertos en la gestión de activos, enfocada en la Seguridad de la Información, pues si bien es cierto, el Banco posee todo un proceso de gestión de activos a nivel organizacional, no se garantiza que este proceso realice la gestión alineada a la Seguridad de la Información y a las especificaciones del estándar ISO/IEC 27002:2005. En la Gráfica 4. Cobertura de los controles del dominio de gestión de activos, se puede observar los resultados de la valoración del presente dominio.

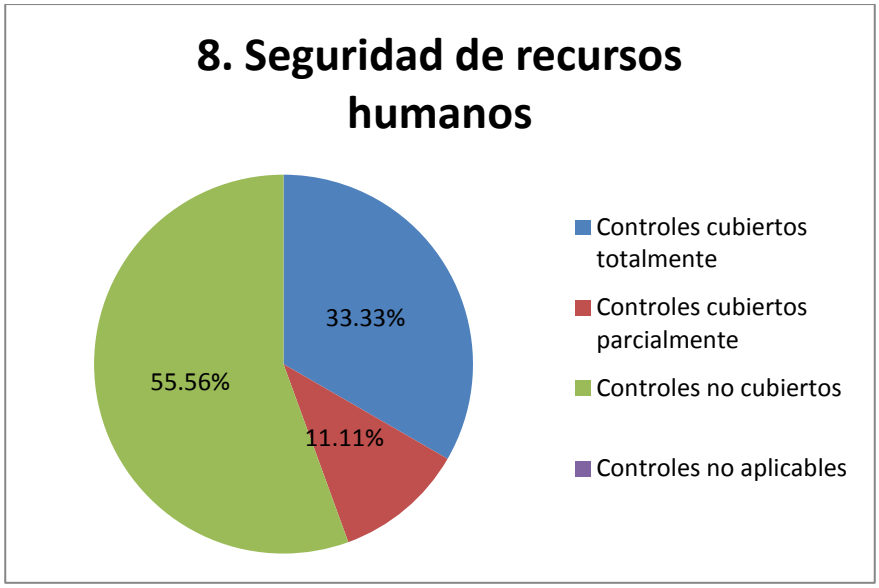


Gráfica 4. Cobertura de los controles del dominio de gestión de activos
Fuente: Elaboración propia.

4.2.1.1.4. Seguridad de recursos humanos

Es importante mencionar que dentro del Banco, la mayoría de controles del dominio de seguridad de recursos humanos podrían verse cubiertos por los procesos de recursos humanos documentados en el Sitio de Calidad de la Institución; sin embargo, no lo están. Como recomendación se debiera verificar si se implementan los controles para los cuales se identificó una brecha documental en la presente valoración y si bien, no se plantean políticas específicas, al menos se debiera documentar los procesos de recursos humanos que no se encuentran en el Sitio de Calidad.

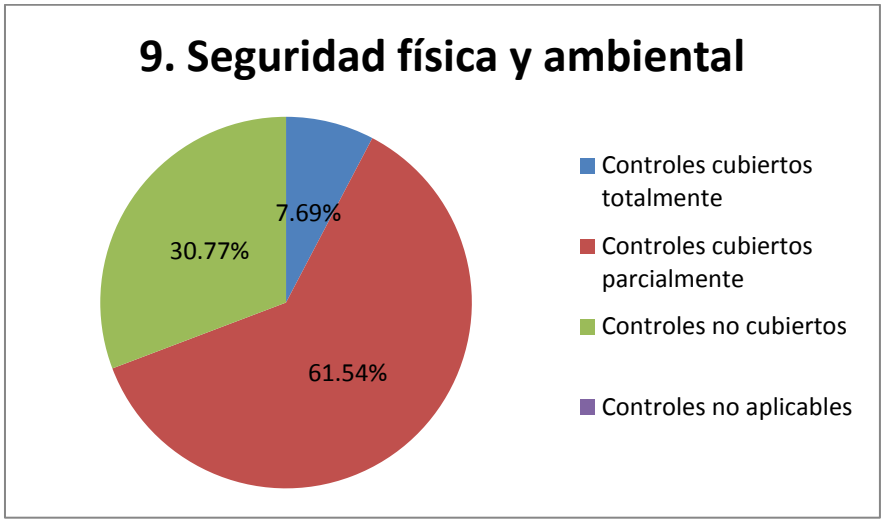
En la Gráfica 5. Cobertura de los controles del dominio de seguridad de recursos humanos, se puede observar los resultados de la valoración del presente dominio.



Gráfica 5. Cobertura de los controles del dominio de seguridad de recursos humanos
Fuente: Elaboración propia.

4.2.1.1.5. Seguridad física y ambiental

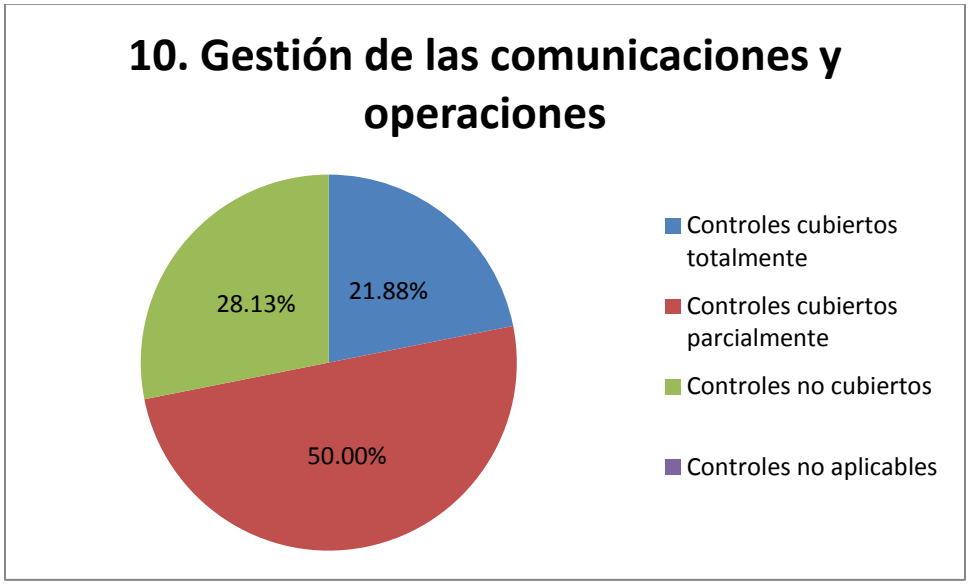
El dominio de seguridad física y ambiental dentro del Banco, en su mayoría está regulado no por políticas, sino por procesos documentados en el Sitio de Calidad de la Institución, por lo cual una mejora documental del dominio sería realizada directamente sobre los procesos o bien, en caso que se desee llevar a un nivel documental de más alto nivel, se podrían plantear políticas específicas. En la Gráfica 6. Cobertura de los controles del dominio de seguridad física y ambiental, se puede observar los resultados de la valoración del presente dominio.



Gráfica 6. Cobertura de los controles del dominio de seguridad física y ambiental
Fuente: Elaboración propia.

4.2.1.1.6. Gestión de las comunicaciones y operaciones

Se logra identificar en este dominio, que hay poca cobertura de sus controles por las Políticas Específicas de Seguridad de la Información. Es fundamental indicar que algunos de los aspectos que no se cumplen podrían llegar a cubrirse no sólo como políticas, sino más bien como controles y lineamientos del negocio en complemento de las políticas de seguridad ya existentes. Esto anterior no debería realizarse sin antes realizar el análisis de riesgo correspondiente para determinar si es necesario y viable implementar dichos controles y posterior a ello, incluirlos documentalmente dentro de las políticas. En la Gráfica 7. Cobertura de los controles del dominio de gestión de las comunicaciones y operaciones, se puede observar los resultados de la valoración del presente dominio.

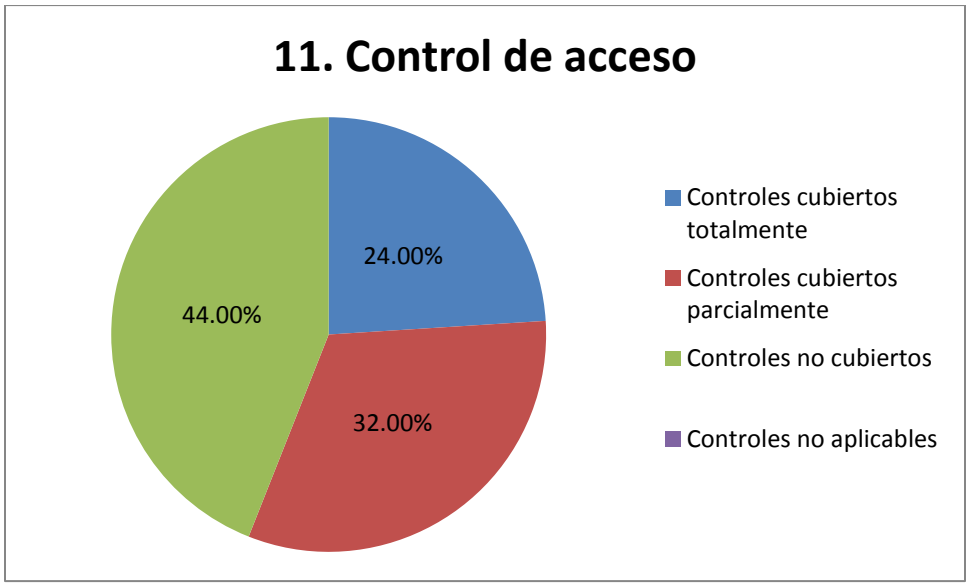


Gráfica 7. Cobertura de los controles del dominio de gestión de las comunicaciones y operaciones
Fuente: Elaboración propia.

4.2.1.1.7. Control de acceso

Se identificó, durante la valoración de los controles del presente dominio que existen políticas que, complementadas con la adecuada documentación de controles y lineamientos de la organización, podrían cubrir de mejor manera la brecha que se detalló.

Se logran identificar políticas de control de acceso globales, por lo cual se considera necesario establecer políticas, controles y lineamientos más detallados y direccionados a los distintos tipos de *software*, *hardware* y demás recursos tecnológicos de la organización, haciendo énfasis en aquellos que requieran un mayor control de acuerdo con su naturaleza. En la Gráfica 8. Cobertura de los controles del dominio de control de acceso, se pueden observar los resultados de la valoración del presente dominio.

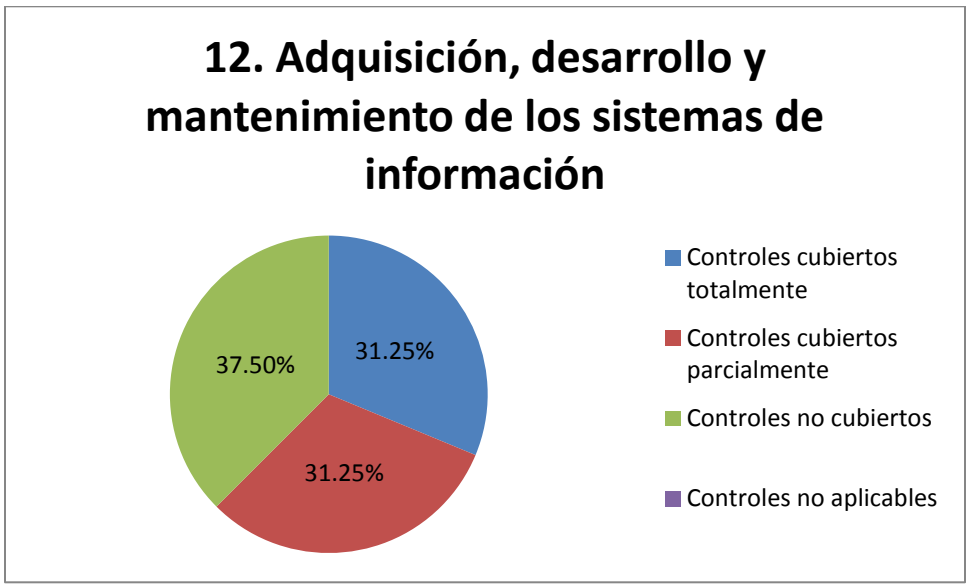


Gráfica 8. Cobertura de los controles del dominio de control de acceso
Fuente: Elaboración propia.

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

Se logra identificar que las políticas, controles y lineamientos del Banco, en la brecha documentada para el dominio de adquisición, desarrollo y mantenimiento de los sistemas de información, se encuentran enfocados en su mayoría al *software* desarrollado internamente, dejando fuera el provisto externamente, ya sean paquetes de *software* o desarrollos a la medida. Es importante incluir dentro de las políticas estos tipos o bien, ampliar el alcance de las políticas ya existentes.

En la Gráfica 9. Cobertura de los controles del dominio de adquisición, desarrollo y mantenimiento de los sistemas de información, se pueden observar los resultados de la valoración del presente dominio.



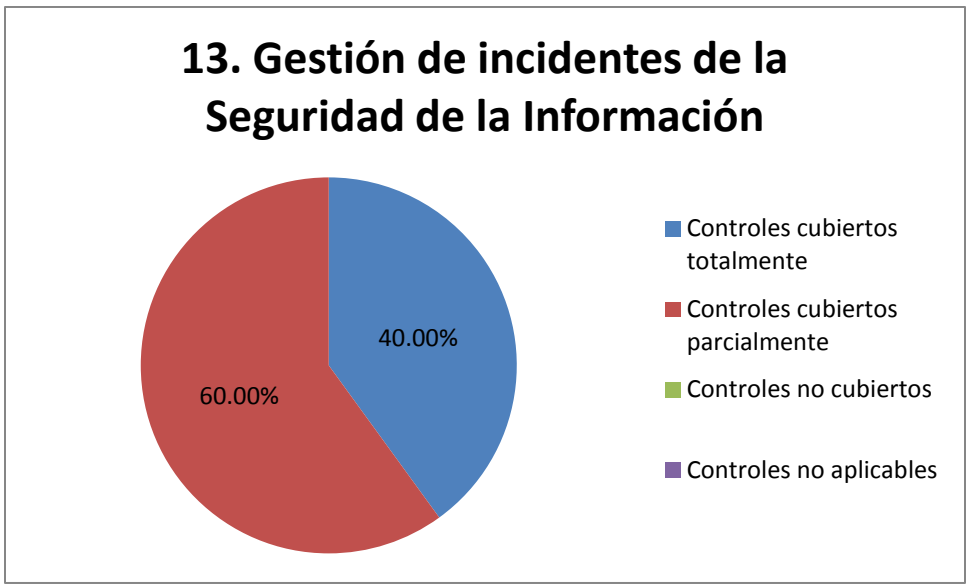
Gráfica 9. Cobertura de los controles del dominio de adquisición, desarrollo y mantenimiento de los sistemas de información
Fuente: Elaboración propia.

4.2.1.1.9. Gestión de incidentes de la Seguridad de la Información

Es importante recalcar que para este dominio se identificó documentalmente, solamente el proceso de gestión de incidentes de seguridad tecnológica, lo cual no engloba todo el campo de la Seguridad de la Información, pero al ser el único insumo, fue este el que se consideró. Es importante mencionar que el Departamento de Riesgos realiza toda una labor en el análisis de incidentes; sin embargo, no se encontró ninguna regulación sobre sus actividades por lo cual, posteriormente se proponen políticas en el tema de gestión de incidentes de la Seguridad de la Información, proponiendo como responsable del proceso a la División Gestión y Desarrollo, área de negocio a la cual pertenece el Departamento de Riesgos.

Aunque existe el proceso de *Atención de Incidentes de Seguridad Tecnológica*, debe valorarse la posibilidad de desarrollar políticas específicas para este dominio pues no existen, de manera tal que se pueda encontrar una sección dentro del documento de Políticas específicas de la Seguridad de la Información que complemente al proceso.

En la Gráfica 10. Cobertura de los controles del dominio de gestión de incidentes de la Seguridad de la Información, se puede observar los resultados de la valoración del presente dominio.

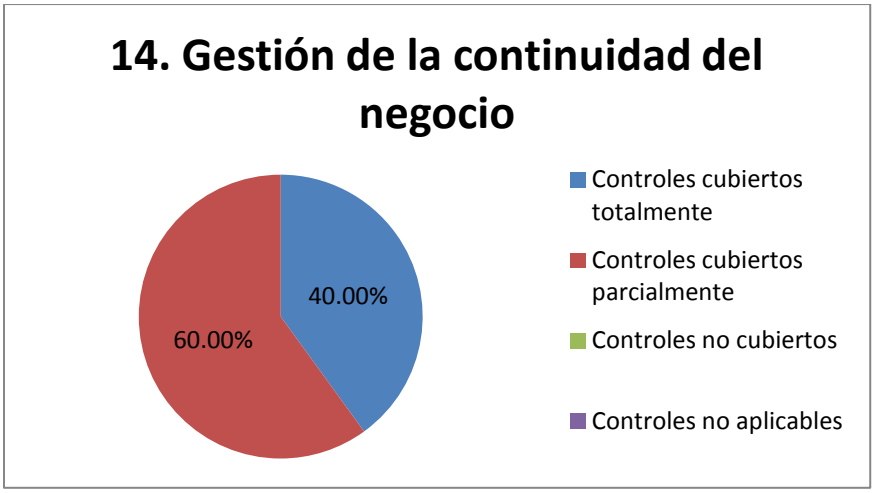


Gráfica 10. Cobertura de los controles del dominio de gestión de incidentes de la Seguridad de la Información
Fuente: Elaboración propia.

4.2.1.1.10. Continuidad del negocio

Se hizo un estudio de las políticas de continuidad del negocio ubicadas en las Políticas específicas del Sistema Interno de Gestión para valorar el dominio de continuidad del negocio del Banco; además, se complementa haciendo análisis de los planes de continuidad específicos de las distintas divisiones del Banco, así como de la distinta información ubicada en la intranet de la Institución, donde se detalla todo el marco referencial para la gestión de la continuidad del negocio.

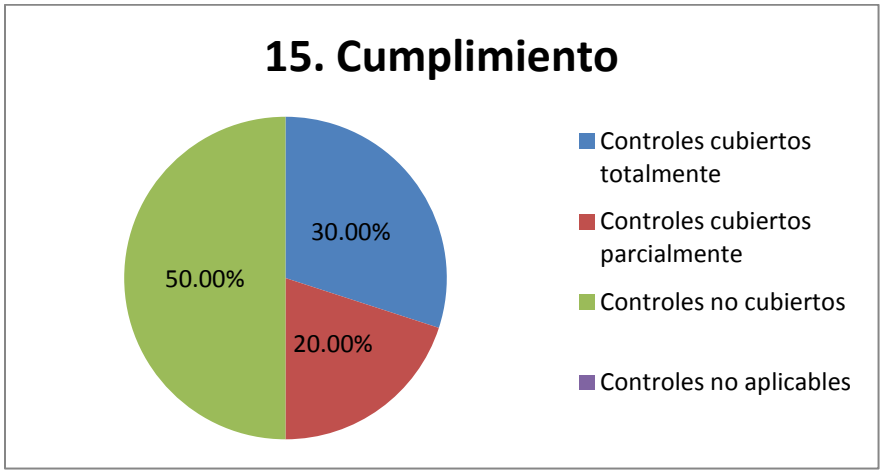
En la Gráfica 11. Cobertura de los controles del dominio de continuidad del negocio, se pueden observar los resultados de la valoración del presente dominio.



Gráfica 11. Cobertura de los controles del dominio de continuidad del negocio
Fuente: Elaboración propia.

4.2.1.1.11. Cumplimiento

Se logra identificar que todos los controles del dominio de cumplimiento son aplicables al Banco. Toda legislación aplicable al Banco, ya sea externa o interna se encuentra disponible al personal a través del sitio *Gobierno Corporativo* ubicado en la intranet. Es fundamental cerrar la brecha para este dominio, pues su objetivo es asegurarse que las metas de Seguridad de la Información se alcancen a través de la aplicación de las políticas, controles, lineamientos y otros mecanismos establecidos para gestionar la Seguridad de la Información dentro del Banco. En la Gráfica 12. Cobertura de los controles del dominio de cumplimiento, se pueden observar los resultados de la valoración del presente dominio.



Gráfica 12. Cobertura de los controles del dominio de cumplimiento
Fuente: Elaboración propia.

4.2.2. Documentación de brecha

La documentación de la brecha se realiza en esta sección y consiste en identificar, por cada control del estándar ISO 27002:2005, aquellos aspectos que no se cubren en las Políticas Específicas de Seguridad de la Información y la documentación complementaria también valorada. Es importante recalcar que cada control fue enumerado, según los identificadores asignados en el estándar ISO/IEC 27002:2005.

4.2.2.1. Dominio: Política de seguridad

Se documentan los aspectos no cubiertos para cada uno de los controles del dominio de política de seguridad del estándar ISO/IEC 27002:2005, en la Tabla 3. Brecha encontrada para el dominio de política de seguridad.

Identificador del control	Control	Brecha
5.1.1.	Documento de la política de Seguridad de la Información	En las Políticas Específicas de Seguridad de la Información, no se define el concepto de Seguridad de la Información. Tampoco los objetivos de Seguridad de la Información y además, no se aclara explícitamente que todas las políticas, controles y lineamientos se alinean a la estrategia del Banco.
5.1.2.	Revisión de la política de Seguridad de la Información	No se establece que se debiera hacer revisiones de la Seguridad de la Información en intervalos planeados y además, debe considerarse llevar un registro de cada una de dichas revisiones.

Tabla 3. Brecha encontrada para el dominio de política de seguridad
Fuente: Elaboración propia.

4.2.2.2. Dominio: Organización de la Seguridad de la Información

Se documentan los aspectos no cubiertos para cada uno de los controles del dominio de organización de la Seguridad de la Información del estándar ISO/IEC 27002:2005, en la Tabla 4. Brecha encontrada para el dominio de organización de la Seguridad de la Información.

Identificador del control	Control	Brecha
6.1.1.	Compromiso de la gerencia con la Seguridad de la Información	No se establece como responsabilidad de la gerencia, brindar los recursos necesarios para administrar la Seguridad de la Información del Banco. Debiera establecerse como responsabilidades de la coordinación aprobar roles y responsabilidades de Seguridad de la Información. Debe ser responsabilidad de la coordinación la búsqueda de consultoría especializada en Seguridad de la Información cuando el Banco no pueda abordar todos los requerimientos de seguridad.
6.1.2.	Coordinación de la Seguridad de la Información	No se establece como responsabilidad de la gerencia el asegurarse que todas las actividades dentro de la organización se ejecuten de acuerdo con las políticas. Tampoco se define como responsabilidad de la coordinación, identificar la manera de abordar las disconformidades.

Identificador del control	Control	Brecha
		Además, debiera establecerse como responsabilidad de la coordinación el aprobar todas las metodologías y procesos y evaluar los datos resultantes de las actividades de monitoreo de la Seguridad de la Información.
6.1.3.	Asignación de las responsabilidades de la Seguridad de la Información.	No se define que la coordinación posee la responsabilidad de asignar roles y responsabilidades, además de identificar activos y procesos junto a la asignación de un encargado para cada uno de ellos. No existe una política que regule los niveles de autorización dentro del Sistema de Gestión de Seguridad de la Información.
6.1.4.	Proceso de autorización para facilidades procesadoras de información.	La sección V de Políticas Específicas de Seguridad de la Información, define que el *software* que se adquiera debe ser acorde con la lista de *software* permitido por la organización; sin embargo, se debe establecer un procedimiento de autorización para *software* y *hardware*, donde se incluyan también la autorización para el uso de dispositivos personales.
6.1.5.	Acuerdos de confidencialidad.	Manejan acuerdos de confidencialidad, pero no existen políticas, controles y lineamientos que regulen su gestión.

Identificador del control	Control	Brecha
6.1.6.	Contacto con las autoridades.	El control se cubre en su totalidad, según los planes de contingencia establecidos en la gestión de la continuidad del negocio, donde se establecen las maneras de contactar a las autoridades pertinentes en caso de ser necesarias.
6.1.7.	Contacto con grupos de interés especial.	No hay una política que diga que el Banco se encuentra en la obligación de mantener contacto con grupos de interés especial expertos o con amplio conocimiento en el área de Seguridad de la Información.
6.1.8.	Revisión independiente de la Seguridad de la Información.	No existen políticas, controles y lineamientos sobre la aplicación de revisiones independientes de la Seguridad de la Información.
6.2.1.	Identificación de los riesgos relacionados con los grupos externos.	Este control se considera cubierto totalmente, según el marco normativo interno del Banco en relación con la gestión de riesgos, específicamente, según las Políticas específicas de Gestión de Riesgos.
6.2.2.	Tratamiento de la seguridad cuando se lidia con clientes.	Este control se considera cubierto totalmente, según el marco normativo interno, específicamente en las regulaciones con clientes en cada uno de los negocios del Banco.

Identificador del control	Control	Brecha
6.2.3.	Tratamiento de la seguridad cuando se lidia con terceros.	Se trata de regular con acuerdos de niveles de servicio y de confidencialidad, pero no existen políticas, controles y lineamientos que especifiquen los requerimientos mínimos de Seguridad de la Información que se debieran satisfacer para tratar con terceros.

Tabla 4. Brecha encontrada para el dominio de organización de la Seguridad de la Información
Fuente: Elaboración propia.

4.2.2.3. Dominio: Gestión de activos

Se documentan los aspectos no cubiertos para cada uno de los controles del dominio de gestión de activos del estándar ISO/IEC 27002:2005, en la Tabla 5. Brecha encontrada para el dominio de gestión de activos.

Identificador del control	Control	Brecha
7.1.1.	Inventario de los activos.	No se establecen políticas que digan que se deba llevar un inventario de activos de Seguridad de la Información, este se diferencia de un inventario convencional, pues debe asegurar que se registre toda la información necesaria para recuperar dicho activo en caso de un desastre; así mismo, este inventario debiera ser capaz de clasificar los activos según su impacto en la Seguridad de la Información. Este debiera estar alineado con los demás inventarios de la organización.

Identificador del control	Control	Brecha
7.1.2.	Propiedad de los activos.	Dentro de las políticas se especifica que se debiera definir un propietario para cada activo; sin embargo, no se detallan cuáles deben ser las responsabilidades de dicho propietario, donde, como mínimo este debiera asegurarse que el activo se clasifique de la manera adecuada y revisar los accesos y restricciones de acceso sobre dicho activo.
7.1.3.	Uso aceptable de los activos.	Este control se considera totalmente cubierto según el Código de Ética establecido dentro de la organización, donde se definen las normas de comportamiento de los empleados con los activos de la organización.
7.2.1.	Lineamientos de clasificación.	Aunque se definen las categorías de clasificación y reclasificación de la información, no se específica en las políticas, la existencia de protocolos de clasificación y reclasificación de la información, donde, como mínimo se considere definir el tiempo requerido para reclasificar alguna información.
7.2.2.	Etiquetado y manejo de la información.	Como se menciona previamente, no se establece el procedimiento para etiquetado de la información y además, no se definen procedimientos que determinen cómo manejar la información según su clasificación.

Tabla 5. Brecha encontrada para el dominio de gestión de activos
Fuente: Elaboración propia.

4.2.2.4 Dominio: Seguridad de recursos humanos

Se documentan los aspectos no cubiertos para cada uno de los controles del dominio de seguridad de recursos humanos del estándar ISO/IEC 27002:2005, en la Tabla 6. Brecha encontrada para el dominio de seguridad de recursos humanos.

Identificador del control	Control	Brecha
8.1.1.	Roles y responsabilidades.	Este control se considera cubierto según las Políticas Específicas de Seguridad de la Información en las consideraciones que sustentan la emisión de dichas políticas específicas, punto E específicamente y según el Código de Ética, en el punto 2.2.13 donde se establece que el personal debe actuar según la disposiciones con respecto a Seguridad de la Información. Cabe mencionar que el alcance de estos puntos debiera ampliarse a contratistas y terceros.
8.1.2.	Investigación de antecedentes.	Se realizan como buenas prácticas, muchos de los aspectos detallados en este control; sin embargo, no está normado documentalmente.
8.1.3.	Términos y condiciones del empleo.	No existe una política que regule este control donde se especifique que la persona contratada deba firmar un contrato con respecto a los términos de Seguridad de la Información.

Identificador del control	Control	Brecha
		Lo anterior debiese considerar regulaciones sobre manejo de la información, dentro y fuera de la organización.
8.2.1.	Responsabilidades de la gerencia.	Este control se considera cubierto según la P-3 de la sección I. Aspectos organizativos para la seguridad, de las Políticas Específicas de Seguridad de la Información.
8.2.2.	Conocimiento, educación y capacitación en Seguridad de la Información.	No se plantea que luego de una actualización a las políticas de Seguridad de la Información, se deba informar a todos los empleados sobre el respectivo cambio.
8.2.3.	Proceso disciplinario.	Este control se considera cubierto, ya que en el Banco existe un trámite preliminar para denuncias de incumplimientos del marco legal interno, normado por el Reglamento para el Trámite de Denuncias e Investigaciones Preliminares en el Banco Central de Costa Rica y sus Órganos de Desconcentración Máxima, complementado con el procedimiento administrativo planteado por la Ley de Administración Pública de Costa Rica.

Identificador del control	Control	Brecha
8.3.1.	Responsabilidades de terminación.	No existen políticas, controles y lineamientos ni otros mecanismos que definan las responsabilidades de la terminación del empleo con el fin de cumplir los objetivos de la Seguridad de la Información en la organización.
8.3.2.	Devolución de los activos.	No se establecen políticas, controles, lineamientos ni otros mecanismos que regulen que todo activo deba ser devuelto por el empleado una vez que se finalice el empleo.
8.3.3.	Retiro de los derechos de acceso.	No se establecen políticas, controles, lineamientos ni otros mecanismos que regulen el retiro de derechos de acceso de un empleado, una vez finalizado su contrato.

Tabla 6. Brecha encontrada para el dominio de seguridad de recursos humanos
Fuente: Elaboración propia.

4.2.2.5 Dominio: Seguridad física y ambiental

Se documentan los aspectos no cubiertos para cada uno de los controles del dominio de seguridad física y ambiental del estándar ISO/IEC 27002:2005, en la Tabla 7. Brecha encontrada para el dominio de seguridad física y ambiental.

Identificador del control	Control	Brecha
9.1.1.	Perímetro de seguridad física.	No existen políticas que evidencien que se define la fuerza del perímetro de seguridad basado en la importancia de los activos.

Identificador del control	Control	Brecha
		Además, no se identifican controles o lineamientos que mencionen que las puertas de emergencia poseen alarmas o que se haga uso de sistemas de detección de intrusos, también se omiten regulaciones sobre las pruebas de estos mecanismos.
9.1.2.	Controles de ingreso físico.	Sobre este control se identifica que no existe una política que indique que se debiera revisar y actualizar los derechos de acceso a áreas seguras.
9.1.3.	Asegurar las oficinas, habitaciones y medios.	No se identificaron políticas que indiquen que se consideran estándares de sanidad dentro de las oficinas, así mismo, no se establece un política de protección de los directorios que indiquen la ubicación de áreas seguras dentro de la organización.
9.1.4.	Protección contra amenazas externas e internas.	No se establecen políticas sobre aspectos como la gestión de materiales peligrosos lejos de áreas seguras, no mantener papelería en áreas seguras o sobre el uso de equipo adecuado anti-incendios.
9.1.5.	Trabajo en áreas seguras.	En general, no se establecen políticas, controles o lineamientos que regulen el trabajo en áreas seguras.
9.1.6.	Áreas de acceso público, entrega y carga.	Este control se considera cubierto según las operaciones de seguridad, ubicadas en el Sitio de Calidad del Banco, donde se identifican en sus procedimientos las áreas de carga y descarga.

Identificador del control	Control	Brecha
		Estas medidas anteriores regulan el acceso de terceros a las instalaciones de la organización.
9.2.1.	Ubicación y protección del equipo.	No se consideran lineamientos sobre comer y beber cerca de los medios de procesamiento de información.
9.2.2.	Servicios públicos de soporte.	No se establecen lineamientos sobre las revisiones de los servicios públicos de soporte y uso de sistemas monitoreo de dicho servicios. Tampoco se regula que se deba hacer el uso de UPS y generador alterno, además, de las revisiones de dichos medios, lo cual incluye asegurarse que haya suministro suficiente de combustible para el generador, así también; hacer uso de múltiples fuentes de energía. Además, no se establece alguna regulación sobre el deber de asegurarse de la estabilidad eléctrica y el establecimiento de dos rutas de conexión con el proveedor eléctrico.
9.2.3.	Seguridad del cableado.	No existe ninguna política, control o lineamiento que regulen la Seguridad de la Información en términos de este control.
9.2.4.	Mantenimiento del equipo.	No se detalla que el mantenimiento del equipo debiera llevarse sólo por aquel personal autorizado. Además, no se establece que se debiera llevar un registro de las fallas y el mantenimiento aplicado.

Identificador del control	Control	Brecha
		No se definen controles cuando el mantenimiento se presenta fuera del edificio. No se establece como política, la obligación de cumplimiento de todos los requerimientos de pólizas de seguros sobre los equipos.
9.2.5.	Seguridad del equipo fuera del local.	En este control se identificó que no existe una política que indique que el equipo fuera de la organización, nunca debiera estar fuera de la vista de su responsable cuando se encuentre en lugares públicos. Además, no se establece que el equipo fuera del local debe gestionarse, siguiendo estrictamente las condiciones y requerimientos establecidos de trato del equipo por el proveedor, tómese como ejemplo: no exponer el equipo a altas temperaturas o situarlo lejos de lugares húmedos.
9.2.6.	Seguridad de la eliminación o re-uso del equipo.	No se documentan políticas sobre la destrucción de todo equipo que deba ser eliminado o bien, algún control sobre el uso de mecanismos seguros para el borrado de la información en dichos equipos.
9.2.7.	Retiro de propiedad.	Este control se encuentra regulado por el proceso de control de ingreso y salida de bienes inmuebles; sin embargo, en el proceso no se identifica que se deba revisar un bien que haya salido de la organización y luego regresado.

Tabla 7. Brecha encontrada para el dominio de seguridad física y ambiental
Fuente: Elaboración propia.

4.2.2.6 Dominio: Gestión de las comunicaciones y operaciones

Se documentan los aspectos no cubiertos para cada uno de los controles del dominio de gestión de las comunicaciones y operaciones del estándar ISO/IEC 27002:2005, en la Tabla 8. Brecha encontrada para el dominio de gestión de las comunicaciones y operaciones.

Identificador del control	Control	Brecha
10.1.1.	Procedimientos de operación documentados.	Este control se considera cubierto según la política P-1 de la sección III Gestión de comunicaciones y operaciones de las Políticas Específicas de Seguridad de la Información, donde se indica que todos los procedimientos de operación se encuentran debidamente documentados.
10.1.2.	Gestión del cambio.	Existen dos procesos de control de cambios dentro del Banco, uno para *software* y otro para infraestructura. La brecha que se identifica es que en dichos procesos no se indica que se debiera llevar un registro de los cambios que se proponen, además, no se establece que se debieran definir procedimientos de respaldo o cancelación en caso de cambios fallidos.
10.1.3.	Segregación de los deberes.	No se establece una política que garantice que la auditoría de seguridad sea independiente.

Identificador del control	Control	Brecha
10.1.4.	Separación de los medios de desarrollo, prueba y operación.	No se establece una política sobre las reglas para el paso de *software* de pruebas a producción y sobre la restricción de acceso a herramientas de desarrollo desde ambientes de producción. No hay una política que defina que deba haber similitud entre el ambiente de pruebas y el ambiente de producción, sobre el manejo de distintos perfiles de usuario, dependiendo si se está en un ambiente de pruebas o en uno de producción y sobre la regulación que los datos operacionales no sean copiados en ambientes de prueba.
10.2.1.	Entrega del servicio.	No se establecen políticas sobre la transición de información a abastecimientos externos ni para asegurar que el tercero que provea un servicio mantenga la capacidad de entrega, según los cambios en la demanda.
10.2.2	Monitoreo y revisión de los servicios de terceros.	En general, no se definen políticas, controles y lineamientos que regulen el monitoreo y revisión de los servicios de terceros.

Identificador del control	Control	Brecha
10.2.3.	Manejo de cambios en los servicios de terceros.	No se establecen políticas, controles y lineamientos para regular cambios en los servicios de terceros, donde se regulen aspectos como el aumento del servicio, ya sea en calidad o cantidad, el cambio de las tecnologías utilizadas, o bien; que se decida cambiar el proveedor del servicio.
10.3.1.	Gestión de la capacidad.	Este control se considera cubierto en su totalidad por la política P-5 de la sección III Gestión de comunicaciones y operaciones de las Políticas Específicas de Seguridad de la Información donde se detalla que el Banco Central gestiona la capacidad actual de los procesos y se hacen estudios y proyecciones para requerimientos futuros.
10.3.2.	Aceptación del sistema.	No se establece en las políticas que indiquen que se deba revisar la capacidad de las computadoras desde las cuales se va a hacer uso de nuevos sistemas, además, tampoco se define una política sobre el establecimiento de procedimientos de recuperación y reinicio de nuevas soluciones, lo anterior va de la mano con los planes de recuperación de cambios fallidos del proceso de gestión de cambios de *software*.

Identificador del control	Control	Brecha
		No hay una política que asegure que se implementen y aprueben controles de seguridad en nuevas soluciones, tampoco hay una política que asegure que las nuevas soluciones debieran ser fáciles de utilizar para los usuarios, esto acompañado de una política que indique que se debe realizar una capacitación al personal para nuevas soluciones.
10.4.1.	Controles contra códigos maliciosos.	En las políticas no se documenta que se deba, además de instalar; actualizar los sistemas para el trato de códigos maliciosos. No se encuentra una política sobre revisiones periódicas de los sistemas y de la información en ellos. No existe una política que evidencie que haya planes para recuperación de ataques de códigos maliciosos y además, no hay una política de capacitación de los usuarios para el trato de estos.
10.4.2.	Controles contra códigos móviles.	No hay ninguna política establecida que indique cómo se gestionan los códigos móviles.

Identificador del control	Control	Brecha
10.5.1.	Respaldos	Aunque en la política P-8 de la sección III Gestión de comunicaciones y operaciones de las Políticas Específicas de Seguridad de la Información se define que en la organización se realizan respaldos de la información, deberían definirse controles como la realización de pruebas regularmente de los medios de respaldo, llevar un registro de las copias realizadas, definir que los respaldos se almacenan en un lugar lejano del sitio principal y definición de procedimientos de respaldo y recuperación.
10.6.1.	Controles de redes.	No se establecen políticas, controles o lineamientos para indicar que se separan las responsabilidades de gestión de redes de otras de cómputo. No hay una política para la gestión del equipo de manera remota, para el registro y monitoreo del ingreso a las redes y sobre la protección de la información cuando se transmita por medios públicos o inalámbricos.
10.6.2.	Seguridad de los servicios de la red.	No hay políticas que indiquen que se deban regir, a través de acuerdos de nivel de servicio, aquellos servicios que son provistos a través de la red, garantizando así el Banco su derecho de monitoreo y auditoría sobre los mismos.

Identificador del control	Control	Brecha
10.7.1.	Gestión de medios removibles.	Aunque el Banco tenga un enfoque de manejo de la información de manera documental a través de la intranet, aún no se realiza al 100% por lo cual debiera establecerse un conjunto de políticas, controles y lineamientos para la gestión de medios removibles.
10.7.2.	Retiro de medios.	Similar a la brecha del control anterior, debería plantearse una política para el retiro de medios.
10.7.3.	Procedimientos para el manejo de información.	Con respecto a este control se identifica una brecha donde no hay una política que indique que se deba mantener una lista de los destinatarios de la información dependiendo de su naturaleza y además, debería venir acompañada de otra para la actualización de dicha lista. Por otro lado, debe establecerse una política para gestionar los medios de almacenamiento de la información, según las especificaciones del proveedor.
10.7.4.	Seguridad de la documentación del sistema.	Se logra identificar que no hay una política que regule que deba haber una lista de usuarios con acceso a la documentación del sistema y que, como requisito, esta sea aprobada por el dueño del sistema.

Identificador del control	Control	Brecha
10.8.1.	Políticas y procedimientos de intercambio de información.	No se establece una política sobre el uso de medios inalámbricos de comunicación, además, debería definirse una política sobre el manejo de la información almacenada en papel. Por otro lado, no se define una política para regular el reenvío de comunicados organizacionales.
10.8.2.	Acuerdos de intercambio.	En general, este control podría cubrirse a través de la política P-12 de la sección III Gestión de comunicaciones y operaciones de las Políticas Específicas de Seguridad de la Información. A pesar de lo anterior, deberían detallarse los controles y lineamientos aplicables para la gestión de acuerdos de intercambio.
10.8.3.	Medios físicos en tránsito.	El Banco posee sus propios mensajeros, la brecha que se identifica es que no existe una política que defina que se deban seleccionar medios de almacenaje, resistentes y seguros de acuerdo con los medios que se deban transportar.
10.8.4.	Mensajes electrónicos.	No se establece una política donde se defina que se requiera autorización para el uso servicios de mensajería públicos externos, como por ejemplo: mensajes instantáneos.

Identificador del control	Control	Brecha
10.8.5.	Sistemas de información comercial.	No se establece una política que indique que el Banco identifica las vulnerabilidades del intercambio de información en sistemas de información comerciales, para lo cual se debería establecer controles como exclusión de alguna información, lugares desde los cuales se pueda acceder al sistema, definir categorías de autorización de usuarios en el sistema y respaldo de la información en los sistemas de información comerciales.
10.9.1.	Comercio electrónico.	Este control se considera cubierto a partir de la política P-14, sus controles y lineamientos, de la sección III Gestión de comunicaciones y operaciones del documento de Políticas Específicas de Seguridad de la Información.
10.9.2.	Transacciones en línea.	Este control se considera cubierto a partir de la política P-15, sus controles y lineamientos, de la sección III Gestión de comunicaciones y operaciones del documento de Políticas Específicas de Seguridad de la Información.
10.9.3.	Información públicamente disponible.	No existe una política que indique que se debe probar un sitio público antes de poner información en él, además, no hay una política que indique que se deba aprobar la información que se va a publicar.

Identificador del control	Control	Brecha
		Tampoco existe una política que indique que se deba restringir el acceso del sitio público a sitios internos del Banco.
10.10.1.	Registro de auditoría.	Este control se considera cubierto a partir de la política P-16, sus controles y lineamientos, de la sección III Gestión de comunicaciones y operaciones del documento de Políticas Específicas de Seguridad de la Información.
10.10.2.	Uso del sistema de monitoreo.	Este control se considera cubierto a partir de los controles C-16.3 y C-16.4 de la política P-16, de la sección III Gestión de comunicaciones y operaciones del documento de Políticas Específicas de Seguridad de la Información.
10.10.3.	Protección del registro de información.	No se establece una política para la protección de los registros de información.
10.10.4.	Registros del administrador y operador.	En las políticas no se indica que, cuando ocurre un evento, se deba registrar los procesos que pudiesen ver afectados.
10.10.5.	Registro de fallas.	Este control se cubre a partir del proceso de Atención de Incidentes de Seguridad Tecnológica.
10.10.6.	Sincronización de relojes.	En este control se encontró como brecha que en las políticas no se hace una referencia a un procedimiento de revisión y corrección de variaciones en los relojes.

Tabla 8. Brecha encontrada para el dominio de gestión de las comunicaciones y operaciones
Fuente: Elaboración propia.

4.2.2.7 Dominio: Control de accesos

Se documentan los aspectos no cubiertos para cada uno de los controles del dominio de control de accesos del estándar ISO/IEC 27002:2005, en la Tabla 9. Brecha encontrada para el dominio de control de acceso.

Identificador del control	Control	Brecha
11.1.1.	Política de control de acceso.	Este control se considera cubierto por la política P-1, de la sección IV Control de accesos del documento de Políticas Específicas de Seguridad de la Información.
11.2.1.	Registro del usuario.	La brecha identificada sobre este control es que no se define como política del Banco que los proveedores de servicios externos no brinden privilegios a un usuario, hasta que el proceso de autorización interno de la institución haya sido completado.
11.2.2.	Gestión de privilegios.	Sobre este control se identifica que no existe ninguna política, control o lineamiento u otro mecanismo que indique que se deba llevar un registro de todos los accesos a los usuarios que se hayan brindado.
11.2.3.	Gestión de las contraseñas de usuarios.	No se encuentra una política, control o lineamiento donde se especifique que antes de brindar una contraseña temporal, se debe verificar la identidad del usuario.

Identificador del control	Control	Brecha
11.2.4.	Revisión de los derechos de acceso.	No se establece una política, control o lineamiento donde se detalle que el Banco revisa periódicamente los privilegios que se han otorgado a los usuarios y cambios que hayan sufrido dichos privilegios.
11.3.1.	Uso de claves secretas.	No existe una política, control o lineamiento que indique que los usuarios de los sistemas y medios de procesamiento del Banco, estén obligados a utilizar contraseñas distintas a las que utilizan en otros medios.
11.3.2.	Equipo del usuario desatendido.	Este control está cubierto a través del lineamiento L-1.1.6., de la política P-1, de la sección IV Control de accesos, del documento Políticas Específicas de Seguridad de la Información.
11.3.3.	Política de escritorio y pantalla limpios.	No se establece una política de pantalla y escritorio limpios con el fin de no exponer información. Tampoco se define una política para gestionar el uso de fotocopiadoras, impresoras, faxes y otros medios de reproducción de información, con el fin de monitorear y llevar un control de la información que se reproduce.
11.4.1.	Política sobre el uso de servicios de la red.	Este control está cubierto a través de la política P-5, de la sección IV Control de accesos, del documento Políticas Específicas de Seguridad de la Información.

Identificador del control	Control	Brecha
11.4.2.	Autenticación del usuario para las conexiones externas.	Este control del estándar está cubierto a través del control C-5.2., de la política P-5, de la sección IV Control de accesos, del documento Políticas Específicas de Seguridad de la Información.
11.4.3.	Identificación del equipo en las redes.	No existe una política que indique que el equipo que se conecte a las redes se identifique automáticamente.
11.4.4.	Protección del puerto de diagnóstico y configuración remoto.	No existe una política que regule la protección física y el uso de puertos de diagnóstico y configuración.
11.4.5.	Segregación de redes.	Este control del estándar está cubierto a través del control C-6.1., de la política P-6, de la sección IV Control de accesos, del documento Políticas Específicas de Seguridad de la Información.
11.4.6.	Control de conexión a la red.	No se establece una política para la revisión de accesos a la red para garantizar que estos se alineen a la política general de control de accesos.
11.4.7.	Control de *routing* de la red.	No se define una política que indique que el enrutamiento dentro de la red sea controlado de manera tal, que se adecue a la política de control de accesos definida.
11.5.1.	Procedimientos para un registro seguro.	Este control hace referencia al registro de un usuario de un determinado sistema operativo.

Identificador del control	Control	Brecha
		En las políticas se definen procedimientos para el registro de usuarios a sistemas operacionales, pero los sistemas operativos poseen otra naturaleza y debieran ser gestionados a través de una política aparte.
11.5.2.	Identificación y autenticación del usuario.	Este control también hace referencia al área de sistemas operativos, por lo que se debería definir una política que regule la identificación y autenticación del usuario adicional a las políticas de autenticación para sistemas operacionales.
11.5.3.	Sistema de gestión de claves secretas.	Se establece una política de gestión de contraseñas para sistemas operacionales, pero no para sistemas operativos.
11.5.4.	Uso de las utilidades del sistema.	No se establecen políticas para la identificación y autenticación para uso de utilidades del sistema, tampoco hay políticas que indiquen que se segregan las utilidades del sistema de los sistemas operacionales. No existen políticas, controles o lineamientos que indiquen que se deba mantener el mínimo de utilidades del sistema y que además, eliminar toda aquella utilidad del sistema que no está siendo utilizada.
11.5.5.	Cierre de una sesión por inactividad.	No existe una política que indique que las sesiones en sistemas operativos se cierren posteriores a un tiempo de inactividad.

Identificador del control	Control	Brecha
11.5.6.	Limitación del tiempo de conexión.	No hay políticas que indiquen que el tiempo de conexión en un sistema operativo es limitado; además, debiera plantearse una política para regular el horario durante el cual se podría establecer una conexión.
11.6.1.	Restricción de acceso a la información.	No existe una política para el control de acceso de otras aplicaciones o sistemas a una determinada aplicación.
11.6.2.	Aislar el sistema confidencial.	No existe una política para la gestión de sistemas confidenciales donde se indique que se deba documentar el propietario del sistema, la criticidad o el nivel de confidencialidad del sistema y que que los sistemas confidenciales se gestionen en ambientes separados de otros sistemas.
11.7.1.	Computación y comunicaciones móviles.	No se define una política sobre el uso de dispositivos móviles. Esta política de uso de dispositivos móviles debe hacer referencia a la protección lógica y física del dispositivo, a procedimientos de respaldo de la información del dispositivo, a procedimientos en caso que suceda algún accidente con el dispositivo y a la capacitación del personal que hace uso de dispositivos móviles.

Identificador del control	Control	Brecha
11.7.2.	Teletrabajo.	Este control se considera cubierto a través de la política P-9, de la sección IV Control de accesos, del documento Políticas Específicas de Seguridad de la Información.

Tabla 9. Brecha encontrada para el dominio de control de acceso
Fuente: Elaboración propia.

4.2.2.8 Dominio: Adquisición, desarrollo y mantenimiento de los sistemas de información

Se documentan en la Tabla 10. Brecha encontrada para el dominio de adquisición, desarrollo y mantenimiento de los sistemas de información, los aspectos no cubiertos para del dominio de adquisición, desarrollo y mantenimiento de los sistemas de información del estándar ISO/IEC 27002:2005.

Identificador del control	Control	Brecha
12.1.1.	Análisis y especificación de los requerimientos de seguridad.	Este control se considera cubierto a través de la política P-1, de la sección V Adquisición, desarrollo y mantenimiento de sistemas, del documento Políticas Específicas de Seguridad de la Información.
12.2.1.	Validación de los datos de entrada.	Se identificó que no hay una política, control o lineamiento que detalle que se deba llevar un registro de las actividades asociadas al ingreso de datos.

Identificador del control	Control	Brecha
12.2.2.	Control del procesamiento interno.	Este se considera cubierto a través de la política P-3, de la sección V Adquisición, desarrollo y mantenimiento de sistemas, del documento Políticas Específicas de Seguridad de la Información.
12.2.3.	Integridad del mensaje.	Este control se considera cubierto a través de la política P-3, de la sección V Adquisición, desarrollo y mantenimiento de sistemas, del documento Políticas Específicas de Seguridad de la Información.
12.2.4.	Validación de los datos de salida.	No se establece una política, control o lineamiento que indique que se lleve un registro de las actividades de validación y prueba de los datos de salida.
12.3.1.	Política sobre el uso de controles criptográficos.	No hay una política sobre el uso de controles criptográficos.
12.3.2.	Gestión de claves.	No hay políticas, controles y lineamientos sobre la gestión de claves criptográficas donde se considere la protección física del equipo utilizado, procedimientos de gestión y un registro de todas las actividades relacionadas con la administración de claves criptográficas.
12.4.1.	Control del *software* operacional.	No existe una política, control o lineamiento que detalle que el *software* operacional se mantenga disponible al usuario, sólo a través de códigos ejecutables.

Identificador del control	Control	Brecha
		No existe una política sobre la gestión de la configuración del *software*, donde se pudiese incluir un registro de todas sus actualizaciones.
12.4.2.	Protección de los datos del sistema.	No se establecen políticas de protección de los datos del sistema, donde se defina que los datos operacionales no deban ser usados para prueba o bien, que haya una serie de controles que protejan la información operacional cuando sea usada para pruebas.
12.4.3.	Control de acceso al código fuente del programa.	Este control se considera cubierto a través de los lineamientos de protección de código fuente, establecidos por la División de Servicios Tecnológicos.
12.5.1.	Procedimientos del control del cambio.	No existe una política referente al control de cambios, pero en el Banco se definen dos procesos para regular la gestión de cambios, uno con el fin de administrar los cambios en *software* y otro para los cambios de infraestructura. En el proceso de gestión de cambios de *software*, se identificó como brecha que no define una actividad donde se registre toda solicitud de cambios como rastro de auditoría.

Identificador del control	Control	Brecha
12.5.2.	Revisión técnica de la aplicación después de cambios en el sistema.	Las pruebas de un sistema no sólo deben realizarse antes de la implementación de un cambio en un sistema, sino también posterior a ello. No se identifica una política, control o lineamiento para las pruebas posteriores a un cambio, donde se contemple que exista un presupuesto para realizarlas; actualizaciones del plan de continuidad y otros controles para asegurar que una aplicación se mantenga íntegra, posterior a un cambio.
12.5.3.	Restricciones sobre los cambios en los paquetes de *software*.	No se define, una política, controles y lineamientos para restringir los cambios en paquetes de *software* y si se tuvieran que realizar, que se implementen los controles adecuados para evitar vulnerabilidades de seguridad a partir del cambio.
12.5.4.	Filtración de información.	Este control se considera cubierto a través de la política P-8, de la sección V Adquisición, desarrollo y mantenimiento de sistemas, del documento Políticas Específicas de Seguridad de la Información.

Identificador del control	Control	Brecha
12.5.5.	Desarrollo de *software* abastecido externamente.	No se define una política para la supervisión del *software* desarrollado externamente, donde se asegure que se le realicen pruebas, que se puedan realizar auditorías de calidad y que se cumplan todos los requerimientos establecidos dentro del contrato.
12.6.1.	Gestión de las vulnerabilidades técnicas.	No se define una política para la gestión de vulnerabilidades técnicas donde se definan los roles y responsabilidades, los recursos necesarios y los tiempos de respuesta y acciones requeridas para solucionar una vulnerabilidad técnica.

Tabla 10. Brecha encontrada para el dominio de adquisición, desarrollo y mantenimiento de los sistemas de información
Fuente: Elaboración propia.

4.2.2.9 Dominio: Gestión de incidentes de la Seguridad de la Información

Se documentan en la Tabla 11. Brecha encontrada para el dominio de gestión de incidentes de Seguridad de la Información, los aspectos no cubiertos para cada uno de los controles del dominio de gestión de incidentes de la Seguridad de la Información del estándar ISO/IEC 27002:2005.

Identificador del control	Control	Brecha
13.1.1.	Reporte de eventos en la Seguridad de la Información.	No existen políticas relacionadas con la gestión de incidentes de Seguridad de la Información, pero sí un proceso de *"Atención de Incidentes de Seguridad Informática",* que aunque no cubre todo el alcance de la Seguridad de la Información, sí lo hace con algunos de los objetivos de gestión de incidentes de esta área. La brecha que se identifica en este control es que no se define en una política ni una actividad dentro del proceso mencionado previamente, cuál es el punto de contacto para reportar los incidentes y que además, se garantice que este punto de contacto sea conocido por toda la organización.
13.2.1.	Reporte de las debilidades en la seguridad.	No se identifica una política que indique que los empleados no deban probar las debilidades y vulnerabilidades de Seguridad de la Información, cuando se sospeche de su existencia, estas debieran ser reportadas.
13.2.1.	Responsabilidades y procedimientos.	Este control se cubre por el proceso de *"Atención de Incidentes de Seguridad Tecnológica"* del Banco, ubicado en el Sitio de Calidad, donde se documentan los procedimientos, roles y responsabilidades para la gestión de incidentes.

Identificador del control	Control	Brecha
13.2.2.	Aprender de los incidentes en la Seguridad de la Información.	Este control se considera cubierto a partir del procedimiento *"Planificar y Ejecutar Estudio de Análisis de Incidentes de Seguridad"* del proceso *"Atención de Incidentes de Seguridad Tecnológica".*
13.2.3.	Recolección de evidencia.	No se define una política explícita para la recolección de evidencia en caso que un incidente deba ser llevado a la corte, de manera tal, que esta evidencia se proteja adecuadamente para mantener su integridad y poder ser presentada ante la corte.

Tabla 11. Brecha encontrada para el dominio de gestión de incidentes de Seguridad de la Información
Fuente: Elaboración propia.

4.2.2.10 Dominio: Continuidad del negocio

Se documentan en la Tabla 12. Brecha encontrada para el dominio de continuidad del negocio, los aspectos no cubiertos para cada uno de los controles del dominio de continuidad del negocio del estándar ISO/IEC 27002:2005.

Identificador del control	Control	Brecha
14.1.1.	Incluir la Seguridad de la Información en el proceso de gestión de continuidad del negocio.	Este control se considera cubierto a partir del proceso de *Atención de Incidentes de Seguridad Tecnológica*, en el cual dentro de su flujo se ubica un procedimiento para recurrir a planes de contingencia para la continuidad del negocio en caso de ser necesario.

Identificador del control	Control	Brecha
14.1.2.	Continuidad del negocio y evaluación del riesgo.	Se identifica como brecha, que dentro de las políticas de continuidad del negocio, no se detalla que la evaluación de riesgos sea llevada a cabo con los propietarios de cada proceso.
14.1.3.	Desarrollar e implementar los planes de continuidad, incluyendo la Seguridad de la Información.	Este control se considera cubierto a partir del plan de continuidad, que se encuentra dividido en un conjunto de sub-planes por cada división del Banco. En estos planes se detallan los roles, responsabilidades y acciones a ejecutar en caso de un determinado incidente.
14.1.4.	Marco Referencial de la planeación de la continuidad del negocio	Se identificó como brecha, que el plan de continuidad no determina las condiciones para su activación. No existe una política que indique que los planes de continuidad se incluyan dentro del proceso de gestión del cambio organizacional. Por otro lado, no se identificó una política sobre el procedimiento para trasladar las operaciones a un sitio interno.
14.1.5.	Prueba, mantenimiento y re-evaluación de los planes de continuidad del Negocio.	No se identificó que se encontrara documentado cómo y cuándo se debiera probar cada elemento de los planes.

Identificador del control	Control	Brecha
		Tampoco hay políticas que determinen que se debieran probar los planes según los distintos escenarios posibles, así mismo; no hay políticas sobre las pruebas del sitio alterno, pruebas recuperación técnica de sistemas y de servicios externos, etc.

Tabla 12. Brecha encontrada para el dominio de continuidad del negocio
Fuente: Elaboración propia.

4.2.2.11 Dominio: Cumplimiento

Se documentan en la Tabla 13. Brecha encontrada para el dominio de cumplimiento, los aspectos no cubiertos para cada uno de los controles del dominio de cumplimiento del estándar ISO/IEC 27002:2005.

Identificador del control	Control	Brecha
15.1.1.	Identificación de la legislación aplicable.	Este control se encuentra cubierto a partir de la documentación de toda legislación externa aplicable al Banco, ubicada y puesta a disposición para todos los empleados en la intranet de la Institución. Esta legislación se ubica específicamente en la intranet en la sección de *Marco regulatorio externo,* situado dentro del Gobierno Corporativo.
15.1.2.	Derechos de propiedad intelectual (IPR)	En este control se identifica como brecha, que no se definen políticas para la adecuada gestión de licencias de *software*.

Identificador del control	Control	Brecha
		Tampoco existen políticas internas para regular la copia de información, aunque podrían regirse según el marco regulatorio externo.
15.1.3.	Protección de registros organizacionales.	No se establecen políticas, controles o lineamientos para la gestión y protección de los registros organizacionales, donde se contemplen los criterios para la clasificación de dichos registros, la protección y revisión de la capacidad de los medios que los almacenan y políticas de retención, manipulación y eliminación de los registros.
15.1.4.	Protección de la *data* y privacidad de la información personal.	Se considera cubierto ya que, aunque no existen políticas internas para la protección de datos, el Banco se rige en dicha área, siguiendo lo establecido por la *Ley N° 8968 - Protección de la Persona frente al tratamiento de sus datos personales.*
15.1.5.	Prevención del mal uso de los medios de procesamiento de la información.	Aunque, basado en el Código de Ética del Banco se indique que todo empleado está en obligación de proteger los activos de la institución, no existe una política para que el uso de cualquier medio de procesamiento de la información deba ser autorizado por la gerencia, así mismo; no existe una política que indique que se realice un monitoreo, asesorado legalmente, sobre el uso de los medios.

Identificador del control	Control	Brecha
15.1.6.	Regulación de controles criptográficos.	No se identificaron regulaciones externas o internas, por lo cual se podría desarrollar, a manera interna de la organización, políticas para llenar la brecha de este control.
15.2.1	Cumplimiento con las políticas y estándares de seguridad.	No hay una política que establezca que los gerentes deban asegurarse que se cumplan las Políticas Específicas de Seguridad de la Información dentro de su área de responsabilidad y que si se diera un incumplimiento, el respectivo gerente debiera asegurarse de identificar la causa y que se lleve a cabo las acciones requeridas para su solución.
15.2.2.	Chequeo del cumplimiento técnico.	Este control se considera cubierto a partir del proceso de *Evaluaciones Internas de Cumplimiento de TI*.
15.3.1.	Controles de auditoría de los sistemas de información.	A pesar que se establece el proceso de *Evaluaciones Internas de Cumplimiento de TI*, no se definen políticas, controles o lineamientos que acompañen el proceso. Por ejemplo, que se establezcan políticas que aseguren que los auditores deban gozar independencia del área auditada, que el alcance de las auditorías sea aprobado por la Gerencia o limitar los privilegios del rol de auditor a sólo lectura de información y no a su modificación.

Identificador del control	Control	Brecha
15.3.2.	Protección de las herramientas de auditoría de los sistemas.	No existen políticas asociadas con la protección de las herramientas de auditoría en sistemas.

Tabla 13. Brecha encontrada para el dominio de cumplimiento
Fuente: Elaboración propia.

4.3 Propuestas de mejora para las Políticas de Seguridad de la Información

Las propuestas de mejora para las Políticas específicas de la Seguridad de la Información consisten en un conjunto de políticas, controles y lineamientos recomendados para cerrar la brecha existente, documentada en la sección 4.2.2, Documentación de brecha, sobre los cuatro dominios prioritarios de la Seguridad de la Información para el Banco, los cuales son:

- Organización de la Seguridad de la Información: Este dominio se selecciona, pues permite definir bases para mejorar el Gobierno de la Seguridad de la Información.
- Gestión de activos: Dado que actualmente no existen políticas específicas que lo regulen.
- Adquisición desarrollo y mantenimiento de los sistemas de información: Para este dominio sí existen políticas específicas; sin embargo, es elegido porque las Políticas específicas de la Seguridad de la Información atienden más robustamente otros dominios, abriendo una ventana para identificar mejoras en la adquisición desarrollo y mantenimiento de los sistemas de información.
- Gestión de incidentes de la Seguridad de la Información: Al igual que el dominio de gestión de activos, este se escoge dado que actualmente no existen políticas específicas que lo regulen.

Las propuestas planteadas son alineadas al estándar ISO/IEC 27002:2005. Es importante mencionar que algunas políticas y controles se inician enumerando desde uno y otras desde otro número, ya que se trata de continuar la enumeración actual según la sección a la que se recomienden.

4.3.2 Propuestas de mejora para el dominio de organización de la Seguridad de la Información

Se plantean las siguientes propuestas de mejora, según la valoración realizada para el presente dominio:

- **Propuesta de mejora:** Agregar las siguientes responsabilidades al Comité de la Seguridad de la Información dentro del Banco:
    - Velar que la Gerencia provea los recursos necesarios para la gestión de la Seguridad de la Información.
    - Aprobar roles y responsabilidades para la gestión de la Seguridad de la Información.
    - Aprobar las metodologías y procesos para la gestión de la Seguridad de la Información.
    - Definir un propietario para cada uno de los procesos de Seguridad de la Información.
    - Establecer los niveles de autorización dentro del Sistema de Gestión de la Seguridad de la Información.

- **Propuesta de mejora:** Definir un comité encargado de labores y toma de decisiones a nivel operativo de la Seguridad de la Información denominado *Comité de Coordinación de la Seguridad de la Información*, el cual tenga por responsabilidades las siguientes:

    - Velar por la asignación de recursos a cada actividad de la gestión de la Seguridad de la Información.
    - Identificar los roles y las responsabilidades para la gestión de la Seguridad de la Información sea aprobado por la Gerencia.

- Solicitar una consultoría especializada para llevar a cabo tareas de la Seguridad de la Información que no puedan ejecutarse con recursos internos.
- Velar que las actividades de la Seguridad de la Información se ejecuten según las políticas.
- Definir las metodologías y procesos para la gestión de la Seguridad de la Información.
- Evaluar la información recibida del monitoreo y recomendar acciones de mejora en caso de ser requeridas.
- Mantener contacto con grupos especializados en el tema de Seguridad de la Información con el fin de apoyar la mejora continua.

- **Propuesta de mejora:** Aunque actualmente se manejan acuerdos de confidencialidad dentro de la organización, no existen políticas específicas que definan los requerimientos que estos acuerdos debiesen tener para mantener la Seguridad de la Información. Dado lo anterior y siguiendo la enumeración de la sección *I. Aspectos organizativos para la seguridad* del documento de Políticas específicas de la Seguridad de la Información, se propone la siguiente política y controles para dicha sección:

P-4. El Comité de Coordinación de la Seguridad de la Información define los acuerdos de confidencialidad y no divulgación con empleados, clientes y terceros, con el fin de proteger toda aquella información puesta a su disposición, los cuales serán sometidos a aprobación por el Comité de Seguridad de la Información.

C-4.1. El Comité de Coordinación de la Seguridad de la Información revisa periódicamente los requerimientos de confidencialidad para garantizar que los acuerdos se ajusten al contexto organizacional.

C-4.2. El Comité de Coordinación de la Seguridad de la Información define un modelo base para el establecimiento de acuerdos de confidencialidad donde se definan los requisitos mínimos a considerar. Todo acuerdo de confidencialidad debe considerar al menos lo siguiente:

- Identificación de la información que va a ser expuesta.
- Identificación de cual información expuesta debe ser protegida.
- Duración del acuerdo de confidencialidad. Se deben considerar los casos en que la duración de los acuerdos deba ser permanente.
- Responsabilidades de las partes.
- Acciones a tomar en caso de finalización del acuerdo.
- Acciones a llevar a cabo en caso de incumplimiento del acuerdo.
- Mecanismos y controles para el retorno o destrucción de la información divulgada.

C-4.3. Los funcionarios que fungen como contraparte para los clientes y terceros deben suscribir acuerdos de confidencialidad que aseguren el cumplimiento de los requerimientos mínimos de confidencialidad para el resguardo de la información expuesta en relación con el Banco. En estos acuerdos, deben definirse los requerimientos para el estudio y análisis de los incidentes de Seguridad de la Información.

- **Propuesta de mejora:** El estándar ISO/IEC 27002:2005 recomienda que se realicen revisiones de la gestión de la Seguridad de la Información, por tal razón, se propone la siguiente política y controles para la sección *I. Aspectos organizativos para la seguridad* del documento de Políticas específicas de la Seguridad de la Información:

P-5. La División Gestión y Desarrollo, a través del Departamento Gestión de Calidad, es responsable de realizar evaluaciones de la Seguridad de la Información, al menos una vez al año, con el fin de verificar el cumplimiento del marco regulatorio establecido e identificar oportunidades de mejora para la Seguridad de la Información.

C-5.1. Para la planeación y ejecución de todas las evaluaciones internas de cumplimiento relacionadas con la Seguridad de la Información, se aplica lo establecido en el proceso de Evaluación del Sistema de Control Interno, detallado en el Sitio de Calidad.

P-6. Es responsabilidad de los directores de división del Banco Central de Costa Rica, asegurar la aplicación de acciones correctivas y preventivas necesarias para eliminar las disconformidades detectadas y sus causas, a la luz de los resultados que arrojen las evaluaciones efectuadas de la Seguridad de la Información.

C-6.1. Una vez que les haya sido entregado el Informe de Evaluación de la Seguridad de la Información, las divisiones deben establecer un cronograma para la ejecución de las acciones correctivas y preventivas. Dicho cronograma debe ser entregado al Departamento de Gestión de Calidad.

C-6.2. El Departamento de Gestión de Calidad debe consolidar todos los cronogramas y darle seguimiento al cumplimiento de las actividades ahí establecidas, mediante la coordinación con las divisiones involucradas.

P-7. El Comité de Seguridad de la Información puede solicitar la contratación de una auditoría externa para la Seguridad de la Información, según los requerimientos del Sistema de Seguridad de la Información y los resultados obtenidos en los procesos de evaluación interna.

- **Propuesta de mejora:** Con el fin de regular la seguridad de los datos expuestos en las relaciones con clientes y terceros, se propone plantear las siguientes políticas y controles para para la sección *I. Aspectos organizativos para la seguridad* del documento de Políticas específicas de la Seguridad de la Información:

P-8. La División Gestión y Desarrollo es responsable de definir los mecanismos necesarios para mantener la confidencialidad, integridad y disponibilidad de la información expuesta en las relaciones con clientes y terceros.

C-8.1. El Departamento de Gestión de Infraestructura debe asignar privilegios a los clientes y terceros, según su relación comercial con el Banco, con el objetivo de restringir el acceso a la información. Al definir los privilegios se deben considerar los siguientes aspectos:

- Todo cliente o tercero posee un nombre de usuario único.
- El método de autenticación de los clientes y terceros es a través del uso de su nombre de usuario y contraseña.
- En caso que cambien las condiciones en los acuerdos con los clientes o terceros, lo privilegios se ajustan a dicho cambio.
- Una vez finalizada la relación con un cliente o tercero se retiran sus derechos de acceso.

P-9. La división del Banco que va a recibir un servicio por parte de un tercero, es responsable de establecer dentro del cartel de contratación los requerimientos relativos a: servicio o producto a recibir, calidad, continuidad del negocio, desempeño, monitoreo y evaluación del servicio, cuando aplique.

C-9.1. Para proteger los activos, dentro de los acuerdos con terceros se exige que estos deban actuar conforme a las normas de comportamiento establecidas en el Código de Ética de la organización.

C-9.2. Las áreas físicas a las cuales puede acceder un tercero se restringen de acuerdo con la relación comercial que posea con el Banco.

C-9.3. En los acuerdos con terceros se definen las responsabilidades de la terminación de la relación y las responsabilidades legales de las partes.

C-9.4. En la relación con terceros, se define el proceso de escalamiento de solución de problemas.

4.3.3 Propuestas de mejora para el dominio de gestión de activos

Se plantean las siguientes propuestas de mejora, según la valoración realizada, para el presente dominio:

- **Propuesta de mejora:** En el documento de Políticas específicas de la Seguridad de la Información no existe una sección específica para la gestión de activos. Dado lo anterior, una propuesta de mejora es agregar una sección (continuando la numeración de secciones de las Políticas específicas de la Seguridad de la Información) denominada *VI. Gestión de activos,* donde se especifiquen las políticas, controles y lineamientos propuestos por el Banco Central de Costa Rica para el proceso de gestión de activos enfocado a la Seguridad de la Información.

- **Propuesta de mejora:** Para la sección propuesta para las Políticas específicas de la Seguridad de la Información denominada *VI. Gestión de activos,* se proponen la siguiente política y controles con respecto a la gestión de inventarios de activos enfocados a la Seguridad de la Información:

P-1. El Comité de Coordinación de la Seguridad de la Información gestiona un inventario de los activos claves para el cumplimiento de los objetivos de la Seguridad de la Información.

C-1.1. Existe un proceso para el mantenimiento y actualización del inventario de activos de Seguridad de la Información, que asegura que cualquier actualización del inventario se alinea a otros inventarios de la organización.

- **Propuesta de mejora:** Para la sección propuesta para las Políticas específicas de la Seguridad de la Información denominada *VI. Gestión de activos,* se proponen la siguiente política y controles con respecto a la clasificación y etiquetado de los activos de información:

P-2. El Comité de Coordinación de la Seguridad de la Información protege los activos de información a través del establecimiento de mecanismos para su clasificación y manejo.

C-2.1. El Comité de Coordinación de la Seguridad de la Información define un protocolo de clasificación y reclasificación de los activos información, considerando los siguientes aspectos:

- Los activos de información se clasifican según los riesgos comerciales asociados a estos.
- Los activos de información se reclasifican según el cambio en los riesgos comerciales asociados a estos.

C-2.2. El Comité de Coordinación de la Seguridad de la Información define niveles de clasificación para los activos de información en términos de tres dimensiones: confidencialidad, integridad y disponibilidad. Se definen los siguientes niveles en los cuales se puede ubicar un activo de información:

- **Confidencialidad**
  - [1] Pública: Activo de dominio público. No hay ningún impacto si se distribuye. La seguridad a este nivel es mínima.

- [2] Uso Interno: Activo no aprobado para la circulación general fuera de la organización, en cuyo caso, su acceso incomodaría a la organización o la gerencia, pero que es poco probable que dé lugar a pérdidas financieras o a un daño serio a la credibilidad o imagen de la organización. La seguridad a este nivel debe ser controlada pero normal.
- [3] Propietaria: Activo normalmente para el uso del personal autorizado solamente. La seguridad a este nivel es alta.
- [4] Confidencial: Activo que se considera crítico para las operaciones de la organización y podría impedirlas si se comparte o se publica. Este no se debe copiar y jamás debe salir del control de la organización sin una previa autorización. La seguridad para estos activos debe ser muy alta.
- [5] Máxima Seguridad: Activos internos altamente sensibles. Los activos clasificados como “Máxima Seguridad” tienen una distribución muy restringida y siempre se deben proteger. La seguridad a este nivel es la más alta posible.

- **Integridad**
  - [1] Baja: La alteración o modificación en este activo representa un riesgo bajo. No importa si el activo es alterado o modificado. En caso de alteración o modificación no se tendrán consecuencias de ningún tipo para la organización. Un ejemplo podría ser una base de datos de pruebas en un servidor de desarrollo de aplicaciones.
  - [2] Media: La alteración o modificación en este activo representa un riesgo medio. Tiene importancia la alteración o modificación, pero no representa un riesgo elevado para la organización. En caso de alteraciones, se pueden alterar algunos servicios o la prestación de los mismos, pero su afectación no es generalizada.

Un ejemplo podría ser la alteración de datos en una base de datos copiada con direcciones de clientes. Si se modifican datos, estos se pueden regenerar a partir de una nueva copia.

- [3] Alta: La alteración o modificación en este activo representa un alto riesgo para la organización. En caso de alteraciones o modificaciones se podría afectar seriamente alguna operación, se podría incurrir en incumplimientos legales, etc.

- **Disponibilidad**
  - [1] Baja: El activo puede estar sin funcionar hasta una semana sin que exista ninguna afectación en los servicios donde este está involucrado.
  - [2] Media: El activo puede estar sin funcionar hasta un día completo sin que exista ninguna afectación en los servicios donde este está involucrado.
  - [3] Alta: El activo, los datos o los servicios asociados pueden estar sin funcionar hasta un máximo de cuatro horas sin que se produzcan fallas o incumplimientos críticos para la organización.
  - Muy Alta: El activo, los datos o los servicios asociados no pueden dejar de estar disponibles. Cualquier fallo o retraso en la prestación del servicio puede llevar a la organización a serios incumplimientos legales o pérdida seria de imagen.

Nota: El control C-2.2 es tomado de los criterios de clasificación de los activos de información en términos de confidencialidad, integridad y disponibilidad del Banco Central de Costa Rica

C-2.3. La información es etiquetada según los niveles de confidencialidad establecidos para los activos de información, considerando aspectos legales, regulatorios, de sensibilidad, criticidad y de su valor para la organización.

C-2.4. El Comité de Coordinación de la Seguridad de la Información vela porque se asigne un propietario para cada uno de los activos de información, de forma que es responsabilidad del propietario del activo asegurar que este sea clasificado según los procedimientos de clasificación de activos del Banco Central.

P-3. El Comité de Coordinación de la Seguridad de la Información define procesos para el etiquetado y manejo de la información, según su clasificación.

C-3.1. Toda información, ya sea en medios físicos o electrónicos, es etiquetada, según los criterios de clasificación de la información del Banco.

C-3.2. El Banco solicita a sus empleados, contratistas y terceros que manejen la información de conformidad con su categoría de clasificación.

4.3.4 Propuestas de mejora para el dominio de adquisición, desarrollo y mantenimiento de los sistemas de información

Se plantean las siguientes propuestas de mejora, según la valoración realizada, para el presente dominio:

- **Propuesta de mejora:** La política P-2 de la sección de las Políticas específicas de la Seguridad de la Información denominada *V. Adquisición, desarrollo y mantenimiento de sistemas*, dice lo siguiente:

  “El Banco Central de Costa Rica establece mecanismos para validar los datos de entrada y de salida de las aplicaciones que se desarrollen o mejoren en la organización para evitar corrupción en el procesamiento, modificaciones deliberadas y la pérdida, la modificación o uso erróneo de datos del usuario en los sistemas de información.” (Banco Central de Costa Rica, 2014b).

Con el fin de llevar un registro de las actividades llevadas a cabo para la prueba de datos de entrada y salida en los sistemas, se propone agregar a la política anterior el siguiente control:

C-2.2. El Área de Validación y Verificación mantiene un registro sobre las actividades relacionadas con la prueba de datos de entrada y salida.

- **Propuesta de mejora:** Con el fin de regular la protección de los datos operacionales de ser expuestos en ambientes de prueba, se propone agregar a la política P-2 de la sección de las Políticas específicas de la Seguridad de la Información denominada *V. Adquisición, desarrollo y mantenimiento de sistemas,* citada en la propuesta de mejora anterior, el siguiente control:

  C-2.3. No se debe utilizar datos operacionales en ambientes de prueba, a menos que sea estrictamente necesario. En caso de utilizarlos se deben considerar los siguientes aspectos:

  - El Área de Validación y Verificación debe solicitar autorización del área del negocio dueña de datos que vayan a ser utilizados en ambientes de prueba.
  - La información operacional utilizada en ambientes de prueba se borra inmediatamente después de su uso.
  - Se mantiene un registro de toda la información operacional que ha sido copiada en ambientes de prueba.

- **Propuesta de mejora:** La política P-4 de la sección de las Políticas específicas de la Seguridad de la Información denominada *V. Adquisición, desarrollo y mantenimiento de sistemas*, dice lo siguiente:

“El Banco Central de Costa Rica establece mecanismos para los procesos de instalación, custodia, uso y manejo del *software*, aplicaciones de escritorio y de los sistemas de información de la organización para mantener un adecuado nivel de seguridad.” (Banco Central de Costa Rica, 2014b).

Con el fin mejorar el control del *software* puesto en operación se propone agregar a la política anterior los siguientes controles:

C-4.5. Los sistemas operacionales son puestos a disposición de los usuarios sólo a través de códigos ejecutables aprobados.

C-4.6. Se documenta y gestiona la configuración de todo *software* puesto en operación para lo que se deben considerar los siguientes aspectos:

- Se mantiene un registro de todas las actualizaciones realizadas sobre un determinado *software*.
- Se almacenan las dos versiones anteriores de un determinado *software* como medida de contingencia.
- Se define el procedimiento para recuperar un sistema operacional.

- **Propuesta de mejora:** La política P-5 de la sección de las Políticas específicas de la Seguridad de la Información denominada *V. Adquisición, desarrollo y mantenimiento de sistemas,* dice lo siguiente:

“El Banco Central de Costa Rica mantiene procesos formales de control de cambios para cuando se implemente o se brinde soporte a una aplicación, paquete de *software* o sistema de información.” (Banco Central de Costa Rica, 2014b)

Con el fin de detallar los controles específicos del proceso de gestión de cambios al *software* dentro de las políticas, se proponen los siguientes:

C-5.2. La División de Servicios Tecnológicos establece una plantilla con los requerimientos mínimos de información para solicitar un cambio, con el fin de garantizar que se contemplen todos los aspectos relevantes a un determinado cambio.

C-5.3. Dentro del proceso de gestión del cambio se definen niveles para la autorización de un cambio. Para la autorización de un cambio debe considerarse lo siguiente:

- Sólo se aprueban aquellas solicitudes emitidas por personal autorizado.
- Ningún cambio se implementa hasta haber sido probado y autorizado por el área de negocios responsable.

C-5.4. Es responsabilidad del Director de División que solicita un cambio a una aplicación, paquete de *software* o sistema de información en coordinación con el Comité de Control de Cambios, evaluar el impacto del cambio en el negocio antes de su aprobación. Para minimizar el impacto en el negocio, se considera lo siguiente:

- Todo cambio se comunica a las personas afectadas por el mismo.
- Se brinda capacitación al usuario para colaborar a la aceptación del cambio.
- Cuando se propone un cambio se evalúa que no afecte otras tecnologías del negocio, de manera tal que no perturbe la operativa del negocio.

C-5.5. Es responsabilidad de la División de Servicios Tecnológicos mantener un control de todas las solicitudes de cambio, ya sean aceptadas o rechazadas.

C-5.6. Es responsabilidad del funcionario de la División de Servicios Tecnológicos que funge como líder técnico de la solución tecnológica, asegurar que se realicen las pruebas previas a la liberación de un cambio, al incluir dentro del cronograma una fase de pruebas pre-implementación, con el fin de minimizar los riesgos una solución vez liberada.

C-5.7. Es responsabilidad del funcionario de la División de Servicios Tecnológicos que funge como líder técnico de la solución tecnológica, asegurar que se realicen las pruebas de verificación, al incluir dentro del cronograma una fase de pruebas pos-implementación, con el fin de asegurar que aquellos ambientes afectados por la modificación se mantengan íntegros. Dentro del presupuesto para la implementación del cambio se debe considerar que este pueda cubrir el costo de la ejecución de las pruebas, si aplica.

C-5.8. Es responsabilidad del Líder de la Solución del cambio asegurar que se actualice toda la documentación requerida.

- **Propuesta de mejora:** Para gestionar las vulnerabilidades identificadas en los sistemas se plantea la política P-7 de la sección *V. Adquisición, desarrollo y mantenimiento de sistemas,* de las Políticas específicas de la Seguridad de la Información, la cual dice lo siguiente:

  “El Banco Central de Costa Rica establece mecanismos para reducir los riesgos asociados a la explotación de las vulnerabilidades existentes y publicadas que afecten los diferentes sistemas que existen en la organización.” (Banco Central de Costa Rica, 2014b).

  Se consideran que la política anterior se puede complementar con el siguiente control:

C-7.4. La División de Servicios Tecnológicos define un proceso para la gestión de vulnerabilidades técnicas identificadas en los sistemas de información donde se define lo siguiente:

- Roles y responsabilidades.
- Una actividad que consiste en la identificación de las acciones requeridas para atender una vulnerabilidad.
- El tiempo mínimo y máximo para atender una vulnerabilidad.

- **Propuesta de mejora:** Para la sección de las Políticas específicas de la Seguridad de la Información denominada *V. Adquisición, desarrollo y mantenimiento de sistemas,* se propone la siguiente política y controles enfocados a la gestión de los controles criptográficos dentro del Banco:

P-8. La División de Servicios Tecnológicos define controles criptográficos a partir de la evaluación del riesgo asociado con la información expuesta en ambientes informáticos, con el fin de resguardarla.

C-8.1. La División de Servicios Tecnológicos documenta el proceso para la gestión de claves criptográficas y define los registros que deben mantenerse para evidenciar la implementación de este proceso.

C-8.2. La División de Servicios Tecnológicos restringe el acceso al equipo utilizado para generar claves criptográficas.

- **Propuesta de mejora:** Con el fin de mantener la integridad en paquetes de *software* provistos externamente, se proponen la siguiente política para la sección *V. Adquisición, desarrollo y mantenimiento de sistemas,* de las Políticas específicas de la Seguridad de la Información:

P-9. El División de Servicios Tecnológicos realiza cambios sobre paquetes de *software* sólo a través de aplicación de parches o cambios de versión, cuando sea requerido.

- **Propuesta de mejora:** Para gestionar los desarrollos externos de *software* y asegurar que se cumplan con los requerimientos establecidos, se proponen la siguiente política y controles para la sección *V. Adquisición, desarrollo y mantenimiento de sistemas,* de las Políticas específicas de la Seguridad de la Información:

P-10. La División de Servicios Tecnológicos es responsable de asegurar que todo *software* desarrollado de manera externa a la organización cumpla con los requerimientos establecidos, asegurando así el cumplimiento de los objetivos del desarrollo.

C-10.1. La División de Servicios Tecnológicos es responsable de asesorar a la división solicitante del desarrollo externo con el fin de establecer en el cartel de contratación todos los requerimientos de funcionalidad y seguridad del desarrollo.

C-10.2. Las divisiones solicitantes de un desarrollo externo son responsables de incluir dentro del contrato con el proveedor el derecho de revisión del desarrollo y la calidad del *software*. Debe considerarse la coordinación con la División de Servicios Tecnológicos para que sean los responsables de la ejecución de dichas revisiones.

C-10.3. Las divisiones solicitantes de un desarrollo externo en conjunto del Área de Validación y Verificación de la División de Servicios Tecnológicos, son responsables de establecer y ejecutar un plan de pruebas para asegurar que el *software* cumpla con los requerimientos establecidos.

C-10.4. Las divisiones solicitantes de un desarrollo externo son responsables de negociar con el proveedor los derechos sobre las licencias, propiedad sobre el código fuente y los derechos de propiedad intelectual.

4.3.5 Propuestas de mejora para el dominio de gestión de incidentes de la Seguridad de la Información

Se plantean las siguientes propuestas de mejora, según la valoración realizada, para el presente dominio:

- **Propuesta de mejora:** En el documento de Políticas específicas de la Seguridad de la Información no existe una sección específica para la gestión de incidentes de la Seguridad de la Información. Dado lo anterior una propuesta de mejora es agregar una sección (posterior a la última sección propuesta, *VI. Gestión de activos, y* continuando la numeración de secciones de las Políticas específicas de la Seguridad de la Información) denominada *VII. Gestión de incidentes de la Seguridad de la Información, donde* se especifiquen las políticas, controles y lineamientos propuestos por el Banco Central de Costa Rica, para el proceso de gestión de incidentes de la Seguridad de la Información.

- **Propuesta de mejora:** Con el fin de complementar el proceso de *Atención de Incidentes* del Banco*,* se recomienda agregar a la sección propuesta para las Políticas específicas de la Seguridad de la Información, *VII. Gestión de incidentes de la Seguridad de la Información,* las siguientes políticas y controles:

P-1. La División Gestión y Desarrollo atiende los incidentes de la Seguridad de la Información, haciendo uso de mecanismos que le permitan minimizar el impacto de los incidentes en el operar de la organización.

C-1.1. La División Gestión y Desarrollo establece un proceso de *Atención de Incidentes* con el fin de atender todos los asociados con la Seguridad de la Información, donde se define que el punto de contacto para reportar incidentes se ubica en la intranet.

C-1.2. La División Gestión y Desarrollo es responsable de definir los tipos de incidente de Seguridad de la Información y las divisiones encargadas de solucionarlos con el fin que estas últimas establezcan los procedimientos y respuestas específicas para su atención.

C-1.3. La División Gestión y Desarrollo es responsable de mantener un registro de los incidentes atendidos y las acciones aplicadas con el fin de mejorar la atención y el conocimiento de los incidentes de la Seguridad de la Información que se presenten en el Banco.

C-1.4. Es establecida como responsabilidad de todo empleado y tercero, reportar los incidentes de Seguridad de la Información.

P-2. La División Gestión y Desarrollo es responsable de minimizar la ocurrencia de incidentes a través de mecanismos de monitoreo y análisis de la información recolectada de los incidentes atendidos, para así reforzar la continuidad de las operaciones diarias del negocio.

C-2.1. La División Gestión y Desarrollo es responsable de planificar y ejecutar estudios de análisis de incidentes de Seguridad de la Información con el fin de identificar posibles tendencias en su ocurrencia.

P-3. Es definida como obligación de todo empleado o tercero, reportar cualquier vulnerabilidad detectada en la Seguridad de la Información. En caso de identificar una vulnerabilidad se debe considerar lo siguiente:

- El punto de contacto para reportar vulnerabilidades de la Seguridad de la Información se ubica en la intranet.
- Ningún empleado o tercero debe hacer prueba de las vulnerabilidades sospechadas.

P-4. El Banco Central es responsable de recolectar evidencia íntegra y que pueda ser presentada en la Corte según los requisitos establecidos en la ley, cuando sea necesario iniciar una acción legal en contra de una persona, para esto la Gerencia debe iniciar el debido proceso administrativo, a través de una investigación preliminar.

C-3.1. La División Asesoría Jurídica es responsable de almacenar la evidencia física y electrónica en un lugar seguro para evitar su modificación, pérdida o destrucción durante el periodo de investigación preliminar. Para aquella evidencia física se considera lo siguiente:

- Registrar la persona, el lugar y la fecha del descubrimiento de un documento utilizado como evidencia.
- Registrar los testigos del hallazgo.

C-3.2. La División de Servicios Tecnológicos es responsable de asegurar que toda evidencia emitida por lo sistemas de información sea admitida por la Corte. Como medida de respaldo de la evidencia electrónica se crea una copia y se realiza un registro.

Capítulo V: Conclusiones y recomendaciones

5.1. Conclusiones

Se analizó una serie de documentos a través del desarrollo del proyecto, se detallaron los resultados más relevantes y además, se llevaron a cabo reuniones con personas claves de la División Gestión y Desarrollo del Banco, lo cual permitió llegar a conclusiones relevantes sobre el proyecto.

A continuación se detallan las conclusiones identificadas y las recomendaciones por cada una de ellas.

1. Se cumplió con el objetivo general el cual, consistía en proponer mejoras a las Políticas específicas de la Seguridad de la Información, a través del cumplimiento de los objetivos específicos establecidos.

2. Se identificó que el Sistema de Gestión de la Seguridad de la Información del Banco Central de Costa Rica está constituido por una serie de documentos donde el más importante es el de Políticas específicas de la Seguridad de la Información. Puede señalarse el documento como el punto de referencia que indica cómo, en muchos dominios de la Seguridad de la Información, el Banco Central de Costa Rica atiende los requerimientos de disponibilidad, integridad y confidencialidad de la información.

   Es importante recalcar que, a pesar de que las Políticas específicas de la Seguridad de la Información se pueden considerar la “columna vertebral” del SGSI del Banco, este documento no contempla los dominios de continuidad del negocio, gestión de incidentes de la Seguridad de la Información, seguridad de los recursos humanos, gestión de activos y el dominio de cumplimiento, pero existen otros documentos que indican cómo debería gestionarse la Seguridad de la Información a través de dichos dominios.

3. En la valoración se logró detectar que existe un alto porcentaje de controles del estándar ISO/IEC 27002:2005 cubierto parcialmente por las Políticas Específicas de Seguridad de la Información. En el Capítulo IV: Análisis de resultados, se documenta la brecha identificada en la valoración donde se identifica que un alto porcentaje de controles está cubierto parcialmente y se detalla que dicha situación se presenta, pues algunas políticas se pueden asociar en lo general a controles del estándar ISO/IEC 27002:2005, pero cuando trata de hacerse un mapeo desde las políticas, controles y lineamientos hacia el detalle de cada control o como se le denomina dentro del estándar, lineamiento de implementación, se lograron identificar brechas, ya fueran pequeñas o grandes, pero que hacían que la cobertura de un determinado control fuera parcial y no total.

4. El marco normativo interno para la Seguridad de la Información puede mejorar, ya que para todo dominio del estándar ISO/IEC 27002:2005 se identificó una o más brechas durante la valoración. Para cerrar algunas de las brechas identificadas se planteó una propuesta de mejora, que consistió en la recomendación de una serie de políticas, controles y lineamientos complementarios a las actuales Políticas específicas de la Seguridad de la Información; sin embargo, esta propuesta fue sólo para los cuatro dominios prioritarios de la Seguridad de la Información para el Banco, por lo cual se mantiene una brecha desatendida para los dominios restantes, la cual debe tratarse con el fin de apegarse lo más posible al estándar ISO/IEC 27002:2005, pues así lo desea la Institución.

5. Se confirmó el enunciado de las Políticas Específicas de Seguridad de la Información que indica que el documento trata de homologar el tratamiento de la Seguridad de la Información establecido por el estándar ISO/IEC 27001:2005.

Haciendo lectura del documento y aplicando la herramienta de valoración, se logra identificar que la mayoría del contenido de las Políticas Específicas de Seguridad de la Información es asociable a una o más secciones del estándar ISO/IEC 27002:2005, complemento del estándar ISO/IEC 27001:2005. Sin embargo, no ocurre de manera contraria, no se puede asociar todo contenido del estándar ISO/IEC 27002:2005 a alguna política, control o lineamiento del documento.

6. Durante la investigación de conceptos para el marco teórico se identificó en las distintas fuentes de información consultadas, que toda medida tomada para garantizar la Seguridad de la Información debe estar basada en una adecuada gestión de riesgos, con el fin de que toda inversión sea justificable al negocio y provea los beneficios esperados. Actualmente no se consideró una evaluación de riesgo previa para la propuesta de políticas, controles y lineamientos, sino solamente el alineamiento al estándar ISO/IEC 27002:2005.

5.2. Recomendaciones

Adicional a la sección anterior, 5.1. Conclusiones, por cada conclusión se logró definir una o más recomendaciones con el objetivo de mejorar o mantener la calidad del Sistema de Gestión de la Seguridad de la Información del BCCR. A continuación se enlistan las recomendaciones, enumeradas según la conclusión a la que se asocian:

1.1. Implementar dentro de la metodología de planteamiento de políticas específicas para la Seguridad de la Información el uso de la herramienta elaborada.

1.2. Considerar la metodología utilizada en el proyecto como complemento con la gestión de riesgos de la Seguridad de la Información.

2.1. Asegurar que el documento de Políticas específicas de la Seguridad de la Información esté disponible para todo empleado, cliente y tercero que debiese tener acceso y cumplir este marco normativo.

2.2. Iniciar una campaña de comunicación a nivel organizacional sobre el tema de la Seguridad de la Información, el documento de las Políticas específicas de la Seguridad de la Información y el impacto del cumplimiento y no cumplimiento en la organización de las regulaciones planteadas.

3.1. Detallar los controles y lineamientos que se establecen en cada política específica de Seguridad de la Información planteada por el Banco.

3.2. Revisar el cumplimiento de las políticas, controles y lineamientos de la Seguridad de la Información actualmente existentes en el Banco.

3.3. Revisar que toda política, control y lineamiento existente cumple con los objetivos de tratamiento de riesgo para los cuales fueron establecidos, con el fin de evaluar si es necesario considerar otras alternativas.

4.1. Evaluar la factibilidad de aplicar las propuestas de mejora planteadas para las Políticas específicas de la Seguridad de la Información, tomando como base la evaluación del riesgo organizacional.

4.2. Desarrollar un plan de trabajo para la implementación de las propuestas de mejora.

4.3. Considerar los dominios para los cuales no se plantearon propuestas de mejora y de igual manera, tomando como base una evaluación del riesgo organizacional, proponer e implementar mejoras para las políticas, controles y lineamientos de dichos dominios.

4.4. Verificar que existan recursos para implementar cualquier propuesta de mejora.

4.5. Mantener el Sistema de Gestión de la Seguridad de la Información bajo el esquema de mejora continua, haciendo uso del ciclo PDCA, planteado por el estándar ISO/IEC 27001:2005.

5.1. Integrar dentro de las Políticas específicas de la Seguridad de la Información, los temas de seguridad de recursos humanos, gestión de activos, gestión de incidentes de la Seguridad de la Información y cumplimiento.

5.2. No incluir el dominio de continuidad del negocio en las Políticas específicas de la Seguridad de la Información, porque está normado en las Políticas específicas del Sistema Interno de Gestión; sin embargo, se debe considerar mantener siempre la relación de la continuidad del negocio con la Seguridad de la Información.

6.1. Identificar si existe la justificación a nivel de riesgos para implementar las propuestas de mejora planteadas.

6.2. Basar toda medida para garantizar la Seguridad de la Información en la adecuada evaluación de riesgos.

6.3. Integrar la Seguridad de la Información como un tema del Departamento de Riesgos, no sólo del de Gestión de Calidad, para que sea el primero el encargado de aplicar las metodologías de evaluación de riesgos que ya tienen definidas y así provean los insumos requeridos, para que se consideren las acciones necesarias para el tratamiento de riesgos de la Seguridad de la Información.

Referencias bibliográficas

AENOR. (2010). *AENOR - Certificación ISO 27001 de Sistemas de gestión de la Seguridad de la Información*. Recuperado el 2014, de http://www.aenor.es/aenor/certificacion/seguridad/seguridad_27001.asp#.VAKUDvl5M4I

Arribas, A. (2000). Comunicación en la empresa. La importancia de la información interna en la empresa. *Revista Latina de Comunicación Social*.

Asociación Española para la Calidad . (2013). *AEC - Seguridad de la Información*. Recuperado el 2014, de http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

Banco Central de Costa Rica. (2014a). *Banco Central de Costa Rica*. Recuperado el 2014, de http://www.bccr.fi.cr

Banco Central de Costa Rica. (2014b). *Políticas específicas de la Seguridad de la Información*. San José, Costa Rica.

Banco Central de Costa Rica. (s.f.). *Estructura de organización y funciones del BCCR.* San José.

Chardon, A. y González, J. (2002). *Indicadores para la Gestión de Riesgos*. Recuperado el 2014, de http://idea.unalmzl.edu.co/documentos/Anne-Catherine%20fase%20I.pdf

Hernández, R., Fernández, C. y Baptista, P. (2010). *Metodología de la investigación.* México D.F.: Mc Graw Hill.

Instituto Nacional de Tecnologías de la Comunicación. (s.f.). *INTECO - Formación, SGSI, Conceptos Básicos, Normativa*. Recuperado el 2014, de http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Normativa_SGSI/

ISO 27000 Directory. (2013). *An Introduction to ISO 27001, ISO 27002....ISO 27008*. Recuperado el 2014, de http://www.27000.org/

ISO/IEC. (2005a). *ISO/IEC 27001 Tecnología de la Información - Técnicas de seguridad - Sistemas de gestión de Seguridad de la Información - Requerimientos.*

ISO/IEC. (2005b). *ISO/IEC 27002 Tecnolgía de la Información - Técnicas de seguridad - Código para la práctica de la gestión de la Seguridad de la Información.*

ISOTools. (3 de octubre de 2013). *ISO 27001: Dominios Tecnológicos de Seguridad de la Información*. Recuperado el 2014, de http://www.isotools.org/2013/10/03/iso-27001-dominios/

ISOTools. (2014). *ISO 27001 Costes vs Beneficios* | *Software ISO*. Recuperado el 2014, de http://www.isotools.org/2013/05/15/iso-27001-costes-vs-beneficios/

IT Governance Institute. (2007). *COBIT 4.1.* Estados Unidos.

Mejía, R. (5 de julio de 2004). La Administración de Riesgos Empresariales. *AD-mister*.

Montuschi, L. (s.f.). *Datos, información y conocimiento. de la sociedad de la información a la sociedad del conocimiento.*

Office of Government Commerce. (2011). *ITIL Service Design.* United Kingdom: The Stationery Office.

Project Management Institute. (2014). *¿Qué es un estándar?* Recuperado el 2014, de http://americalatina.pmi.org/latam/pmbokguideandstandards/whatisastandar.aspx

Saint-Germain, R. (2005). Information Security Management Best Practice Based on ISO/IEC 17799. *The Information Management Journal*.

Suárez, M., y Ramis, J. (2008). Aplicación y Evolución de la Mejora Continua de Procesos en la Administración Pública. *Globalización, Competitividad y Gobernabilidad*.

Vera, L. (2008). *LA INVESTIGACION CUALITATIVA*. Recuperado el 2014, de http://www.ponce.inter.edu/cai/Comite-investigacion/investigacion-cualitativa.html

Glosario

Administración de riesgos: Coordinación de las acciones, la cual permite manejar la incertidumbre a través del establecimiento de medidas para identificar, valorar y manejar los riesgos.

Amenaza: Fenómeno de origen natural, socio-natural, tecnológico o antrópico en general, definido por su naturaleza, ubicación, recurrencia, probabilidad de ocurrencia, magnitud e intensidad (capacidad destructora).

Confidencialidad: Hecho que la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Control: Mecanismos utilizados para el tratamiento de riesgos.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por aquellos que lo requieran, siempre y cuando posean la debida autorización.

Estándar: Documento establecido por consenso, aprobado por un cuerpo reconocido y que ofrece reglas, guías o características para que se use repetidamente.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de procesamiento.

Mejora continua: Metodología sistemática desarrollada para ayudar a una organización a tener avances significativos en la manera que operan sus procesos

Política: Intención y dirección general expresada formalmente por la gerencia.

Riesgo: Posibilidad que un evento ocurra y sea capaz de poner en peligro el cumplimiento de los objetivos de la organización.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento.

Sistema de Gestión de Seguridad de la Información: Sistema basado en el riesgo y tiene por objetivo establecer, implementar, operar, monitorear, mantener, revisar y mejorar la Seguridad de la Información.

Vulnerabilidad: Probabilidad de sufrir daños a causa de la exposición a una determinada amenaza.

Anexos

Anexo 1: Control de cambios de proyecto

El presente documento detalla los cambios realizados al proyecto “Propuesta de mejora para las Políticas de Seguridad de la Información del Banco Central de Costa Rica, basado en el estándar ISO/IEC 27002:2005”, desde el planteamiento inicial, hasta la fecha de cierre. El objetivo es justificar formalmente las decisiones tomadas, por parte del patrocinador, profesor asesor, coordinadora del proyecto de graduación o el estudiante, que modifiquen de alguna forma el alcance del proyecto. En el siguiente cuadro se detallan los cambios realizados:

ID del cambio	Nombre del cambio	Descripción del cambio	Justificación	Solicitante del cambio	Responsable de ejecutar el cambio	Fecha en que el cambio fue propuesto
RC1	Ajuste del alcance del proyecto	Este cambio recomienda realizar las propuestas de mejora para las Políticas de Seguridad de la Información sobre los cuatro dominios del estándar IOS/IEC 27002:2005, prioritarios para el Banco Central de Costa Rica. Inicialmente se planteó realizar las propuestas de mejora sobre los once dominios establecidos por este.	Este cambio se plantea con el fin de realizar propuestas de mejora alineadas a los dominios de Seguridad de la Información de mayor prioridad para la institución. Con esto se busca brindar un resultado de mayor valor para el BCCR. Además, como recomendación en el tema de adaptación del estándar a una organización, es mejor iniciar con lo prioritario para la entidad.	Profesor Asesor: Rodrigo Bogarín.	Estudiante: Manfred Sierra Montoya.	11 de agosto de 2014.
RC2	Cambio del nombre del proyecto	Este cambio propone modificar el nombre del proyecto. Inicialmente el nombre era “Propuesta de mejora para la Política de Seguridad de la Información del Banco Central de Costa Rica” y el cambio propuesto es que se denomine de ahora en adelante “Propuesta de mejora para las Políticas de Seguridad de la Información del Banco Central de Costa Rica, basado en el estándar ISO/IEC 27002:2005”. Se agrega el nombre del estándar con el fin de especificar el marco de trabajo utilizado para realizar la propuesta de valor del proyecto.	Este cambio se plantea con el fin de que el nombre del proyecto represente de mejor manera su alcance y objetivos.	Estudiante: Manfred Sierra Montoya.	Estudiante: Manfred Sierra Montoya.	19 de agosto de 2014.

Anexo 2: Hoja de valoración completa

Se omite la columna de observaciones de la misma para poder ajustar la herramienta al tamaño de la página en este anexo.

Banco Central de Costa Rica

Herramienta de valoración de Políticas Específicas de Seguridad de la Información

Objetivo: El objetivo de esta herramienta es evaluar el contenido de los documentos que plantean políticas, controles, lineamientos, procesos o procedimientos cuya área de aplicación es mapeable a los dominios del estándar ISO/IEC 27002:2005.

Dominio		**5. Política de seguridad**			
Documentos evaluados					
Objetivo de control	**Control**	**Aspectos que políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir.**	**¿Se cumple el aspecto?**	**Evidencia**	**Cobertura del control**
5.1. Política de Seguridad de la Información	5.1.1. Documento de la política de Seguridad de la Información	Aprobación de la política de seguridad.			**Nula**
		La política define el término de Seguridad de la Información.			
		La política define objetivos de la Seguridad de la Información.			
		La política establece el alcance de la Seguridad de la			

		Información.			
		La política establece la intención de la gerencia, alineada a la estrategia de la institución.			
		La política identifica el marco referencial para definir controles.			
		La política define responsabilidades de la seguridad.			
		La política referencia a documentos que la sustentan.			
	5.1.2. Revisión de la política de Seguridad de la Información	Está identificado el dueño de la política.			**Nula**
		Se definen intervalos planeados de revisión.			
		Se define llevar un registro de la revisión gerencial.			
Dominio		**6.Organización de la Seguridad de la Información**			
Documentos evaluados					
Objetivo de control	**Control**	**Aspectos: qué políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir**	**¿Se cumple el aspecto?**	**Evidencia**	**Cobertura del control**
6.1. Organización interna	6.1.1. Compromiso de la gerencia con la Seguridad de la Información	La gerencia debe asegurarse de que los objetivos de seguridad se identifiquen y se alineen al negocio.			**Nula**
		Obligatoriedad de la gerencia de revisar y aprobar las políticas.			
		Obligatoriedad de la gerencia de revisar la efectividad de las políticas.			
		Obligatoriedad de la gerencia a brindar los recursos necesarios para la Seguridad de la Información.			
		Aprobación, por parte de la gerencia, sobre los roles y responsabilidades de Seguridad de la Información.			
		Iniciación, por parte de la gerencia, de planes y programas para mantener la conciencia sobre seguridad			

		Verificación de que la implementación de controles se coordine en toda la organización.			
		La gerencia debe identificar necesidades de consultoría con respecto a la Seguridad de la Información.			
	6.1.2. Coordinación de la Seguridad de la Información	Las actividades de Seguridad de la Información son coordinadas por representantes de distintas áreas.			Nula
		La coordinación debe asegurar que las actividades de seguridad se ejecuten de acuerdo con las políticas.			
		La coordinación debe identificar como manejar las disconformidades.			
		La coordinación es responsable de aprobar las metodologías y procesos para la seguridad.			
		La coordinación debe identificar cambios significativos en las amenazas y la exposición de la información.			
		La coordinación debe evaluar la idoneidad y coordinar la implementación de los controles de seguridad.			
		La coordinación debe promover la educación y capacitación de la Seguridad de la Información.			
		La coordinación debe evaluar la información recibida del monitoreo y recomendar las acciones apropiadas.			
	6.1.3. Asignación de las responsabilidades de la Seguridad de la Información	Definición de las responsabilidades para el trato de activos.			Nula
		Definición de responsabilidades para la ejecución de procesos de Seguridad de la Información.			
		Identificación de activos y procesos de seguridad asignados a cada sistema en particular.			
		Asignación de un responsable de cada activo o proceso de seguridad. Documentación de esta responsabilidad.			
		Definición y documentación de niveles de autorización.			
	6.1.4. Proceso de	Existencia de un proceso de autorización para nuevas			Nula

	autorización para facilidades procesadoras de información	facilidades.			
		Verificación de que *software* y *hardware* nuevos son compatibles con la tecnología actual.			
		Verificación del uso de dispositivos personales (laptops, tabletas electrónicas, smartphones, etc.).			
	6.1.5. Acuerdos de confidencialidad	Obligatoriedad de revisión de requerimientos de confidencialidad para acuerdos de no divulgación.			**Nula**
		Los acuerdos de confidencialidad deben indicar qué información debe protegerse.			
		Los acuerdos de confidencialidad deben indicar la duración del mismo.			
		Los acuerdos de confidencialidad deben indicar las acciones a realizar cuando estos se terminen.			
		Los acuerdos de confidencialidad deben indicar las responsabilidades y acciones de los firmantes.			
		Derechos de uso de la información confidencial.			
		Proceso de notificación de información confidencial divulgada. (Incumplimiento del acuerdo).			
		Destrucción o retorno de información cuando se termine el acuerdo.			
		Acciones esperadas en caso de incumplirse el acuerdo de confidencialidad.			
		Conformidad de los acuerdos de confidencialidad con las leyes aplicables.			
	6.1.6. Contacto con las autoridades	Procedimientos que indiquen qué autoridades contactar y cómo reportar incidentes de seguridad.			**Nula**
		Identificación de acciones y agentes externos que las lleven a cabo, en caso de ataques desde Internet.			
		Contacto con organismos reguladores.			

	6.1.7. Contacto con grupos de interés especial	Contacto con grupos especializados en Seguridad de la Información.			Nula
		Mejora del conocimiento y actualización en temas de Seguridad de la Información.			
		Recepción alertas tempranas sobre ataques y vulnerabilidades.			
		Establecimiento de vínculos adecuados en la trata de Seguridad de la Información.			
	6.1.8. Revisión independiente de la Seguridad de la Información	Revisión independiente del enfoque de Seguridad de la Información.			Nula
		Establecimiento de revisiones independientes de seguridad en intervalos planeados.			
		Exigencia de oportunidades de mejora de las revisiones independientes.			
		Registros de iniciación y finalización de revisiones independientes.			
		Ejecución de acciones correctivas a partir de los resultados de revisiones independientes.			
6.2. Grupos o personas externas	6.2.1. Identificación de los riesgos relacionados con los grupos externos	Evaluación del riesgo para la información por cada acceso que un grupo externo tenga a la organización.			Nula
		Identificación de los medios de procesamiento de información a los cuales acceden los grupos externos.			
		Identificación del tipo de acceso de los grupos externos a los medios de procesamiento de la información.			
		Identificación del valor de la información involucrada en la relación con grupos externos.			
		Definición de controles necesarios para aquella información no disponible a grupos externos.			
		Identificación de personal externo involucrado en el manejo de la información.			
		Verificación y autorización del grupo externo que accede a la			

		información.			
		No brindar acceso a grupos externos hasta que los controles debidos hayan sido implementados.			
	6.2.2. Tratamiento de la seguridad cuando se lidia con clientes	Procedimientos para proteger activos y determinar si algún activo está comprometido.			**Nula**
		Restricciones sobre el copiado y divulgación de información.			
		Métodos de acceso permitidos y el control y uso de identificadores como ID's y contraseñas.			
		Proceso de autorización para el acceso y privilegios para el cliente.			
		Proceso de revocación de derechos de acceso para el cliente.			
		Acuerdos para el reporte, reportes e investigación de incidentes de seguridad asociados a los clientes.			
		Descripción de los servicios e información disponible a los clientes.			
		Niveles de aceptables de servicio.			
		Obligaciones de la organización y el cliente.			
		Responsabilidades en aspectos legales.			
		Derechos de propiedad y la asignación de derechos de autor.			
	6.2.3. Tratamiento de la seguridad cuando se lidia con terceros	Procedimientos para protección de activos organizacionales.			**Nula**
		Controles de protección física.			
		Controles para la protección de *software* malicioso.			

		Procedimientos para detectar si algún activo está comprometido.			
		Procedimiento para destrucción o retorno de información.			
		Restricciones sobre el copiado y divulgación de información.			
		Capacitación en métodos y procedimientos de seguridad.			
		Responsabilidades relacionadas con instalación y mantenimiento de *software* y *hardware*.			
		Establecimiento de una estructura de reportes.			
		Especificación de un proceso de gestión de cambio.			
		Proceso para revocar accesos o interrupción en sistemas.			
		Acuerdos para el reporte, reportes e investigación de incidentes de seguridad asociados a terceros.			
		Descripción de los servicios e información disponibles a los terceros.			
		Niveles de aceptables de servicio.			
		Criterios de desempeño, su monitoreo y reporte.			
		Monitoreo y revocación de actividades relacionadas a activos de la organización.			
		Derecho de auditorías sobre las responsabilidades del acuerdo, pueden ser ejecutadas por terceros.			
		Proceso escalonado para la solución de problemas.			
		Requerimientos para continuidad del negocio.			

		Responsabilidades en aspectos legales.			
		Condición para negociación/terminación de acuerdos.			
Dominio		**7.Gestión de activos**			
Documentos evaluados					
Control	**Control**	**Aspectos: qué políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir**	**¿Se cumple el aspecto?**	**Evidencia**	**Cobertura del control**
7.1. Responsabilidad por los activos	7.1.1. Inventario de los activos	Identificación de todos los activos y su importancia.			**Nula**
		Información de activos suficiente para recuperación de desastres.			
		Alineamiento del inventario de activos con otros inventarios.			
		Identificación del propietario del activo.			
		Identificación niveles de importancia de los activos.			
	7.1.2. Propiedad de los activos	El propietario de los activos debe asegurarse su correcta clasificación.			**Nula**
		El propietario de los activos debe definir y revisar las restricciones y clasificación de accesos.			
	7.1.3. Uso aceptable de los activos	Definición de reglas para uso aceptable de los activos			**Nula**
		Obligatoriedad de empleados, contratistas y terceros de seguir las reglas de uso aceptable de los activos.			
7.2. Clasificación de la información	7.2.1. Lineamientos de clasificación	Protocolos de clasificación inicial y reclasificación			**Nula**
		Definición de categorías de clasificación de la información.			

		Consideración del tiempo de clasificación de la información antes de reclasificarla.			
	7.2.2. Etiquetado y manejo de la información	Procedimientos de etiquetado de información, tanto en medios físicos como electrónicos.			Nula
		Procedimientos de manejo de la información según su clasificación.			
Dominio		**8. Seguridad de recursos humanos**			
Documentos evaluados					
Objetivo de control	**Control**	**Aspectos: qué políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir**	**¿Se cumple el aspecto?**	**Evidencia**	**Cobertura del control**
8.1. Antes del empleo	8.1.1. Roles y responsabilidades	Los empleados, contratistas y terceros deben actuar en concordancia con las políticas de seguridad.			Nula
		Comunicación de roles y responsabilidades de seguridad al empleado.			
	8.1.2. Investigación de antecedentes	La revisión de antecedentes debe ser de acuerdo con la legislación relevante a privacidad personal.			Nula
		Revisión de referencias de la persona.			
		Revisión de curriculum vitae de la persona.			
		Confirmación de calificaciones académicas y profesionales de la persona.			
		Chequeos detallados (de crédito o criminales) de la persona.			
		Proceso de investigación de antecedentes de contratistas y terceros.			
	8.1.3. Términos y condiciones del empleo	Empleados, contratistas y empleados deben firmar un contrato con los términos y condiciones de su empleo.			Nula
		Empleados deben firmar acuerdos de confidencialidad cuando tengan acceso a información.			
		Derechos y responsabilidades de empleados en relación con la			

		protección de datos personales			
		Responsabilidades para la clasificación de información y protección de activos organizacionales			
		Responsabilidades en relación con el manejo de información de otras organizaciones			
		Responsabilidades de la organización en la protección de la información personal del empleado			
		Responsabilidades que se extienden fuera de la organización			
		Acciones a tomar en caso que un empleado no cumpla con los requerimientos de seguridad			
8.2. Durante el empleo	8.2.1. Responsabilidades de la gerencia	Verificación de la gerencia que los empleados conozcan sus roles y responsabilidades de seguridad			**Nula**
		Motivación de la gerencia para que los empleados cumplan las políticas de Seguridad de la Información			
		Verificación de la gerencia que los empleados cumplan con los términos de trabajo y las políticas de seguridad			
		La gerencia debe velar porque los empleados continúen teniendo las capacidades y calificaciones adecuadas.			
	8.2.2. Conocimiento, educación y capacitación en Seguridad de la Información	Capacitaciones a empleados sobre Seguridad de la Información			**Nula**
		Notificación a los empleados de actualizaciones en las políticas de Seguridad de la Información			
		Proceso de inducción formal en políticas de Seguridad de la Información			
	8.2.3. Proceso disciplinario	Existencia de un proceso disciplinario para la seguridad para empleados que incumplen la seguridad.			**Nula**
		El proceso disciplinario se inicia hasta que se verifique el incumplimiento de seguridad.			
		El proceso debe garantizar el tratamiento correcto y justo para un empleado sospechoso de incumplimiento			

		La respuesta del proceso debe estar en función de la naturaleza, gravedad e impacto del incumplimiento.			
8.3 Terminación o cambio de empleo	8.3.1. Responsabilidades de terminación	La finalización de empleo se contempla en acuerdos de confidencialidad.			Nula
		En el contrato del empleado se documentan las responsabilidades después de su finalización.			
		Cambios de empleo o responsabilidad se manejan como terminación de un empleo.			
		En un cambio de empleo se consideran todo lo requerido como si fuese un nuevo empleado.			
	8.3.2. Devolución de los activos	Todo activo en posesión de un empleado debe ser devuelto cuando finalice el contrato.			Nula
		Procedimientos de borrado de datos cuando el equipo pertenece al empleado y termina su contrato.			
		Documentación del conocimiento tácito, de importancia, del empleado cuando termine su contrato.			
	8.3.3. Retiro de los derechos de acceso	Cuando un empleado termina su contrato se revocan sus derechos de acceso.			Nula
		Cuando hay un cambio de empleo los derechos de acceso son reconsiderados.			
		Cambio de contraseñas de activos importantes cuando un empleado termina contrato y las conoce.			
		Consideración de los retiros de acceso del empleado antes de la terminación del contrato, cuando aplique.			
Dominio		**9. Seguridad física y ambiental**			
Documentos evaluados					
Objetivo de control	**Control**	**Aspectos: qué políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir**	**¿Se cumple el aspecto?**	**Evidencia**	**Cobertura del control**
9.1 Áreas seguras	9.1.1. Perímetro de seguridad física	Definición de los perímetros de seguridad			Nula
		Según la importancia del activo, así se define la ubicación y			

		fuerza del perímetro de seguridad.			
		Los edificios que contienen medios de procesamiento de información son físicamente sólidos.			
		Existencia de un área de recepción que regule el acceso al edificio o local.			
		Cuando es aplicable, crear barreras físicas para evitar el acceso no autorizado.			
		Las puertas de emergencia poseen alarma, son probadas y monitoreadas			
		Instalación y prueba de sistemas de detección de intrusos.			
	9.1.2. Controles de ingreso físico	Registro de hora y fecha de ingreso de visitantes a áreas seguras			**Nula**
		Sólo se permite el ingreso de visitantes con la debida autorización y con propósitos específicos			
		Uso de métodos de autenticación de personas autorizadas para el acceso a áreas seguras sensibles			
		Todos los empleados, contratistas y terceras personas deben hacer uso de algún medio de identificación			
		Revisión y actualización de derechos de acceso a áreas seguras.			
	9.1.3. Asegurar las oficinas, habitaciones y medios	Considerar estándares relevantes de sanidad y seguridad.			**Nula**
		Identificación de medios para evitar el acceso público.			
		Protección de directorios internos que identifiquen la ubicación de medios de procesamiento de información.			
	9.1.4. Protección contra amenazas externas e internas	Consideración de amenazas provenientes de locales vecinos.			**Nula**
		Materiales peligrosos o combustibles deben almacenarse lejos de las áreas seguras.			

		Papelería no debería guardarse en las áreas seguras.			
		Equipo de reemplazo y medios de respaldo deben almacenarse lejos de las instalaciones principales			
		Uso de equipo adecuado anti-incendios.			
	9.1.5. Trabajo en áreas seguras	El personal sólo debe conocer las actividades en áreas seguras en caso de requerirlo			**Nula**
		Evitar trabajo no supervisado en áreas seguras			
		Áreas seguras vacías deben estar bajo llave y revisadas periódicamente			
		Prohibición de equipo fotográfico, de vídeo, audio y otro equipo de grabación sin autorización			
	9.1.6. Áreas de acceso público, entrega y carga	Restricción, desde fuera del edificio, de acceso al área de carga y entrega.			**Nula**
		El área carga y entrega no debería permitir al personal de entrega acceder a otras partes del edificio			
		Las puertas externas del área de carga deben estar aseguradas cuando se abren las puertas internas			
		Inspección del material que se entrega antes de llegar al punto de uso			
		Registro del material ingresado según procedimientos de gestión de activos			
9.2 Seguridad del equipo	9.2.1. Ubicación y protección del equipo	Ubicación del equipo en un área que minimice el acceso innecesario a áreas de trabajo			**Nula**
		Ubicación de los medios de procesamiento que restrinja la visión de la información almacenada en ellos			
		Aislamiento de ítems que requieren protección especial			
		Controles para minimizar amenazas como: robo, fuego,			

		explosivos, humo, agua, polvo, vibración, entre otros.			
		Lineamientos sobre comer, beber o fumar cerca de los medios de procesamiento de información.			
		Monitoreo de condiciones ambientales.			
		Protección contra rayos al edificio y líneas de ingreso de energía y comunicaciones			
		Métodos de protección para el equipo en ambientes industriales.			
		Protección al equipo que almacena información confidencial			
	9.2.2. Servicios públicos de soporte	Inspección regular de los servicios de soporte: electridad, agua, desagüe, calefacción y A/C.			**Nula**
		Revisión de que el suministro eléctrico sea adecuado a las especificaciones del fabricante del equipo.			
		Uso de UPS para apagar o hacer funcionar continuamente el equipo que soporta las operaciones comerciales.			
		Uso de un generador de emergencia en sí, se requiere la operación continua en caso de falla.			
		Revisión regular de las capacidades de UPS y generadores.			
		Uso de múltiples fuentes de energía.			
		Disposición de un suministro adecuado de combustible para el generador.			
		Interruptores de energía de emergencia para cerrar el paso de corriente al equipo en caso de emergencia.			
		Estabilidad del suministro de energía.			
		Instalación de un sistema de alarma para el monitoreo de servicios públicos de soporte.			

		Dos rutas de conexión entre el equipo de comunicaciones y el proveedor del servicio			
	9.2.3. Seguridad del cableado	Líneas de energía y comunicaciones debieran ser subterráneas o sujetas a otra alternativa de protección			Nula
		Protección del cableado de red de interrupciones no autorizadas (usando tubo o evitando rutas públicas)			
		Separación de los cables de energía de los de comunicaciones.			
		Uso de marcadores en los cables para minimizar el error en su manipulación.			
		Lista documentada de los empalmes.			
		En sistemas sensibles, uso de tubo blindado y uso de cajas con llave en puntos de inspección y terminación			
		En sistemas sensibles, uso de rutas o medios de transmisión alternativos.			
		En sistemas sensibles, uso de cableado de fibra óptica.			
		En sistemas sensibles, acceso controlado para empalmar los paneles y los cuartos de cableado.			
	9.2.4. Mantenimiento del equipo	Mantenimiento del equipo en intervalos de tiempo según lo recomendado por el proveedor.			Nula
		Sólo personal autorizado debe dar mantenimiento al equipo.			
		Registro de fallas y mantenimiento preventivo y correctivo.			
		Controles de protección de información cuando el mantenimiento sea fuera de las instalaciones.			
		Cumplimiento de todos los requerimientos de las pólizas de seguros.			
	9.2.5. Seguridad del	El uso de cualquier equipo fuera del local debe ser autorizado			Nula

	equipo fuera del local	por la gerencia.			
		El equipo fuera del local nunca debe ser desatendido en sitios públicos.			
		Revisión de las recomendaciones del fabricante para proteger el equipo.			
		Controles para el teletrabajo.			
		Seguro para protección del equipo fuera del local.			
	9.2.6. Seguridad de la eliminación o re-uso del equipo	Dispositivos con información confidencial deben ser destruidos			**Nula**
		En caso de no destrucción del equipo, se debe borrar o sobrescribir la información con técnicas especializadas			
	9.2.7. Retiro de propiedad	Autorización requerida para el retiro de información, *software* o equipo			**Nula**
		Identificación de aquellos con autorización de permitir el retiro de equipo			
		Límites de tiempo para el retiro de equipo			
		Revisión del equipo devuelto después de un retiro.			
		Registros de retiro y retorno de equipo			
Dominio		**10. Gestión de las comunicaciones y operaciones**			
Documentos evaluados					
Objetivo de control	**Control**	**Aspectos: qué políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir**	**¿Se cumple el aspecto?**	**Evidencia**	**Cobertura del control**
10.1. Procedimientos y responsabilidades operacionales	10.1.1. Procedimientos de operación documentados	Procedimientos documentados sobre actividades ligadas a medios de procesamiento de información.			**Nula**
		Procedimientos de operación deben indicar cómo manejar la información.			

		Procedimientos de operación deben abarcar respaldos o copias de seguridad.			
		Procedimientos de operación deben abarcar requerimientos de horarios de operación.			
		Procedimientos de operación deben abarcar interdependencias con otros sistemas.			
		Procedimientos de operación deben indicar instrucciones para el manejo de errores.			
		Procedimientos de operación deben indicar contactos de soporte en el evento de dificultades.			
		Procedimientos de operación deben indicar cómo manejar sus salidas o resultados.			
		Procedimientos de operación deben indicar cómo reiniciar y recuperar el sistema.			
		Procedimientos de operación deben abarcar la gestión del rastro de auditoría y registros del sistema.			
	10.1.2. Gestión del cambio	Control de cambios sobre sistemas y medios de procesamiento de la información			**Nula**
		Identificación y registro de cambios significativos			
		Planeación y prueba de cambios			
		Evaluación del impacto de los cambios			
		Procedimiento formal para la aprobación de cambios propuestos			
		Comunicación de los cambios relevantes a las personas interesadas en ellos			
		Procedimientos de emergencia, respaldo, cancelación y recuperación de cambios fallidos			
		Establecimiento de responsabilidades para el control de			

		cambios.			
	10.1.3. Segregación de los deberes	Separación de áreas de responsabilidad.			Nula
		Separación de la iniciación de un evento de su autorización.			
		Monitoreo de actividades, rastros de auditoría y supervisión gerencial en caso de no segregar deberes.			
		Independencia de la auditoría de seguridad.			
	10.1.4. Separación de los medios de desarrollo, prueba y operación	Identificación del nivel de separación entre ambientes de desarrollo, pruebas y operación.			Nula
		Documentación de las reglas para el paso del *software* de desarrollo a operación.			
		Software de desarrollo y operación debe correr en sistemas procesadores distintos.			
		Restricción de acceso a herramientas de desarrollo desde sistemas operacionales.			
		El ambiente de prueba debe simular el ambiente real de operación.			
		Distintos perfiles de usuario dependiendo si se está en ambiente de prueba y operación.			
		Mensajes que indique si se están en un ambiente de prueba u operación.			
		Los datos confidenciales no deben ser copiados en ambientes de prueba.			
10.2. Gestión de la entrega del servicio de terceros	10.2.1. Entrega del servicio	Definiciones del servicio y acuerdos de gestión del servicio en servicios brindados por terceros.			Nula
		Planeación de transiciones de información o medios de procesamiento con respecto a abastecimientos externos.			
		El tercero debe mantener la capacidad de brindar el servicio luego de una falla.			

	10.2.2 Monitoreo y revisión de los servicios de terceros	Revisión de cumplimiento de condiciones de seguridad definidos en acuerdos con terceros.			Nula
		Monitoreo del desempeño de los servicios.			
		Revisión de reportes de los servicios brindados por terceros.			
		Revisión de información sobre incidentes de seguridad por parte de la organización y el tercero			
		Revisar rastros de auditoría y registros de cualquier evento, problema o falla del servicio brindado			
		Resolución de problemas identificados en el servicio			
	10.2.3. Manejo de cambios en los servicios de terceros	Gestión de los cambios en aumento de los servicios brindados actualmente.			Nula
		Gestión de nuevos sistemas o aplicaciones.			
		Gestión de políticas y procedimientos en la organización			
		Gestión de cambios en redes que afecten servicios de terceros			
		Gestión de nuevas tecnologías que afecten servicios de terceros			
		Gestión de actualizaciones de productos que afecten servicios de terceros			
		Gestión de herramientas y nuevos ambientes que afecten servicios de terceros			
		Gestión de cambios en la ubicación de los medios de brindar el servicio			
		Gestión de cambios de vendedores que afecten servicios de terceros.			
10.3. Planeación y	10.3.1. Gestión de la	Identificación de requerimientos de capacidad de actividades en			Nula

aceptación del sistema	capacidad	proceso.			
		Identificación de requerimientos de capacidad de nuevas actividades.			
		Identificación de actividades y proyecciones a futuro del negocio para conocer requerimientos de capacidad			
		Atención especial en recursos claves del sistema.			
	10.3.2. Aceptación del sistema	Responsabilidad gerencial de asegurar que se definan, acepten, documenten y prueben criterios de aceptación.			**Nula**
		Nuevas soluciones deben ser aceptadas para migrar a operación.			
		Verificación del desempeño y requerimientos de capacidad para la computadora.			
		Procedimientos de recuperación de errores y reinicio para nuevas soluciones.			
		Preparación y prueba de procedimientos de operación para nuevos sistemas.			
		Controles de seguridad acordados y aceptados para nuevas soluciones.			
		Capacitación de nuevas soluciones al usuario			
		Facilidad de uso de la nueva solución para el usuario			
10.4. Protección contra el código malicioso y móvil	10.4.1. Controles contra códigos maliciosos	Prohibición de *software* no autorizado.			**Nula**
		Política de protección en la obtención de archivos.			
		Revisiones regulares del *software* y datos de los sistemas que soportan procesos críticos.			
		Instalación y actualización de *software* para detección o reparación de códigos maliciosos			

		Revisiones de archivos recibidos a través de la red, usando *software* para detección de códigos maliciosos.			
		Revisiones de archivos recibidos por correo, usando *software* para detección de códigos maliciosos.			
		Revisiones de páginas Web para detección de códigos maliciosos.			
		Definición de procedimientos y responsabilidades para lidiar con códigos maliciosos.			
		Capacitación para lidiar con códigos maliciosos.			
		Planes de recuperación de ataques de código malicioso.			
	10.4.2. Controles contra códigos móviles	El código móvil no debe ejecutarse sin autorización			**Nula**
		El código móvil se ejecuta en un ambiente aislado lógicamente.			
		Bloqueo de código móvil no autorizado.			
		Bloqueo de lo recibido de código móvil no autorizado.			
		Control de recursos disponibles para el acceso de código móvil.			
		Controles criptográficos para autenticar singularmente el código móvil.			
10.5. Respaldo o back-up	10.5.1.Respaldos	Definición de medios de respaldo adecuados para recuperación de un desastre.			**Nula**
		Pruebas de los medios de respaldo regularmente.			
		Definición del nivel de respaldo requerido.			
		Registro de las copias de respaldo realizadas.			

		Procedimientos documentados para la restauración.			
		Las copias de seguridad son almacenadas en un lugar lejano del sitio principal.			
		Pruebas de los procedimientos de respaldo y recuperación.			
10.6. Gestión de seguridad de la red	10.6.1. Controles de redes	Separación de responsabilidades de redes de las responsabilidades de cómputo.			**Nula**
		Definición de responsabilidades y procedimientos para la gestión de equipo remoto.			
		Protección de la información cuando pase por redes publicas			
		Protección de la información cuando se transmita por medios inalámbricos.			
		Aplicación de registros de ingreso y monitoreo.			
	10.6.2. Seguridad de los servicios de la red	Monitoreo regular de la capacidad del servicio de red.			**Nula**
		Establecer el derecho de auditoría del servicio de red.			
		Acuerdos de seguridad para los servicios de red.			
10.7. Gestión de medios	10.7.1. Gestión de medios removibles	Información no requerida, en medios removibles que se mantengan en la organización, no debe ser recuperable.			**Nula**
		Autorización para remover medios.			
		Los medios deben almacenarse según las especificaciones del proveedor.			
		Si el ciclo de vida del medio sea menor que el tiempo de almacenaje de información, esta se debe respaldar.			

		Registro de medios removidos para evitar pérdida de datos.			
		Medios removidos sólo deben estar disponibles si hay una razón de negocio que lo respalde.			
	10.7.2. Retiro de medios	Procedimientos de almacenaje y retiro de medios que contengan información sensible.			**Nula**
		Identificación de ítems que pudiesen requerir una eliminación segura.			
		Registro de eliminación de ítems confidenciales como registro de auditoría.			
	10.7.3. Procedimientos para el manejo de información	Procedimientos para manipulación y etiquetado de los medios según su clasificación.			**Nula**
		Restricciones de acceso a los medios.			
		Registro formal de los destinatarios de los datos.			
		Procedimientos de validación de entradas y salidas de los procesos.			
		Protección de los datos de salida según su confidencialidad requerida.			
		Almacenaje de los medios según especificaciones de los fabricantes.			
		Mantener mínima la distribución de la información.			
		Revisar regularmente las listas de distribución y las listas de destinatarios.			
	10.7.4. Seguridad de la documentación del sistema	Almacenamiento seguro de la documentación del sistema.			**Nula**
		La lista de acceso a la documentación del sistema debe ser mínima.			
		La lista de acceso a la documentación del sistema debe ser			

		autorizada por el dueño de la aplicación.			
		Documentación del sistema en redes públicas debe protegerse.			
10.8. Intercambio de Información	10.8.1. Políticas y procedimientos de intercambio de información.	Procedimientos para proteger información de intercepción, copiado, modificación, destrucción, etc.			**Nula**
		Procedimientos de detección y protección contra códigos maliciosos, origen de comunicaciones electrónicas.			
		Procedimientos de protección de información electrónica confidencial comunicada como un adjunto.			
		Políticas y lineamientos para el uso de medios de comunicación electrónicos.			
		Procedimientos para el uso de comunicación inalámbrica.			
		Responsabilidades de empleados, contratistas o terceros para que no comprometan a la organización.			
		Uso de técnicas de codificación.			
		Lineamientos de retención y eliminación de toda la correspondencia del negocio.			
		No dejar información crítica en medios impresos.			
		Controles y restricciones de reenvío de medios de comunicación.			
		No dejar mensajes con contenido confidencial en máquinas contestadoras.			
		Recordar al personal los riesgos asociados con los medios de comunicación y su mal uso.			
	10.8.2. Acuerdos de intercambio	Acuerdos de intercambio contienen responsabilidades para el control y notificación de la transmisión.			**Nula**
		Procedimientos para notificar al remitente de la transmisión, despacho y recepción.			

		Procedimientos para asegurar el rastreo y no-repudio.			
		Estándares técnicos mínimos para el empaque y la transmisión.			
		Estándares de identificación del mensajero.			
		Responsabilidades en el evento de incidentes de Seguridad de la Información, como la pérdida de *data*.			
		Uso de un sistema de *etiquetado* acordado para la información confidencial o crítica.			
		Propiedad y responsabilidades de la protección de *data*, derechos de autor, licencias de *software*, entre otros.			
		Estándares técnicos para grabar y leer la información y *software*.			
	10.8.3. Medios físicos en tránsito	Uso de transporte o medios de mensajería confiables.			**Nula**
		Acuerdo con la gerencia de una lista de mensajerías confiables.			
		Procedimientos para revisar la identificación de mensajeros.			
		Empaques que puedan proteger el medio de cualquier evento durante su transporte.			
	10.8.4. Mensajes electrónicos	Protección de mensajes de acceso no autorizado, modificación o negación del servicio.			**Nula**
		Aseguramiento de la correcta dirección y transporte del mensaje.			
		Previa autorización para uso de servicios públicos externos como un mensaje instantáneo.			
		Control del acceso público a las redes.			
	10.8.5. Sistemas de	Definición de políticas y controles para el intercambio de			**Nula**

	información comercial	información.			
		Identificación de vulnerabilidades en el intercambio de información.			
		Exclusión de información confidencial cuando el intercambio no sea seguro.			
		Categorizar el personal con autorización del sistema de intercambio.			
		Definición de los lugares desde los cuales se puede hacer uso del sistema de intercambio.			
		Retención y respaldo de la información en los sistemas de información comercial.			
10.9. Servicios de comercio electrónico	10.9.1. Comercio electrónico.	Identificación del nivel de confianza requerida entre las partes que participan en el comercio electrónico.			**Nula**
		Procesos de autorización para aquellos que pueden establecer precios, emitir o firmar documentos.			
		Definición de requerimientos para la confidencialidad, integridad, prueba de despacho y recepción de documentos.			
		Confidencialidad e integridad de cualquier transacción, información de pago, entre otros.			
		Evitar la pérdida o duplicación de la información de la transacción.			
		Aplicación de controles criptográficos.			
	10.9.2. Transacciones en línea	Uso de firmas digitales por cada una de las partes que interactúan en la transacción.			**Nula**
		Codificación de las transacciones.			
		Uso de protocolos seguros.			
	10.9.3. Información públicamente	Pruebas del sitio público disponible antes de poner en él la información.			**Nula**

	disponible	Aprobación para que la información sea publicada en un sitio público.			
		Restricción de acceso desde el sitio público a sitios internos de la organización.			
10.10. Monitoreo	10.10.1. Registro de auditoría	Registros de ID´s.			**Nula**
		Registros de fechas y horas de eventos claves.			
		Registros de intentos de acceso fallidos y rechazados al sistema.			
		Registros de intentos de acceso fallidos y rechazados a los datos y otros recursos.			
		Registros de cambios en la configuración del sistema.			
		Registros de uso de privilegios.			
		Registros de uso de las utilidades y aplicaciones del sistema.			
		Registros de archivos a los cuales se tuvo acceso y los tipos de acceso.			
		Registros de direcciones y protocolos de la red.			
		Registros de alarmas activadas por el sistema de control de acceso.			
		Registros de activación y desactivación de los sistemas de protección.			
	10.10.2. Uso del sistema de monitoreo	Definición del nivel de monitoreo para medios individuales.			**Nula**
		Definición de la frecuencia en que se deben revisar los resultados de los sistemas de monitoreo.			
	10.10.3. Protección del	Protección de registros contra cambios no autorizados.			**Nula**

	registro de información				
		Protección de registros contra problemas operacionales.			
	10.10.4. Registros del administrador y operador.	Registro de fecha y hora en que ocurre un evento cuando se es administrador u operador del sistema.			Nula
		Registro de información de un evento cuando se es administrador u operador del sistema.			
		Registro de la cuenta de operador o administrador cuando se presente un evento.			
		Registro de los procesos involucrados.			
		Revisión, de manera regular, de registros de administrador y operador.			
	10.10.5. Registro de fallas	Registro de fallas reportado por usuarios o por el sistema.			Nula
		Revisión de registros de fallas para asegurarse que se hayan solucionado.			
		Revisión de las acciones correctivas para las fallas.			
	10.10.6. Sincronización de relojes	Todos los relojes de los sistemas relevantes deben estar sincronizados.			Nula
		Sincronización del reloj con una fuente que proporcione la hora exacta acordada.			
		Procedimiento que revise y corrija cualquier variación significativa en los relojes.			
Dominio		**11. Control de acceso**			
Documentos evaluados					
Objetivo de control	**Control**	**Aspectos: qué políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir**	**¿Se cumple el aspecto?**	**Evidencia**	**Cobertura del control**
11.1.Requerimientos de control de acceso	11.1.1. Política de control de acceso	Definición de política de control de acceso que determine las reglas de control de acceso físico y lógico.			Nula

11.2. Gestión de acceso del usuario	11.2.1. Registro del usuario	Procedimiento formal para registro de usuarios.			Nula
		Procedimiento formal para des-registro de usuarios.			
		Proporcionar a usuarios un enunciado con sus derechos de acceso.			
		Los nombres de usuario deben ser únicos.			
		Proveedores del servicio no deben garantizar permisos hasta que se complete el proceso de autorización.			
		Eliminación o bloque de accesos a funcionarios que han cambiado de puesto.			
		Revisión periódica para eliminar nombres de usuario redundantes.			
	11.2.2. Gestión de privilegios	Proceso formal de garantía de privilegios.			Nula
		Los privilegios deben ser mínimos de acuerdo con el rol del usuario.			
		Registro de privilegios asignados.			
	11.2.3. Gestión de las contraseñas de usuarios	Los usuarios deben mantener secretas sus contraseñas.			Nula
		Inicialmente a los usuarios se les debe brindar una clave temporal para luego cambiarla.			
		Antes de brindar una contraseña temporal al usuario se le debe verificar su identidad.			
		Claves secretas provistas por el vendedor deben ser cambiadas.			
	11.2.4. Revisión de los derechos de acceso	Revisión en intervalos regulares de tiempo de los derechos de acceso de los usuarios.			Nula
		Revisión y modificación de los derechos de acceso cuando un			

		empleado cambia de puesto.			
		Revisión de los otorgamientos de privilegios en periodos regulares.			
		Registro de cambios en cuentas privilegiadas.			
11.3. Responsabilidades del usuario	11.3.1. Uso de claves secretas	Los usuarios deben mantener secretas sus contraseñas.			**Nula**
		Los usuarios deben evitar mantener un registro de sus contraseñas.			
		Cambio de contraseñas cuando se sospeche de algún peligro para la misma.			
		Definir un estándar de calidad de las contraseñas y exigir que se cumpla.			
		Cambios periódicos de las contraseñas.			
		No usar la misma contraseña de otros medios.			
		No compartir contraseñas.			
	11.3.2. Equipo del usuario desatendido	Los usuarios deben cerrar sesiones activas, a menos que haya un mecanismo de protección adicional.			**Nula**
		Aplicar controles como clave secreta cuando el equipo está desatendido.			
	11.3.3. Política de escritorio y pantalla limpios	Definición de una política de escritorio y pantalla limpios.			**Nula**
		La información comercial crítica debe guardarse bajo llave.			
		Computadoras desatendidas deben apagarse o protegerse a través de algún mecanismo.			
		Protección puntos de salida en ingreso de correo y máquinas de fax desatendidas.			

		Autorización requerida para uso de fotocopiadoras y otros medios de reproducción.			
11.4. Control de acceso a la red	11.4.1. Política sobre el uso de servicios de la red	Procedimientos para autorizar acceso a servicios de la red.			Nula
		Controles para proteger el acceso no autorizado a servicios de la red.			
	11.4.2.Autenticación de usuario remoto	Uso de medios de autenticación de usuarios remotos.			Nula
	11.4.3. Identificación del equipo en las redes	Identificación automática del equipo que accede a la red.			Nula
		Asignación de identificadores a los equipos que acceden la red.			
	11.4.4. Protección del puerto de diagnóstico y configuración remoto	Procedimientos de uso seguro de puertos de diagnóstico y configuración.			Nula
		Controles para regular el acceso físico de los puertos.			
		Puertos de diagnóstico y configuración remota no requeridos, deben ser removidos del equipo.			
	11.4.5. Segregación de redes	Uso de segregación de redes dentro de la organización.			Nula
		Criterio de segregación de redes debe basarse en la política de control de acceso.			
	11.4.6. Control de conexión a la red	Restricción de la capacidad de los usuarios de conectarse a la red.			Nula
		Los derechos de acceso a la red se deben revisar y actualizar según la política de control de acceso.			
	11.4.7. Control de *routing* de la red	Las conexiones de la computadora y los flujos de información no violan la política de control de acceso			Nula
11.5. Control de acceso al sistema operativo	11.5.1. Procedimientos para un registro seguro	Procedimiento para registro seguro en un sistema operativo.			Nula
		El procedimiento de registro contiene poca información acerca			

		del sistema.			
		El procedimiento no debe ayudar al usuario hasta que se complete el registro.			
		Limitación del número de intentos infructuosos de registro en el sistema.			
		Limitación del tiempo máximo y mínimo para llevar a cabo el proceso de registro.			
		Controles para proteger la contraseña en el registro.			
	11.5.2. Identificación y autenticación del usuario	Uso de ID's únicos para personal de soporte técnico, operadores, administradores de red y demás.			**Nula**
		Utilización de medios de autenticación de los usuarios.			
	11.5.3. Sistema de gestión de claves secretas	ID´s individuales con su clave secreta asociada.			**Nula**
		Permisión al usuario del cambio de su contraseña.			
		Obligar al usuario a cambiar sus claves secretas temporales en el primer ingreso.			
		Llevar un registro de contraseñas previas y evitar el reúso.			
		No mostrar contraseñas en pantallas cuando son ingresadas.			
		Los datos de claves secretas se almacenan en distinta ubicación que los archivos del sistema.			
		Almacenamiento y transmisión de claves secretas de manera codificada.			
	11.5.4. Uso de las utilidades del sistema	Procedimientos para identificación, autenticación y autorización de utilidades del sistema.			**Nula**
		Segregación de las utilidades del sistema de la aplicación.			

		Limitación del uso de las utilidades del sistema a un nivel mínimo de usuarios.			
		Registro de las utilidades del sistema.			
		Definición y documentación de los niveles de autorización de utilidades del sistema.			
		Eliminación de utilidades innecesarias del sistema.			
	11.5.5. Cierre de una sesión por inactividad	Cierre de una sesión posterior a un determinado periodo de inactividad.			**Nula**
		Cierre de aplicaciones posterior a un tiempo de inactividad.			
	11.5.6. Limitación del tiempo de conexión	Limitar el tiempo de conexión.			**Nula**
		Restringir o no la conexión fuera del horario normal de trabajo.			
11.6. Restricción de acceso a la información y a las aplicaciones	11.6.1. Restricción de acceso a la información.	Restricción del personal a la información.			**Nula**
		Restricción del personal a las funciones del sistema.			
		Controlar derechos de acceso de los usuarios (lectura, escritura, eliminar y ejecutar).			
		Control de derechos de acceso de otras aplicaciones.			
	11.6.2. Aislar el sistema confidencial	Identificar y documentar el propietario de la aplicación.			**Nula**
		Identificar y documentar la sensibilidad o confidencialidad del sistema de aplicación.			
		Aislamiento del sistema confidencial de otros sistemas.			
11.7. Computadores	11.7.1. Computación y	Política de uso de dispositivos móviles.			**Nula**

portátiles y teletrabajo	comunicaciones móviles				
		Protección física de dispositivos móviles.			
		Control de acceso de dispositivos móviles.			
		Protección lógica de dispositivos móviles.			
		Reglas y lineamientos de conexión de dispositivos móviles a las redes.			
		Respaldos de información comercial ubicada en dispositivos móviles.			
		Procedimiento en caso de pérdida o robo de un dispositivo móvil.			
		Capacitación del personal que usa dispositivos móviles sobre la necesidad de mantener su seguridad.			
	11.7.2. Teletrabajo	Existencia de una política de teletrabajo.			**Nula**
		Planes operacionales de teletrabajo.			
		Procedimientos para actividades de teletrabajo.			
		Las actividades de teletrabajo deben ser aprobadas por la gerencia.			
		Provisión del equipo necesario para el teletrabajo.			
		Definición del trabajo permitido.			
		Reglas y lineamientos sobre el acceso de la familia y amigos al equipo y la información.			
		Provisión y soporte de *software* y *hardware*.			

		Provisión de seguridad física.			
		Provisión de un seguro.			
		Procedimientos de respaldo.			
		Procedimientos de continuidad del negocio.			
		Monitoreo para la auditoría y seguridad.			
		Revocación de derechos de acceso y equipo una vez terminado el teletrabajo.			
Dominio		**12. Adquisición, desarrollo y mantenimiento de los sistemas de información**			
Documentos evaluados					
Objetivo de control	**Control**	**Aspectos: qué políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir**	**¿Se cumple el aspecto?**	**Evidencia**	**Cobertura del control**
12.1. Requerimientos de seguridad de los sistemas de información	12.1.1. Análisis y especificación de los requerimientos de seguridad	Especificación y documentación de los requerimientos de seguridad.			**Nula**
		La especificación de requerimientos de seguridad debe establecerse en las primeras etapas del proyecto.			
		Para sistemas comprados se deben igualmente establecer los requerimientos de seguridad.			
		Definición de procesos de adquisición y prueba de sistemas.			
12.2. Procesamiento correcto de las aplicaciones	12.2.1. Validación de los datos de entrada	Validaciones que los datos de entrada sean correctos y sigan los formatos requeridos.			**Nula**
		Revisión periódica de los datos y archivos para verificar su integridad.			
		Los cambios a datos o archivos entrados del sistema deben ser autorizados.			
		Procedimientos para responder a errores de validación.			

		Procedimientos para probar la validez de los datos de entrada.			
		Responsabilidades del personal involucrado en el ingreso de datos al sistema.			
		Registro de actividades relacionadas al ingreso de datos.			
	12.2.2. Control del procesamiento interno	Controles para la prevención de pérdida de integridad de los datos durante el procesamiento.			**Nula**
		Documentación de las actividades de revisión que defina qué se debe revisar y cómo.			
	12.2.3. Integridad del mensaje	Definición de requerimientos para mantener la integridad del mensaje en los sistemas.			**Nula**
	12.2.4. Validación de los datos de salida	Revisión que las salidas sean razonables.			**Nula**
		Procedimientos para validación de salidas.			
		Registro de actividades de validación de datos de salida.			
12.3. Controles criptográficos	12.3.1. Política sobre el uso de controles criptográficos	Uso de controles criptográficos basados en una evaluación de riesgo.			**Nula**
		Establecimiento de política del uso de controles criptográficos.			
	12.3.2. Gestión de claves	Las claves criptográficas se protegen contra una modificación, pérdida y destrucción.			**Nula**
		Protección física del equipo utilizado para generar, almacenar y archivar claves.			
		Definición de procedimientos para la gestión de claves.			
		Registro de actividades relacionadas a la gestión de claves.			

12.4. Seguridad de los archivos del sistema	12.4.1. Control del *software* operacional	Las actualizaciones de *software* se realizan por personas capacitadas y autorizadas por la gerencia.			**Nula**
		Los sistemas operacionales deben mantenerse sólo como códigos ejecutables aprobados.			
		El *software* no debe pasar a operación a menos que haya pasado por una etapa satisfactoria de pruebas.			
		Gestión de la configuración del *software* puesto en operación.			
		Registro de las actualizaciones realizadas al *software*.			
		Almacenamiento de versiones viejas de *software* para contingencia.			
	12.4.2. Protección de la *data* del sistema	No utilizar información de bases de datos operacionales para realizar pruebas.			**Nula**
		En caso de utilizar información operacional se debe restringir el acceso a esta.			
		Autorización para copiar información operacional a ambientes de prueba.			
		Información operacional debe ser borrada de ambientes de prueba una vez realizadas las pruebas.			
		Registro de información operacional copiada a ambientes de prueba.			
	12.4.3. Control de acceso al código fuente del programa	Restricción de acceso al código fuente del programa.			**Nula**
		Restricción de acceso a ítems del programa como diseños, especificaciones, planes de validación y otros.			
		No almacenar bibliotecas de código fuente en sistemas operacionales.			
		Definición de procedimientos para la gestión de códigos fuentes.			
		Restricción de acceso del personal de soporte al código fuente.			

		Autorización para actualización de bibliotecas fuentes.			
		Registro de auditoría de los accesos realizados a las bibliotecas fuentes.			
12.5. Seguridad en los procesos de desarrollo y soporte	12.5.1. Procedimientos del control del cambio	Establecimiento de procedimientos de implementación de cambios en sistemas.			Nula
		Los procedimientos de cambio deben poseer un registro de los niveles de autorización acordados.			
		Los procedimientos de cambio deben asegurar que sólo usuarios autorizados hagan solicitudes de cambio.			
		Los procedimientos de cambio deben verificar que la integridad no se vea comprometida por un cambio.			
		Los procedimientos de cambio garantizan que se identifiquen otras tecnologías afectadas por el cambio.			
		Los procedimientos deben asegurar que se apruebe formalmente el cambio antes de implementarlo.			
		Los procedimientos de cambio aseguran que los usuarios aceptan el cambio.			
		Los procedimientos de cambio indican que se debe actualizar la documentación debida.			
		Mantener un registro de auditoría de solicitudes de cambio.			
		Los cambios no deben afectar la operativa del negocio.			
	12.5.2. Revisión técnica de la aplicación después de cambios en el sistema	Revisión de la integridad de la aplicación posterior a un cambio.			Nula
		Aseguramiento que exista el plan y el presupuesto anual cubran las pruebas posteriores a un cambio.			
		La notificación de cambios se hace con tiempo suficiente para planear y preparar las pruebas.			

		Actualizaciones del plan de continuidad cuando se realicen cambios.			
	12.5.3. Restricciones sobre los cambios en los paquetes de *software*	No se debiera realizar cambios a los paquetes de *software* de los vendedores.			**Nula**
		Un cambio de un paquete de *software* requiere validar la integridad de los controles de seguridad.			
		Un cambio del paquete de *software* se realiza sólo con autorización del vendedor.			
		Se deber verificar la posibilidad de que un cambio sea hecho por el vendedor en forma de actualización.			
		Evaluación del impacto que la empresa deba mantener el *software* a futuro a razón del cambio.			
		Mantener el *software* original y realizar los cambios en una copia identificada.			
	12.5.4. Filtración de información	Escaneo del flujo de salida de los medios y comunicaciones en búsqueda de información oculta.			**Nula**
		Enmascarar y modular la conducta del sistema y comunicaciones.			
		Hacer uso de *software* considerado de alta integridad.			
		Monitoreo del uso de la información en los sistemas.			
	12.5.5. Desarrollo de *software* abastecido externamente.	Supervisión del desarrollo de *software* abastecido externamente.			**Nula**
		Gestión de contratos de licencias, propiedad de códigos, derechos de propiedad intelectual.			
		Derechos de acceso para la auditoría de la calidad.			
		Definición de requerimientos contractuales para la funcionalidad de calidad y seguridad del código.			
		Pruebas antes de la instalación del *software*.			

12.6. Gestión de la vulnerabilidad técnica	12.6.1. Gestión de las vulnerabilidades técnicas	Definición de un proceso de gestión de las vulnerabilidades técnicas.			Nula
		La organización define los roles y responsabilidades asociadas con la gestión de las vulnerabilidades técnicas.			
		Identificación de recursos de información necesarios para identificar las vulnerabilidades técnicas.			
		Definición del tiempo de respuesta adecuado para responder a las vulnerabilidades técnicas.			
		Identificación de riesgos a partir una vulnerabilidad técnica y las acciones requeridas.			
		Evaluación del riesgo de usar un parche para solucionar una vulnerabilidad técnica.			
Dominio		**13. Gestión de incidentes de la Seguridad de la Información**			
Documentos evaluados					
Objetivo de control	**Control**	**Aspectos: qué políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir**	**¿Se cumple el aspecto?**	**Evidencia**	**Cobertura del control**
13.1. Reporte de los eventos y debilidades de la Seguridad de la Información	13.1.1. Reporte de eventos en la Seguridad de la Información	Definición de un procedimiento para reporte de incidentes de Seguridad de la Información.			Nula
		Definición de un procedimiento para atención y respuesta de incidentes de Seguridad de la Información			
		Establecimiento de un punto de contacto para el reporte de incidentes.			
		Aseguramiento que el punto de contacto de reporte de incidentes es conocido por toda la organización.			
		Responsabilidad de empleados, contratistas y terceros de reportar incidentes de Seguridad de la Información.			
	13.2.1. Reporte de las debilidades en la seguridad	Todo empleado, contratista y tercero reportan debilidades identificadas en la seguridad.			Nula
		Definición de un mecanismo de reporte que sea fácil, accesible y disponible.			

		Los empleados, contratistas y terceros no deben probar las debilidades sospechadas.			
13.2. Gestión de los incidentes y mejoras en la Seguridad de la Información	13.2.1. Responsabilidades y procedimientos	Monitoreo del sistema para detectar incidentes en la Seguridad de la Información.			**Nula**
		Definición de procedimientos para distintos tipos de incidentes de seguridad.			
		Establecimiento de planes de acción para la atención de incidentes.			
		Rastros de auditoría de los incidentes que se presenten.			
	13.2.2. Aprender de los incidentes en la Seguridad de la Información	Mecanismos para cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad.			**Nula**
		Uso de información de los incidentes atendidos para identificar incidentes recurrentes y su impacto.			
	13.2.3. Recolección de evidencia	Cuando un incidente origina una acción legal en contra de una persona se debe recolectar evidencia.			**Nula**
		La evidencia debe poder ser presentada en la corte.			
		La evidencia debe ser íntegra.			
		Aseguramiento que los sistemas de información generen evidencia admisible.			
		Rastros en papel deben guardase físicamente de una manera segura.			
		Rastros en papel requieren que se documente quién, cuándo y dónde se encontró el documento.			
		Rastros en papel requiere que se documenten testigos del hallazgo del documento.			
		Rastros digitales requieren que se cree una copia y haya todo un registro del proceso de copiado.			
Dominio		**14. Gestión de la continuidad del negocio**			

Documentos evaluados					
Objetivo de control	**Control**	**Aspectos: qué políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir**	**¿Se cumple el aspecto?**	**Evidencia**	**Cobertura del control**
14.1. Aspectos de la Seguridad de la Información de la gestión de la continuidad del negocio	14.1.1. Incluir la Seguridad de la Información en el proceso de gestión de continuidad del negocio	Proceso de continuidad del negocio que contempla la Seguridad de la Información.			**Nula**
		Identificación de los activos involucrados en los procesos críticos.			
		Identificación del impacto de incidentes de Seguridad de la Información en la continuidad del negocio.			
		Garantizar la seguridad del personal, medios de procesamiento y la propiedad organizacional.			
		Formulación y documentación de planes de continuidad que contemplen la Seguridad de la Información.			
		Pruebas de los planes y procesos de continuidad.			
		La continuidad del negocio se incorpora en los procesos de la estructura organizacional.			
	14.1.2. Continuidad del negocio y evaluación del riesgo	Identificación de eventos que puedan causar interrupciones en los procesos del negocio.			**Nula**
		La evaluación del riesgo de la continuidad el negocio se lleva a cabo con los propietarios de los procesos.			
	14.1.3. Desarrollar e implementar los planes de continuidad incluyendo la Seguridad de la Información	Identificación de todas las responsabilidades de Seguridad de la Información.			**Nula**
		Identificación de la pérdida aceptable de la información y los servicios.			
		Implementación de los procedimientos para permitir la recuperación y restauración de las operaciones.			
		Procedimientos operacionales a seguir dependiendo de la culminación de la recuperación y restauración.			
		Documentación de los procedimientos de continuidad del negocio.			

		Capacitación del personal en procedimientos de continuidad del negocio.			
		Prueba y actualización de los planes.			
	14.1.4. Marco referencial de la planeación de la continuidad del negocio	Mantenimiento de un solo marco referencial de los planes de continuidad del negocio.			**Nula**
		El plan describe las condiciones para la activación.			
		El plan se debe actualizar conforme aparezcan nuevos requerimientos.			
		El plan de continuidad se incluye dentro del proceso de gestión del cambio organizacional.			
		El plan posee un propietario con responsabilidades asignadas.			
		El plan define procedimientos para actuar posterior a un incidente que amenace la actividad comercial.			
		Procedimientos para trasladar las operaciones a sitios de contingencia.			
		Procedimientos operacionales temporales a seguirse hasta la recuperación.			
		Un programa de pruebas del plan de continuidad.			
		Un programa de mantenimiento del plan de continuidad.			
		Actividades de capacitación para la continuidad del negocio.			
	14.1.5. Prueba, mantenimiento y re-evaluación de los planes de continuidad del	Los planes de continuidad se prueban regularmente.			**Nula**
		Los involucrados en los planes de continuidad deben conocer sus roles y responsabilidades.			
		El plan de pruebas indica cómo y cuándo probar cada elemento			

	negocio	del plan.			
		Pruebas de distintos escenarios.			
		Simulaciones para capacitar a las personas en sus roles de continuidad del negocio.			
		Prueba de recuperación técnica de los sistemas.			
		Prueba de recuperación en el sitio alterno.			
		Prueba de medios y servicios del proveedor.			
		Ensayos completos.			
Dominio		**15. Cumplimiento**			
Documentos evaluados					
Objetivo de control	**Control**	**Aspectos: qué políticas, controles, lineamientos, enunciados, procesos o procedimientos deben cubrir**	**¿Se cumple el aspecto?**	**Evidencia**	**Cobertura del control**
15.1. Cumplimiento de los requerimientos legales	15.1.1. Identificación de la legislación aplicable	Identificación de requerimientos estatutarios, reguladores y contractuales relevantes.			**Nula**
		Definición del enfoque de la organización para cubrir estos requerimientos.			
		Definición de controles propuestos para cubrir con los requerimientos.			
	15.1.2. Derechos de propiedad intelectual (IPR)	Política de cumplimiento de los derechos de propiedad intelectual sobre el uso legal de *software* e información			**Nula**
		Adquisición de *software* a través de fuentes conocidas y acreditadas.			
		Notificación al personal de las medidas a tomar si se viola la política.			
		Identificar los requerimientos de protección de derechos de propiedad intelectual de los activos.			

		Mantener prueba y evidencia de la propiedad de las licencias, discos maestros, manuales, etc.			
		Controlar que no se exceda el número de usuarios permitidos por licencia.			
		Política para mantener las condiciones establecidas en las licencias.			
		Política para transferir y eliminar *software*.			
		No duplicar o extraer registros comerciales aparte de los permitidos por la Ley de Derechos de Autor.			
		No copiar, completa o parcialmente, documentos fuera de los permitidos por la Ley de Derechos de Autor.			
	15.1.3. Protección de registros organizacionales	Clasificación de los registros según su tipo.			**Nula**
		Procedimientos de manipulación para los medios en los que se almacenan los registros.			
		Verificación de la capacidad de los medios para almacenar los registros del periodo.			
		Clasificación de los registros según el periodo al que pertenecen.			
		El sistema de almacenaje de registros debe permitir su eliminación después del periodo adecuado.			
		Definición de lineamientos de retención, almacenaje, manipulación y eliminación de registros.			
		Programa de retención de registros y el tiempo durante el cual se van a retener.			
		Inventario de fuentes de información claves.			
		Controles para la protección de los registros.			
	15.1.4. Protección de	Definición de política de protección de la información personal.			**Nula**

	la *data* y privacidad de la información personal				
		Comunicado de la política a empleados que manejen información personal.			
		Control gerencial del cumplimiento de la política de protección de información personal.			
	15.1.5. Prevención del mal uso de los medios de procesamiento de la información	Aprobación gerencial del uso de los medios de procesamiento de información.			**Nula**
		Uso de monitoreo, asesorado legalmente, para controlar el uso de los medios de procesamiento de información			
	15.1.6.Regulación de controles criptográficos	Controles criptográficos se utilizan en cumplimiento con todos los acuerdos, leyes y regulaciones relevantes.			**Nula**
		Asesoría legal para el traslado de controles criptográficos e información codificada.			
15.2 Cumplimiento de las políticas y estándares de seguridad y cumplimiento técnico	15.2.1 Cumplimiento con las políticas y estándares de seguridad	Revisión del gerente, en su área de responsabilidad, el cumplimiento de las políticas de seguridad.			**Nula**
		El gerente debe identificar las causas de un incumplimiento.			
		El gerente debe identificar las acciones para que no ocurra de nuevo un incumplimiento.			
		El gerente debe asegurar que se identifique e implemente una acción correctiva.			
	15.2.2. Chequeo del cumplimiento técnico	Los sistemas de información se revisan para ver el cumplimiento de los estándares de seguridad.			**Nula**
		Las revisiones técnicas son realizadas por un experto y haciendo uso de herramientas automatizadas.			
		Las pruebas se deben planear y documentar.			
15.3. Consideraciones de auditoría de los sistemas de información	15.3.1. Controles de auditoría de los sistemas de información	Acordar con la gerencia los requerimientos de auditoría.			**Nula**
		Definición del alcance de las auditorías.			

		La auditoría se limita a sólo lectura de información.			
		Documentación de los procedimientos, requerimientos y responsabilidades.			
		Los auditores deben ser independientes a las actividades auditadas.			
	15.3.2. Protección de las herramientas de auditoría de los sistemas.	Las herramientas de auditoría de los sistemas de información se separan de otro *software*.			**Nula**
		Establecimiento de controles en caso que las auditorías sean realizadas por terceras personas.			