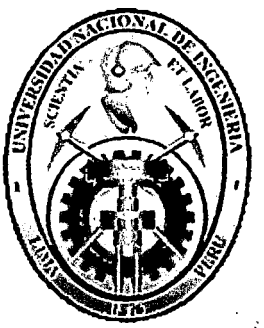
Universidad Nacional de Ingeniería

Facultad de Ingeniería Industrial y de Sistemas



METODOLOGÍA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SECTOR FINANCIERO PERUANO

TESIS

Para optar el Título Profesional de:

INGENIERO DE SISTEMAS

AQUIJE QUIJANDRIA JORGE GILMER

JAVE BOBADILLA LIZ LAURA

LIMA – PERÚ

2012

DEDICATORIA

A nuestros padres por su apoyo incondicional durante toda nuestra formación universitaria.

A nuestra alma mater que nos formó como profesionales en Ingeniería de Sistemas para servir con ética en beneficio de nuestra patria.

AGRADECIMIENTO

Damos gracias al Ing. Juan Carlos Sotelo quien nos motivó a iniciar y terminar nuestra tesis.

Gracias a todo el jurado: Dra. Gloria Huamaní, Ing. Carlos Trigo e Ing. Ernesto Bringas, por su apoyo y tiempo brindado.

Y un agradecimiento especial al Ing. Carlos Cárdenas Fernández quien, sin saberlo, desde su blog http://unimauro.blogspot.com fue de gran ayuda como referencia de los trámites y pasos a seguir para la titulación.

ÍNDICE

ANEXOS

TABLAS

DESCRIPTORES TEMÁTICOS

1. Seguridad de Información
2. Circular SBS G-140
3. ISO 27001
4. ISO 17799
5. SGSI
6. Metodología de Gestión
7. Riesgos
8. Activos de Información

RESUMEN

La presente tesis realiza una propuesta metodológica para realizar una implementación exitosa del Sistema de Gestión de Seguridad de la Información (SGSI) en las empresas del Sector Financiero Peruano y de este modo dar cumplimiento a la regulación vigente que, de acuerdo a la Circular G-140 de la SBS (Superintendencia de Banca, Seguros y AFP), exige la implementación del SGSI.

El problema abordado es la dificultad de las empresas de este sector para implementar el SGSI, es por ello que, el mencionado ente regulador ha venido aplazando las fechas límites de implementación al constatar que no ha sido posible que las empresas logren implementar el SGSI en el plazo previsto. Según se plantea en la tesis y de acuerdo a estudios internacionales, uno de los factores más importantes que no permiten una implementación exitosa del SGSI es el poco entendimiento que aún tienen las empresas sobre la Seguridad de la Información.

Con la finalidad de dar solución al problema identificado, es que en la presente tesis se brindan una serie de pasos, herramientas y formatos que ayudarán y facilitarán la gestión de la seguridad de la información considerando las etapas del ciclo Deming: Establecimiento, Implementación, Monitoreo y Mejora Continua.

El trabajo desarrollado tiene como eje principal la circular G-140-SBS, la misma que ha sido alineada al estándar internacional ISO 27001 para identificar todos los componentes necesarios para establecer, implantar, mantener y mejorar un SGSI.

Finalmente, se brindan unas conclusiones y recomendaciones que se centran en el aporte que la presente propuesta brindaría a las empresas para el desarrollo de un SGSI.

INTRODUCCIÓN

La seguridad de la información es un tema del cual las empresas de nivel mundial están muy conscientes y se le considera como un aspecto crítico en la organización. Es por ello que, existen algunas normas y metodologías que ayudan a implementar los sistemas de gestión de seguridad de la información que las organizaciones requieren para asegurar la confidencialidad, integridad y disponibilidad de sus activos de información.

En nuestro país existen dos normas referentes al tema: la NTP 17799 y la circular N° G-140-2009. Para la presente tesis es de interés la circular que obliga a las instituciones financieras a implementar un Sistema de Gestión de Seguridad de la Información.

Para el cumplimiento de la circular G-140-2009 es necesario seguir una metodología de implementación. Es por ello que, en esta propuesta de tesis se desea desarrollar dicha metodología que es requerida por las instituciones financieras para la implementación del SGSI tanto como un medio para cumplir con la norma y, en especial, asegurar a los activos de información más críticos de la entidad financiera.

CAPÍTULO I
TEMA DE INVESTIGACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

En el Perú el 02 de abril del 2009 la Superintendencia de Banca y Seguros emitió la circular N° G-140-2009 que obliga a las instituciones financieras a implementar un sistema de gestión de seguridad de la información (SGSI).

La realización de esta actividad no es sencilla considerando que en el Perú el nivel de madurez de la gestión de la seguridad de la información aún es bajo, si bien se carece de estudios hechos específicamente para el Perú, esto es sustentable con estadísticas a nivel de Latinoamérica como se muestra a continuación.

En la encuesta Latinoamericana de Seguridad de la Información 2010[1] elaborada por SegurInfo[2], reconocido portal en seguridad de la información que tiene el respaldo de prestigiosas instituciones de este rubro como ISACA[3], donde participaron países como Colombia, Argentina, Venezuela, México, Uruguay, Paraguay y Perú, se obtuvo como resultado que el principal obstáculo

[1] Jeimy J. Cano, Ph.D. Seguridad de la Información en Latinoamérica Tendencias 2010.[PDF] http://www.acis.org.co

[2] http://www.segurinfo.org/home.php

[3] Information Systems Audit and Control Association

para desarrollar una adecuada seguridad dentro de las empresas es el poco entendimiento de la seguridad informática.

	2009%	2010%
Inexistencia de política de seguridad	10,40	13,04
Falta de tiempo	12,70	13,4
Falta de formación técnica	10,10	4,71
Falta de apoyo directivo	**18,50**	15,21
Falta de colaboración entre áreas/departamentos	14,00	10,86
Complejidad tecnológica	7,50	9,78
Poco entendimiento de la seguridad informática	14	**18,47**
Poco entendimiento de los flujos de la información en la organización	4,20	5,79

Tabla 1 Principal obstáculo para desarrollar una adecuada seguridad

Estos factores como el poco entendimiento de la seguridad informática, falta de apoyo directivo y el poco entendimiento de los flujos de la información en la organización pueden traer como consecuencia el siguiente resultado; el cual muestra que, más del 50% de las empresas aún no tienen definida una política de seguridad o está en desarrollo.

	2009%	2010%
No se tienen políticas de seguridad definidas	24,40	14,85
Actualmente se encuentran en desarrollo	**41,60**	**43,84**
Política formal, escrita documentada e informada a todo el personal	34,10	41,30

Tabla 2 Estado actual de las políticas de seguridad

Entonces podemos identificar un problema en la gestión de la seguridad del cual, en esta tesis, se tratará de plantear una solución para entender y desarrollar mejor todo el ciclo de la gestión del sistema de seguridad de la información.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo una institución del sector financiero peruano puede gestionar la seguridad de la información?

1.3 HIPÓTESIS

Las instituciones del sector financiero peruano pueden gestionar la seguridad de la información a través de una metodología sencilla y flexible que le permita cumplir con las regulaciones vigentes y establecer los controles apropiados para proteger sus activos de información.

1.4 OBJETIVO

Diseñar una metodología de gestión de seguridad de la información orientada al sector financiero peruano, que involucre desde la identificación de activos hasta el monitoreo y control de los riesgos.

1.5 JUSTIFICACIÓN

Actualmente sólo existen buenas prácticas y lineamientos con respecto a la seguridad de la información, no existe una metodología que brinde herramientas para todo el ciclo de la gestión de un sistema de seguridad de la información. El tener de apoyo una metodología clara y sencilla que sea entendible y no genere mayores confusiones a los encargados de implementar el Sistema de Gestión de Seguridad de la Información, les ayudará a poder implementarlo con mayor confianza sin las dudas y dificultades que se tienen acerca de la seguridad de la información debido al poco entendimiento que aún se tiene de la misma; permitiéndoles medir y, por tanto, gestionar el nivel de

seguridad de la información de la institución de acuerdo a la estrategia del negocio y a las regulaciones vigentes.

CAPÍTULO II
MARCO TEÓRICO

2.1 CONCEPTOS PREVIOS

2.1.1 Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.

2.1.2 Sistema de gestión de seguridad de la información

Parte del sistema gerencial general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información

2.1.3 Riesgos de seguridad de la información

Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos de información causando así daño a la organización.

2.1.4 Gestión de riesgos de seguridad de la información

La gestión del riesgo en la seguridad de la información es un proceso continuo. Tal proceso debería establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable.

2.1.5 Return on Security Investment (ROSI)4

Es un indicador clave de rendimiento (KPI) que ayuda a medir la eficiencia y eficacia del gasto en seguridad de TI. La métrica es una medida de arriba hacia abajo que relaciona los gastos de seguridad y su productividad en un indicador conciso y comparativo para la evaluación del desempeño actual y la planificación.

2.2 ANTECEDENTES

Durante la revisión de papers se encontró uno muy general sobre los niveles de madurez de la gestión de la seguridad de la información en las empresas. Los autores[5] dividen estos niveles en cuatro. En el primer nivel la seguridad de la información es un problema estrictamente técnico, responsabilidad de los técnicos en computación o afín. En el segundo nivel se registra la información concerniente a los ataques y vulnerabilidades y se

[4] ISACA, IT Audit and Assurance Guideline. G41 Return on Security Investment (ROSI).

[5] Orlando Viloria, Marianella Villegas, Walter Blanco. La Seguridad de la Información bajo una Perspectiva de la Madurez Organizacional. Venezuela.

realimenta el proceso de toma de decisiones, para evitar el desarrollo de otras amenazas y formular nuevas acciones. El tercer nivel investiga cuáles son los modelos mentales que condicionan las interpretaciones de los trabajadores del conocimiento y tienen un efecto directo en las decisiones destinadas a resolver problemas. Finalmente en el último nivel el departamento de seguridad llega a un máximo estado de aprendizaje, están presentes las cinco disciplinas de las organizaciones inteligentes: los modelos mentales, el dominio personal, la visión compartida, el aprendizaje en equipo y el pensamiento sistémico.

En el paper titulado "Information security risk assessment: the qualitative versus quantitative dilemma"[6], se llega a la conclusión que los enfoques cuantitativo y cualitativo se complementan entre sí. Ambos tienen una influencia subjetiva en su resultado por la misma naturaleza del hombre. Por tanto debe existir un balance entre ambos análisis, en el caso del análisis cuantitativo se presta a subjetividad en la valoración de los activos y así como en otros valores que son decisión del analista.

En el paper desarrollado por Vidalina De Freitas[7] se propone conocer las fortalezas y debilidades a las que pudieran estar sometidos los activos de información que están en custodia en la Dirección de Servicios Telemáticos (DST) de la Universidad Simón Bolívar ubicada en Caracas, Venezuela, con el fin de sugerir estrategias que minimicen la ocurrencia de posibles amenazas que en la mayoría de los casos explotan las vulnerabilidades organizacionales.

Y siendo más innovador el CISSP Omar Herrera desarrolló el paper titulado "Graphical Risk Analysis (GRA): A Methodology To Aid In Modeling

[6] Adrian Munteanu. Information security risk assessment: the qualitative versus quantitative dilemma. Rumania.

[7] Vidalina De Freitas. Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. 2009

Systems For Information Security Risk Analysis". GRA pretende ser una metodología de análisis de riesgos sencilla centrada en la disponibilidad y la dependencia que existe entre los servicios y sistemas. Aunque no pretende ser una solución integradora, será útil en combinación con otras metodologías, en todas las actividades de análisis de riesgo para la seguridad de la información. Además, el GRA no eliminará la subjetividad del análisis (que seguirá dependiendo de la experiencia, conocimiento y buen juicio para definir algunos elementos). El elemento clave de GRA es que permite al analista definir los elementos y las relaciones (que llama "sistema") en lugar de valores. Es más fácil para definir e identificar la importancia de los activos en un diagrama donde el flujo del negocio es ilustrado y las fórmulas sencillas que se definen en la metodología GRA están diseñadas para cuantificar su importancia.

El paper "Modelos para seguridad de la información en TIC"[8] que presenta un modelo para facilitar la obtención de nivel se control de riesgos adecuado en TIC, el cual se basa en estándares (ISO 17799, COBIT) y normas internacionales (ITIL, COSO) para evitar y/o disminuir las fallas en los sistemas, redes y todo el patrimonio informático. El aporte del paper es básicamente de carácter descriptivo respecto a los pasos que se deberían utilizar al implementar una metodología que asegure los activos de información.

Córdova Rodríguez presenta en el 2003 su tesis titulada "Plan de seguridad informática para una entidad financiera" con el objetivo de diseñar un Plan de Seguridad que permita desarrollar operaciones seguras basadas en políticas y estándares claros y conocidos por todo el personal de un determinado Banco. Adicionalmente define la estrategia y los proyectos más importantes que deben ser llevados a cabo para culminar con el Plan de

[8] Jorge Burgos Salazar, Pedro G. Campos. Chile.

Implementación. Cabe resaltar que esta tesis y la que se expone en el párrafo siguiente toman como referencia la Circular SBS N° G-105-2002 que ha quedado sin efecto el 31 de marzo del 2010, ante la nueva Circular SBS N° G-140-2009.

En el 2006, la tesis de Villena Aguilar[9] establece los principales lineamientos para poder implementar de manera exitosa, un adecuado modelo de sistema de gestión de seguridad de información (SGSI) en una institución financiera en el Perú, el cual apunta a asegurar que la tecnología de información usada esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización. En el punto Administración de Riesgos plantea que para el caso de una institución financiera, generalmente el riesgo es la probabilidad de que un evento o transacción produzca pérdida monetaria, daño a la imagen, su personal y a sus activos.

2.3 NORMATIVIDAD

2.3.1 Circular G-140-2009

Esta circular emitida por la Superintendencia de Banca y Seguros (SBS) el 2 de abril del 2009, es de aplicación obligatoria para todas las entidades del sector financiero incluidas las cajas municipales de ahorro y crédito, las Administradoras Privadas de Fondos de Pensiones (AFP) y la Corporación Financiera de Desarrollo.

[9] Villena Aguilar, Moisés. PUCP. Sistema de gestión de seguridad de información para una institución financiera. 2006

Tomando como referencia estándares internacionales, como la ISO 17799 y la ISO 27001, establece los criterios mínimos para una adecuada gestión de la seguridad de la información, que incluye aspectos referidos a la estructura organizacional, controles de seguridad de información, seguridad en operaciones de transferencia de fondos por canales electrónicos, así como la subcontratación del procesamiento de datos, cuando éste sea realizado en el exterior.

2.3.2 ISO 27001

Es el estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) fue aprobado y publicado como estándar internacional en octubre de 2005.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido Ciclo de Deming: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

2.3.3 ISO 17799

ISO/IEC 17799 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo

quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2005 del estándar incluye las siguientes once secciones principales:

- Política de Seguridad de la Información.
- Organización de la Seguridad de la Información.
- Gestión de Activos de Información.
- Seguridad de los Recursos Humanos.
- Seguridad Física y Ambiental.
- Gestión de las Comunicaciones y Operaciones.
- Control de Accesos.
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de Incidentes en la Seguridad de la Información.
- Gestión de Continuidad del Negocio.
- Cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

2.3.4 ISO 27005

Publicada en junio de 2008, consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI.

No proporciona una metodología concreta de Análisis de Riesgos, sino que describe a través de su clausulado el proceso recomendado de análisis incluyendo las fases que lo conforman:

- Establecimiento del contexto (Cláusula 7)
- Evaluación del riesgo (Cláusula 8)
- Tratamiento del riesgo (Cláusula 9)
- Aceptación del riesgo (Cláusula 10)
- Comunicación del riesgo (Cláusula 11)
- Monitorización y revisión del riesgo (Cláusula 12)

2.4 BUENAS PRÁCTICAS

2.4.1 Information Technology Infrastructure Library: ITIL

ITIL es el método más ampliamente adoptado para la Gestión de Servicios TI en el mundo. Proporciona un marco práctico para identificar, planificar, entregar y mantener los servicios de TI del negocio.

ITIL aboga por que los servicios de TI deben estar alineados a las necesidades del negocio y apoyar los procesos de negocio. Proporciona orientación a las organizaciones sobre la manera de utilizarlo como una herramienta para facilitar los cambios en el negocio, la transformación y el crecimiento.

Las mejores prácticas de ITIL son detallados en la actualidad dentro de las cinco principales publicaciones que ofrecen un enfoque sistemático y

profesional para la gestión de servicios de TI, permitiendo a las organizaciones ofrecer servicios apropiados y asegurarse de que continuamente están cumpliendo los objetivos de negocio y proporcionar beneficios.

Las cinco guías básicas mapa de todo el ciclo de vida del Servicio de ITIL, comenzando con la identificación de las necesidades del cliente y los conductores de los requisitos de TI, pasando por el diseño y la implementación del servicio en funcionamiento y, por último, a la fase de seguimiento y la mejora del servicio.

La adopción de ITIL puede ofrecer a los usuarios una amplia gama de beneficios que incluyen:

- mejora de los servicios de TI
- reducción de los costos
- satisfacción del cliente a través de un enfoque más profesional a la prestación de servicios
- mejora de la productividad
- una mejor utilización de las habilidades y la experiencia
- mejorar la prestación de servicios de terceros.

2.4.2 Control Objectives For Information And Related Technology: COBIT

En el documento oficial versión 4.1 de COBIT se define:

"COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders).

COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma."

Los beneficios de implementar COBIT como marco de referencia de gobierno sobre TI incluyen:

- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los Interesados, con base en un lenguaje común
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI

2.5 METODOLOGÍAS DE ANÁLISIS DE RIESGO

2.5.1 Metodología De Análisis Y Gestión De Riesgos De Los Sistemas De Información De Las Administraciones Públicas: MAGERIT

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, como respuesta a la percepción de que la Administración, y, en general, toda la

sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

Persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista, y presenta como objetivos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

Como método describe los pasos y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de aspectos prácticos. Describe la metodología desde tres ángulos:

- Describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación. Es una presentación netamente conceptual.
- Describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, entendiendo que no basta con tener los conceptos claros, sino que es conveniente pautar roles, actividades, hitos y documentación para que la realización del proyecto de análisis y gestión de riesgos esté bajo control en todo momento.
- Aplica la metodología al caso del desarrollo de sistemas de información, en el entendimiento que los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento, tanto los riesgos a que están expuestos, como los riesgos que las propias aplicaciones introducen en el sistema.

2.5.2 Méthode Harmonisée D'analyse De Risques: MEHARI

MEHARI fue inicialmente diseñado para apoyar a los responsables de seguridad en sus tareas de gestión de la seguridad de los sistemas de información, pero está en permanente evolución para satisfacer la naturaleza cambiante del entorno del negocio.

Provee una serie de herramientas específicamente diseñadas para la gestión de la seguridad, que comprende una serie de acciones de gestión, y que cada una de ellas tiene un objetivo específico. Algunos ejemplos:

- Desarrollar planes de seguridad, o planes estratégicos,
- Implementar políticas o normas de seguridad, las cuales se agruparán bajo el término "marco de referencia de seguridad",
- Estado de situación o evaluaciones detalladas del estado de la seguridad,
- Evaluación y gestión del riesgo
- Asegurar la inclusión de la seguridad en la gestión de proyectos de desarrollo,
- Sensibilización sobre la seguridad y sesiones de formación,
- Gestión operativa de la seguridad y control/monitorización de las acciones ejecutadas.

2.5.3 Operationally Critical Threat, Asset, And Vulnerability Evaluation: OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es un conjunto de herramientas, técnicas y métodos para desarrollar análisis de riesgos basados en gestión y la planeación estratégica

de la organización. Son todas las acciones que necesitan ser llevadas a cabo dentro de la organización para realizar la gestión de activos, conocer posibles amenazas y evaluar vulnerabilidades.

Dentro de las ventajas de OCTAVE se pueden listar:

- Está enfocado en los riesgos y estrategias organizacionales, asuntos relacionados con la práctica, riesgos balanceados operacionales, prácticas de seguridad y tecnología.
- El método Octave usa 3 fases para examinar asuntos tecnológicos y de organización.
- La tecnología se examina únicamente en relación a las prácticas de seguridad
- Usa múltiples niveles de la organización, principalmente se enfocan en:
- Identifica asuntos y labores críticas así como las amenazas a esos asuntos.
- Identificar vulnerabilidades organizacionales y tecnológicas, que exponen amenazas creando riesgo a la organización.
- Desarrollar una estrategia de protección basada en la práctica así como planes de migración de riesgos para mantener la misión y prioridades de la organización.
- Existen diferentes versiones de octave, dependiendo de las necesidades de la compañía
- Método octave; Desarrollado para organizaciones con 300 o más empleados
- Octave-s desarrollado para compañías donde hay menos de 100 personas.
- Octave Allegro diseñado para organizaciones de 100 o un poco menos de 100 empleados).

CAPÍTULO III
PROPUESTA DE SOLUCIÓN

3.1 ALINEAMIENTO DE LA CIRCULAR CON ESTÁNDARES INTERNACIONALES

La circular G-140 toma como referencia estándares internacionales como la ISO 17799 y la ISO 27001. Sin embargo, los enunciados son muy genéricos es por ello que se ha visto conveniente realizar un alineamiento de la circular con estos estándares para un mayor entendimiento.

3.1.1 Alineamiento de la Circular G-140 con la ISO 27001

A continuación se muestra cómo los primeros artículos de la circular G-140 se alinean con la ISO 27001.

Tabla 3 Alineamiento G-140 vs ISO 27001

CIRCULAR G-140-2009-SBS		NORMA ISO 27001	
Nº	**Clausulas**	**Nº**	**Control**
Introducción	Referencia ISO 27001 y a la ISO 17799	Anexo A	Referencia ISO 27002 (ISO 17799)
Articulo1	Alcance al sistema financiero	1.2	Alcance a todas las organizaciones
Articulo 2	Definiciones		

Articulo 3	Establecer, mantener y documentar el SGSI	4.1	Establecer, implementar, operar, realizar seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de las actividades del negocio global de la organización
Articulo 3 a)	Definición de una política de seguridad de información aprobada por el Directorio.	4.2.1 b)	Políticas del SGSI
Articulo 3 b)	Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.	4.2.1 c)	Definir un enfoque de evaluación del riesgo de Seguridad de la Información
Articulo 3 c)	Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.	4.3.3	Los registros deben establecerse y mantenerse para proporcionar evidencias de la conformidad con los requisitos, así como de la operación eficaz del SGSI
Articulo 4	Las empresas deben contar con una estructura organizacional que les permita implementar y mantener el sistema de gestión de la seguridad de información.	6.1.1	Comité de gestión de seguridad de la información
Articulo 4 a)	Asegurar el cumplimiento de la política de seguridad de información y de la metodología definida por la empresa.	5.1.2	Revisión y evaluación
Articulo 4 b)	Coordinar y monitorear la implementación de los controles de seguridad de información.	4.2.3	Monitorear y Revisar el SGSI
Articulo 4 c)	Desarrollar actividades de concientización y entrenamiento en seguridad de información.	5.2.2	Concienciación y formación de seguridad de la información

Articulo 4 d)	Evaluar los incidentes de seguridad de información y recomendar acciones apropiadas	8.2 y 8.3	Acciones preventivas y correctivas

3.1.2 Alineamiento de la Circular G-140 con la ISO17799

A continuación se realiza un alineamiento de los controles de seguridad de la información mencionados en la circular G-140 con los controles de la ISO 17799.

3.1.2.1 Seguridad Lógica

A continuación, se especifica en que parte de la norma ISO 17799 se cubre cada punto que la circula de la SBS exige para el cumplimiento de este dominio. Para más detalle ir al ANEXO 1.1.

Tabla 4 G-140 vs ISO 17799: Seguridad Lógica

CIRCULAR G-140-2009-SBS		**NORMA ISO 17799**	
5.1	**Seguridad Lógica**		
5.1 a)	Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.		
	Procedimientos formales para la concesión	11.2.1	Registro de usuarios
	Procedimientos formales para la administración de derechos y perfiles, así como la revocación de usuarios.	11.2.2	Gestión de privilegios
5.1 b)	Revisiones periódicas sobre los derechos concebidos	11.2.4	Revisión de los derechos de acceso de los usuarios
5.1 c)	Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.	11.2.3	Gestión de contraseñas de usuario
		11.3.1	Uso de contraseñas
5.1 d)	Controles especiales sobre utilidades del sistema y herramientas de auditoría.		

	Controles especiales sobre utilidades del sistema	11.5.4	Utilización de las facilidades del sistema
	Controles especiales sobre herramientas de auditoría	15.3.1	Controles de auditoría de sistemas
		15.3.2	Protección de las herramientas de auditoría de sistemas
5.1 e)	Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.	10.10.2	Monitoreando el uso del sistema
5.1 f)	Controles especiales sobre usuarios remotos y computación móvil.	11.7.1	Información móvil y comunicaciones
		11.7.2	Teletrabajo/Teleservicio

3.1.2.2 Seguridad Personal

A continuación, se especifica en que parte de la norma ISO 17799 se cubre cada punto que la circula de la SBS exige para el cumplimiento de este dominio. Para más detalle ir al ANEXO 1.2.

Tabla 5 G-140 vs ISO 17799: Seguridad de Personal

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
5.2	**Seguridad de Personal**		
5.2 a)	Definición de roles y responsabilidades establecidos sobre la seguridad de información.	8.1.1	Inclusión de la seguridad en las responsabilidades y funciones laborales
5.2 b)	Verificación de antecedentes, de conformidad con la legislación laboral vigente.	8.1.2	Selección y política de personal
5.2 c)	Concientización y entrenamiento.	8.2.2	Conocimiento, educación y entrenamiento de la seguridad de información
5.2 d)	Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.	8.2.3	Proceso disciplinario
5.2 e)	Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos	8.3.3	Retiro de los derechos de acceso

3.1.2.3 Seguridad Física y ambiental

A continuación, se especifica en que parte de la norma ISO 17799 se cubre cada punto que la circula de la SBS exige para el cumplimiento de este dominio. Para más detalle ir al ANEXO 1.3.

Tabla 6 G-140 vs ISO 17799: Seguridad Física y Ambiental

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
5.3	**Seguridad Física y Ambiental**		
5.3 a)	Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.		
	Controles para evitar el acceso físico no autorizado	9.1.1	Perímetro de seguridad física
		9.1.2	Controles físicos de entradas
	Controles para evitar daños o interferencias a los locales y a la información de la empresa.	9.1.3	Seguridad de oficinas, despachos y recursos
5.3 b)	Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales.		
	Controles para prevenir pérdidas, daños o robos de los activos	9.2.1	Instalación y protección de equipos
		9.2.2	Suministro eléctrico
		9.2.3	Seguridad del cableado
		9.2.4	Mantenimiento de equipos
		9.2.5	Seguridad de equipos fuera de los locales de la organización
		9.2.6	Seguridad en el rehúso o eliminación de equipos
		9.2.7	Retiro de la propiedad
	Controles para la protección de los equipos frente a amenazas físicas y ambientales.	9.1.4	Protección contra amenazas externas y ambientales

3.1.2.4 Inventario de activos y clasificación de la información

A continuación, se especifica en que parte de la norma ISO 17799 se cubre cada punto que la circula de la SBS exige para el cumplimiento de este dominio. Para más detalle ir al ANEXO 1.4.

Tabla 7 G-140 vs ISO 17799: Inventario de activos y clasificación de la información

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
5.4	**Inventario de activos y clasificación de la información**		
5.4 a)	Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.		
	Realizar y mantener un inventario de activos asociados a la tecnología de información	**7.1.1**	**Inventario de activos**
	Asignar responsabilidades respecto a la protección de estos activos.	**7.1.2**	**Propiedad de los activos**
5.4 b)	Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.		
	Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa	7.2.1	Guías de clasificación
	Realizar las medidas apropiadas de control que deben asociarse a las clasificaciones.	7.2.2	Marcado y tratamiento de la información

3.1.2.5 Administración de las operaciones y comunicaciones

A continuación, se especifica en que parte de la norma ISO 17799 se cubre cada punto que la circula de la SBS exige para el cumplimiento de este dominio. Para más detalle ir al ANEXO 1.5.

Tabla 8 G-140 vs ISO 17799: Administración de las operaciones y comunicaciones

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
5.5	**Administración de las operaciones y comunicaciones**		
5.5 a)	Procedimientos documentados para la operación de los sistemas	10.1.1	Documentación de procedimientos operativos
5.5 b)	Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.	10.1.2	Gestión de Cambios
5.5 c)	Separación de funciones para reducir el riesgo de error o fraude.	10.1.3	Segregación de tareas
5.5 d)	Separación de los ambientes de desarrollo, prueba y producción.	10.1.4	Separación de los recursos para desarrollo y para producción
5.5 e)	Monitoreo del servicio dado por terceras partes	10.2.2	Monitoreo y revisión de los servicios externos
5.5 f)	Administración de la capacidad de procesamiento	10.3.1	Planificación de la capacidad
5.5 g)	Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.	10.4.1	Medidas y controles contra software malicioso
		10.4.2	Medidas y controles contra código móvil
5.5 h)	Seguridad sobre las redes	10.6.1	Controles de red
		10.6.2	Seguridad en los servicios de redes
	Seguridad sobre los medios de almacenamiento	10.7.1	Gestión de medios removibles
	Seguridad de la documentación de sistemas	10.7.3	Procedimientos de manipulación de la información
		10.7.4	Seguridad de la documentación de sistemas
5.5 i)	Seguridad de intercambio de información	10.8.1	Políticas y procedimientos para el intercambio de información y software
		10.8.2	Acuerdos de intercambio
	Seguridad de intercambio de información por correo electrónico	10.8.4	Seguridad en la mensajería electrónica
5.5 j)	Seguridad de canales electrónicos	10.9.2	Transacciones en línea
5.5 k)	Mantenimiento de registros de auditoría y monitoreo del uso de sistemas	10.10.1	Registro de la auditoria

3.1.2.6 Adquisición, desarrollo, mantenimiento de sistemas de informáticos

A continuación, se especifica en que parte de la norma ISO 17799 se cubre cada punto que la circula de la SBS exige para el cumplimiento de este dominio. Para más detalle ir al ANEXO 1.6.

Tabla 9 G-140 vs ISO 17799: Adquisición, desarrollo, mantenimiento de sistemas

CIRCULAR G-140-2009-SBS		**NORMA ISO 17799**	
5.6	**Adquisición, desarrollo, mantenimiento de sistemas informáticos**		
5.6 a)	Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales	12.1.1	Análisis y especificación de los requisitos de seguridad
	controles sobre el ingreso de información	12.2.1	Validación de los datos de entrada
	controles sobre el procesamiento	12.2.2	Control del proceso interno
	Controles sobre la información de salida.	12.2.3	Integridad de los mensajes
		12.2.4	Validación de los datos de salida
5.6 b)	Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.	12.3.1	Política de uso de los controles criptográficos
5.6 c)	Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.	12.4.1	Control del software en producción
		12.4.2	Protección de los datos de prueba del sistema
5.6 d)	Controlar el acceso a las librerías de programas fuente.	12.4.3	Control de acceso a los códigos de programas fuente
5.6 e)	Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.	12.5.1	Procedimientos de control de cambios
		12.5.2	Revisión técnica de los cambios en el sistema operativo
		12.5.3	Restricciones en los cambios a los paquetes de software
5.6 f)	Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.	12.6.1	Control de las vulnerabilidades técnicas

3.1.2.7 Procedimiento de respaldo

A continuación, se especifica en que parte de la norma ISO 17799 se cubre cada punto que la circula de la SBS exige para el cumplimiento de este dominio. Para más detalle ir al ANEXO 1.7.

Tabla 10 G-140 vs ISO 17799: Procedimientos de Respaldo

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
5.7	**Procedimientos de Respaldo**		
5.7 a)	Procedimientos de respaldo regulares y periódicamente validados	10.5.1	Recuperación de la información
5.7 b)	Conservar la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación.	10.5.1	Recuperación de la información

3.1.2.8 Gestión de incidentes de seguridad de la información

A continuación, se especifica en que parte de la norma ISO 17799 se cubre cada punto que la circula de la SBS exige para el cumplimiento de este dominio. Para más detalle ir al ANEXO 1.8.

Tabla 11 G-140 vs ISO 17799: Gestión de incidentes de seguridad de la información

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
5.8	**Gestión de incidentes de seguridad de la información**		
5.8 a)	Procedimientos formales para el reporte de incidentes de seguridad de la información	13.1.1	Reportando los eventos en la seguridad de información
	Procedimientos formales para el reporte de las vulnerabilidades asociadas con los sistemas de información.	13.1.2	Reportando debilidades en la seguridad de información
5.8 b)	Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.	13.2.1	Responsabilidades y procedimientos

3.1.2.9 Cumplimiento Normativo

A continuación, se especifica en que parte de la norma ISO 17799 se cubre cada punto que la circula de la SBS exige para el cumplimiento de este dominio. Para más detalle ir al ANEXO 1.9.

Tabla 12 G-140 vs ISO 17799: Cumplimiento normativo

CIRCULAR G-140-2009-SBS		**NORMA ISO 17799**	
5.9	**Cumplimiento normativo**		
5,9 a)	Las empresas deberán asegurar que los requerimientos legales, contractuales, o de regulación.	15.1.1	Identificación de la legislación aplicable
		15.1.2	Derechos de propiedad intelectual (DPI)
		15.1.3	Salvaguarda de los registros de la organización
		15.1.6	Regulación de los controles criptográficos
	y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.	15.2.2	Comprobación de la conformidad técnica

3.1.2.10 Privacidad de la información

A continuación, se especifica en que parte de la norma ISO 17799 se cubre cada punto que la circula de la SBS exige para el cumplimiento de este dominio. Para más detalle ir al ANEXO 1.10.

Tabla 13 G-140 vs ISO 17799: Privacidad de la información

CIRCULAR G-140-2009-SBS		**NORMA ISO 17799**	
5.10	**Privacidad de la información**		
5,10 a)	Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la normatividad vigente sobre la materia.	15.1.4	Protección de los datos y de la privacidad de la información personal

El alineamiento de la circular G-140-2009 de la SBS con los estándares internacionales ISO-27001 e ISO-17799 ha servido para demostrar que cada punto en la Circular es cubierto por los estándares ofreciendo incluso, estos últimos, puntos adicionales para la gestión de la seguridad de la información en los diversos dominios incluidos.

Se recomienda que las empresas puedan evaluar si están en la capacidad y nivel de madurez necesarios para poder implementar puntos adicionales que no son considerados por la circular de la SBS y que son descritos en alguno de los estándares internacionales.

Se recomienda que las pequeñas empresas como micro-financieras se centren en el cumplimiento de la Circular evitando incluir puntos que no se encuentran en ella y que a pesar de mejorar el nivel de seguridad de la empresa podría ser un distractor. Se debe tener en cuenta que el incluir nuevos controles será parte del mejoramiento continuo del sistema de gestión de seguridad de la información.

3.2 METODOLOGÍA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PROPUESTA

La metodología propuesta tiene en cuenta lo recomendado por la ISO 27001 y sigue las fases del ciclo de Deming o también llamado Plan-Do-Check-Act.

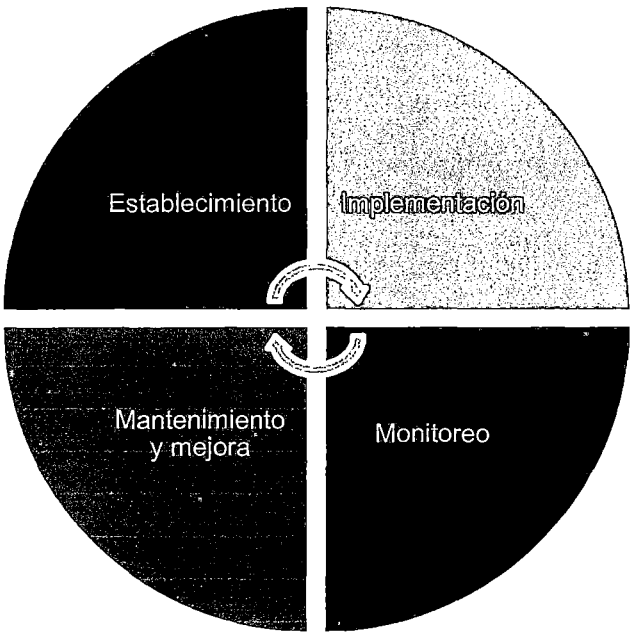


Gráfico 1 Ciclo Deming (PDCA)

3.2.1 Establecimiento

En esta primera fase se busca definir el área que asumirá las funciones relacionadas a la seguridad de la información para que posteriormente defina el alcance del SGSI y una política a nivel organizacional. Luego se definirá la metodología de análisis de riesgos con la cual se determinarán los controles que se implementarán en la siguiente fase.

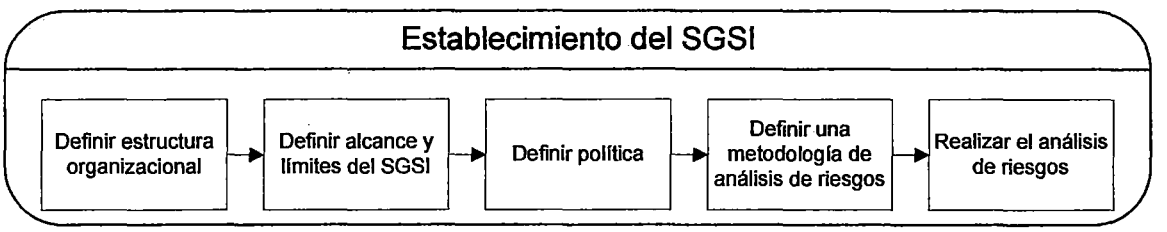


Gráfico 2 Establecimiento del SGSI

3.2.1.1 Definir estructura organizacional

Definición

Una pregunta que se deben haber realizado todas las entidades financieras es: "*¿Dónde ubicar el Departamento o Área de Seguridad de la Información en la estructura organizacional de la empresa?*".

Esta pregunta no es fácil de contestar ni existe una respuesta única para ella. Sin embargo, es fundamental el definir la ubicación en la estructura organizacional por lo que los autores de esta tesis han tenido contacto con bancos que ubican su área de seguridad de la información dentro del departamento de informática, dentro de la unidad de riesgos y en operaciones centrales.

Entonces, ¿De qué depende dónde ubicar las funciones de seguridad de la información? Julio César Ardita[10] (CISM) expuso sobre cómo podría organizarse el departamento de seguridad en la empresa y mencionó algunas variables que influyen en la definición de la ubicación del departamento de seguridad en la estructura organizacional de la compañía:

- Tipo de compañía: para nuestro caso si es una financiera o micro financiera.
- Cultura organizacional
- Tamaño de la compañía: cantidad de personal, número de sucursales.
- Presupuesto a nivel de personal/gastos/inversión

[10] En la Conferencia Internacional de ISACA realizada el 22 de Octubre del 2010 en la ciudad de Lima-Perú.

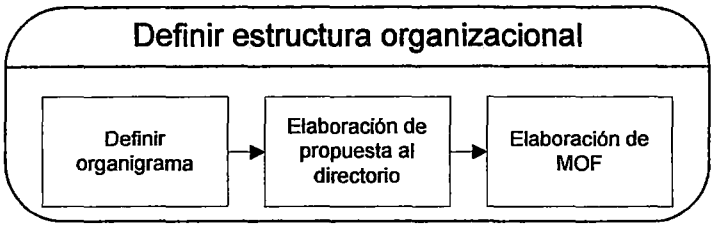
- Rol del Jefe de Seguridad: ¿qué funciones cumplirá?
- Grado de madurez de la compañía

Dentro de estas variables mostró especial énfasis en la madurez de la organización, es decir el grado de entendimiento que la organización tiene sobre la seguridad, una pregunta clave para darse cuenta del grado de madurez es *¿en nuestra empresa se habla de seguridad informática o seguridad de la información?* Lo cual implica comprender que seguridad de la información no solo abarca la seguridad de los activos de TI sino también a nivel de personas, servicios no tecnológicos, manejo de documentos físicos y todo aquel activo que transmita y/o almacene temporal o permanentemente información de la organización.

Cabe señalar que el grado de madurez que la organización posee sobre SI nace desde los altos directivos. Si el directorio no tiene claro la diferencia entre seguridad de la información y seguridad informática, no le dará la atención ni la importancia que se merece y por tanto las decisiones que afectan a toda la empresa se harán en base a este paradigma tecnológico de seguridad y no se tendrá en cuenta las implicancias de una adecuada gestión, regulación y concientización sobre SI.

Al terminar la descripción del presente subproceso, teniendo en cuenta las variables anteriormente listadas, se muestran posibles alternativas para que la organización pueda tomar la decisión de dónde ubicar el área de SI teniendo en cuenta sus ventajas y desventajas.

Flujo



Matriz RACI

Funciones→	Directorio	Gerente General	Gerente de Finanzas	Jefe de Organización y Métodos	Jefe de RRHH
Actividades↓					
Definir organigrama		A	I	R	C
Elaboración de propuesta al directorio	A	R	C		I
Elaboración de MOF		A	I	R	C

Una matriz RACI identifica quién es Responsable, a quién se le debe rendir cuentas (A), quién debe ser Consultado y/o Informado

Métricas

Porcentaje de roles de SI documentados.

Actividades:

P.1.1 Definir organigrama

Entradas-Herramientas-Salidas

P.1.2 Elaboración de propuesta al directorio

Entradas-Herramientas-Salidas

P.1.3 Elaboración de MOF de seguridad

Entradas-Herramientas-Salidas

Algunos ejemplos de la ubicación del área de SI se describen a continuación, con un breve resumen de las ventajas y desventajas de cada uno:

A. Seguridad de la Información dentro de Tecnologías de la Información

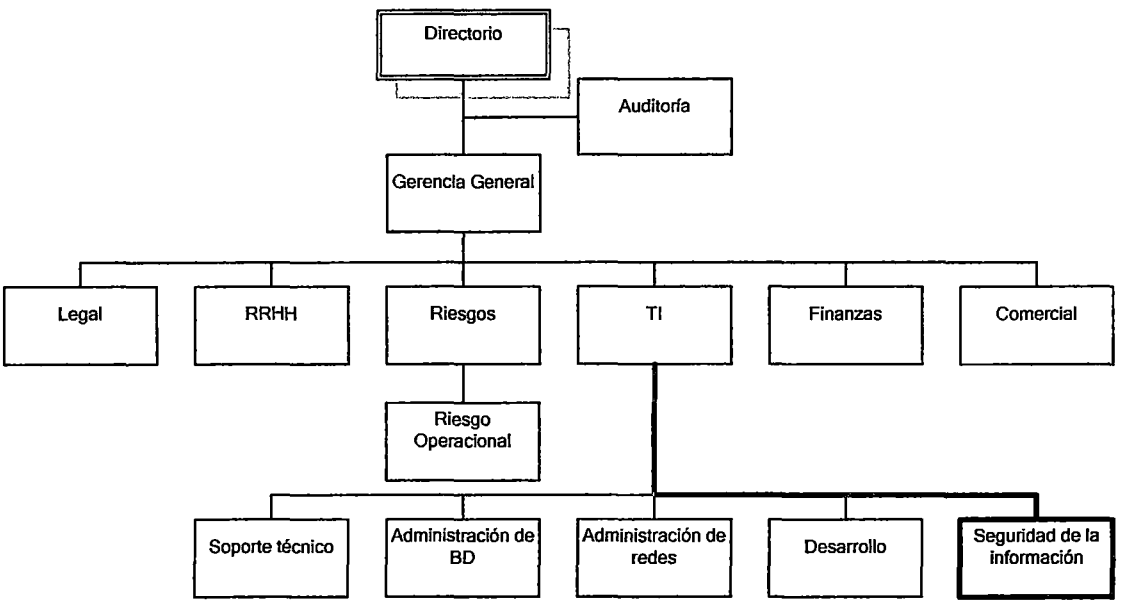


Gráfico 3 Organigrama: SI dentro de Tecnologías de la información

VENTAJAS Y DESVENTAJAS DENTRO DE TI

VENTAJAS	DESVENTAJAS
• Es más fácil de crear ya que no requiere un cambio organizacional drástico. • Permite optimizar recursos en compañías pequeñas. • Mejor gestión de los riesgos de TI de la organización. • Facilita el establecimiento e implementación de controles y procedimientos relacionados a TI. • Se tiene un contacto directo con personal de TI, lo cual facilita el conocimiento	• La seguridad de la información se convierte o se percibe como "seguridad informática", lo cual origina que el alcance se reduzca a la información digital y otros sistemas netamente informáticos, de redes o infraestructura. • Tiene un presupuesto dependiente y compartido con el resto de áreas del departamento de TI. • Se percibe al área de seguridad como un área operativa y no como un área

sobre la realidad de la administración del software, hardware y redes en la empresa.	estratégica, lo cual dificulta la implementación de políticas a lo largo de toda la empresa y la difusión de una cultura y concienciación de seguridad de la información.

B. Seguridad de la Información dentro de Riesgos

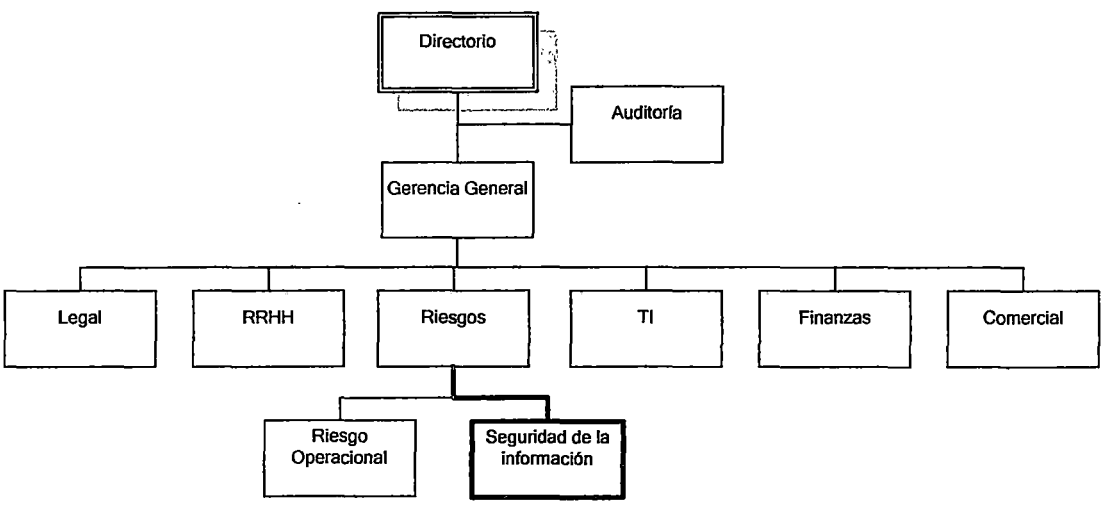


Gráfico 4 Organigrama: SI dentro de Riesgos

VENTAJAS	DESVENTAJAS
• Existe una gestión integral de los riesgos de la organización. • La gestión de riesgos de SI no estará únicamente relacionada a TI sino que también a personas, servicios, información almacenada en documentos, etc.	• Podría ser difícil delimitar funciones relacionadas a la gestión de riesgos o identificar al responsable del tratamiento de un riesgo. • Al ubicarse debajo de una gerencia es difícil monitorear y hacer cumplir los controles hacia las unidades de línea superiores.

C. Seguridad de la Información como área independiente

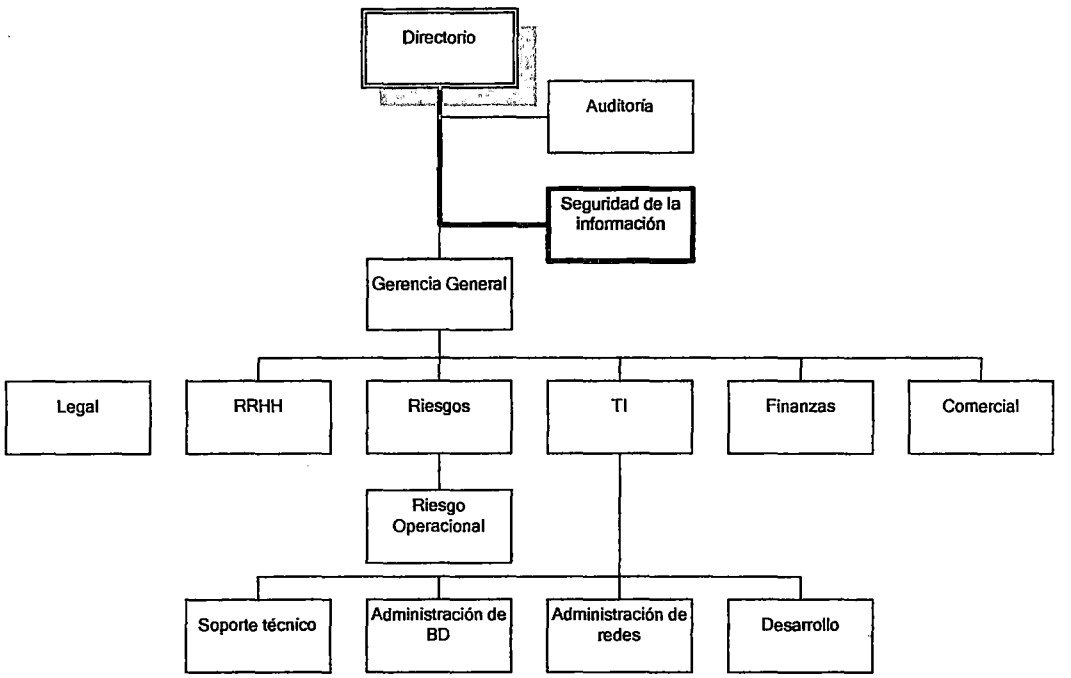


Gráfico 5 Organigrama: SI independiente

VENTAJAS	DESVENTAJAS
• Mayor apoyo y compromiso de la alta gerencia. Lo que hace más fácil la difusión de una cultura de seguridad de la información a lo largo de toda la empresa. • El cambio en la percepción de los empleados de la organización (en todos los niveles) con respecto a qué es seguridad es mejor recibido pues su emisor y su mensaje tienen de por sí más peso. • El área de seguridad se convierte y se percibe como un área estratégica de la organización. • Presupuesto independiente.	• Costos de creación y cambio organizacional • Demoras en su puesta en marcha real. • Resistencia por parte del área de IT, debido a el deseo del área de TI de no perder el control de la seguridad de los activos informáticos o el temor a que se descubran controles existentes inadecuados. • Se requiere que sea liderada por una persona con un perfil más amplio e inclusive más gerencial que técnico: conocimientos técnicos y gerenciales, conocimiento de todos los aspectos y procesos del negocio, etc.

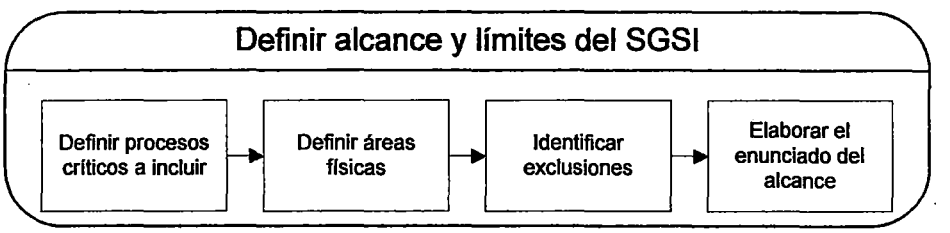
3.2.1.2 Definir alcance y límite del SGSI

Si bien lo dispuesto por la circular G-140 no hace mención a la definición del alcance del SGSI, es recomendable hacerlo tomando como referencia el estándar internacional ISO 27001 donde en el numeral 4.3.1 b) solicita la definición del alcance y límites del SGSI. La importancia de esta definición radica en esclarecer a las partes interesadas la cobertura que tendrá dentro de la organización la implementación del SGSI.

Definición

En el alcance se define qué procesos y áreas de la organización serán considerados dentro de la gestión de la seguridad de la información en función a las necesidades del negocio. Además, se ha de tener en cuenta el análisis realizado por otras áreas de la empresa, por ejemplo si el área de riesgos operativos tiene identificado los procesos críticos de la empresa el alcance del SGSI debería estar alineado y considerar estos procesos dentro de su alcance.

Flujo



Matriz RACI

Funciones→	Directorio	Gerente General	Responsable de SI	Dueño del proceso de negocio	Riesgos Operativos
Actividades↓					
Definir procesos críticos a incluir	A		R	I	C
Definir áreas físicas a incluir	A	CI	R		
Identificar exclusiones	A	CI	R		
Elaborar enunciado	A	CI	R		I

Una matriz RACI identifica quién es Responsable, a quién se le debe rendir cuentas (A), quién debe ser Consultado y/o Informado.

Métricas

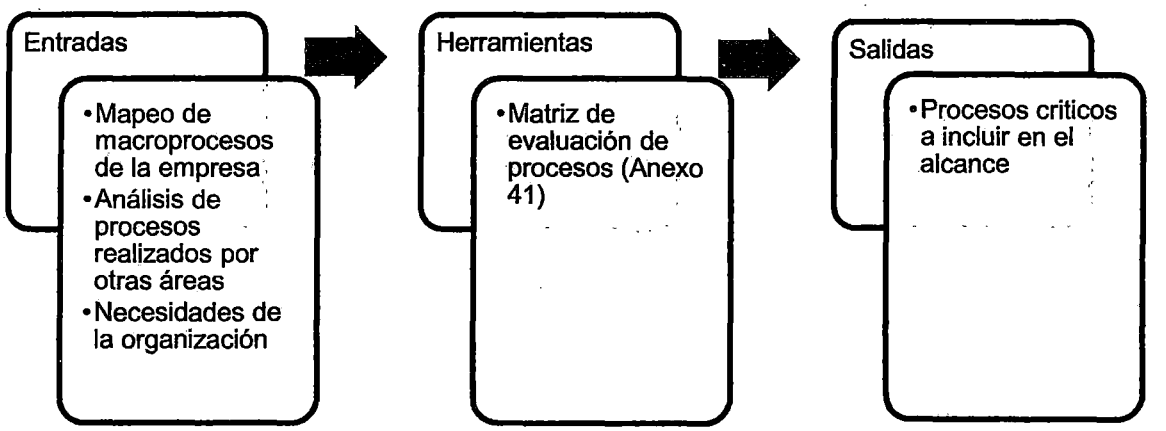
Numero de procesos críticos a incluir

Numero de exclusiones

Actividades:

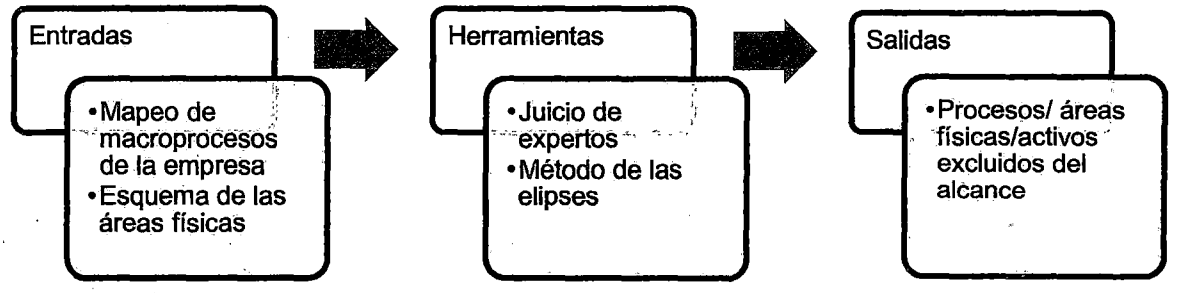
P.2.1 Definir procesos críticos a incluir

Entradas-Herramientas-Salidas



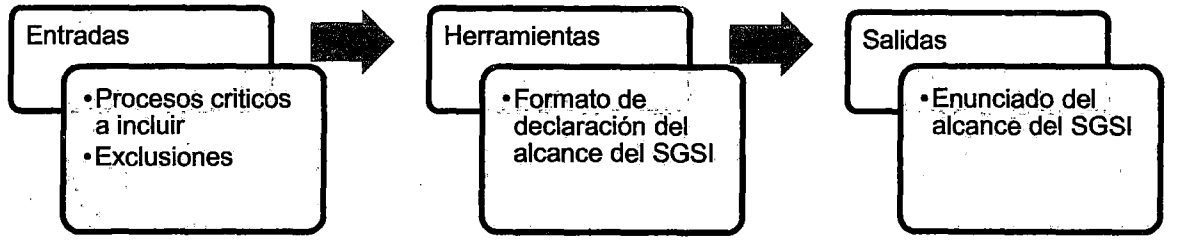
P.2.2 Identificar exclusiones

Entradas-Herramientas-Salidas



P.2.3 Elaborar enunciado de alcance

Entradas-Herramientas-Salidas



En el ANEXO 2, se encuentra un formato que ayudará en la definición y descripción del alcance del SGSI.

3.2.1.3 Definir políticas

Definición

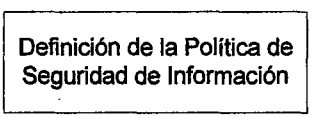
La política de SI establece el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización. No es una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, es

más bien una descripción de lo que deseamos proteger y el porqué de ello, además de establecer responsabilidades.

Cada política de seguridad de la información es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos. Invitación que debe concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos de información y servicios informáticos críticos de la empresa.

El documento de las políticas de SI no debe ser muy extenso, ni entrar a detalles técnicos, se debe recordar que es un documento de gestión que será de conocimiento a toda la organización. Sus enunciados deben ser imperativos y establecer responsabilidades específicas.

Flujo



Matriz RACI

	Directorio	**Gerencia General**	**Responsable de SI**	**Todos los colaboradores**
Actividades↓				
Definir política de seguridad de información	A	C	R	I

Una matriz RACI identifica quién es **R**esponsable, a quién se le debe rendir cuentas (**A**), quién debe ser **C**onsultado y/o **I**nformado

Métricas

Estado de la política (Elaboración, revisión, aprobada, publicada)

Actividades:

P.3.1 Definir política de seguridad de información

Entradas-Herramientas-Salidas

En el ANEXO 3 se podrá encontrar un formato para realizar la descripción de las políticas de Seguridad de la Información.

3.2.1.4 Definir y aplicar metodología de gestión de riesgos

Definición

La circular G-140 en su Artículo 3 b) menciona que las entidades financieras deben definir una metodología de gestión de riesgos de seguridad de la información consistente con la metodología de gestión de riesgo operacional.

Entonces, teniendo en cuenta los incisos 4.2.1 c) al 4.2.1 d) de la ISO 27001 se plantean las actividades necesarias para la definición de la metodología de gestión de riesgos.

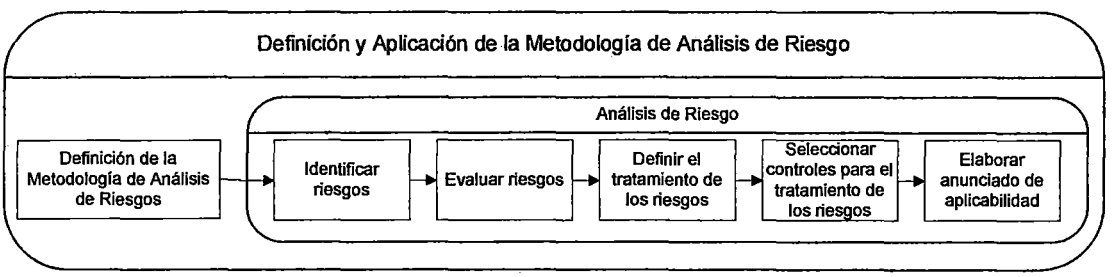
La metodología de gestión de riesgos es transversal al ciclo PDCA:

Ciclo PDCA	Metodología de Gestión de Riesgos
Establecimiento	Definir y aplicar metodología de análisis de riesgos
Implementación	Implementación de los controles seleccionados
Monitoreo	Monitoreo del cumplimiento y efectividad de los controles
Mantenimiento y Mejora	Implementar mejoras, acciones correctivas y preventivas

Tabla 14 Ciclo PDCA vs Metodología de Gestión de Riesgos

Por encontrarnos en la fase de Establecimiento, a continuación se define las actividades que comprende la definición de la Metodología del Análisis del riesgo.

Flujo



Matriz RACI

Funciones→	Directorio	Responsable de SI	Gerente General	Dueño del proceso de negocio	Gerente de Riesgos Operacionales
Actividades↓					
Definir metodología de Análisis de Riesgo	A	R	I		C
Identificar riesgos	I	R	A	C	
Evaluar riesgos	A	R	I	C	
Definir el tratamiento de los riesgos	A	R	I	C	
Seleccionar los controles para el tratamiento de los riesgos	A	R	I	CI	
Elaborar enunciado de aplicabilidad	A	R	CI		

Una matriz RACI identifica quién es Responsable, a quién se le debe rendir cuentas (A), quién debe ser Consultado y/o Informado

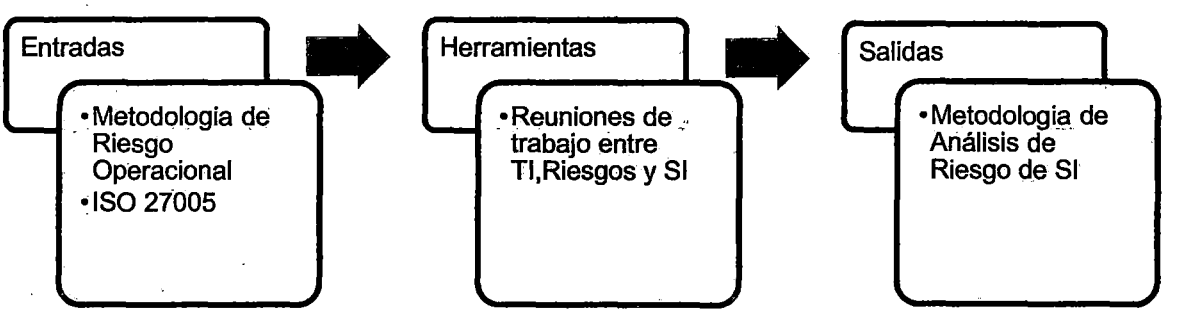
Métricas

Estado de la documentación de la metodología (Elaboración, revisión, aprobada, publicada)

Actividades:

P.4.1 Definir metodología de análisis de riesgo de seguridad de información

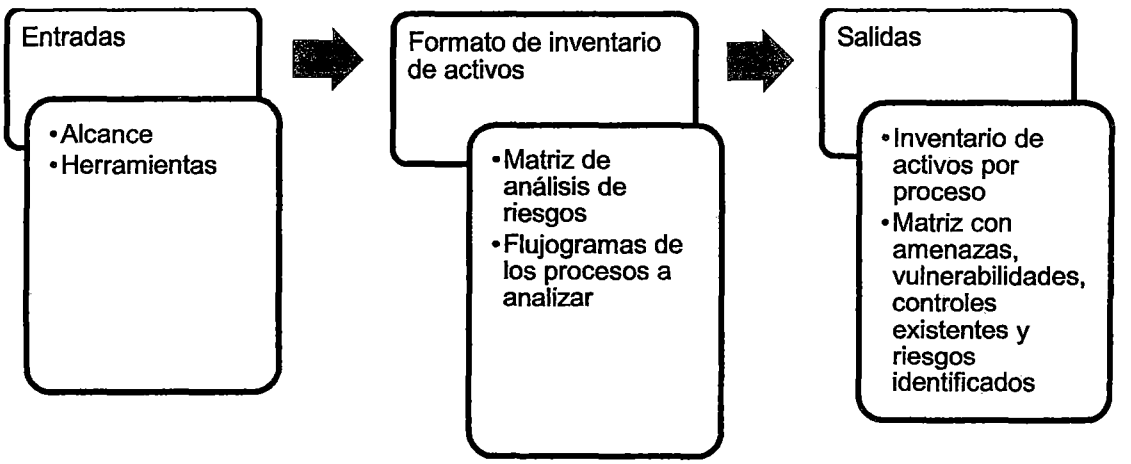
Entradas-Herramientas-Salidas



P.4.2 Identificar riesgos

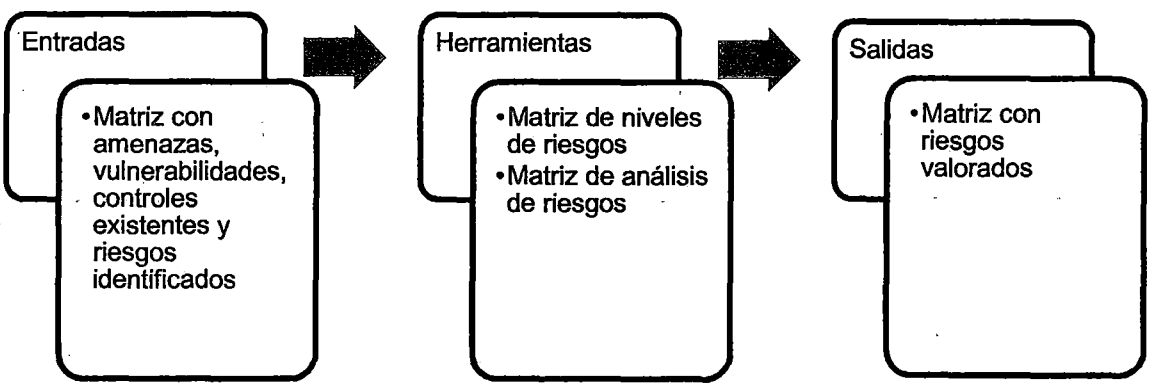
Los pasos que se deben ejecutar al realizar esta actividad se describen en la sección "***Descri0070ción del Análisis de Riesgos***" en la que se detallan las definiciones y criterios para llevar a cabo esta actividad.

Entradas-Herramientas-Salidas



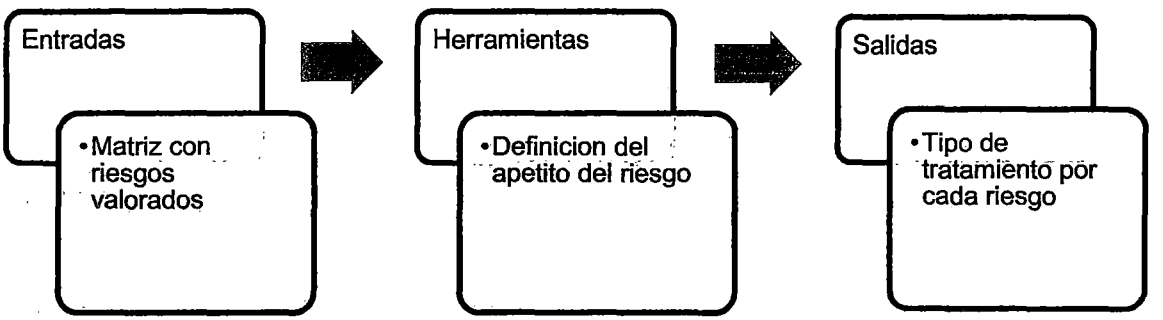
P.4.3 Evaluar riesgos

Entradas-Herramientas-Salidas



P.4.4 Definir el tratamiento de los riesgos

Entradas-Herramientas-Salidas

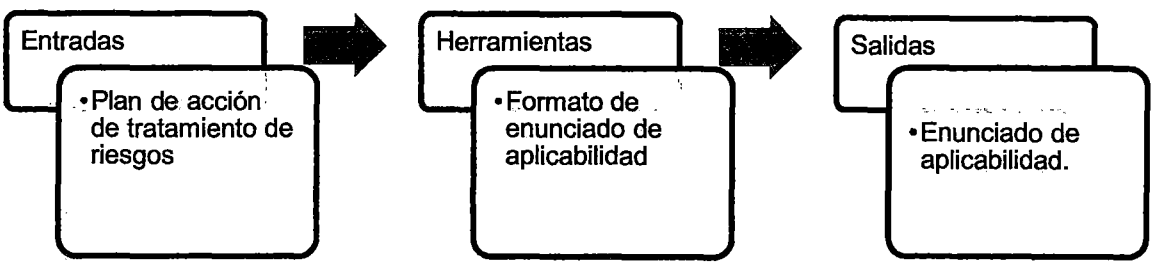


P.4.5 Seleccionar controles para el tratamiento de los riesgos

Entradas-Herramientas-Salidas

P.4.6 Elaborar enunciado de aplicabilidad

Entradas-Herramientas-Salidas



Descri0070ción del Análisis de Riesgos:

A. Identificar Riesgos

La identificación de riesgos se debe realizar por cada proceso identificado dentro del alcance del SGSI, y comprende las siguientes actividades:

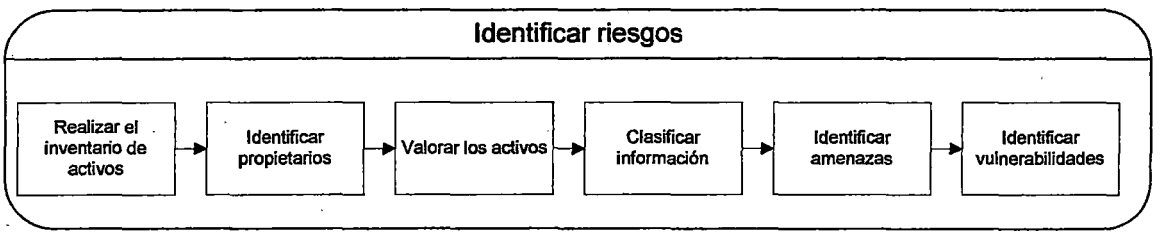


Gráfico 6 Identificar Riesgos

a) Realizar el inventario de activos

De acuerdo a la ISO 27001 un activo de información es todo aquello que da valor a la organización. Específicamente un activo puede ser:

Tipo	Descripción
Información (física y lógica)	Aquellos datos (en cualquier formato) que se generan, recopilan, gestionan, transmiten y destruyen en la organización.
Software	Aplicaciones informáticas que se utilizan para gestionar la información.
Hardware	Equipos utilizados para gestionar la información y las comunicaciones (servidores, PCs, teléfonos, impresoras, routers, cableado, etc.).
Personas	Personal propio de la organización, personal subcontratado, clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización
Servicios	Servicios internos (aquellos que una parte de la organización suministra a otra) y externos (aquellos que son suministrados por un tercero a la organización).
Entorno	Lugares en los que se alojan los sistemas de información (oficinas, edificios, agencias, áreas restringidas, etc.)

Para realizar el inventario de activos, utilizaremos el "ANEXO 4-Matriz de inventario de activos y clasificación de informaciónANEXO 1".

b) Identificar propietarios

Se establece por cada activo del inventario. Es la persona con autoridad para solicitar y autorizar los controles de acceso, quien debe preocuparse por la confidencialidad, integridad y disponibilidad del activo en cuestión.

c) Clasificar información

Para los activos de tipo Información (Física, Lógica), se ha de especificar una clasificación de acuerdo a su confidencialidad; es decir, la importancia del control de acceso a la información por parte únicamente de quienes estén autorizados.

La clasificación más sencilla de la información de acuerdo a su confidencialidad se basa en tres niveles:

Tipo	Criterios para considerar
Confidencial	✓ Si existe una fuga de esta información fuera de la Organización, resultará en una pérdida financiera o un perjuicio en la imagen de la empresa. ✓ Comprometer la confidencialidad de esta información resultará en un no cumplimiento de la ley o del estatuto. ✓ El acceso a esta información debe ser restringido basándose en el concepto del mínimo privilegio. ✓ Su acceso requiere la aprobación del dueño de la información, y en el caso necesite ser comunicada a un tercero se requiere un acuerdo de confidencialidad firmado.
Uso Interno	✓ La fuga de esta información hacia afuera de la Organización, resultará en una pérdida financiera menor o un perjuicio menor a la empresa. ✓ La transferencia de esta información no causará daño serio a la empresa. ✓ El acceso es dado libremente a todos los usuarios internos.
Pública	✓ Si existe una fuga de esta información hacia afuera de la Organización, no habrá perjuicios.

	✓ La no disponibilidad de esta información no tendrá efecto en la continuidad de negocio.

d) Valorar activos

Consiste en calcular la importancia del activo a partir de la evaluación de la Confidencialidad, Integridad y Disponibilidad, dimensiones conocidas como "CID".

Para valorar el CID, dividiremos los activos en:

- Activos de información
- Activos de hardware, software, servicios, entorno
- Activos Personas

		Información	Hardware, Software, Servicios, Entorno	Personas
CONFIDENCIALIDAD	Baja	✓ Puede darse a conocer a externos y no ocasionaría perjuicios a la entidad.	✓ La información procesada, almacenada o transportada a través de este activo es de confidencialidad Baja para el proceso.	✓ La información que maneja esta persona puede darse a conocer a externos y no ocasionaría perjuicios a la entidad.
	Media	✓ Sólo de uso interno en la entidad. Todos los trabajadores de la empresa la pueden conocer	✓ La información procesada, almacenada o transportada a través de este activo es de confidencialidad Media para el proceso.	✓ La información que maneja esta persona es de uso interno a la entidad. Todos los trabajadores de la empresa la pueden conocer.
	Alta	✓ Conocida sólo por algunas personas	✓ La información procesada,	✓ La información que maneja esta persona

		dentro de la entidad. Es muy sensible y ocasionaría serios daños si se hace pública.	almacenada o transportada a través de este activo es de confidencialidad Alta para el proceso.	es de confidencialidad Alta. Ocasionaría serios daños si se hace pública.

Tabla 15 Confidencialidad por tipo de Activo

		Información	Hardware, Software, Servicios, Entorno	Personas
INTEGRIDAD	Baja	✓ El impacto es mínimo si la exactitud de esta información se degrada	✓ El proceso no depende del correcto funcionamiento de este activo. La información que procesa, almacena o transporta tiene una integridad baja.	✓ Esta persona sólo requiere de información pública para el cumplimiento de sus funciones.
	Media	✓ Si la exactitud de esta información se degrada ocasionaría un impacto significativo en el proceso de negocio	✓ Fallas en este activo ocasionaría daños considerables en la información de integridad media que procesa, almacena o transporta.	✓ Esta persona sólo requiere de información pública e interna para el cumplimiento de sus funciones.
	Alta	✓ La degradación de la integridad de esta información es inaceptable porque originaría una interrupción del proceso	✓ Fallas en este activo ocasionaría serios daños en la información de integridad alta que procesa, almacena o transporta.	✓ Esta persona requiere de información confidencial para el cumplimiento de sus funciones.

Tabla 16 Integridad según tipo de activo

		Información	Hardware, Software, Servicios, Entorno	Personas
DISPONIBILIDAD	Baja	✓ La no disponibilidad de esta información por varios días originaria un impacto mínimo en la entidad.	✓ La no disponibilidad de este activo por varios días originaria un impacto mínimo en la entidad	✓ La no disponibilidad de esta persona no ocasionaría problemas en la ejecución del proceso.
	Media	✓ La no disponibilidad de esta información por más de 24 horas tendría un impacto significativo para la entidad.	✓ La no disponibilidad de este activo por más de 24 horas tendría un impacto significativo para la entidad.	✓ La no disponibilidad de esta persona afectaría levemente al proceso.
	Alta	✓ La disponibilidad de esta información debe ser 24x7	✓ La disponibilidad de este activo debe ser 24x7	✓ La no disponibilidad de esta persona afectaría seriamente al proceso.

Tabla 17 Disponibilidad según tipo de activo

e) Identificar Amenazas

Las amenazas es aquello que podría desencadenar un evento no deseado para la seguridad de la información. Es decir, aquello que afecta al CID de los activos.

f) Identificar Vulnerabilidades

Las vulnerabilidades son aquello de lo que las Amenazas se aprovechan o toman ventaja para materializar el riesgo.

B. Evaluar Riesgos

- ✓ Calcular el impacto comercial sobre la organización que podría resultar de una falla en la seguridad, tomando en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.
- ✓ Calcular la probabilidad realista de que ocurra dicha falla a la luz de las amenazas y vulnerabilidades prevalecientes, y los impactos asociados con estos activos, y los controles implementados actualmente.
- ✓ Calcular los niveles de riesgo.

C. Definir Tratamiento de los Riesgos

- ✓ Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido.
- ✓ Aplicar los controles apropiados.
- ✓ Aceptar los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo de la organización.
- ✓ Evitar los riesgos; y
- ✓ Transferir los riesgos comerciales asociados a otras entidades; por ejemplo: aseguradoras, proveedores.

D. Seleccionar Controles para el Tratamiento de los Riesgos

Seleccionar e implementar los objetivos de control y controles para cumplir con los requerimientos identificados por el proceso de tasación del riesgo y tratamiento del riesgo

E. Elaborar el Enunciado de Aplicabilidad

Preparar un Enunciado de Aplicabilidad. El cual debe incluir:

- ✓ Los objetivos de control y los controles seleccionados y las razones para su selección.
- ✓ Los objetivos de control y controles implementados actualmente.
- ✓ La exclusión de cualquier objetivo de control y control en el Anexo A y la justificación para su exclusión.

3.2.2 Implementación

En esta sección se detallarán los controles que la circular de la SBS exige que sean implementados como mínimo y la documentación, actividades periódicas a realizar y registros a mantener para sustentar su cumplimiento.

3.2.2.1 Seguridad Lógica

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
5.1 a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.	11.2.1 Registro de usuarios 11.2.2 Gestión de privilegios	Procedimiento de gestión de accesos Matriz de perfiles Matriz de acceso brindado a los sistemas	Revisión y actualización de perfiles	Informe periódicos sobre la revisión de perfiles de los sistemas.	Oracle Identity Management IBM Tivoli Identity Manager Quest One Identity Manager	ANEXO 6- Matriz de Perfiles de Acceso ANEXO 7 - Registro de Revisión de Perfiles
5.1 b) Revisiones periódicas sobre los derechos concebidos	11.2.4 Revisión de los derechos de acceso de los usuarios		Concesión y baja de accesos	Reportes periódicos de las altas y bajas.	Oracle Identity Management IBM Tivoli Identity Manager Quest One Identity Manager	ANEXO 8 - Reportes de las altas y bajas del Personal ANEXO 9 - Matriz de acceso brindado a los sistemas
5.1 c) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles	11.2.3 Gestión de contraseñas de usuario 11.3.1 Uso de contraseñas	Guía para el monitoreo de las actividades de los usuarios en los sistemas	Revisión de accesos a los sistemas. Revisión de la ejecución de transacciones	Informe periódico sobre la actividad de los usuarios en los sistemas.		ANEXO 10 - Actividad de los usuarios en los sistemas

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
responsabilidades puedan ser seguidas e identificadas.			críticas en los sistemas.			
			Revisión de altas y bajas de usuarios en los sistemas.	Informe sobre altas y bajas de usuarios en los sistemas.	Oracle Identity Management IBM Tivoli Identity Manager Quest One Identity Manager	ANEXO 8 - Reportes de las altas y bajas del Personal
		Procedimiento de gestión de usuarios remotos	Concesión y baja de accesos remotos Monitoreo de accesos remotos	Revisión de la actividad de usuarios con acceso remoto.	Fortiguard Report	ANEXO 10 - Actividad de los usuarios en los sistemas
		Política de computación móvil				
5.1 d) Controles especiales sobre utilidades del sistema y herramientas de auditoría.	11.5.4 Utilización de las facilidades del sistema 15.3.1 Controles de auditoría de sistemas 15.3.2 Protección de las herramientas de auditoría de sistemas	Procedimiento de gestión de utilitarios del sistema y software de auditoria	Revisión de usuarios con accesos críticos.	Inventario de software utilitario y herramientas de auditoria	Software Asset Management Aranda 360 ENDPOINT SECURITY	ANEXO 11 - Inventario de software utilitarios y herramientas de auditoria

3.2.2.2 Seguridad de personal

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
5.2 a) Definición de roles y responsabilidades establecidos sobre la seguridad de información.	8.1.1 Inclusión de la seguridad en las responsabilidades y funciones laborales	Manual de organización y funciones Ficha de funciones del personal de seguridad de información Reglamento de trabajo y Reglamento disciplinario. Cláusula de confidencialidad en los contratos de proveedores Acuerdo de confidencialidad para el personal interno y externo.	Realizar la entrega del Reglamento de Trabajo y Reglamento Disciplinario al personal nuevo y comunicar cambios a todo el personal.	Cargo de entrega a todo el personal del Reglamento de Trabajo y Reglamento Disciplinario.	--	ANEXO 12 - Documentos en File de Personal ANEXO 13 - Modelo de Acuerdo de confidencialidad para personal externo e interno ANEXO 14 - Modelo de cláusula de confidencialidad en un contrato con terceros
5.2 b) Verificación de antecedentes, de conformidad con la legislación laboral vigente.	8.1.2 Selección y política de personal	Procedimiento de selección de personal	Verificación de antecedentes, estado en la central de riesgos	File del personal	Software de verificación de calificación de personas en el sistema financiero:	ANEXO 12 - Documentos en File de Personal

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
					Equifax Sentinel	
5.2 c) Concientización y entrenamiento.	8.2.2 Conocimiento, educación y entrenamiento de la seguridad de información	Política de capacitación y concientización en Seguridad de la información	Elaboración de material didáctico Dictado de capacitaciones Actividades de concientización	Programa anual capacitación y concientización Lista de asistencia a las capacitaciones Evaluaciones al personal	Plataformas e-learning: E Front Moodle Dokeos	ANEXO 15 - Formato para definir programas de capacitación y concientización
5.2 d) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.	8.2.3 Proceso disciplinario	Procedimiento disciplinario	Reportar faltas Registrar faltas Investigar faltas Sancionar faltas	Evidencia de la comunicación de la falta Informe de investigación de la falta Memorándums al personal por faltas	--	ANEXO 16 - Registro de medidas disciplinarias
5.2 e) Procedimientos definidos en caso de	8.3.3 Retiro de los derechos de acceso	Procedimiento de gestión de accesos	Retiro de accesos Devolución de activos	Log de deshabilitación de accesos en	Gestores de identidades:	ANEXO 17 - Registro de activos

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos		Procedimiento de asignación y devolución de activos de información.	Verificación de deshabilitación de accesos	los sistemas Informes periódicos de verificación de deshabilitación de accesos Constancias de devolución de activos	Oracle Identity Management IBM Tivoli Identity Manager Quest One Identity Manager	entregados al personal

3.2.2.3 Seguridad física y ambiental

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
5.3 a) Controles para evitar el acceso físico no autorizado Controles para evitar daños o interferencias a los locales y a la información de la empresa.	9.1.1 Perímetro de seguridad física 9.1.2 Controles físicos de entradas	Procedimiento de ingreso a las instalaciones	Identificación de las áreas restringidas Identificación del personal autorizado a ingresar a áreas restringidas	Bitácora de ingresos y salidas	Tarjetas De Proximidad: Hid Proximity Card Honeywell	ANEXO 18 - Bitácora de Ingresos y Salidas
	9.1.3 Seguridad de oficinas, despachos y recursos	Procedimiento de gestión de incidentes	Instalación de cámaras de vigilancia y sensores de movimiento	Grabaciones de las cámaras de vigilancia.	Software de monitoreo remoto de cámaras:	ANEXO 19 - Registro de eventos de video vigilancia

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
			Uso de cajas fuerte y gabinetes con llave donde se requiera.		RASPlus	
5.3 b) Controles para prevenir pérdidas, daños o robos de los activos	9.2.1 Instalación y protección de equipos 9.2.2 Suministro eléctrico 9.2.3 Seguridad del cableado 9.2.4 Mantenimiento de equipos 9.2.5 Seguridad de equipos fuera de los locales de la organización 9.2.6 Seguridad en el rehúso o eliminación de equipos 9.2.7 Retiro de la propiedad	Diagrama de red de los equipos de seguridad instalados en los ambientes de la empresa.	Instalación de UPS Verificación del funcionamiento de UPS Mantenimiento preventivo de equipos	Bitácora de los mantenimientos preventivos a los equipos.	Software de monitoreo de estado de UPS: PowerAlert Intelligent Power Manager	ANEXO 20 - Registro de mantenimiento de equipos
Controles para la protección de los equipos frente a amenazas físicas	9.1.4 Protección contra amenazas externas y ambientales	Diagrama de equipos instalados.	Instalación de equipos para el control y monitoreo de las	Registro de la temperatura y humedad del CC.	Sistema Control de temperatura y humedad	ANEXO 21– Registro de Temperatura y Humedad del

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
y ambientales.			condiciones ambientales adecuadas en las áreas que así lo requieran. (Ej. Centro de cómputo)			Centro de Cómputo

3.2.2.4 Inventario de activos y clasificación de información

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
5.4 a) Realizar y mantener un inventario de activos asociados a la tecnología de información Asignar responsabilidades respecto a la protección de estos activos.	7.1.1 Inventario de activos	Procedimiento de inventario de activos y clasificación de información	Realizar un inventario de activos de información Actualizar el inventario de activos de información	Inventario de activos de información	Software para el registro y control de inventario de activos de información: e-Pulpo GesConsultor	ANEXO 4-Matriz de inventario de activos y clasificación de información.
	7.1.2 Propiedad de los activos	Procedimiento de inventario de activos y clasificación de información	Identificación del propietario de cada activo de información	Inventario de activos de información	Software para el registro y control de inventario de activos de información:	ANEXO 4-Matriz de inventario de activos y clasificación de información.

					e-Pulpo GesConsultor	
5.4 b) Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa. Realizar las medidas apropiadas de control que deben asociarse a las clasificaciones.	7.2.1 Guías de clasificación	Procedimiento de inventario de activos y clasificación de información Guía de clasificación y tratamiento de la información	Clasificación de la información	Inventario de activos de información	Software para el registro y control de inventario de activos de información: e-Pulpo GesConsultor	ANEXO 4- Matriz de inventario de activos y clasificación de información.
	7.2.2 Marcado y tratamiento de la información	Guía de clasificación y tratamiento de la información	Marcado de la información de acuerdo a su clasificación.	Ejemplos de archivos, reportes, formatos con su respectiva clasificación.	Software para el registro y control de inventario de activos de información: e-Pulpo GesConsultor	ANEXO 4- Matriz de inventario de activos y clasificación de información.

3.2.2.5 Administración de las operaciones y comunicaciones

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
5.5 a) Procedimientos documentados para la operación de los sistemas	10.1.1 Documentación de procedimientos operativos	Guías operativas de administración de los equipos de comunicación y sistemas	Elaboración y actualización de las guías.	Control de cambios	Gestor documental: Alfresco OpenKM Documany	ANEXO 22 - Registro de Control de cambios de documentos
5.5 b) Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.	10.1.2 Gestión de Cambios	Procedimiento de cambios en producción	Documentar casos de uso de los cambios Realizar pruebas en ambientes de QA previos al pase a producción	Formatos de pases a producción	Altiris GMF	ANEXO 23– Formato de Pase a Producción
5.5 c) Separación de funciones para reducir el riesgo de error o fraude.	10.1.3 Segregación de tareas	Manual de Organización y Funciones (MOF)	Los procedimientos y modificaciones al MOF sean analizados por organismos de	Control de cambios de los procedimientos y MOF	Gestor documental: Alfresco OpenKM	ANEXO 22 - Registro de Control de cambios de documentos

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
			control interno de la empresa para verificar la correcta segregación de funciones.		Documany	
5.5 d) Separación de los ambientes de desarrollo, prueba y producción.	10.1.4 Separación de los recursos para desarrollo y para producción	Procedimiento de desarrollo Procedimiento de pruebas de QA Procedimiento de cambios en producción Procedimiento de enmascaramiento de Bases de Datos	Verificación de accesos de los colaboradores de los ambientes de desarrollo, prueba y producción. Enmascaramiento de Bases de Datos.	Diagrama de red de los 3 ambientes Organigrama de las áreas TI (incluyendo desarrollo, prueba y producción) Lista de integrantes de cada área	Software para enmascaramiento de datos: Oracle DataMasking DataMaker DataMasker IBM InfoSphere DataStage Pack IBM Optim Data Privacy Solution	--
5.5 e) Monitoreo del servicio dado por terceras partes	10.2.2 Monitoreo y revisión de los servicios externos	Procedimiento de adquisiciones	Gestión de riesgos en el servicio dado por terceros	Contratos que incluyan cláusulas de seguridad y SLA Informes periódicos del cumplimiento de	--	ANEXO 14 - Modelo de cláusula de confidencialidad en un contrato con terceros

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
				SI en el servicio dado por terceros		
5.5 f) Administración de la capacidad de procesamiento	10.3.1 Planificación de la capacidad	Procedimiento de planificación de capacidad	Monitoreo de la utilización de recursos de los servidores, mainframes Proyectar requerimientos futuros	Histórico de demanda de capacidad Proyecciones de los futuros requerimientos de capacidad	Monitoreo del estado de los servidores y servicios de red: Nagios IBM Director	ANEXO 25– Registro del estado de la red
5.5 g) Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.	10.4.1 Medidas y controles contra software malicioso 10.4.2 Medidas y controles contra código móvil	Procedimiento para la instalación de software Procedimiento para autorización de uso de medios extraíbles Políticas de uso de internet de los usuarios. Procedimiento de actualización de antivirus y verificación de actividad en todas	Instalación y actualización de antivirus Configuración de reglas en el firewall que bloqueen IPs maliciosas Filtro de navegación web Limitar uso de medios extraíbles	Log de los equipos de seguridad perimetral Log del software de filtro de navegación web Log de vulnerabilidades detectadas por antivirus	Equipos de control perimetral Fortigate UTM FireEye Malware Protection System	ANEXO 26– Registro de equipos de seguridad perimetral

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
		las terminales de la red.				
5.5 h) Seguridad sobre las redes Seguridad sobre los medios de almacenamiento Seguridad de la documentación de sistemas	10.6.1 Controles de red 10.6.2 Seguridad en los servicios de redes	Procedimiento para la administración remota de los equipos de comunicación	Administración de las reglas del firewall	Log del firewall Diagrama de seguridad perimetral	Fortigate UTM	ANEXO 26– Registro de equipos de seguridad perimetral
	10.7.1 Gestión de medios removibles	Procedimiento de gestión de medios removibles Guía de eliminación segura de información	Controlar el acceso de lectura y escritura de medios removibles Controlar el acceso a carpetas compartidas Realizar procedimientos de eliminación segura de información en discos dados de baja, CD dañados, etc.	Actas/bitácoras de eliminación segura de medios removibles	McAfee DLP MyDLP Symantec DLP	ANEXO 27– Formato de eliminación segura
	10.7.3 Procedimientos de manipulación de la	Procedimiento de gestión de accesos	Revisión de usuarios con accesos críticos.	Lista de personal autorizado a acceder a la	--	ANEXO 4 - Matriz de inventario de

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
	información 10.7.4 Seguridad de la documentación de sistemas	Guía de clasificación y tratamiento de la información		documentación de los sistemas		activos y clasificación de información
5.5 i) Seguridad de intercambio de información	10.8.1 Políticas y procedimientos para el intercambio de información y software 10.8.2 Acuerdos de intercambio	Política de intercambio de información Procedimientos de intercambio de información Cláusula de confidencialidad en los contratos de proveedores Acuerdo de confidencialidad para el personal interno y externo.	El área legal deberá revisar que se incluyan cláusulas de confidencialidad en los contratos críticos	Relación de personal con acuerdos de confidencialidad		ANEXO 13– Modelo de Acuerdo de confidencialidad para personal externo e interno
Seguridad de intercambio de información por correo electrónico	10.8.4 Seguridad en la mensajería electrónica	Política de intercambio de información	Implementación de certificados y firmas digitales Implementación de filtros de	Log del servicio de correo	FortiMail	ANEXO 28– Log del servicio de correo

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
			correos (antispam, antivirus, antiphishing, etc)			
5.5 j) Seguridad de canales electrónicos	10.9.2 Transacciones en línea	Procedimientos de encriptación y uso de protocolos seguros de intercambio de datos.	Implementación de 2 factores de autenticación donde al menos 1 sea dinámico Monitoreo de transacciones.	Log de transacciones	N-VISION QRadar SIEM McAfee Enterprise Log Manager	ANEXO 24 - Log de transacciones
5.5 k) Mantenimiento de registros de auditoría y monitoreo del uso de sistemas	10.10.1 Registro de la auditoria	Procedimientos y guías para el análisis periódico de logs	Revisión de los logs de auditoria Revisión del uso de las opciones criticas Revisión de las actividades de los usuarios privilegiados (administradores de sistemas, DBA)	Logs de auditoría de los sistemas Informes de revisión	N-VISION QRadar SIEM McAfee Enterprise Log Manager	ANEXO 24 - Log de transacciones

3.2.2.6 Adquisición, desarrollo y mantenimiento de sistemas informáticos

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
Participar en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales	Análisis y especificación de los requisitos de seguridad	Procedimiento para la aprobación de requerimientos	Participar de la definición de análisis de requerimientos	Documento de requerimientos funcionales donde se incluya los requisitos de seguridad	---	ANEXO 29ANEXO 29-Formato de especificación del requerimiento
Controles sobre el ingreso de información	Validación de los datos de entrada	Metodología de desarrollo Procedimiento de pruebas de QA	Definir rangos y características de los campos de entrada. Incluir validaciones a los campos de entrada en la aplicación y en el servidor Incluir casos de prueba de validación de datos de entrada	Documentación de los casos de pruebas	QA Complete	ANEXO 30 - Controles de aplicación
controles sobre el procesamiento	Control del proceso interno	Documentación de los procesos batch	Inclusión de rutinas de validación en el procesamiento de la información	Log del resultado exitoso o no del procesamiento de la información.	Business Activity Monitoring for IT Operations Splunk	ANEXO 30 - Controles de aplicación

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
				Bitácora de ejecución de los procesos batch		
Controles sobre la información de salida.	Integridad de los mensajes	Metodología de desarrollo	Verificar que la metodología de desarrollo contemple estandarización de mensajes de la aplicación y codificación de los mismos	Listado de la codificación de los mensajes de la aplicación	---	ANEXO 30 - Controles de aplicación
	Validación de los datos de salida	Metodología de pruebas de QA	Verificar que la metodología de pruebas cumpla con estándares de seguridad Incluir validación de datos de salida en los casos de prueba	Documentación de los casos de pruebas	Business Activity Monitoring for IT Operations	ANEXO 30 - Controles de aplicación
Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.	Política de uso de los controles criptográficos	Política de encriptación de información	Adquisición e implementación de una herramienta de encriptación.	Reporte de activos de información encriptados.	DataSecure	---
Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.	Control del software en producción	Procedimiento de control de cambios	Realización de pruebas y aceptación del usuario antes del pase a producción.	Documento de aceptación del usuario. Formatos de	Altiris GMF	ANEXO 23 - Formato de Pase a Producción

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
			La actualización del software debe realizarla personal capacitado y autorizado. Respaldo de las versiones antiguas de las aplicaciones, configuración y documentación.	pase a producción.		ANEXO 31 - Aceptación del usuario para pase a producción
	Protección de los datos de prueba del sistema	Política de encriptación de información Guía de revisión del enmascaramiento de base de datos de prueba	Enmascaramiento de la base de datos de prueba Revisión del enmascaramiento de la base de datos de prueba	Informes de revisión del enmascaramiento de la base de datos de prueba	Software para enmascaramiento de datos: Oracle DataMasking DataMaker DataMasker IBM InfoSphere DataStage Pack IBM Optim Data Privacy Solution	---
Controlar el acceso a las librerías de	Control de acceso a los códigos de	Procedimiento de almacenamiento,	Control de acceso a las fuentes de las	Inventario de fuentes,	GIT Mercurial	

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
programas fuente.	programas fuente	custodia y acceso a los programa fuente.	aplicaciones. Revisión de usuarios con accesos críticos.	versiones y usuarios autorizados	Subversion Rational-ClearCase	
Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.	Procedimientos de control de cambios	Procedimiento de control de cambios.	Realización de pruebas y aceptación del usuario antes del pase a producción. Actualización de los manuales de los sistemas actualizados.	Documentos de aceptación del usuario. Manuales actualizados de los sistemas.	Altiris GMF	ANEXO 31 - Aceptación del usuario para pase a producción
	Revisión técnica de los cambios en el sistema operativo	Procedimiento de control de cambios.	Notificar a tiempo los cambios en el sistema operativo. Realizar pruebas de compatibilidad y seguridad de las aplicaciones críticas de negocio.	Informe de las pruebas realizadas.	QA Complete	---
	Restricciones en los cambios a los paquetes de software	Procedimiento de control de cambios	Evaluación del impacto de modificar paquetes de software	Informe de evaluación del impacto		

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.	Control de las vulnerabilidades técnicas	Procedimiento de gestión de vulnerabilidades técnicas	Definición de roles y responsabilidades de la gestión de las vulnerabilidades técnicas Identificar las vulnerabilidades técnicas, riesgos y acciones a tomarse	Inventario de activos de TI Matriz de análisis de riesgos	e-Pulpo GesConsultor	ANEXO 4 - Matriz de inventario de activos y clasificación de información

3.2.2.7 Procedimientos de respaldo

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
5.7 a) Procedimientos de respaldo regulares y periódicamente validados	10.5.1Recuperación de la información	Política de respaldos y restauración (información a respaldar, periodicidad, permanencia y custodia de backup) Procedimiento de generación de copias de respaldo Procedimiento de restauración de copias de respaldo	Generación de respaldos Pruebas de restauración de backups históricos	Logs de realización de Backups Resultados de pruebas de restauración	Brightstor ARC Serve Backup	ANEXO 32– Log de backup

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
5.7 b) Conservar la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación.	10.5.1Recuperación de la información	Política de respaldos Procedimiento de generación de copias de respaldo Procedimiento de restauración de copias de respaldo	Custodia de copias de respaldo	Cargos de recepción de copias de respaldo del custodio		ANEXO 33– Formato de cargo de recepción de copias de respaldo

3.2.2.8 Gestión de incidentes

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
5.8 a) Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.	13.1.1 Reportando los eventos en la seguridad de información 13.1.2 Reportando debilidades en la seguridad de información	Procedimiento de gestión de incidentes Formato de reporte de comunicación de incidentes y/o vulnerabilidades de Seguridad de la Información.	Comunicación de incidentes de seguridad	Relación de incidentes de seguridad.	e-Pulpo Aranda SERVICE DESK	ANEXO 35- Bitácora de incidentes de seguridad ANEXO 36 - Formato de comunicación de incidentes de seguridad
5.8 b)						

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.	13.2.1 Responsabilidades y procedimientos	Procedimiento de gestión de incidentes Procedimiento de gestión de vulnerabilidades	Evaluar y definir planes de acción de incidentes y vulnerabilidades	Relación de incidentes de seguridad y tratamiento Relación de vulnerabilidades reportadas y tratamiento	e-Pulpo Aranda SERVICE DESK	ANEXO 35-Bitácora de incidentes de seguridad

3.2.2.9 Cumplimiento normativo

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
Las empresas deberán asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos.	15.1.1 Identificación de la legislación aplicable	Procedimientos de comunicación de la legislación aplicable.	Documentar todos los requerimientos legales y regulatorios a los que está sujeta la organización Definir y documentar los controles y responsabilidades para cumplir con requerimientos	Documentación de los requerimientos legales Documentación de los controles y sus responsables para cumplir con los requerimientos legales o		

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
			legales y regulatorios	regulatorios		
	15.1.2 Derechos de propiedad intelectual (DPI)	Política de protección de la propiedad intelectual	Monitorear los activos propietarios Mantener prueba y evidencia de la propiedad de las licencias Implementar controles para no exceder el número máximo de usuarios permitidos	Reporte de activos propietarios Informe de número de licencias vs número de usuarios	ProactivaNET® Inventario OCS Inventory	ANEXO 34 - Inventario de software
	15.1.3 Salvaguarda de los registros de la organización	Política de almacenamiento, manipulación y eliminación de registros clave	Mantener un inventario de fuentes de información clave	Inventario de fuentes de información clave		ANEXO 39– Inventario de fuentes de información clave

3.2.2.10 Privacidad de la información

G140	ISO 17799	DOCUMENTACION	ACTIVIDADES	REGISTROS	SOFTWARE	ESTRUCTURA DATOS
5,10 a) Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la normatividad vigente sobre la materia.	15.1.4 Protección de los datos y de la privacidad de la información personal	Procedimiento para el etiquetado de información	Clasificación y etiquetado de información confidencial Concientización y capacitación sobre la protección de datos personales	Relación y clasificación de activos de información.	e-pulpo	ANEXO 4 - Matriz de inventario de activos y clasificación de información

3.2.3 Monitoreo

3.2.3.1 Ejecutar procedimientos de monitoreo y revisión

Seguridad lógica

Monitoreo del uso de cuentas privilegiadas

- ✓ Se recomienda mantener un inventario de las cuentas administrador de los servidores y otros equipos de red e identificar al responsable de cada cuenta.
- ✓ Verificar que la funcionalidad de guardar pistas de auditoría este activa en los equipos de red principales.
- ✓ Identificar los eventos críticos que se pueden presentar en los equipos y que serán los principales registros a revisar durante el monitoreo.

Revisión de derechos concedidos a los usuarios

- ✓ Mantener actualizada la matriz de accesos a los sistemas.
- ✓ Llevar registro de los accesos excepcionales concedidos.
- ✓ Revisar que los accesos concedidos a un empleado estén acordes a la matriz de accesos y que se hayan concedido dentro del procedimiento regular de gestión de accesos.

Seguridad de personal

Revisión del procedimiento de selección de personal

- ✓ Revisar que los legajos del personal contengan los documentos (certificados, diplomas, etc) que sustenten el currículo vitae.
- ✓ Revisar que se hayan presentado o verificado los antecedentes policiales y penales.

- ✓ Revisar que el personal haya pasado por todas las evaluaciones correspondientes como examen psicológico, técnico, médico, de acuerdo a lo establecido por la institución.

Revisión de deshabilitación de cuentas de personal cesado

- ✓ Revisar que los accesos concedidos a un empleado se hayan deshabilitado después de su cese.
- ✓ Determinar tiempo máximo para la deshabilitación de accesos después de comunicada la fecha de cese.
- ✓ Identificar el uso de cuentas de personal cesado.

Seguridad física y ambiental

Monitoreo de cámaras y alarmas

- ✓ Determinar por cuánto tiempo se almacenarán como mínimo las grabaciones de las cintas de video.
- ✓ Establecer procedimientos de respuesta ante la recepción de una alarma.
- ✓ Llevar registro diario de los eventos sospechosos o inusuales que se observen durante el monitoreo.

Monitoreo de las condiciones ambientales del Centro de Cómputo Principal y Alterno

- ✓ Verificar que las condiciones de temperatura y humedad de los centro de cómputo estén dentro de los rangos permitidos.
- ✓ Guardar registro histórico de las variaciones de las condiciones ambientales.

Revisión del cumplimiento del cronograma de mantenimiento preventivo de equipos

- ✓ Revisar que los mantenimientos programados a lo largo del año se estén efectuando.
- ✓ El mantenimiento preventivo debe ser a equipos de cómputo como a los equipos de monitoreo, cámaras y detectores.

Inventario de activos y clasificación de información

Revisión de clasificación de información

- ✓ Actualizar la clasificación de los activos de información que con el paso del tiempo pueden haber perdido vigencia
- ✓ Verificar que los documentos lógicos, físicos y los reportes de sistemas están etiquetados correctamente con la clasificación de información correspondiente.

Administración de las operaciones y comunicaciones

Revisión del uso adecuado del servicio de correo

- ✓ Detectar el reenvío de cadenas de correo, publicidad
- ✓ Analizar el volumen de tráfico de correo por usuario y detectar usuarios top
- ✓ Analizar las cuotas de envío/recepción asignadas a cada usuario que deben estar acorde a su perfil o permisos concedidos.

Monitoreo del uso adecuado del servicio de internet

- ✓ Realizar estadísticas de páginas más visitadas y páginas bloqueadas
- ✓ Analizar tráfico de internet por horas
- ✓ Verificar la correcta asignación de perfiles de navegación

Monitoreo de desempeño y disponibilidad de servidores

- ✓ Monitoreo de uso de memoria, uso de CPU, disponibilidad

Monitoreo de tráfico de comunicaciones de red

- ✓ Monitorear en especial el tráfico a través de puertos importantes como ftp, rdp, pop3, smtp, telnet
- ✓ Monitoreo de tráfico de aplicaciones, determinar uso de ancho de banda, horarios de mayor uso, etc.

Revisión de la configuración de equipos de seguridad perimetral

- ✓ Revisión de las reglas en el firewall y control de cambios efectuados
- ✓ Revisión de los eventos del IPS (Intrusion prevention system).

Revisión del uso de los sistemas (opciones críticas)

- ✓ Determinar con las áreas usuarias las opciones críticas de cada sistema.
- ✓ Revisar que las opciones críticas estén asignadas a los perfiles y usuarios que lo requieran de acuerdo a las necesidades operativas de la institución.
- ✓ Analizar el uso que los usuarios realizan de las opciones críticas: para qué la usan, frecuencia de uso y horario en que la usan.

Revisión del servicio dado por terceros (cumplimiento de controles y SLA)

- ✓ Llevar registro de los tiempos de respuesta ante requerimientos o incidentes.
- ✓ Realizar un checklist de cumplimiento por cada servicio y proveedor.
- ✓ Determinar la forma cómo se realizará la verificación del cumplimiento de controles de seguridad en las instalaciones del proveedor, y realizarlo de manera periódica.

Adquisición, desarrollo y mantenimiento de sistemas informáticos

Revisión del cumplimiento de control de cambios

- ✓ Verificar que los pases a producción hayan pasado por control de calidad
- ✓ Verificar que los pases a producción cuenten con la documentación requerida según procedimientos definidos.

Revisión de encriptación de información sensible

- ✓ Verificar que los datos sensibles en ambientes de prueba estén enmascarados.
- ✓ Verificar en producción que los datos sensibles estén encriptados de acuerdo al perfil del usuario que realiza la consulta.
- ✓ Asegurar la encriptación de información cuando se envíe a través de canales electrónicos.

Revisión del acceso a programas fuente

- ✓ Verificar los usuarios que tienen acceso a los repositorios de programas fuente.

Procedimientos de respaldo

Revisión de pruebas de recuperación históricas

- ✓ Realizar pruebas de recuperación de información de años atrás a fin de validar tiempos de recuperación e integridad de la información respaldada.

Gestión de incidentes

Revisión de resolución de incidentes

- ✓ Verificar que los incidentes se hayan atendido y cerrado oportunamente.
- ✓ Llevar estadísticas de tiempos de respuesta y registrar las soluciones para conformar una base de conocimiento.

Cumplimiento normativo

Revisión del número de licencias vs el número de usuarios

- ✓ Revisar el que el número de usuarios no supere el número de licencias de una determinada aplicación.
- ✓ Revisar que los servicios o appliance que tienen licencia por número de usuarios no estén llegando o superando el límite.

Privacidad de la información

Monitoreo de fuga de información

- ✓ Revisar los eventos de carga de documentos a páginas web, envíos de documentos a través de correo electrónico.
- ✓ Verificar que los puertos usb estén bloqueados. Probar con distintos dispositivos que posean memoria externa y conexión usb como celulares y cámaras.

3.2.3.2 Medir efectividad de controles

Definir, medir, revisar e informar la efectividad de los controles de seguridad de información fortalece la política, justifica la asignación de recursos, las decisiones presupuestarias y facilita la comprensión de la postura de seguridad para el tratamiento de riesgos de la empresa.

En la presente tesis se define 1 plantilla para definir métricas en el ANEXO 37. A continuación un ejemplo:

FORMATO: DEFINICION DE METRICAS DE EFECTIVIDAD DE SEGURIDAD DE INFORMACIÓN	
DOMINIO	Seguridad Lógica
CONTROL	Los usuarios deben contar con una identificación para su uso personal
METRICA ID	Usuarios sin responsable
OBJETIVO	Identificación de responsabilidades y seguimiento de las actividades de los usuarios en los sistemas
PREGUNTA	¿Cuántas cuentas de usuarios no están asociadas a un responsable directo?

METRICA(S)	Porcentaje de usuarios sin asignación de responsable directo.
FRECUENCIA(S)	Mensual
FORMULA(S)	#usuarios sin responsable / # total de usuarios
RESPONSABLE	Analista de Seguridad de Información

3.2.4 Mantenimiento y Mejora

Se debe realizar revisiones periódicas del SGSI para identificar no-conformidades y no-conformidades potenciales y determinar acciones correctivas y preventivas respectivamente. Para lo cual se debe usar un cuestionario de autoevaluación sobre el cumplimiento del SGSI de acuerdo a lo exigido en la G-140.

En el ANEXO 38 se encuentra un modelo de cuestionario para determinar acciones correctivas y preventivas.

CAPÍTULO IV
BENEFICIOS DE IMPLEMENTAR LA METODOLOGÍA PROPUESTA

Para mostrar de manera cuantitativa el beneficio que una empresa obtendría después de aplicar la metodología propuesta, vamos a aplicar la técnica del análisis de brechas en una empresa real del sector financiero peruano.

La empresa, por razones de confidencialidad, será denominada como "Financiera ABC". Tiene su sede administrativa en el distrito de San Isidro y como producto principal ofrece créditos a los pequeños y micro empresarios.

4.1 MATRIZ DE ANÁLISIS DE BRECHAS

Para medir el nivel de cumplimiento, se ha utilizado los niveles de madurez de COBIT:

Nivel	Valor	Descripción
No existente	**0**	La empresa no ha reconocido que existe un problema por resolver.
Inicial	**1**	La empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso.
Repetible	**2**	Se realizan procedimientos estándar pero no están documentados ni formalizados. El conocimiento radica en los colaboradores.

Definido	**3**	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Los procedimientos formalizan las prácticas existentes.
Administrado	**4**	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva.
Optimizado	**5**	Se han automatizado los flujos de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Tabla 18 Niveles de Madurez de COBIT

En la siguiente matriz de análisis de brechas hemos usados los siguientes campos:

Campo	Descripción
Clausulas	Cláusula de la Circular G-140
N1	Nivel actual de cumplimiento de la cláusula.
N2	Nivel esperado de mejora al aplicar la metodología
N3	Nivel deseado de cumplimiento
Observaciones	Detalle de cómo se cumple actualmente con la cláusula
Mejoras	Mejoras que aporta la metodología para aumentar el nivel de cumplimiento de la cláusula

MATRIZ DE ANALISIS DE BRECHAS – FINANCIERA ABC

Los niveles nivel inicial, esperado y deseado de cumplimiento mostrados a continuación, corresponden a información que ha sido relevada con el Jefe de Seguridad de Información en el periodo de Noviembre 2011 – Enero 2012.

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
Nº	Clausulas					

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
Nº	Clausulas					
3	**Sistema de gestión de la seguridad de la información**	2,0	3,0	4,0		
3 a)	Definición de una política de seguridad de información aprobada por el Directorio.	3	3	4	Se cuenta con una política de seguridad de información definida.	Con la metodología propuesta se pueden establecer métricas para medir el cumplimiento de la política.
3 b)	Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.	2	3	4	Se tiene una metodología de análisis de riesgos no alineada a la de Riesgo Operacional y no está documentada ni aprobada formalmente.	La metodología propone un procedimiento de definición de esta metodología de riesgos de seguridad de información.
3 c)	Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.	1	3	4	No se tiene identificado los registros necesarios para verificar el cumplimiento de lo exigido por la circular.	La metodología propuesta identifica los registros necesarios para cumplir con la circular y realizar un monitoreo oportuno.
4	**Estructura organizacional**	2,6	3,6	4		
4	Las empresas deben contar con una estructura organizacional que les permita implementar y mantener el sistema de	2	3	4	Se cuenta con una persona a cargo de la administración del SGSI perteneciente al área de TI.	La metodología identifica los factores a considerar para determinar una estructura adecuada

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
N°	Clausulas					
	gestión de la seguridad de información.					e identifica los pros y contras de la ubicación del área de SI dentro de otras áreas.
4 a)	Asegurar el cumplimiento de la política de seguridad de información y de la metodología definida por la empresa.	3	4	4	Se cuenta con una política de seguridad de información definida, pero no se mide su cumplimiento.	Con la metodología propuesta se pueden establecer métricas para medir el cumplimiento de la política.
4 b)	Coordinar y monitorear la implementación de los controles de seguridad de información.	3	3	4	Se cuenta con el Documento de aplicabilidad y las acciones de implementación tienen responsables asociados.	La metodología propuesta identifica los registros necesarios para cumplir con la circular y realizar un monitoreo oportuno.
4 c)	Desarrollar actividades de concientización y entrenamiento en seguridad de información.	2	4	4	Se realiza de forma esporádica el envío de correos masivos de concientización, los temas no se encuentran pre definidos.	La metodología propone un formato para la elaboración de un plan de concientización y capacitación, y una plantilla para la definición de métricas.
4 d)	Evaluar los incidentes de seguridad de información y recomendar acciones apropiadas	3	4	4	Se tiene definido un procedimiento de gestión de incidentes.	La metodología propone formatos para la comunicación de incidentes, así como una plantilla para la definición de

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
N°	Clausulas					
						métricas.
5.1	**Seguridad Lógica**	2,50	3,50	4,00		
5.1 a)	Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.	3,0	3,0	4,0	Se cuenta con un procedimiento de Gestión y Control de Accesos Lógicos.	La metodología propuesta contiene registros para la adecuada administración de accesos.
5.1 b)	Revisiones periódicas sobre los derechos concebidos	2	4	4	Las revisiones de los derechos concedidos son esporádicas y tediosas pues no se cuenta con formatos pre definidos	La metodología propuesta contiene formatos de Matriz de perfiles y Matriz de acceso brindado a los sistemas.
5.1 c)	Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.	3	4	4	Los usuarios tienen asignado en todos los sistemas un identificador personal de acuerdo a lo estipulado en el Procedimiento de Gestión y Control de Accesos Lógicos. Pero no se cuenta con el diccionario de datos de los logs de los sistemas a fin de identificar la actividad de los usuarios.	La metodología propone la estructura de la *Actividad de los usuarios en los sistemas*
5.1 d)	Controles especiales sobre utilidades del sistema y herramientas de	2	3	4	No se tiene identificado las herramientas de auditoría, ni un	La metodología propone el *Inventario de software utilitario y*

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
Nº	Clausulas					
	auditoría.				procedimiento formal de concesión de acceso a software utilitario.	*herramientas de auditoría*, así como tener documentado el *Procedimiento de gestión de utilitarios del sistema y software de auditoría.*
5.2	**Seguridad de Personal**	2,6	3,8	4,0		
5.2 a)	Definición de roles y responsabilidades establecidos sobre la seguridad de información.	2	3	4	No se cuenta con cláusulas de confidencialidad en los contratos ni con acuerdos de confidencialidad con terceros.	La metodología propone la inclusión de las cláusulas de confidencialidad, así como un formato de acuerdo de confidencialidad con terceros.
5.2 b)	Verificación de antecedentes, de conformidad con la legislación laboral vigente.	3	4	4	Se cuenta con el Procedimiento de Selección de Personal donde se estipula la verificación de antecedentes pero no se tiene registro de ello.	La metodología propone el registro de *Documentos en File de Personal*
5.2 c)	Concientización y entrenamiento.	2	4	4	Se realiza de forma esporádica el envío de correos masivos de concientización, los temas no se encuentran pre definidos.	La metodología propone un formato para la elaboración de un plan de concientización y capacitación, y una plantilla para la definición de métricas.

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
Nº	Clausulas					
5.2 d)	Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.	3	4	4	Se tiene un Procedimiento Disciplinario definido, pero no se tienen registros formales definidos que evidencien su cumplimiento.	La metodología propone los siguientes registros: Evidencia de la comunicación de la falta, Informe de investigación de la falta, Memorándums al personal por faltas
5.2 e)	Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos	3	4	4	En el Procedimiento de Gestión y Control de accesos lógicos se incluyen pautas para la revocación de accesos a personal cesado. No se tiene evidencia de la devolución de activos.	La metodología propone Constancias de devolución de activos, así como la estructura del registro de la revocación de accesos y devolución de activos.
5.3	**Seguridad Física y Ambiental**	3,0	4,0	4,0		
5.3 a)	Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.	3	4	4	Se cuenta con procedimientos definidos para el ingreso de personal, bitácoras de ingresos y salidas, personal de vigilancia permanente, uso de fotocheck.	Con la metodología propuesta se podrían definir métricas para monitorear el cumplimiento y llevar estadística de los incidentes.
5.3 b)	Controles para prevenir pérdidas, daños o robos de los activos	3	4	4	Se cuenta con Instalación de UPS, Verificación del funcionamiento de UPS, Mantenimiento preventivo de equipos,	Con la metodología propuesta se podrían definir métricas para monitorear el cumplimiento y llevar estadística de los

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
N°	Clausulas					
					uso de cajas fuertes.	incidentes.
5.4	**Inventario de activos y clasificación de la información**	2,5	3,0	4		
5.4 a)	Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.	2	3	4	Sólo se lleva inventario de los activos de TI, y no se tiene un procedimiento formal documentado.	La metodología propone establecer un procedimiento de Inventario de Activos de Información y establece una *Matriz de inventario de activos y clasificación de información*
5.4 b)	Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.	3	3	4	Se tiene definido las categorías de clasificación en un procedimiento de Clasificación y tratamiento de Información.	La metodología propone una *Matriz de inventario de activos y clasificación de información*
5.5	**Administración de las operaciones y comunicaciones**	2,5	3,2	4		
5.5 a)	Procedimientos documentados para la operación de los sistemas	3	3	4	Se cuenta con procedimientos documentados de la operación de los diferentes sistemas de Financiera ABC	

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
N°	Clausulas					
5.5 b)	Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.	3	4	4	Se tiene procedimientos definidos para el control de cambio en los sistemas/aplicativos, pero no para el cambio de configuración de los equipos de red como switches, servidores, routers, firewall.	La metodología propone formatos de control de cambios tanto para sistemas como para cambios en la configuración de equipos de red.
5.5 c)	Separación de funciones para reducir el riesgo de error o fraude.	2	3	4	No se lleva un control de la separación de funciones.	La metodología propone la revisión de los cambios efectuados al manual de organización y funciones para asegurar mantener una adecuada segregación de funciones.
5.5 d)	Separación de los ambientes de desarrollo, prueba y producción.	3	3	4	Se cuenta con la separación lógica y física de los ambientes de desarrollo, QA y producción.	
5.5 e)	Monitoreo del servicio dado por terceras partes	1	3	4	No se tiene definido realizar monitoreo del servicio dado por terceros.	La metodología propone elaborar Contratos que incluyan cláusulas de seguridad y SLA, y realizar Informes periódicos del cumplimiento de SI en el servicio dado

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
Nº	Clausulas					
						por terceros
5.5 f)	Administración de la capacidad de procesamiento	3	3	4	Se realizan monitoreo de la utilización de recursos de los servidores y proyecciones de requerimientos futuros.	
5.6	**Adquisición, desarrollo, mantenimiento de sistemas informáticos**	2,3	3,0	4		
5.6 a)	Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.	2	3	4	No se identifican requisitos de seguridad como parte de los requerimientos no funcionales.	La metodología propone que el área de seguridad de la información debe participar de la definición de los requisitos no funcionales de los sistemas. Incluir casos de prueba de validación de datos de entrada y salida y la Inclusión de rutinas de validación en el procesamiento de la información
5.6 b)	Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.	3	3	4	Se cuenta con una política de encriptación definida. Y con el software que permite la encriptación de bases de datos sensibles, así como protocolos seguros	

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
Nº	Clausulas					
					para transferencia de información como sftp, https, cifrado de backup.	
5.6 c)	Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.	2	3	4	Se realizan pruebas de calidad hasta conseguir la aceptación del líder usuario antes del ingreso a producción. Las bases de datos de prueba no se enmascaran.	La metodología propone la documentación (guía) y el enmascaramiento de las bases de datos de prueba.
5.6 d)	Controlar el acceso a las librerías de programas fuente.	1	3	4	No se realiza un control del accesos a los programa fuente.	La metodología propone un control del acceso a programas fuente a través del inventario de los mismos y la definición de usuarios autorizados a acceder y modificar.
5.6 e)	Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.	3	3	4	Existe un procedimiento de control de cambios implementado. Existen formatos definidos para pases a producción y cambios de configuración en los equipos.	
5.6 f)	Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.	3	3	4	Se identifican las vulnerabilidades técnicas, riesgos y acciones a tomarse como parte del análisis	

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
Nº	Clausulas					
					de riesgo	
5.7	**Procedimientos de Respaldo**	4	4	4		
5.7 a)	Procedimientos de respaldo regulares y periódicamente validados	3	4	4	Existe un procedimiento de respaldo de información implementado. Las cintas se prueban trimestralmente.	Con la metodología propuesta se pueden definir métricas para medir el cumplimiento del control
5.7 b)	Conservar la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación.	4	4	4	Se cuenta con un proveedor que custodia las cintas de respaldo. Adicionalmente existe replica en línea de la BD principal en una sede distante de la central.	
5.8	**Gestión de incidentes de seguridad de la información**	3	4	4		
5.8 a)	Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.	3	4	4	Existe un Procedimiento de Gestión de Incidentes de Seguridad de la Información implementado, que define los canales de comunicación, el registro y atención de un incidente.	Con la metodología propuesta se podrían definir métricas para monitorear el cumplimiento y llevar estadística de los incidentes.

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
Nº	Clausulas					
5.8 b)	Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.	3	4	4	Existe un Procedimiento de Gestión de Incidentes de Seguridad de la Información implementado, que define los canales de comunicación, el registro y atención de un incidente.	Con la metodología propuesta se podrían definir métricas para monitorear el cumplimiento y llevar estadística de los incidentes.
5.9	**Cumplimiento normativo**	2	3	4		
5,9 a)	Las empresas deberán asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.	2	3	4	Se tiene estipulado en la Política de Seguridad de la Información el cumplimiento normativo pero no existe registro que evidencie esto.	en la metodología se propone: Documentación de los requerimientos legales Documentación de los controles y sus responsables para cumplir con los requerimientos legales o regulatorios
5.10	**Privacidad de la información**	3	3	4		
5,10 a)	Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la normatividad vigente sobre la materia.	3	3	4	Se ha realizado la Clasificación y etiquetado de información confidencial. Se aplican controles de acuerdo a su clasificación. Y continuamente se realiza charlas de	

CIRCULAR G-140-2009-SBS		N1	N2	N3	Observaciones	Mejoras
Nº	Clausulas					
					concientización y capacitación sobre la protección de datos personales	

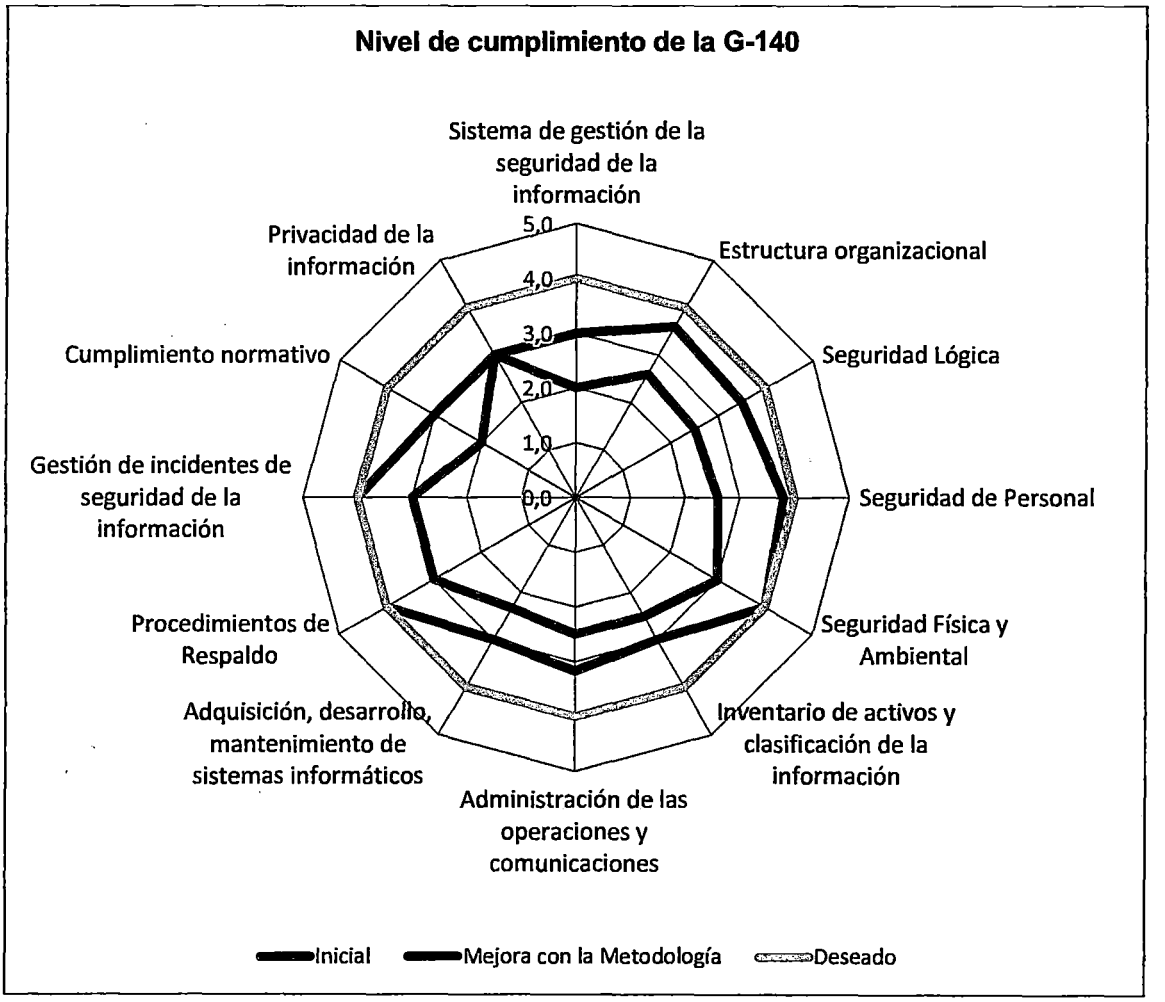
Tabla 19 Análisis de Brechas "Financiera ABC"

Como síntesis de los resultados obtenidos de la matriz tenemos un promedio de cumplimiento por dominio de control:

Tabla 20 Resultado por dominio del análisis de Brechas "Financiera ABC"

CIRCULAR G-140		NIVEL DE CUMPLIMIENTO		
Nº	Clausulas	Inicial	Mejora con la Metodología	Deseado
3	Sistema de gestión de la seguridad de la información	2,0	3,0	4,0
4	Estructura organizacional	2,6	3,6	4,0
5.1	Seguridad Lógica	2,5	3,5	4,0
5.2	Seguridad de Personal	2,6	3,8	4,0
5.3	Seguridad Física y Ambiental	3,0	4,0	4,0
5.4	Inventario de activos y clasificación de la información	2,5	3,0	4,0
5.5	Administración de las operaciones y comunicaciones	2,5	3,2	4,0
5.6	Adquisición, desarrollo, mantenimiento de sistemas informáticos	2,3	3,0	4,0
5.7	Procedimientos de Respaldo	3,0	4,0	4,0
5.8	Gestión de incidentes de seguridad de la información	3,0	4,0	4,0
5.9	Cumplimiento normativo	2,0	3,0	4,0
5.10	Privacidad de la información	3,0	3,0	4,0

Como podemos apreciar en el gráfico radial, el nivel de cumplimiento esperado con la metodología propuesta en esta tesis se incrementa respecto al inicial. Así mismo, se debe tener en cuenta que la correcta aplicación de la metodología y de la aplicación del proceso de mejora continua, el nivel de cumplimiento de la empresa podría incrementarse y llegar a un nivel cercano al deseado (teniendo en cuenta el análisis costo/beneficio).



4.2 RETORNO DE INVERSION EN SEGURIDAD

ROSI, Retorno Sobre la Inversión de Seguridad, concepto derivado del conocido indicador financiero ROI, Retorno Sobre la Inversión. Así el ROSI busca justificar la inversión en seguridad de la información en términos monetarios. Para ello se tiene presente que los efectos de una implementación de seguridad en general no surgen en forma directa como beneficios económicos para una empresa, sino como una reducción en las pérdidas que producen incidentes de seguridad como ataques, fallas o errores.

Una ecuación para calcular el ROSI es la siguiente[11]:

$$ROSI = \frac{(ER\ x\ \%\ RM) - CSS}{CSS}$$

Donde:

- ER: pérdida por Exposición al Riesgo
- %RM: % del Riesgo Mitigado con la solución de seguridad
- CSS: Costo de la Solución de Seguridad

De los estados de pérdidas y ganancias de Financiera ABC12 se sabe que la utilidad neta por cliente es de S/.43

Si un empleado sustrajera los registros de 100,000 clientes de la Financiera ABC, esta tendría una pérdida bruta de S/. 4'300,000 debido al riesgo de fuga de información.

---

[11] Extraída de ISACA JOURNAL VOLUME 2, 2009

[12] Disponibles en el módulo de estadísticas de la página web de la Superintendencia de Banca y Seguros http://www.sbs.gob.pe

Sin embargo, si la Financiera ABC decidiera implementar un sistema DLP el cual tiene una efectividad del 75% y un costo de implementación aproximado de 270,000 para 900 empleados. Para calcular el ROSI, tendríamos lo siguiente:

$$\text{ROSI} = \frac{(4\,300\,000 \text{ x } 0.75) - 270\,000}{270\,000}$$

$$\text{ROSI} = 10{,}94$$

Del resultado obtenido, se puede concluir que el retorno de la inversión en la reducción del riesgo de fuga de información de la "Financiera ABC", a través de la implementación de un sistema DLP, es aproximadamente 11 veces el valor del costo de implementación de dicha solución.

Se debe tener en cuenta que el caso descrito corresponde a una situación en la que sólo se analiza el ROSI de la implementación de una solución de seguridad. Sin embargo, esto cambiará de acuerdo a la cantidad de controles que la empresa desee implementar teniendo en cuenta el apetito de riesgo que tenga de acuerdo a su Metodología de Gestión de Riesgos y su presupuesto.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. El principal aporte de la propuesta es el brindar un apoyo metodológico con técnicas y herramientas, basadas en estándares y normas internacionales ampliamente reconocidas y aceptadas, para lograr una implementación exitosa del SGSI.

2. Para la implementación del Sistema de Seguridad de la Información es vital la concientización y apoyo de la alta dirección quienes deben considerarlo como un asunto estratégico y no sólo de cumplimiento regulatorio. Es por ello que, la propuesta metodológica inicia, en su fase de establecimiento, con la ubicación de la función de seguridad de la información en la estructura organizacional.

3. La implementación de un Sistema de Gestión de Seguridad de la Información permitirá asegurar los activos de información más importantes de la empresa y gestionar los riesgos existentes, es por ello que la propuesta metodológica brinda pautas para definir una metodología de gestión de riesgos consiste y alineada a la utilizada por riesgo operacional.

4. El análisis de brechas (GAP Analysis) es una herramienta fundamental que permitirá a la empresa y sus decisores en seguridad de la información no

sólo medir el nivel de cumplimiento de la regulación; sino que, principalmente, les permitirá gestionar las estrategias requeridas para alcanzar el nivel de implementación del SGSI que el negocio requiere.

5. A través de la matriz de análisis de brechas se demuestra que la implementación de la metodología propuesta en la presente tesis incrementaría el nivel de cumplimiento de la circular G-140 acercándolas también a su nivel deseado de madurez en cada dominio de control.

6. Uno de los principales obstáculos que tienen los responsables de la Seguridad de Información en las empresas es el mostrar el valor que aporta el invertir en seguridad. Es por ello que, la metodología propuesta explica la aplicabilidad del ROSI (Return on Security Investment) para expresar, en términos cuantitativos, los beneficios de invertir en la seguridad de la Información.

7. Si bien, la metodología propuesta no ha sido probada de forma íntegra en una empresa real, uno de sus factores críticos de éxito (FCE) es el encontrarse alineada a los estándares mundialmente aceptados para la implementación de la gestión de la seguridad de la información y sus componentes asociados en el ámbito informático. Sin embargo, se debe tener en cuenta que, existen otros factores críticos de éxito como: la correcta aplicación de la metodología, la adecuada y oportuna toma de decisiones y el apoyo de la alta dirección.

8. La presente tesis está orientada a que las empresas del sector financiero puedan implementar el SGSI de acuerdo a la regulación vigente de la SBS. Sin embargo, es posible que los responsables de la seguridad de la información de empresas de otros sectores puedan utilizarla como

referencia ya que los puntos descritos se encuentran alineados a la ISO 27001.

RECOMENDACIONES

1. Se debe involucrar a la alta dirección para definir, de forma clara, el nivel de importancia que la seguridad de la información tendrá para la empresa en términos estratégicos y no sólo en términos regulatorios.

2. Las empresas del sector financiero, deberían identificar los objetivos estratégicos de la organización y procesos críticos de la misma, y verificar que el alcance del SGSI atienda a estos objetivos.

3. Realizar una implementación progresiva del SGSI, primero con un alcance pequeño, 1 o 2 procesos importantes para la organización, para luego ampliarlo a los demás procesos. Ya que, de tener un alcance inicial muy amplio, la implementación del SGSI se volverá más compleja y con ello la probabilidad de no lograr el éxito esperado se incrementaría.

4. El análisis de brechas debe recoger las expectativas de los principales usuarios de la empresa Realizar un análisis de brechas inicial que permita definir las estrategias a seguir para implementar el SGSI

5. Se recomienda a las empresas del Sector Financiero, adecuar la metodología de acuerdo a sus necesidades, tamaño de la empresa y nivel de cumplimiento deseado ya que en la propuesta se consideran una serie de procedimientos, herramientas y formatos generales que deberían ser adecuados a la realidad de la empresa.

6. Definir indicadores apropiados y realistas que permitan realizar un monitoreo frecuente del proceso de implementación del Sistema de Gestión de Seguridad de la Información.

7. Evaluar la fuerza laboral que se requerirá incrementar y las competencias necesarias que deberá tener el área responsable de la seguridad de información para que opere y monitoree todos controles una vez implementados.

8. Establecer alianzas estratégicas internas con áreas como RRHH, TI y Administración para poder realizar una implementación eficiente de los controles de seguridad ya que el cumplimiento de muchos de ellos involucran la participación activa de estas áreas.

GLOSARIO DE TÉRMINOS

1. SBS

Superintendencia de Banca, Seguros y AFP (SBS), organismo encargado de la regulación y supervisión del Sistema Financiero, de Seguros y del Sistema Privado de Pensiones en el Perú, así como de prevenir y detectar el lavado de activos y financiamiento del terrorismo. Su objetivo primordial es preservar los intereses de los depositantes, de los asegurados y de los afiliados al Seguro Privado de Pensiones. La Superintendencia de Banca y Seguros es una institución de derecho público cuya autonomía funcional está reconocida por la Constitución Política del Perú.

La SBS tiene como fin generar las condiciones que permitan maximizar el valor de los sistemas financieros, de seguros y privado de pensiones, propiciando una mayor confianza y adecuada protección de los intereses del público usuario, a través de la transparencia, veracidad y calidad de la información; cautelando la estabilidad y solvencia de las instituciones que conforman los sistemas.

2. G-140

Circular emitida por la SBS que establece los criterios mínimos para una adecuada gestión de la seguridad de la información, que incluye aspectos referidos a la estructura organizacional, controles de seguridad de información, seguridad en operaciones de

transferencia de fondos por canales electrónicos, así como la subcontratación del procesamiento de datos, cuando éste sea realizado en el exterior.

3. ISO 27001

Estándar Internacional que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido Ciclo de Deming: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

4. Sistema de gestión de seguridad de la información SGSI

Parte del sistema gerencial general basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información

Se debe tener en cuenta que, el sistema gerencial incluye la estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos

5. Seguridad de la información

La preservación de la confidencialidad, integridad y disponibilidad de la información.

- Confidencialidad: garantía de que acceden a la información, sólo aquellas personas autorizadas a hacerlo.
- Integridad: mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.
- Disponibilidad: garantía de que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

6. Activo de información

Algo de valor para la empresa que almacena, transfiere o procesa información.

7. Evaluación de riesgos

La evaluación de las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamiento y/o almacenamiento de la misma, y a la probabilidad de que ocurran.

8. Gestión de riesgos

El proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información.

9. Evento de seguridad de la información

Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. (ISO/IEC TR 18044:2004)

10. Incidente de seguridad de la información

Evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información. (ISO/IEC TR 18044:2004)

BIBLIOGRAFÍA

1. **Alexander, Alberto G.** *Diseño de un Sistema de Gestión de Seguridad de la Información.* s.l. : Alfaomega, 2007. ISBN 978-958-682-713-3.

2. **ISACA.** *Manual de Preparación al Examen CISA.* 2012.

3. **Superintendencia de Banca y Seguros.** Circular N° G-140. *Gestión de Seguridad de la Información.* Lima : s.n., 2009.

4. **International Organization for Standardization.** *ISO 17799: Código para la práctica de la gestión de la seguridad de la información.* 2005.

5. **Córdova Rodriguez, Norma.** *Plan de Seguridad informática para una entidad financiera.* [PDF] Lima : Universidad Nacional Mayor de San Marcos, 2003.

6. **Villega Aguilar, Moisés.** *Sistema de gestión de seguridad de la información para una entidad financiera.* [PDF] Lima : Pontificia Universidad Católica del Perú, 2006.

7. **Burgos Salazar, Jorge y Campos, Pedro G.** *Modelos para seguridad de la información en TIC.* [PDF] Chile : Universidad del Bío-Bío.

8. **De Freitas, Vidalina.** *Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolivar.* 2009.

9. **Munteanu, Adrian.** *Information security risk assessment: the qualitive versus quantitative dilemma.* Rumania : s.n.

10. **Vilora, Orlando, Villegas, Marianella y Blanco, Walter.** *La seguridad de la información bajo una perspectiva de la madurez organizacional.* [PDF] Venezuela : s.n.

11. **INTECO.** Sistema de Gestión de Seguridad de la Información en una Organización. *CERT INTECO.* [En línea] http://cert.inteco.es.

12. **Cano, Jeimy J.** *Seguridad de la Información en Latinoamérica Tendencias 2010.* [PDF] s.l. : Asociación Colombiana de Ingenieros de Sistemas (ACIS), 2010.

13. **ITIL-Site oficial.** Information Technology Infraestructure Library. [En línea] http://www.itil-officialsite.com.

14. **Consejo Superior de Administración Electrónica.** [En línea] España. http://www.csae.map.es.

15. **Carnegie Mellon University.** Community Emergency Response Teams (CERT). [En línea] Pittsburgh-Pennsylvania. http://www.cert.org/octave.

16. **Giles, Timothy.** How to develop and implement a security master plan. [En línea] http://www.books24x7.com/toc.asp?bkid=26432.

17. **Purser, Steven.** *A Practical Guide to Managing Information Security.* [PDF] London : Artech House, 2004. ISBN 1-58053-702-2.

18. **Department of State Foreign Affairs Handbook.** *Performance Measures for Information Assurance.* [PDF] Vol. 5.

19. **Chew, Elizabeth y Otros.** *Performance Measurement Guide for Information Security.* [PDF] s.l. : National Institute of Standards and Technology (NIST). [en línea] http://crsc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

20. **Borghello, Cristian F.** Serie 800-National Institute of Standars and Technology (NIST). *Segu-Info.* [En línea] http://www.segu-info.com.ar/guias/nist.htm.

21. **SecurityArtwork.** Medición de un SGSI: diseñando el cuadro de mandos. [En línea] http://www.securityartwork.es.

22. **Almanza, Andrés R.** *XI Jornada de Seguridad Informática. Seguridad de la Información: Una nueva década para avanzar. Mediciones para la seguridad de la información.* [PDF]

23. **Morales Zamudio, Pedro Andrés.** *Diseño de una solución de un sistema de seguridad informática en empresas estatales.* Lima : UNI-FIIS, 2010. IS.2004.

24. **Angeles Ayala, Sócrates Luis.** *Sistema de Gestión de Seguridad de Información ISO 27001 para un datacenter.* Lima : UNI-FIIS, 2010. IC.2040.

25. **Blas Rivera, Martín Felipe.** *Implantación de la función de seguridad de tecnología de información en una entidad bancaria.* Lima : UNI-FIIS, 2003. IS.1188.

ANEXOS

ANEXO 1. ALINEAMIENTO ENTRE CIRCULAR G-140-SBS Y NORMA ISO 17

ANEXO 1.1. SEGURIDAD LÓGICA

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
N°	**Clausulas**	**N°**	**Control**
5.1	**Seguridad Lógica**		
5.1 a)	Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.		
		11.2.1	**Registro de usuarios**
			Procedimiento de altas y bajas
			Utilización de identificador
			Autorización del propietario
			Verificación de nivel de acceso
			Entrega escrita de los derechos y condiciones
			Completar procedimientos de autorización para dar acceso
			Mantener registros de accesos
			No Mantener cuentas de usuarios e identificadores redundantes
		11.2.2	**Gestión de privilegios**
			Identificar privilegios por cada sistema
			Principio de "necesidad de uso" y "caso por caso"
			Evitar la asignación de privilegios
			Asignar los privilegios a un ID distinto al de uso normal
			Promover el desarrollo y uso de sistemas y programas para la asignación de privilegios.
5.1 b)	Revisiones periódicas sobre		

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
	los derechos concebidos		
		11.2.4	**Revisión de los derechos de acceso de los usuarios**
			Proceso formal de revisión de privilegios
			Revisiones periódicas
			Reasignación de privilegios por cambio de empleo
			Revisiones más frecuentes de privilegios especiales
			Comprobar asignaciones de privilegios
			Registrar cambios en cuentas privilegiadas
5.1 c)	Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.		
		11.2.3	**Gestión de contraseñas de usuario**
			Proceso formal de asignación de contraseñas
			Firma de compromiso de mantener en secreto las contraseñas
			Cambio forzado e inmediato de contraseña temporal
			Procedimiento de verificación de identidad
			Entrega segura de claves temporales
			Claves temporales únicas y difíciles de adivinar
			El usuario reconoce la recepción de su contraseña
			No almacenar contraseñas en sistemas de computo
			Cambiar las contraseñas predeterminadas
		11.3.1	**Uso de contraseñas**
			Buenas prácticas en la selección y uso de contraseñas
			Confidencialidad de las contraseñas
			Evitar guardar registros de las contraseñas
			Cambio de contraseña ante indicios de vulnerabilidad
			Contraseñas de buena calidad
			Cambio periódico de contraseñas
			No incluir contraseñas en procesos de registro automatizado
			No compartir contraseñas individuales
			No utilizar la misma contraseña para propósitos personales y de trabajo
5.1 d)	Controles especiales sobre utilidades del sistema y herramientas de auditoría.		

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
	Controles especiales sobre utilidades del sistema	**11.5.4**	**Utilización de las facilidades del sistema**
			Restringir y controlar las utilidades del sistema
			Procedimientos de autenticación, identificación y autorización para las utilidades del sistema
			Separar las utilidades de las aplicaciones
			Limitar el uso de las utilidades
			Autorizar uso de utilidades con un propósito concreto
			Registrar el uso de las utilidades
			Definir niveles de autorización para las utilidades
			Desactivar o eliminar utilidades no necesarias
	Controles especiales sobre herramientas de auditoría	**15.3.1**	**Controles de auditoría de sistemas**
			Planificar auditorias de sistemas
			Acordar requisitos de auditoría con la gerencia apropiada
			Acordar y controlar el alcance
			Acceso sólo de lectura al software y data
			Borrar las copias aisladas de archivos del sistema
			Identificar los recursos TI para realizar las verificaciones
			Identificar los requisitos para procesos especiales
			Registrar y supervisar los accesos
			Documentar procedimientos, requisitos y responsabilidades
			Los auditores deben ser independientes de las actividades auditadas
	Controles especiales sobre herramientas de auditoría	**15.3.2**	**Protección de las herramientas de auditoría de sistemas**
			Proteger los accesos a las herramientas de auditoria
			Separar las herramientas de auditoría de los sistemas de desarrollo y producción
			No mantener las herramientas de auditoría en librerías de cintas o en áreas de los usuarios sin protección

ANEXO 1.2. SEGURIDAD PERSONAL

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
5.2	**Seguridad de Personal**		

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
5.2 a)	Definición de roles y responsabilidades establecidos sobre la seguridad de información.	8.1.1	Inclusión de la seguridad en las responsabilidades y funciones laborales
			Definir y documentar responsabilidades de empleados, contratistas y terceros
			Incluir "actuar en concordancia con la política SI"
			Incluir la protección de los activos
			Incluir requisitos para ejecutar procesos de seguridad particulares
			Asegurar que la persona sea responsable por sus acciones
			Incluir reportar eventos de seguridad
			Comunicar las responsabilidades en el proceso de selección
5.2 b)	Verificación de antecedentes, de conformidad con la legislación laboral vigente.	8.1.2	Selección y política de personal
			Verificación de antecedentes de candidatos, contratistas y terceros
			Disponibilidad de referencias personales
			Chequeo del CV
			Confirmación de calificaciones académicas y profesionales
			Chequeo de identidad independiente
			Chequeos más detallados
			Definir criterios y limitaciones para los chequeos de verificación
			Proceso de investigación de antecedentes para personal temporal y subcontratado
5.2 c)	Concientización y entrenamiento.	8.2.2	Conocimiento, educación y entrenamiento de la seguridad de información
			Capacitación del personal en seguridad
			Capacitar de acuerdo al rol, responsabilidades de la persona
			Incluir información sobre amenazas conocidas
			Incluir cómo reportar incidentes
5.2 d)	Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.	8.2.3	Proceso disciplinario

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
N°	**Clausulas**	**N°**	**Control**
			Proceso formal disciplinario ante faltas en SI
			Verificación previa del incumplimiento de la SI
			Respuesta disciplinaria graduada de acuerdo a factores
			En casos serios el proceso debe permitir retiro de labores, accesos
5.2 e)	Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos	8.3.3	Retiro de los derechos de acceso
			Remover derechos de acceso culminado el empleo o contrato.
			Reajuste de derechos de acceso en caso de cambio en el empleo o contrato
			Retiro de cualquier documentación que identifique a la persona como miembro actual de la empresa
			Cambio de las contraseñas a las que tuvo acceso el empleado cesante.

ANEXO 1.3. SEGURIDAD FÍSICA Y AMBIENTAL

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
N°	**Clausulas**	**N°**	**Control**
5.3	**Seguridad Física y Ambiental**		
5.3 a)	Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.		
		9.1.1	**Perímetro de seguridad física**
			Proteger áreas que contengan información o recursos de procesamiento de información
			Definir perímetros de seguridad
			Perímetro físicamente sólido del local que contiene los medios de procesamiento de información
			Área de recepción para controlar el acceso físico al local
			Todas las puertas de emergencia deben contar con alarma, ser monitoreadas y probadas
			Instalar Sistemas de detección de intrusos

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
N°	**Clausulas**	**N°**	**Control**
			Separar los medios de procesamiento de información manejados por la empresa de los manejados por terceros
		9.1.2	**Controles físicos de entradas**
			Asegurar que sólo acceda personal autorizado a las áreas seguras
			Registrar fecha y hora de ingreso y salida de los visitantes
			Usar controles de autentificación para autorizar y validar el acceso
			Exigir al personal una identificación visible
			Acceso restringido y monitoreado al personal de apoyo de terceros
			Revisar y actualizar derechos de acceso a áreas seguras
		9.1.3	**Seguridad de oficinas, despachos y recursos**
			Aplicar la seguridad física para oficinas, despachos y recursos
			Estándares de sanidad y seguridad
			Localizar medios claves para evitar acceso del público
			Edificios discretos
			Directorios y teléfonos internos no deben ser accesibles al público
		9.1.4	**Protección contra amenazas externas y ambientales**
			Protección física contra desastres naturales o causados por el hombre
			Almacenar materiales peligrosos y combustibles lejos de las áreas seguras
			Evitar que equipos y medios de respaldo se dañen por un desastre en el área principal
			Equipo apropiado contra incendio
		9.1.5	**El trabajo en las áreas seguras**
			Protección física y pautas para el trabajo en áreas seguras
			Sólo el personal que lo necesite debe conocerlas áreas seguras
			Evitar el trabajo no supervisado en áreas seguras
			Áreas seguras cerradas y vigiladas cuando estén vacías
			No permitir equipos de grabación

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
N°	**Clausulas**	**N°**	**Control**
		9.1.6	**Acceso público, áreas de carga y descarga**
			Controlar las áreas de carga y descarga
			Restringir accesos al área de carga y descarga
			Diseño seguro del área de carga y descarga
			Puerta externa cerrada cuando la interna esté abierta
			Inspección del material entrante
			El material entrante y saliente debería ser físicamente separado

ANEXO 1.4. INVENTARIO DE ACTIVOS Y CLASIFICACIÓN DE LA INFORMACIÓN

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
N°	**Clausulas**	**N°**	**Control**
5.4	**Inventario de activos y clasificación de la información**		
5.4 a)	Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.		
		7.1.1	**Inventario de activos**
			Identificar los activos y mantener un inventario
			Registrar los propietarios y clasificación de la información
			Incluir tipo de activo, formato, ubicación, información de respaldo, licencia y valor dentro del negocio.
		7.1.2	**Propiedad de los activos**
			Toda la información y los activos asociados con el procesamiento de la información deben tener propietario
			Los propietarios deben asegurar una adecuada clasificación
			Los propietarios deben definir y revisar restricciones de acceso
5.4 b)	Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las		

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
	clasificaciones.		
		7.2.1	Guías de clasificación
			Clasificar la información
			Guías de clasificación
		7.2.2	Marcado y tratamiento de la información
			Procedimiento para marcar y tratar la información clasificada
			La salida de información (secreta y confidencial) de los sistemas debe ser etiquetada
			Definir procesos de manipulación para cada nivel de clasificación
			Incluir en los acuerdos con otras organizaciones procedimientos de identificación de la clasificación de información

ANEXO 1.5. ADMINISTRACIÓN DE LAS OPERACIONES Y COMUNICACIONES

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
5.5	**Administración de las operaciones y comunicaciones**		
5.5 a)	Procedimientos documentados para la operación de los sistemas	10.1.1	Documentación de procedimientos operativos
			Documentar y mantener procedimientos de operación
			Incluir procesamiento y utilización correcta de la información
			Incluir actividades de backup
			Incluir requerimientos de programación de horarios
			Instrucciones para el manejo de errores u otras excepciones
			Incluir contactos de apoyo
			Instrucciones especiales de utilización de resultados
			Incluir reinicio del sistema y procedimientos de recuperación
			Incluir gestión de la información del rastro de auditoria

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
5.5 b)	Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.	10.1.2	Gestión de Cambios
			Controlar los cambios en los sistemas y recursos de tratamiento de información
			Registrar cambios significativos
			Planeamiento y prueba de cambios
			Evaluación de impactos
			Comunicar los detalles del cambio
			Identificar responsabilidades de abortar y recobrarse de cambios sin éxito
			Implantar responsabilidades y procedimientos formales de gestión
			Conservar registros de auditoria
5.5 c)	Separación de funciones para reducir el riesgo de error o fraude.	10.1.3	Segregación de tareas
			Segregar tareas y áreas de responsabilidad
			La iniciación de un evento debe estar separado de su autorización
5.5 d)	Separación de los ambientes de desarrollo, prueba y producción.	10.1.4	Separación de los recursos para desarrollo y para producción
			Separación de los entornos de desarrollo, prueba y producción
			Documentar reglas de transferencia de desarrollo a producción
			Procesadores diferentes, o dominios o directorios distintos
			Los compiladores y editores no deben ser accesibles desde producción
			El entorno de prueba debe emular el entorno operacional
			Diferentes perfiles de usuario para sistemas operacionales y de prueba
			No copiar datos sensibles en el entorno de prueba

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
N°	**Clausulas**	**N°**	**Control**
5.5 e)	Monitoreo del servicio dado por terceras partes	10.2.2	Monitoreo y revisión de los servicios externos
			Monitorear los niveles de servicio
			Revisar los reportes de servicio producidos por terceros
			Acuerdos de gestión de incidentes de seguridad con terceros
			Revisar los rastros de auditoría de terceros
			Monitorear fallas e interrupciones del servicio entregado
			Asignar la responsabilidad de manejar la relación con terceros
			Asegurar que los terceros asignen responsabilidades para verificar la conformidad y el cumplimiento
5.5 f)	Administración de la capacidad de procesamiento	10.3.1	Planificación de la capacidad
			Monitorear el uso de recursos
			Realizar proyecciones de capacidades futuras
			Identificar requisitos de capacidad para cada actividad nueva
			Instalar controles de detección de problemas de eficiencia y disponibilidad de sistemas
			Identificar tendencias de uso
5.5 g)	Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.		
		10.4.1	**Medidas y controles contra software malicioso**
			Procedimientos para concientizar a los usuarios
			Política formal prohibiendo el uso de software no autorizado
			Política formal de protección contra riesgos por descarga de archivos/software de redes externas

			Revisiones del software y contenido de data de los sistemas críticos
			Verificación de virus en archivos electrónicos
			Verificación de todo archivo adjunto a un email
			Verificación de código malicioso en páginas web
			Procedimientos y responsabilidades sobre la protección antivirus
			Planes de continuidad para recuperarse de los ataques antivirus
			Procedimientos para recolectar información sobre nuevos virus
			Procedimientos para verificar que la información relativa al código malicioso es veraz
		10.4.2	**Medidas y controles contra código móvil**
			Ejecutar código móvil en un ambiente lógico aislado
			Bloquear cualquier uso de código móvil
			Activar medidas técnicas para asegurar el uso del código móvil
			Controlar los recursos disponibles al acceso de código móvil
			Controles criptográficos para autenticar individualmente un código móvil
5.5 h)	Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas		
		10.6.1	**Controles de red**
			La responsabilidad operativa de las redes debería estar separada de las operaciones de cómputo
			Procedimientos y responsabilidades para la gestión de equipos remotos
			Proteger los datos que pasen por redes públicas

			Controles para mantener la disponibilidad de los servicios de las redes y computadores conectados
			Registros de ingreso y monitoreo
		10.6.2	**Seguridad en los servicios de redes**
			Incluir dentro del contrato de servicio de red: características de seguridad, niveles de servicio, y requisitos de gestión.
			Acordar el derecho a auditoria
			Monitoreo del servicio
			Controles de autenticación, codificación y conexión de red
			Parámetros técnicos para una conexión segura
			Procedimientos para la utilización del servicio de red
		10.7.1	**Gestión de medios removibles**
			Procedimientos para la gestión de medios removibles
			Borrar contenidos de los medios reutilizables antes de desecharlos
			Registros de la remoción de medios
			Almacenamiento seguro de los medios
			Registro de medios removibles
			Sólo activar medios removibles por una razón de negocio
			Documentación de procedimientos y niveles de autorización
		10.7.2	**Eliminación de medios**
			Eliminación segura de medios que contengan información sensible
			Procedimiento para identificar items que requieran eliminación segura
			Registrar la eliminación de items confidenciales
		10.7.3	**Procedimientos de manipulación de la información**

			Procedimientos de manipulación y almacenamiento de la información
			Etiquetado de los medios
			Restricciones de acceso
			Mantener un registro formal de destinatarios de la data
			Asegurar un input de data completo, procesamiento apropiado y validación del output
			Almacenar medios según especificaciones de los fabricantes
			Minimizar la distribución de data
			Revisión de las listas de distribución y destinatarios autorizados
		10.7.4	**Seguridad de la documentación de sistemas**
			Protección de la documentación de sistemas de acceso no autorizado
			Almacenamiento seguro de la documentación de sistemas
			Lista de acceso a la documentación de sistemas
			Proteger la documentación en redes públicas
5.5 i)	Seguridad de intercambio de información, incluido el correo electrónico		
		10.8.1	**Políticas y procedimientos para el intercambio de información y software**
			Políticas, procedimientos y controles formales de intercambio
			Procedimientos para proteger la información de la intercepción, copiado, modificación, desvío de ruta y destrucción.
			Procedimientos para la detección y protección contra código malicioso

			Procedimientos para proteger información que esta como archivo adjunto.
			Política para el uso aceptable de los medios de comunicación electrónica
			Procedimientos para el uso de comunicaciones inalámbricas
			Responsabilidades de todo usuario de no comprometer a la organización
			Uso de técnicas criptográficas
			Pautas de disposición y retención de toda la correspondencia de negocios
			No dejar información sensible en las instalaciones de impresión
			Controles asociados con el reenvío de los medios de comunicación
			Concientización del personal de no revelar información confidencial ante el riesgo de ser escuchado o interceptado
			Concientización del personal de no dejar mensajes con información sensible en máquinas contestadoras
			Concientización del personal de los problemas de usar el fax
			Concientización del personal de no dejar datos demográficos en cualquier software
			Concientizar al personal sobre las páginas caché de los fax y fotocopiadoras
		10.8.2	**Acuerdos de intercambio**
			Acuerdos de intercambio de información y software con terceros
			Responsabilidades para el control y notificación de la transmisión, despacho y recepción
			Procedimientos para notificar al remitente la transmisión, despacho y recepción

			Procedimientos para asegurar la trazabilidad y no repudio
			Estándares técnicos mínimos para el empaque y transmisión
			Acuerdos de custodia
			Estándares de identificación del mensajero
			Responsabilidades en los incidentes de seguridad de información
			Acuerdo de un sistema de etiquetado de información
			Propiedades y responsabilidades de la protección de datos, copyright, licencias
			Estándares técnicos para grabar y leer información y software
			Controles especiales para proteger ítems sensibles
		10.8.3	**Medios físicos en tránsito**
			Proteger los medios que contienen información durante el transporte
			Uso de transportes o mensajeros fiables
			Acordar con la gerencia una lista de mensajeros autorizados
			Procedimiento para comprobar la identificación de los mensajeros
			El empaque debe proteger el contenido contra cualquier daño físico
			Controles para proteger la información sensible de la divulgación o modificación no autorizada
		10.8.4	**Seguridad en la mensajería electrónica**
			Proteger los mensajes de accesos no autorizados, modificaciones o negación del servicio
			Asegurar una dirección y un transporte correcto del mensaje
			Confiabilidad y disponibilidad general del servicio

			Consideraciones legales
			Obtener aprobación antes de utilizar servicios externos públicos
			Niveles mayores de autenticación controlando el acceso a las redes públicas
5.5 j)	Seguridad de canales electrónicos		
		10.9.2	**Transacciones en línea**
			Uso de firmas electrónicas por cada una de las partes
			Asegurar que las credenciales de los usuarios sean válidas y verificadas
			Asegurar la confidencialidad de la transacción
			Asegurar la privacidad de las partes involucradas
			Cifrar los medios de comunicación entre las partes implicadas
			Utilizar protocolos seguros para comunicarse entre las partes
			Asegurar que el almacenaje de los detalles de la transacción se localice fuera de cualquier ambiente público
			Cuando una autoridad confiable sea usada la seguridad es integrada a todo el proceso de gestión del certificado/firma
5.5 k)	Mantenimiento de registros de auditoría y monitoreo del uso de sistemas	10.10.1	Registro de la auditoria
			Registrar actividades de los usuarios, excepciones y eventos de seguridad
			Incluir identificaciones de los usuarios
			Incluir fecha y hora de conexión y desconexión
			Incluir identidad de terminal o locación
			Registrar éxitos y fracasos de intentos de acceso al

			sistema y recursos
			Registrar cambios en la configuración del sistema
			Registrar uso de privilegios
			Registrar uso de las utilidades y aplicaciones del sistema
			Registrar archivos accesados y el tipo de acceso
			Registrar direcciones y protocolos de red
			Registrar las alarmas activadas por el sistema de control de accesos
			Registrar la activación y desactivación de los sistemas de protección
			Mantener medidas de protección de privacidad apropiadas
			Los administradores del sistema no deben tener permiso para borrar o desactivar los registros de sus propias actividades

ANEXO 1.6. ADQUISICIÓN, DESARROLLO, MANTENIMIENTO DE SISTEMAS INFORMÁTICOS

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
N°	**Clausulas**	**N°**	**Control**
5.6	**Adquisición, desarrollo, mantenimiento de sistemas informáticos**		
5.6 a)	Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.		
		12.1.1	**Análisis y especificación de los requisitos de seguridad**
			Especificar los requerimientos de controles de seguridad en los requisitos de los sistemas

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
			Para los productos comprados se debe realizar una prueba formal y un proceso de adquisición.
			Los contratos con el proveedor deben indicar los requisitos de seguridad
		12.2.1	**Validación de los datos de entrada**
			Validar los datos de entrada a las aplicaciones del sistema
			Revisión periódica del contenido de los campos clave o archivos de datos para confirmar su integridad
			Inspección de los documentos físicos de entrada
			Procedimientos para responder a los errores de validación
			Procedimientos para comprobar la integridad de los datos de entrada
			Definición de las responsabilidades de todos los implicados en el proceso de entrada de datos
			Crear un registro de las actividades involucradas en el proceso de input de data
		12.2.2	**Control del proceso interno**
			Incorporar a los sistemas comprobaciones de validación durante el proceso
			Uso de funciones "añadir" y "borrar" para cambiar datos
			Procedimientos para evitar programas que corran en orden equivocado o después de fallo del proceso anterior
			Uso de programas apropiados para recuperación después de fallas
			Protección contra ataques utilizando corridas o desbordes de buffer
			Controles de sesión o de lotes, para conciliar los cuadres de los archivos tras las actualizaciones de las transacciones
			Controles para comprobar saldos de apertura comparándolos con los saldo de cierre anteriores
			Validación de datos generados por el sistema

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
			Comprobaciones de la integridad, autenticidad de la data o software cargado o descargado entre la computadora central y las remotas
			Chequeo de totales hash de registros y archivos
			Comprobaciones que aseguren que los programas de aplicaciones se ejecutan en el momento adecuado
			Comprobaciones que aseguren que los programas se ejecutan en el orden correcto, y finalizan en caso de falla
			Crear un registro de las actividades envueltas en el procesamiento
		12.2.3	**Integridad de los mensajes**
			Identificar los requerimientos para asegurar la autenticación y protección de la integridad de los mensajes en aplicaciones
			Identificar e implementar controles apropiados para asegurar la integridad de los mensajes que lo ameriten
		12.2.4	**Validación de los datos de salida**
			Validar los datos de salida de un sistema de aplicación
			Validaciones de verosimilitud
			Cuentas de control de conciliación
			Suministro de suficiente información para poder determinar la exactitud, completitud, precisión y clasificación de la información
			Procedimientos para responder a las pruebas de validación de salida
			Definir las responsabilidades de todo el personal involucrado en el proceso de output de la data
			Crear un registro de las actividades en el proceso de validación del output de la data

ANEXO 1.7. PROCEDIMIENTO DE RESPALDO

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
5.7	**Procedimientos de Respaldo**		
5.7 a)	Procedimientos de respaldo regulares y periódicamente validados	10.5.1	Recuperación de la información
			Definir el nivel necesario de recuperación de la información
			Documentar los procedimientos de restauración
			La extensión y frecuencia de los backup deben reflejar las necesidades de la organización, requisitos de seguridad de la información y continuidad del negocio
			Probar regularmente los medios de respaldo
			Revisar y probar los procedimientos de restauración
			Encriptar los backups cuando la confidencialidad es importante
5.7 b)	Conservar la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación.	10.5.1	Recuperación de la información
			Almacenar los backup en un lugar apartado
			Adecuado nivel de protección física y ambiental a la información de los backup

ANEXO 1.8. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
N°	**Clausulas**	**N°**	**Control**
5.8	**Gestión de incidentes de seguridad de la información**		
5.8 a)	Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.		
		13.1.1	Reportando los eventos en la seguridad de información
			Procedimiento formal de reporte de eventos de seguridad de la información
			Procedimiento de respuesta a incidentes
			Empleados y terceros deben conocer el procedimiento de reporte y sus responsabilidades
			Procesos de retroalimentación
			Formatos de reporte
			Proceso disciplinario para los empleados y terceros que comenten violaciones a la seguridad
		13.1.2	Reportando debilidades en la seguridad de información
			Empleados, contratistas y terceros deben reportar cualquier debilidad de seguridad observada.
			El mecanismo de reporte debe ser fácil, accesible y estar disponible.
			Empleados, contratistas y terceros deben ser informados que no deben tratar de probar una debilidad sospechada.

ANEXO 1.9. CUMPLIMIENTO NORMATIVO

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
N°	**Clausulas**	**N°**	**Control**
5.9	**Cumplimiento normativo**		
5,9 a)	Las empresas deberán asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.		
		15.1.1	**Identificación de la legislación aplicable**
			Definir, documentar y actualizar todos los requerimientos legales, regulatorios y contractuales para cada sistema de información
			Definir controles, medidas y responsabilidades para cumplir con los requerimientos legales, regulatorios y contractuales.
		15.1.6	**Regulación de los controles criptográficos**
			Utilizar controles criptográficos en conformidad con los acuerdos, leyes y regulaciones
			Considerar restricciones en la importación y/o exportación de hardware y software para realizar funciones criptográficas.
			Considerar restricciones en el uso de encriptación
			Considerar métodos de acceso obligatorios o discrecionales a información encriptada por autoridades de los países.
		15.2.1	**Conformidad con la política de seguridad y los estándares**
			Los gerentes deben realizar revisiones regulares que aseguren el cumplimiento de las políticas y normas de seguridad.
			Determinar causas de no conformidad.
			Determinar e implementar una acción correctiva apropiada.

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
			Realizar revisiones de la acción correctiva que se implementó.
			Registrar y mantener los resultados de las revisiones y acciones correctivas.
			Reportar los resultados a las personas que llevan a cabo las revisiones independientes.
		15.2.2	**Comprobación de la conformidad técnica**
			Comprobar regularmente la implementación de estándares de seguridad en los sistemas de información.
			Las pruebas de intrusión o evaluaciones de vulnerabilidades deben ser planeadas, documentadas y repetibles.
			Toda revisión de cumplimiento técnico debe ser realizada por personas autorizadas y competentes.

ANEXO 1.10. PRIVACIDAD DE LA INFORMACIÓN

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
5.10	**Privacidad de la información**		
5,10 a)	Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la normatividad vigente sobre la materia.		
		15.1.2	**Derechos de propiedad intelectual (DPI)**
			Publicar una política de cumplimiento de derechos de propiedad intelectual
			Adquirir software a través de fuentes conocidas y acreditadas
			Mantener la concientización sobre los derechos de autor, notificar la adopción de medidas disciplinarias en caso de incumplimiento.

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
			Identificar todos los activos que requieran proteger el derecho de propiedad intelectual
			Mantener pruebas y evidencias de la propiedad de licencias, master disks, manuales, etc.
			Implementar controles para no exceder el máximo número de usuarios permitidos
			Comprobar que sólo se ha instalado software autorizado y licenciado
			Política para mantener las condiciones de licencia
			Política para eliminar o transferir software a otros
			Usar herramientas de auditoría apropiadas
			Cumplir con los términos y condiciones para el software e información obtenida de las redes públicas.
			No duplicar, convertir a otro formato o extraer de registros comerciales lo que no sea permitido por copyright
			No copiar parcial ni totalmente libros, artículos, reporte u otros que no sean permitidos por copyright
		15.1.3	**Salvaguarda de los registros de la organización**
			Clasificación de los registros en tipo, cada uno con detalles de los periodos de retención y el medio de almacenamiento
			Publicar guías sobre la retención, almacenamiento, tratamiento y eliminación de los registros y la información
			Proteger los registros y la información de su pérdida, destrucción o falsificación
		15.1.4	**Protección de los datos y de la privacidad de la información personal**
			Desarrollar e implementar una política de privacidad y protección de los datos.
			Cumplir con la legislación de protección de datos personales vigente.
		15.1.5	**Prevención en el mal uso de los recursos de tratamiento de la información**
			Disuadir al personal de utilizar los recursos de tratamiento de información para propósitos no autorizados

CIRCULAR G-140-2009-SBS		NORMA ISO 17799	
Nº	**Clausulas**	**Nº**	**Control**
			Los usuarios deben ser conscientes del alcance del acceso dado y del monitoreo que se lleva a cabo para detectar un uso no autorizado.

ANEXO 2. FORMATO DE DEFINICIÓN DE ALCANCE DEL SGSI

[Empresa]	[Área responsable]
ALCANCE DEL SGSI	
1. COMPROMISO INSTITUCIONAL	
2. ALCANCE DEL SGSI	
2.1. Procesos implicados	
2.2. Localizaciones físicas	
3. INTERFACES DEL SGSI	
4. DEPENDENCIAS	

REALIZADO POR:		
Nombre	Cargo	Firma
REVISADO POR:		
Nombre	Cargo	Firma
APROBADO POR:		
Nombre	Cargo	Firma

ANEXO 3. FORMATO DE DEFINICIÓN DE LA POLÍTICA DE SI

[Empresa] [Área responsable]
POLITICA DE SEGURIDAD DE LA INFORMACION
1. ALCANCE
2. OBJETIVO
3. TERMINOS Y DEFINICIONES
<<Incluir términos relacionados a seguridad de la información que ayuden a su entendimiento. Por ejemplo: Seguridad de la información, Evaluación de riesgos, Administración de riesgos, Comité de seguridad de la información, Responsable de seguridad, Incidente de Seguridad, entre otros. >>
4. ESTRUCTURA ORGANIZACIONAL DE LA SI
<<Definir las responsabilidades de cada área de la organización respecto a la gestión de la seguridad de la información>>
5. DOMINIOS DE LA SEGURIDAD DE LA INFORMACION
Para cada dominio se incluir: • *Quién definirá los controles* • *Definir el objetivo de implementar controles en ese dominio* • *Quién es el responsable de implementar los controles*
5.1. SEGURIDAD LOGICA
5.2. SEGURIDAD DEL PERSONAL
5.3. SEGURIDAD FISICA Y AMBIENTAL
5.4. INVENTARIO DE ACTIVOS Y CLASIFICACION DE LA INFORMACION
5.5. ADMINISTRACION DE LAS OPERACIONES Y COMUNICACIONES
5.6. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS INFORMATICOS
5.7. PROCEDIMIENTOS DE RESPALDO
5.8. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

5.9. CUMPLIMIENTO NORMATIVO
5.10. PRIVACIDAD DE LA INFORMACION

REALIZADO POR:		
Nombre	Cargo	Firma
REVISADO POR:		
Nombre	Cargo	Firma
APROBADO POR:		
Nombre	Cargo	Firma

ANEXO 4. MATRIZ DE INVENTARIO DE ACTIVOS Y CLASIFICACIÓN DE INFORMACIÓN

INFORMACION

DATOS GENERALES DEL ACTIVO						RESPONSABILIDAD SOBRE LOS ACTIVOS			UBICACIÓN LOGICA			UBICACIÓN FISICA			RESPECTO A LA INFORMACION				
Codigo del Activo	Macroproceso	Proceso	Tipo Física/Lógica	Descripción	Formato de almacenamiento	Propietario	Custodio	Usuario	IP Servidor	Ruta	Nombre Archivo	Edificio	Piso	Estante / Archivador	Confidencialidad ¿Qué daño causaría que sea conocida por quien no debe?	Integridad ¿Que perjuicio causaría que estuviera dañada o corrupta?	Disponibilidad ¿Qué perjuicio causaría no tenerla o no poder utilizarla?	Tasación del Activo	Clasificación del Activo
INF001									0.0.0.0	\\Ruta\Carpeta	Nombre Archivo								
INF002																			

SOFTWARE

DATOS GENERALES DEL ACTIVO					RESPONSABILIDAD SOBRE EL ACTIVO			UBICACIÓN		DATOS COMPLEMENTARIOS								RESPECTO A LOS DATOS PROCESADOS POR EL SOFTWARE				
										LICENCIAMIENTO												
Codigo del Activo	Macrproceso	Proceso	Activo de Información	Descripción del Activo de Información	Propietario	Custodio	Usuario	Ubicación Servidor - PC - DVD	Ubicación Backup	Tipo de Software	Versión	Tipo y detalles de la licencia	Número de Licencias	Proveedor / Fabricante	Requerimientos específicos Especificación configuración especial o requerimiento técnico para su ejecución	Contacto Técnico	Propósito, Servicio - Rol - Función	Confidencialidad ¿Qué daño causaría que sean conocidos por quienes no deben?	Integridad ¿Que perjuicio causaría que estuvieran dañados o corruptos?	Disponibilidad ¿Qué perjuicio causaría no tenerlos o no poder utilizarlos?	Tasación del Activo	Clasificación del Activo
SWR001																						
SWR002																						

HARDWARE

DATOS GENERALES DEL ACTIVO					RESPONSABILIDAD SOBRE LOS ACTIVOS			DATOS DEL EQUIPO			CAPACIDAD DE PROCESAMIENTO				RESPECTO A LOS DATOS ALMACENADOS				
Codigo del Activo	Macroproceso	Proceso	Tipo de Activos de Información	Descripción del Activo de Información	Propietario	Custodio	Usuario	Ubicación del activo	Dirección IP	Nombre en la red	Marca / Modelo	CPU	Memoria RAM	HDD	Confidencialidad ¿Qué daño causaría que sean conocidos por quienes no deben?	Integridad ¿Qué perjuicio causaría que estuvieran dañados o corruptos?	Disponibilidad ¿Que perjuicio causaría no tenerlos o no poder utilizarlos?	Tasación del Activo	Clasificación del Activo
HWR001																			
HWR002																			

PERSONAS

INVENTARIO DE ACTIVOS DE INFORMACIÓN															
DATOS GENERALES DEL COLABORADOR							FUNCIONES Y HABILIDADES TÉCNICAS			RESPECTO AL COLABORADOR				
Codigo del Activo	Macroproceso	Proceso	Rol dentro de la organización	Departamento	Jefe inmediato superior	Rol alterno ¿Quién lo puede reemplazar?	Tipo de privilegios en componentes de TI	Perfil del empleado Responsabilidad principal de un individuo	Capacidades mínimas requeridas	Confidencialidad ¿Qué daño causaría que revele información a quien no debe?	Integridad ¿Qué perjuicio causaría que altere la información?	Disponibilidad ¿Qué perjuicio causaría la ausencia del colaborador?	Tasación del Activo	Clasificación del Activo

SERVICIOS

DATOS GENERALES DEL ACTIVO					RESPONSABILIDAD SOBRE LOS ACTIVOS			DATOS COMPLEMENTARIOS		RESPECTO A LA INFORMACIÓN CONTENIDA				
Codigo del Activo	Macroproceso	Proceso	Nombre del servicio	Descripción	Propietario	Custodio	Usuario	Proveedor	Datos de Contacto	Confidencialidad ¿Qué daño causaría que sea conocida por quien no debe?	Integridad ¿Qué perjuicio causaría que estuviera dañada o corrupta?	Disponibilidad ¿Qué perjuicio causaría no tenerla o no poder utilizarla?	Tasación del Activo	Clasificación del Activo
SER001														
SER002														

ENTORNO

DATOS GENERALES DEL ACTIVO					RESPONSABILIDAD DE LOS ACTIVOS			UBICACIÓN			RESPECTO A LA BASE DE DATOS				
Codigo del Activo	Macroproceso	Proceso	Nombre del entorno	Descripción	Propietario	Custodio	Usuario	Dirección	Piso	Oficina	Confidencialidad ¿Qué daño causaría que sea conocida por quien no debe?	Integridad ¿Qué perjuicio causaría que estuviera dañada o corrupta?	Disponibilidad ¿Qué perjuicio causaría no tenerla o no poder utilizarla?	Tasación del Activo	Clasificación del Activo
ENT001															
ENT002															

ANEXO 5. MATRIZ DE GESTIÓN DE RIESGOS

AMENAZA		VULNERABILIDAD		ANTES de la implantación de controles			CONTROLES EXISTENTES							DESPUES de la implantación de los controles			PLAN DE TRATAMIENTO DEL RIESGO			
Código Amen.	Amenaza	Código Vuln.	Vulnerabilidades	Probabilidad	Impacto	Nivel de Riesgo Inherente	Código Control	Controles existentes	¿Tiene asignado un responsable?	Puesto del Responsable	Ejecución del control	Documentado Registro y/o evidencia	Frecuencia de uso	Tipo del control	Probabilidad	Impacto	Nivel de Riesgo Residual	Opción de Tratamiento	Control Propuesto	Responsable Nombre del Funcionario	Fecha de implementación
											Débil		Mensual	Preventivo Manual							
											Moderado			Preventivo Automático							
											Fuerte			Detectivo Automático							
														Detectivo Manual							

ANEXO 6. MATRIZ DE PERFILES DE ACCESO

		SISTEMA A			SISTEMA B			SISTEMA C				SISTEMA D		
ÁREA	CARGO/PUESTO	PERFIL 1	PERFIL 2	PERFIL 3	PERFIL 4	PERFIL 5	PERFIL 6	PERFIL 7	PERFIL 8	PERFIL 9	PERFIL 10	PERFIL 11	PERFIL 12	PERFIL 13
AREA A	CARGO 1			X		X					X			
AREA A	CARGO 2	X			X						X		X	
AREA A	CARGO 3		X			X			X				X	
AREA A	CARGO 4			X			X					X		
AREA A	CARGO 5	X			X					X				X
AREA B	CARGO 6		X			X			X				X	
AREA B	CARGO 7		X				X	X						X
AREA B	CARGO 8	X			X					X		X		
AREA B	CARGO 9		X						X				X	
AREA B	CARGO 10			X			X				X			X
AREA B	CARGO 11		X			X			X					
AREA C	CARGO 12							X						
AREA C	CARGO 13	X											X	
AREA C	CARGO 14					X				X				
AREA C	CARGO 15		X				X							X

SISTEMA	PERFIL	OPCION
SISTEMA A	PERFIL A1	OPC 1
SISTEMA A	PERFIL A1	OPC 2
SISTEMA A	PERFIL A1	OPC 3
SISTEMA A	PERFIL A2	OPC 2
SISTEMA A	PERFIL A2	OPC 3
SISTEMA A	PERFIL A2	OPC 4
SISTEMA A	PERFIL A2	OPC 5
SISTEMA A	PERFIL A2	OPC 6
SISTEMA A	PERFIL A3	OPC 4
SISTEMA A	PERFIL A3	OPC 5
SISTEMA A	PERFIL A3	OPC 6
SISTEMA B	PERFIL B1	OPC 10
SISTEMA B	PERFIL B1	OPC 11
SISTEMA B	PERFIL B1	OPC 12
SISTEMA B	PERFIL B1	OPC 13
SISTEMA B	PERFIL B2	OPC 12
SISTEMA B	PERFIL B2	OPC 13
SISTEMA B	PERFIL B2	OPC 14
SISTEMA C	PERFIL C1	OPC 30
SISTEMA C	PERFIL C1	OPC 33
SISTEMA C	PERFIL C1	OPC 34

ANEXO 7. REGISTRO DE REVISIÓN DE PERFILES

SISTEMA	PERFIL	ÁREA	CARGO/PUESTO	F. INICIO REVISIÓN	F. FIN REVISIÓN	COMENTARIOS
Sistema A	PERFIL 1	AREA A	CARGO 1	01/04/2011	10/04/2011	Conforme
Sistema A	PERFIL 1	AREA A	CARGO 2	01/04/2011	10/04/2011	Se eliminó trx 001
Sistema A	PERFIL 1	AREA A	CARGO 3	01/04/2011	10/04/2011	Se adicionó trx 010
Sistema A	PERFIL 2	AREA A	CARGO 4	01/02/2012	05/02/2012	Conforme
Sistema A	PERFIL 2	AREA A	CARGO 5	01/02/2012	05/02/2012	Conforme
Sistema B	PERFIL 1	AREA B	CARGO 6	01/04/2012	07/04/2012	Conforme
Sistema B	PERFIL 2	AREA B	CARGO 7	05/05/2012	08/05/2012	Se retiraron todas las trx al cargo
Sistema B	PERFIL 3	AREA B	CARGO 8	01/10/2012	11/10/2012	Conforme
Sistema B	PERFIL 3	AREA B	CARGO 9	01/10/2012	11/10/2012	Conforme

ANEXO 8. REPORTES DE LAS ALTAS Y BAJAS DEL PERSONAL

CODIGO	NRO DOC	NOMBRE	ÁREA	CARGO	USER	F. SOLICITUD ALTA	F. ALTA	F. SOLICITUD BAJA	F. BAJA
10001	04000010	Trabajador 1	Area 1	Cargo 1	user1	27/12/2011	03/01/2012		
10002	10123403	Trabajador 2	Area 2	Cargo 2	user2	27/12/2011	03/01/2012		
10003	34568790	Trabajador 3	Area 1	Cargo 3	user3	01/02/2012	10/02/2012	30/05/2012	31/05/2012
10004	09873324	Trabajador 4	Area 3	Cargo 4	user4	10/03/2012	15/03/2012		
10005	76379849	Trabajador 5	Area 6	Cargo 5	user5	14/04/2012	16/04/2012		
10006	24729034	Trabajador 6	Area 2	Cargo 6	user6	15/05/2012	23/05/2012	28/10/2012	31/10/2012
10007	39857804	Trabajador 7	Area 4	Cargo 7	user7	10/07/2012	12/07/2012		
10008	43985435	Trabajador 8	Area 5	Cargo 8	user8	05/10/2012	13/10/2012		

ANEXO 9. MATRIZ DE ACCESO BRINDADO A LOS SISTEMAS

								SISTEMA A			SISTEMA B			SISTEMA C			
Codigo	Nro Doc	Nombre	Área	Cargo	User	Fecha Alta	Fecha Cese	PERFIL 1	PERFIL 2	PERFIL 3	PERFIL 4	PERFIL 5	PERFIL 6	PERFIL 7	PERFIL 8	PERFIL 9	PERFIL 10
10001	04000010	Trabajdor 1	Area 1	Cargo 1	user1	03/01/2012				X		X					X
10002	10123403	Trabajdor 2	Area 2	Cargo 2	user2	03/01/2012		X			X						X
10003	34568790	Trabajdor 3	Area 1	Cargo 3	user3	10/02/2012	31/05/2012		X			X			X		
10004	09873324	Trabajdor 4	Area 3	Cargo 4	user4	15/03/2012				X			X				
10005	76379849	Trabajdor 5	Area 6	Cargo 5	user5	16/04/2012		X			X					X	
10006	24729034	Trabajdor 6	Area 2	Cargo 6	user6	23/05/2012	31/10/2012		X			X			X		
10007	39857804	Trabajdor 7	Area 4	Cargo 7	user7	12/07/2012			X				X	X			
10008	43985435	Trabajdor 8	Area 5	Cargo 8	user8	13/10/2012		X			X					X	

ANEXO 10. ACTIVIDAD DE LOS USUARIOS EN LOS SISTEMAS

SISTEMA	USER	PERFIL	ESTADO	F. CREACIÓN	ULT. MODIFICACIÓN	ULT. CAMBIO DE PWD	F. INGRESO AL SISTEMA	IP INGRESO AL SISTEMA
Sistema 1	user1	Perfil 1	Activo	27/12/2011	27/12/2011	30/09/2012	10/10/2012	10.25.0.1
Sistema 1	user1	Perfil 1	Activo	27/12/2011	27/12/2011	30/09/2012	11/10/2012	10.25.9.2
Sistema 2	user3	Perfil 2	Activo	01/02/2012	10/02/2012	01/10/2012	01/10/2012	10.25.0.10
Sistema 2	user4	Perfil 3	Inactivo	10/03/2012	10/06/2012			
Sistema 2	user3	Perfil 2	Activo	14/04/2012	10/06/2012	14/09/2012	20/10/2012	10.25.9.20
Sistema 3	user4	Perfil 3	Activo	15/05/2011	10/10/2011	14/09/2012	20/10/2012	10.25.9.20
Sistema 4	user5	Perfil 4	Inactivo	06/06/2012	14/10/2012	14/09/2012	14/09/2012	10.25.9.20

ANEXO 11. INVENTARIO DE SOFTWARE UTILITARIOS Y HERRAMIENTAS DE AUDITORIA

CODIGO	TIPO SOFTWARE	APLICACIÓN	DESARROLLADOR	NIVEL DE SEGURIDAD	VERSION	AUTORIZADO	COMENTARIO
SW0001	Antivirus	Aplicación 1	Desarrolador 1	Muy Alto	10,1	SI	
SW0002	Base	Aplicación 2	Desarrolador 2	Alto	4,0	SI	
SW0003	Utilitario	Aplicación 3	Desarrolador 3	Medio	4,0	SI	
SW0004	Sist. Operativo	Aplicación 4	Desarrolador 4	Bajo	2,0	NO	Nivel de seguridad no aceptable
SW0005	Aplicación	Aplicación 5	Desarrolador 5	Muy Bajo	1,2	NO	Nivel de seguridad no aceptable
SW0006	Aplicación	Aplicación 6	Desarrolador 5	Medio	4,0	NO	Aplicación permitiría fuga de información
SW0007	Aplicación	Aplicación 7	Desarrolador 7	Alto	7,0	SI	

ANEXO 12. DOCUMENTOS EN FILE DE PERSONAL

								Documentos File						
COD	NRO DOC	NOMBRE	ÁREA	CARGO	F. ENVIO ALMACEN	UBICACIÓN	CAJA	Documento 1	Documento 2	Documento 3	Documento 4	Documento 5	Documento 6	Documento 7
10001	04000010	Trabajador 1	Area 1	Cargo 1	03/01/2012	Cuostodio 1	CJ00123			X		X		
10002	10123403	Trabajador 2	Area 2	Cargo 2	03/01/2012	Cuostodio 1	CJ00456	X			X			
10003	34568790	Trabajador 3	Area 1	Cargo 3	10/02/2012	Cuostodio 1	CJ00123		X			X		
10004	09873324	Trabajador 4	Area 3	Cargo 4	15/03/2012	Cuostodio 1	CJ00124			X			X	
10005	76379849	Trabajador 5	Area 6	Cargo 5	16/04/2012	Cuostodio 1	CJ00134	X			X			
10006	24729034	Trabajador 6	Area 2	Cargo 6	23/05/2012	Cuostodio 1	CJ00134		X			X		
10007	39857804	Trabajador 7	Area 4	Cargo 7	12/07/2012	Cuostodio 1	CJ00123		X				X	X
10008	43985435	Trabajador 8	Area 5	Cargo 8	13/10/2012	Cuostodio 1	CJ00134	X			X			

ANEXO 13. MODELO DE ACUERDO DE CONFIDENCIALIDAD PARA PERSONAL EXTERNO E INTERNO

ACUERDO DE CONFIDENCIALIDAD DE LA INFORMACIÓN

I. OBJETO

CON EL PRESENTE CONTRATO LAS PARTES FIJAN FORMALMENTE Y POR ESCRITO LOS TÉRMINOS Y CONDICIONES BAJO LAS QUE LAS PARTES MANTENDRÁN LA CONFIDENCIALIDAD DE LA INFORMACIÓN SUMINISTRADA Y CREADA ENTRE ELLAS.

Que a los efectos de este acuerdo, tendrá la consideración de información confidencial, toda la información susceptible de ser revelada por escrito, de palabra o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro, intercambiada como consecuencia de este acuerdo.

Este acuerdo no constituye ningún acuerdo de licencia, contrato de desarrollo o similar, obligándose las partes a adoptar las medidas oportunas para asegurar el tratamiento confidencial de dicha información, medidas que no serán menores que las aplicadas por ellas a la propia información confidencial de su compañía.

II. DURACIÓN

Este acuerdo tendrá una duración indefinida desde el momento de su firma.

En caso de que no se renueve el contrato, ambas partes deberán devolver a la otra toda la información remitida entre sí, comprometiéndose a la destrucción de cualquier copia de la misma, independientemente del soporte o formato en el que se encuentre almacenada.

No obstante, lo dispuesto en el párrafo anterior, cada parte se compromete a mantener el compromiso de confidencialidad respecto a la información y material intercambiado entre las partes, de forma indefinida tras la finalización del presente acuerdo.

III. CONFIDENCIALIDAD

Las partes se obligan a entregarse todo el material que sea necesario, y en el caso de ser este confidencial se comprometen a:

a. Utilizar dicha información de forma reservada.

b. No divulgar ni comunicar la información técnica facilitada por la otra parte.

c. Impedir la copia o revelación de esa información a terceros, salvo que gocen de aprobación escrita de la otra parte, y únicamente en términos de tal aprobación.

d. Restringir el acceso a la información a sus empleados y subcontratados, en la medida en que razonablemente puedan necesitarla para el cumplimiento de sus tareas acordadas.

e. No utilizar la información o fragmentos de ésta para fines distintos de la ejecución de este contrato.

Las partes serán responsables entre sí, ante el incumplimiento de esta obligación, ya sea por sus empleados o por subcontratados.

Las partes mantendrán ésta confidencialidad y evitarán revelar la información a toda persona que no sea empleado o subcontratado, salvo que:

a. La parte receptora tenga evidencia de que conoce previamente la información recibida.

b. La información recibida sea de dominio público.

c. La información recibida proceda de un tercero que no exige secreto.

IV. DERECHOS PREVIOS SOBRE LA INFORMACIÓN

Toda información puesta en común entre las partes es de propiedad exclusiva de la parte de donde proceda, y no es precisa la concesión de licencia para dicho intercambio. Ninguna de las partes utilizará información previa de la otra parte para su propio uso, salvo que se autorice lo contrario.

La información que se proporciona no da derecho o licencia a la empresa que la recibe sobre las marcas, derechos de autor o patentes que pertenezcan a quien la proporciona. La divulgación de información no implica transferencia o cesión de derechos, a menos que se redacte expresamente alguna disposición al respecto.

V. CLÁUSULA PENAL

Las partes se comprometen a cumplir con todos los términos fijados en el presente contrato, y muy especialmente aquellos relativos a las cláusulas sobre propiedad intelectual e industrial, confidencialidad y obligación de secreto.

Independientemente de las responsabilidades que pudieran derivarse del incumplimiento del presente acuerdo, así como de las eventuales indemnizaciones por daños y perjuicios de cualquier naturaleza que pudieran establecerse, el incumplimiento de estas obligaciones determinará a elección de la parte que no incumplió el contenido de los términos fijados en el presente contrato:

a. La resolución del contrato.

b. El abono de..... € en concepto de penalización.

VI. DERECHOS DE PROPIEDAD

Toda información intercambiada es de propiedad exclusiva de la parte de la cual proceda. Ninguna de las partes utilizará información de la otra para su beneficio independiente.

VII. PROTECCIÓN DE DATOS

Para la correcta aplicación del presente acuerdo, ambas partes podrían tener acceso a datos de carácter personal protegidos por la Ley de Protección de Datos de Personales, por lo que se comprometen a efectuar un uso y tratamiento de los datos afectados que será acorde a las actuaciones que resulten necesarias para la correcta prestación de servicios regulada en este acuerdo, según las instrucciones facilitadas en cada momento.

Asimismo, las partes asumen la obligación de guardar secreto profesional sobre cuanta información pudieran recibir, gestionar y articular con relación a los datos personales y a no comunicarlos a terceros, salvo las excepciones mencionadas, así como a destruirlos, cancelarlos o devolverlos en el momento de la finalización de la relación contractual entre ambas partes, así como a aplicar las medidas de seguridad necesarias.

Los derechos de acceso, rectificación, cancelación y oposición podrán ejercitarse mediante escrito dirigido a las direcciones de los firmantes del presente documento que constan en el encabezamiento.

VIII. CONFIDENCIALIDAD DEL ACUERDO

Las partes acuerdan que este acuerdo reviste el carácter de confidencial y por tanto se prohíbe su divulgación a terceros.

IX. MODIFICACIÓN O CANCELACIÓN

Este acuerdo sólo podrá ser modificado con el consentimiento expreso de ambas partes, en documento escrito y mencionando la voluntad de las partes de modificar el presente acuerdo.

X. JURISDICCIÓN.

Las partes se comprometen a resolver de manera amistosa cualquier desacuerdo que pueda surgir en el desarrollo del presente contrato.

En caso de conflicto ambas partes acuerdan el sometimiento a los Tribunales de....., con renuncia de su propio fuero.

Y en prueba de conformidad de cuanto antecede, firman el presente acuerdo por duplicado y a un solo efecto en el lugar y fecha citados.

Ambas partes están interesadas en firmar este ACUERDO a fin de mantener salvaguardados sus intereses.

"Declaro haber leído y estar de acuerdo con el presente Acuerdo de Confidencialidad de la Información, en prueba de lo cual suscribo el presente documento".

Personal Externo	**Líder del Proyecto en ----ENTIDAD----- S.A.**
Nombres y Apellidos:	**Nombres y Apellidos:**
Tipo de Documento de Identidad (DI):	**Cargo:**
N° de DI:	**Firma:**
Compañía:	
Cargo:	
Firma:	

ANEXO 14. MODELO DE CLÁUSULA DE CONFIDENCIALIDAD EN UN CONTRATO CON TERCEROS

CLÁUSULA DE CONFIDENCIALIDAD

Las partes acuerdan que toda la información y/o documentación suministrada directa o indirectamente por ***LA ENTIDAD FINANCIERA*** a ***EL PROVEEDOR*** y viceversa en virtud de este contrato deberá ser considerada como información Confidencial, la misma que es de exclusiva propiedad de ***LA ENTIDAD FINANCIERA***, ***EL PROVEEDOR*** no podrá usar la información provista para propósito distinto al permitido o requerido en el presente contrato.

EL PROVEEDOR se obliga a que la Información Confidencial sólo será conocida y utilizada por ciertos y determinados empleados que tengan la necesidad de conocer dicha información en el curso de las prestación de los servicios materia de este contrato, previa comunicación de ***EL PROVEEDOR*** a ***LA ENTIDAD FINANCIERA***. Todos ellos deberán estar sujetos a la obligación de confidencialidad de la información.

En los casos que ***EL PROVEEDOR*** requiera involucrar a terceros proveedores para la prestación de los servicios materia del presente contrato requerirá previamente de la autorización expresa y por escrito por cualquier medio escrito por parte de ***LA ENTIDAD FINANCIERA*** obligándose en estos casos a incorporar en los acuerdos contratos de trabajo que suscriba con éstos la obligación de reserva con respecto a la información Confidencial a la que puedan tener acceso, quedando de esta forma los terceros proveedores igualmente sujetos a la obligación de confidencialidad de la información.

EL PROVEEDOR se hace responsable del cumplimiento de la obligación asumida en esta cláusula respecto de sus empleados, sean éstos contratados o sub contratados, así como los terceros proveedores mencionados en los párrafos anteriores, comprometiéndose a tomar todas las medidas que sean necesarias, para salvaguardar la información confidencial y evitar

cualquier divulgación y a indemnizar a ***LA ENTIDAD FINANCIERA*** por los daños que pudiera causarle dicho incumplimiento.

Las restricciones antes señaladas no será aplicable aquella información que:

a) A la fecha sea o se vuelva de dominio público sin culpa de la parte que hace la divulgación;
b) Estaba legalmente en posesión de ***EL PROVEEDOR*** antes de que hubiera sido proporcionada por ***LA ENTIDAD FINANCIERA***.

Si ***EL PROVEEDOR*** o sus representantes fueren requeridos por un tribunal de justicia peruana o por una autoridad gubernamental peruana, en forma legalmente obligatoria, y por escrito, a revelar la existencia y/o contenido de este acuerdo o de información Confidencial, ésta se obliga a informar este hecho a ***LA ENTIDAD FINANCIERA*** dentro de los dos días de recibido el requerimiento, solicitud o notificación, con la finalidad de que éste pueda tomar las medidas correctivas o de defensa que sean pertinentes.

EL PROVEEDOR devolverá a ***LA ENTIDAD FINANCIERA*** toda la información que le hubiese sido proporcionada con relación a los servicios prestados y la eliminará de cualquier medio de almacenamiento, debiendo entregar al término del Contrato, una declaración en ese sentido.

ANEXO 15. FORMATO PARA DEFINIR PROGRAMAS DE CAPACITACIÓN Y CONCIENTIZACIÓN

Fecha:	**Área de Seguridad de la información**
Objetivo	
• ... •	
Programa de concienciación	
Tópicos de concienciación:	
• ... • ...	
Dirigido a:	
• ... • ...	
Actividades	Fecha
1. Actividad 1	dd/mm/aa
2. ...	
3.	
4.	

Programa de capacitación	
Rol 1:	Gerentes y ejecutivos
Áreas de capacitación:	
• .. • .. • ..	
Objetivos de aprendizaje:	
• .. • .. • ..	

Criterios de evaluación	Definición
Actividades	Fecha
1. Actividad 1	dd/mm/aa
2. ...	
3.	
4.	

Requerimientos y costos	
Ítem	**Costo**
1.	S/.
2.	
3.	
4.	
5.	
Total:	S/.

ANEXO 16. REGISTRO DE MEDIDAS DISCIPLINARIAS

COD	NRO DOC	NOMBRE	ÁREA	CARGO	ESTADO	TIPO FALTA	DESCRIPCION FALTA	TIPO MEDIDA DISCIPLINARIA	FECHA COMUNICACIÓN	FECHA APLICACIÓN	IMPLICANCIA	DURACIÓN
10001	04000010	Trabajador 1	Area 1	Cargo 1	ACTIVO	Tipo 1	Descripción falta 1	Amonestación	20/01/2012			
10002	10123403	Trabajador 2	Area 2	Cargo 2	ACTIVO	Tipo 2	Descripción falta 2	Sanción	20/01/2012	01/02/2012	Sin goce de haber	2 semanas
10003	34568790	Trabajador 3	Area 1	Cargo 3	CESADO	Tipo 3	Descripción falta 3	Amonestación	03/03/2012			
10004	09873324	Trabajador 4	Area 3	Cargo 4	CESADO	Tipo 4	Descripción falta 4	Sanción	28/05/2012	01/06/2012	Despido	
10005	76379849	Trabajador 5	Area 6	Cargo 5	LICENCIA	Tipo 5	Descripción falta 5	Sanción	28/05/2012	01/06/2012	Sin goce de haber	1 Semana
10006	24729034	Trabajador 6	Area 2	Cargo 6	ACTIVO	Tipo 6	Descripción falta 6	Amonestación	05/02/2012			
10007	39857804	Trabajador 7	Area 4	Cargo 7	ACTIVO	Tipo 7	Descripción falta 7	Amonestación	10/10/2012			
10008	43985435	Trabajador 8	Area 5	Cargo 8	ACTIVO	Tipo 8	Descripción falta 8	Amonestación	03/08/2012			

ANEXO 17. REGISTRO DE ACTIVOS ENTREGADOS AL PERSONAL

Cod Empleado: _____ **Nombre:** _____ **Fecha:** _____

☐ Tarjeta Proximidad ☐ Laptop ☐ Modem VPN ☐ Celular

☐ Otros: _____

Observaciones:

_____

_____

_____

_____

Requiere reparar: ☐ SI, Incluir Costo (S/.): _____
☐ NO

Firma Trabajador	Firma Seguridad	Firma RRHH

							ACTIVOS ENTREGADOS						
COD	NRO DOC	NOMBRE	ESTADO	FECHA ENTREGA	FECHA DEVOLUCION	COMENTARIO DEVOLUCIÓN	FOTOCHECK	LAPTOP	CARGADOR	MODEM USB	CELULAR	ACTIVO X	ACTIVO Y
10001	04000010	Trabajador 1	Activo	03/01/2012					X		X		
10002	10123403	Trabajador 2	Cesado	03/01/2012	30/06/2012	Conforme	X			X			
10003	34568790	Trabajador 3	Cesado	10/02/2012	30/09/2012	Conforme		X			X		
10004	09873324	Trabajador 4	Activo	15/03/2012					X			X	
10005	76379849	Trabajador 5	Activo	16/04/2012			X			X			
10006	24729034	Trabajador 6	Activo	23/05/2012				X			X		
10007	39857804	Trabajador 7	Activo	12/07/2012				X				X	X
10008	43985435	Trabajador 8	Activo	13/10/2012			X			X			

ANEXO 18. BITÁCORA DE INGRESOS Y SALIDAS

TIPO DOC	NRO DOC	NOMBRE	PISO	AREA / UNIDAD	TRABAJADOR DE CONTACTO	FECHA INGRESO	HORA INGRESO	FECHA SALIDA	HORA SALIDA
DNI	04000010	Visitante 1	4	Sistemas	Trabajador 1	05-mar	4:00 PM	05-mar	8:00 PM
DNI	10123403	Visitante 2	4	Sistemas	Trabajador 2	05-mar	4:00 PM	06-mar	10:00 AM
CE	34568790	Visitante 3	4	Sistemas	Trabajador 3	05-mar	4:00 PM	06-mar	10:00 AM
CE	09873324	Visitante 4	4	Sistemas	Trabajador 4	05-mar	4:00 PM	05-mar	8:00 PM
DNI	76379849	Visitante 5	5	Contabilidad	Trabajador 5	09-mar	10:00 AM	09-mar	1:00 PM
DNI	24729034	Visitante 6	5	Contabilidad	Trabajador 6	10-mar	9:00 AM	10-mar	11:00 AM
DNI	39857804	Visitante 7	6	Operaciones	Trabajador 7	11-mar	2:00 PM	11-mar	5:00 PM
DNI	43985435	Visitante 8	7	Finanzas	Trabajador 8	12-mar	3:00 PM	12-mar	4:00 PM

ANEXO 19. REGISTRO DE EVENTOS DE VIDEO VIGILANCIA

Lugar	Cámara	Evento	Fecha	Hora	Nombre de Grabación
Agencia Miraflores	CA-E3	Alarma activada	13/10/2011	5:00:34 AM	CA-E340829
Agencia San Borja	CA-C7	Detección de Movimiento	09/11/2011	8:33:45 AM	CA-C740856
Agencia La Molina	CA-A1	Pérdida de video	18/11/2011	1:21:03 PM	CA-A140865
Agencia San Isidro	CA-H9	Error de grabación	23/11/2011	11:09:54 PM	CA-H940870
Agencia Cercado	CA-O9	Gravación de emergencia activada	30/11/2011	9:45:22 AM	CA-O940877
Agencia Lince	CA-P5	Alarma desactivada	01/12/2012	10:04:33 AM	CA-P541244

ANEXO 20. REGISTRO DE MANTENIMIENTO DE EQUIPOS

COD INVENTARIO	EQUIPO	FECHA ALTA	TIPO MANTENIMIENTO	ULTIMO MANTENIMIENTO	PROX. MANTENIMIENTO	OBSERVACIONES
EQP00123	Equipo 1	01/01/2010	Preventivo	13/06/2012	10/12/2012	
EQP00127	Equipo 2	01/01/2010	Preventivo	13/06/2012	10/12/2012	
EQP00134	Equipo 3	01/01/2010	Preventivo	13/06/2012	10/12/2012	
EQP00134	Equipo 4	01/01/2010	Correctivo	13/08/2011	09/02/2012	
EQP00457	Equipo 5	01/04/2011	Preventivo	11/09/2011	09/03/2012	
EQP00567	Equipo 6	01/03/2010	Correctivo	11/08/2011	07/02/2012	

ANEXO 21. REGISTRO DE TEMPERATURA Y HUMEDAD DEL CENTRO DE COMPUTO

POSICIÓN	FECHA DD/MM/AAAA	HORA HH:MM:SS	TEMPERATURA C°	HUMEDAD %HR
1	22/01/2011	13:15:00	22	29.1
2	22/01/2011	19:30:01	23.3	30.2
3	23/01/2011	13:15:00	22.9	31.5
4	23/01/2011	19:30:01	23.4	30.4

ANEXO 22. REGISTRO DE CONTROL DE CAMBIOS DE DOCUMENTOS

PROCESO	SUBPROCESO	DOCUMENTO	TIPO DE DOCUMENTO	VERSION	FECHA PUBLICACIÓN	COMENTARIOS
Proceso 1	Subproceso 1.1	Afiliación de clientes	Procedimiento	1	01/01/2010	
Proceso 1	Subproceso 1.1	Afiliación de clientes	Procedimiento	1,1	01/07/2010	
Proceso 1	Subproceso 1.1	Afiliación de clientes	Procedimiento	2	05/08/2011	
Proceso 1	Subproceso 1.2	Polítrica de seguridad	Política	1	01/01/2011	
Proceso 2	Subproceso 2.1	Adquisiciones	Política	1	01/01/2009	
Proceso 2	Subproceso 2.2	Uso de dispositivos móviles	Norma	1	01/01/2009	

ANEXO 23. FORMATO DE PASE A PRODUCCIÓN

FORMULARIO DE PASE A PRODUCCION

Tipo (plataforma) :		**Nro:**	000X
Aplicación o sistema :		**Fecha:**	

Descripción (Breve)

Nro. Requerimiento		**Tiempo estimado:**	
Nombre del archivo/programa			
Directorio de Origen (QA)			
Directorio de destino			
Fecha de Ejecución:		**Hora de ejecución:**	
		Tiempo utilizado:	

Observaciones :	
Documentos adicionales :	

	Nombre	**Cargo**	**Firma**
Solicitante			
Autorizante			
Responsable del Pase			

ANEXO 24. LOG DE TRANSACCIONES

SISTEMA	USER	COD	TIPO_ACCION	FECHA TRX	HORA TRX	TABLA_BD	CAMPO	DATO INICIAL	DATO FINAL
Sistema 1	User 1	TRX001	Creación	02/10/2012	10:00 AM	Cliente	DNI		46231430
Sistema 1	User 1	TRX002	Consulta	02/10/2012	10:04 AM	Cliente	DNI		
Sistema 1	User 1	TRX004	Actualización	02/10/2012	11:00 AM	Cliente	Nombre		Jose
Sistema 2	User 2	TRX005	Eliminación	02/10/2012	1:24 PM	Cliente	DNI		46231430
Sistema 2	User 3	TRX005	Actualización	02/10/2012	3:48 PM	Prestamos	Autorizado	NO	SI
Sistema 3	User 4	TRX007	Consulta	02/10/2012	6:12 PM	Prestamos	Cod_prestamo	6778802	
Sistema 3	User 5	TRX008	Actualización	02/10/2012	10:00 PM	Prestamos	Tasa	58	30
Sistema 3	User 6	TRX009	Actualización	02/10/2012	10:10 PM	Prestamos	Deuda	1000	50

ANEXO 25. REGISTRO DEL ESTADO DE LA RED

HOST	SERVICIO	ESTADO	ULTIMA REVISION	DURACION	INTENTO	INFORMACION DEL SERVICIO
Dev1	\Disk Usage	OK	01-11-2011 11:47:35	1d 23h 42m 21s	1/3	DISK OK – free space /6497 MB
	Backups: MySQL	CRITICAL	01-11-2011 11:47:18	2d 1h 45m 50s	3/3	CRITICAL: mysql_2011-01-02_07h00m. Wednwsdat.sdl.gz is too old (9d 4h 47m 16 s old)

ANEXO 26. REGISTRO DE EQUIPOS DE SEGURIDAD PERIMETRAL

Log del Firewall

Fecha	Hora	IP Origen	Puerto Origen	IP destino	Puerto Destino	Servicio	Protocolo	Regla	Acción
2011-02-14	12:28:53	10.10.3.21	53361	66.220.156.32	80	http	6	24	Block

Log de Navegación

Fecha	Hora	IP Origen	Usuario	Url destino	Categoría	Perfil de Navegación	Tiempo de Cnx	Acción
2011-02-14	12:28:53	10.10.3.21	atucno	www.foroi nformatica.com	Information Technology	PX_Gerencial	00h10m34s	Pass

Log de Antivirus

Fecha	Hora	Nombre de Archivo	Estado	Acción	Resultado	Severidad	IP de PC infectada
2011-02-14	12:28:53	Hostsystem.exe	Detectado	Eliminar	Falló	Alta	10.10.0.34

ANEXO 27. FORMATO DE ELIMINACIÓN SEGURA

FORMATO DE ELIMINACIÓN SEGURA DE INFORMACIÓN	
Tipo de Activo:	CD/DVD/HDD/Files
Información que contiene:	
Cantidad:	
Nombre del Propietario:	
Cargo del Propietario:	
Método de eliminación:	
Propietario de la Información	
Reconozco que, al completar este procedimiento, los datos ya no estarán disponibles, por lo cual asumo la responsabilidad de resguardar previamente cualquier dato, archivo o documento que necesite retener para utilización futura.	
Firma y sello:	
Responsable de la eliminación	
Certifico que la información de los activos antes descritos ha sido eliminada de forma segura de modo que no sea factible su recuperación.	
Firma y sello:	
Fecha de eliminación:	
Hora de eliminación:	

ANEXO 28. LOG DEL SERVICIO DE CORREO

Date	Time	From	To	Subject	Size	Attachment	Status
2011-04-12	10:34:55	operador@line.com	mcortez@ financieraabc.com	Acta de informe	2mb	Acta.doc	Clean

ANEXO 29. FORMATO DE ESPECIFICACIÓN DEL REQUERIMIENTO

DOCUMENTO DE ESPECIFICACIÓN DEL REQUERIMIENTO

CODIGO DE SOLICITUD:							
TIPO DE SOLICITUD:	Nuevo Desarrollo		Corrección de error		Optimización		
SOLICITANTE:							
ANALISTA FUNCIONAL:							

REQUISITOS FUNCIONALES

CODIGO	DESCRIPCION
RF01	
RF02	

REQUISITOS NO FUNCIONALES

TIPO	CODIGO	DESCRIPCION
SEGURIDAD		
RENDIMIENTO		
PORTABILIDAD		

CASOS DE USO

Código		
Nombre		
Actores		
Descripción		
Flujo Principal	Actor	Sistema
Flujo Alternativo	Actor	Sistema
Post Condición		
Referencia	RFxx	

ANEXO 30. CONTROLES DE APLICACIÓN

1. Controles de Entrada/salida

Objetivo: Asegurar que toda transacción que se vaya a procesar se reciba, procese y registre correcta y completamente. Estos controles deben asegurar que sólo se introduzca información válida y autorizada, y que estas transacciones sean procesadas una sola vez.

a. Controles de autorización de entrada de datos:

- Firmas en formularios por lotes
- Controles de acceso en línea
- Contraseñas
- Identificación del Terminal o de estación de trabajo
- Documentos Fuente

b. Controles de procesamiento por lote y balance:

- Valor monetario total
- Total de elementos
- Total de documentos
- Totales de comprobación (Hash Totals)

c. Controles de reporte y manejo de errores:

- Rechazar sólo las transacciones que tengan errores
- Rechazar todo el lote de transacciones
- Mantener el lote en espera
- Aceptar el lote y marcar las transacciones que contienen errores
- Registro de logs de transmisión

2. Controles de Procedimientos y Procesamiento

Objetivo: Garantizar la confiabilidad del procesamiento mediante programas de aplicaciones.

a. Técnicas de control de procesamiento para validar integridad y exactitud de datos acumulados:

- Recálculos manuales
- Totales de ejecución en ejecución (run-to-run totals)
- Verificación de razonabilidad de los valores calculados
- Verificación de límite sobre los valores calculados
- Reconciliación de los totales de los archivos
- Reportes de excepción
- Secuencia verificar
- Verificación de límites
- Verificación del rango
- Verificación de validez (validity check)
- Comprobación de razonabilidad

- Búsquedas en tabla
- Verificación de existencia
- Verificación de claves
- Dígito de control (check digit)
- Verificación de integridad (completeness check)
- Verificación de duplicados
- Verificación de relaciones lógicas

b. Controles sobre los archivos de datos:

- Mantenimiento y reportes de errores de manejo
- Retención de documentación fuente
- Etiquetado interno y externo
- Uso de versión
- Seguridad en archivos de datos
- Verificación individual

3. Controles de Salida

Objetivo: Proveer garantía de que los datos entregados a los usuarios sean presentados, formateados y entregados en una forma consistente y segura. Los controles de salida incluyen lo siguiente:

- Registro y almacenamiento de formularios negociables, sensibles y críticos en un lugar seguro.
- Generación automática de instrumentos negociables, formularios y firmas.
- Balance y conciliación
- Manejo de errores de salida
- Retención de reportes de salida
- Verificación de recepción de reportes

ANEXO 31. ACEPTACIÓN DEL USUARIO PARA PASE A PRODUCCIÓN

ACTA DE ACEPTACIÓN DEL USUARIO - PASE A PRODUCCIÓN					
Proyecto		Fecha		Hora	
Proceso		Nuevo		Update	
Solicitante				Gerencia	

Descripción del Pase a Producción

Observaciones		
A. Aprobado sin Observaciones		Revisor:
B. Aprobado con Observaciones no invalidantes		
C. No aprobado		Descripción de Observaciones:

Responsable Técnico	Solicitante o Usuario	Gerencia de Operaciones	Gerencia de Riesgos

ANEXO 32. LOG DE BACKUP

Cod Cinta	Fecha Backup	Servidor	Base de datos	Tabla	N° Registros Procesados	Hora inicio	Hora fin	Estado
C0010	13-03-2011	DOPSI05	SOPSI14	TCNT	38598	24:00	1:32	Successful

ANEXO 33. FORMATO DE CARGO DE RECEPCIÓN DE COPIAS DE RESPALDO

CARGO DE RECEPCION

Fecha:	
Hora:	
Código cintas:	

Personal que entrega:

Nombre:	
Cargo:	
Firma:	

Personal que recepciona:

Nombre:	
Cargo:	
Empresa:	
Firma:	

Ambas partes confirman que el motivo de la entrega/recepción de las cintas es por el motivo siguiente:

Motivo:	

ANEXO 34. INVENTARIO DE SOFTWARE

SOFTWARE INSTALADO				SOFTWARE LICENCIADO					
Fabricante	Nombre del Programa	Versión	Total de instalaciones	Licencias pre-instaladas	Licencias al por menor	Licencias por volumen	Otro tipo de licencias	Total Adquisiciones	Licencia Exceso/Déficit

ANEXO 35. BITÁCORA DE INCIDENTES DE SEGURIDAD

Bitácora de Incidentes de Seguridad										
Cod Incidente	Descripción del Incidente	Tipo	Vulnerabilidad	Severidad (Gravedad)	Fecha Inicio Incidente	Hora Inicio Incidente	Fecha Fin Incidente	Hora Fin Incidente	Acciones Tomadas	Impacto Final

ANEXO 36. FORMATO DE COMUNICACIÓN DE INCIDENTES DE SEGURIDAD

Registro de Incidencias
FORMATO FRISI

Fecha de Reporte		Hora de Reporte	

DATOS DEL USUARIO QUE REPORTA EL INCIDENTE			
Nombres y Apellidos:		Cargo:	
		Departamento/Área:	

INFORMACIÓN DEL INCIDENTE			
Fecha que observó el incidente:		Hora que observó el incidente:	

MARQUE CON UNA X TODOS LOS ENUNCIADOS QUE CONSIDERE APLICABLES:

	Robo o pérdida de información confidencial		Denegación de servicio
	Modificación o eliminación no autorizada de datos.		Ingeniería social, fraude, pishing
	Divulgación no autorizada de información personal.		Interrupción prologangada en un sistema o servicio de red.
	Eliminación insegura de información		Uso indebido de los servicios, información o activos
	Robo o pérdida de un recurso informático.		Acceso o intento de acceso no autorizado a un sistema informatico
	Daños a los activos de TI físicos		Detección de intrusos
	Mal funcionamiento de un recurso informático.		Modificación. Instalación o eliminación no autorizada de software.
	Ataque o infección por código malicioso		Otro no contemplado:
	Reportes de comportamientos inusuales del sistema		

Descripción del incidente
¿Cómo detectó el incidente?

¿El incidente está aún en progreso?	Si		No		
Tiempo estimado de duración del incidente:					
Personas que han accedido al sistema afectado desde que se detectó el incidente:					

INFORMACIÓN SOBRE EL ACTIVO AFECTADO	
Sistema, computadora o red afectada:	Localización Física:
Describa brevemente la informacion contenida en el sistema/computador:	Sistema Operativo:

¿Existe copia de respaldo de los datos/software afectado?	Si		No		
¿El recurso afectado tiene conexión a la red de [LA ORGANIZACIÓN]	Si		No		
¿El recurso afectado tiene conexión a Internet?	Si		No		

OBSERVACIONES O COMENTARIOS ACERCA DE LA INCIDENCIA O EL REPORTE

ELABORADO POR:

RECIBIDO POR:

ANEXO 37. FORMATO PARA LAS MÉTRICAS

FORMATO: DEFINICION DE METRICAS DE EFECTIVIDAD DE SEGURIDAD DE INFORMACIÓN	
DOMINIO	Dominio al que pertenece el control a medir
CONTROL	Control a medir
METRICA ID	Identificador de la métrica
OBJETIVO	Objetivo que la métrica soporta
PREGUNTA	Describe en formato de pregunta qué está midiendo la métrica
METRICA(S)	Sentencia de la métrica
FRECUENCIA(S)	Cada cuánto tiempo se medirá la métrica
FORMULA(S)	Fórmula para calcular la métrica
RESPONSABLE	Persona responsable de obtener la data para la medición

ANEXO 38. CUESTIONARIO PARA IDENTIFICAR NO CONFORMIDADES

Indicaciones:

a. Si la respuesta a una pregunta es "Implementado", deberá proporcionar: una breve descripción de la implementación, en la sección "Comentarios", y adjuntar las evidencias que sustentan la respuesta.

b. Si la respuesta a una pregunta es "No implementado", deberá indicar las razones de tal situación, en la sección "Comentarios", y de ser el caso, adjuntar el plan de trabajo detallado con actividades, fechas y responsables. Asimismo, deberá adjuntar evidencia documentaria de los avances.

c. Si la respuesta a una pregunta es "No aplica", debe indicar las razones que sustentan su no aplicabilidad, en la sección "Comentarios".

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
01. Políticas y organización del SGSI	1 - 001. La empresa cuenta con políticas de seguridad de la información aprobadas por el directorio u órgano equivalente.							
	2 - 002. Las políticas de seguridad de la información son revisadas periódicamente y ante cambios importantes en el ambiente operativo o informático.							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÓN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	3 - 003. Todas las responsabilidades de seguridad de la información se encuentran establecidas como parte de la descripción de puestos de trabajo							
	4 - 004. La gerencia general aprueba un presupuesto anual para la gestión de la seguridad de la información.							
	5 - 005. La gerencia general recibe reportes periódicos del cumplimiento de las políticas de seguridad de la información.							
	6 - 006. Las funciones de gestión de la seguridad de la información se encuentran asignadas formalmente.							
	7 - 007. La empresa ha implementado una metodología de gestión de riesgos de seguridad de la información, que incluye las etapas de: identificación, evaluación, control, reporte y monitoreo de riesgos.							
	8 - 008. La empresa realiza evaluaciones de riesgos de seguridad de la información periódicamente o							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	ante cambios importantes en el ambiente operativo o informático							
	9 - 009. Los resultados de la evaluación de riesgos de seguridad de la información son incorporados en la gestión de los riesgos operacionales de la empresa.							
	10 - 010. El sistema de gestión de seguridad de la información es sometido a una revisión periódica independiente.							
	11 - 011. Los contratos y acuerdos con terceros, que implican acceso, comunicación o procesamiento de información de la empresa, incluyen cláusulas de seguridad de la información.							
02. Gestión de activos	1 - 012. La empresa mantiene inventarios actualizados tanto de activos de información como de tecnología de la información.							
	2 - 013. Se han designado los propietarios de los activos de							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	información y de tecnología de la información.							
	3 - 014. La empresa ha establecido procedimientos para asegurar el uso aceptable de la información y los activos relacionados a los medios de procesamiento de la información.							
	4 - 015. La empresa ha implementado medidas de control acorde con los niveles de riesgo asociados a la clasificación de la información.							
03. Seguridad de personal	1 - 016. El proceso de selección de personal incluye verificaciones de los antecedentes, perfil personal y profesional de los candidatos.							
	2 - 017. Existe un proceso disciplinario formal para los empleados que cometan una infracción de seguridad de la información							
	3 - 018. La empresa ha implementado un proceso para la finalización de la relación laboral con empleados propios y de terceros relevantes							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	4 - 019. El proceso de finalización de la relación laboral incluye la devolución de activos asignados al personal para el desempeño de sus funciones.							
	5 - 020. El proceso de finalización de la relación laboral incluye la verificación de que los permisos de acceso a la información y recursos de procesamiento de información asignados han sido deshabilitados.							
	6 - 021. La empresa desarrolla actividades de capacitación y difusión hacia todo el personal para promover la cultura de la seguridad de la información							
	7 - 022. El personal encargado de la gestión de la seguridad de la información es capacitado continuamente.							
	8 - 023. La empresa firma acuerdos de confidencialidad de la información con empleados propios y de terceros relevantes.							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	9 - 024. Se han implementado políticas de escritorio limpio para papeles y medios de almacenamiento removibles.							
04. Seguridad lógica	1 - 025. Se han implementado procedimientos de administración de accesos de usuarios a los sistemas informáticos.							
	2 - 026. Se ha implementado un proceso formal de revisión periódica de los derechos de acceso a los sistemas informáticos.							
	3 - 027. Se han implementado controles para la selección y uso de contraseñas para el acceso a los sistemas informáticos.							
	4 - 028. Se han implementado controles automáticos para prevenir accesos no autorizados en caso de equipos informáticos desatendidos.							
	5 - 029. Se han implementado controles y procedimientos para el acceso de usuarios remotos							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	6 - 030. Se han implementado controles respecto al acceso físico y lógico a puertos de diagnóstico y de configuración de los equipos de cómputo.							
	7 - 031. Los usuarios de los sistemas informáticos y el personal del área de sistemas se encuentran segregados en las redes internas de la empresa							
	8 - 032. Se han implementado controles y procedimientos para restringir el acceso de los empleados a redes compartidas, conforme a las políticas definidas por la empresa.							
	9 - 033. Los empleados tienen un identificador personal para sus accesos a los sistemas informáticos, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.							
	10 - 034. Se han implementado controles y procedimientos para el uso de programas utilitarios capaces de eludir los controles de sistemas y							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	aplicación.							
	11 - 035. Se han implementado controles automáticos que desactiven las sesiones tras un período definido de inactividad.							
05. Seguridad física y ambiental	1 - 036. La empresa ha definido perímetros de seguridad para establecer medidas de protección de la información y de los recursos de procesamiento							
	2 - 037. La empresa ha implementado controles de acceso físico a los ambientes que resguardan los recursos de procesamiento de información.							
	3 - 038. Se han implementado controles de seguridad para los ambientes que resguardan los recursos de procesamiento de información, frente a incendios, inundaciones, explosiones y otros eventos adversos.							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	4 - 039. Se han definido lineamientos para el resguardo de los recursos de procesamiento de información cuando se realizan trabajos en las zonas incluidas en los perímetros de seguridad.							
	5 - 040. Los equipos usados para almacenar, procesar o transmitir información se encuentran protegidos contra fallos de energía u otras anomalías relacionadas al suministro eléctrico							
	6 - 041. Se ejecutan procedimientos periódicos de mantenimiento de los equipos de almacenamiento, procesamiento y transmisión de información							
	7 - 042. Se han implementado medidas de seguridad adicionales para los equipos que se utilizan fuera de los locales de la empresa, de acuerdo a los riesgos a los que se encuentran expuestos.							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
06. Seguridad de las operaciones y comunicaciones	1 - 043. Se cuenta con procedimientos actualizados de operaciones de los sistemas informáticos.							
	2 - 044. Se cuenta con procedimientos para controlar los cambios en la infraestructura tecnológica del ambiente de producción de los sistemas informáticos.							
	3 - 045. Se han segregado las funciones del personal para reducir el riesgo de uso accidental o mal uso de los recursos de procesamiento de información							
	4 - 046. Se han implementado controles para separar los entornos de desarrollo, prueba y producción.							
	5 - 047. Se realizan revisiones periódicas de los controles de seguridad de información implementados en los procesos de tecnología de información subcontratados							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	6 - 048. Se realiza el monitoreo y revisión de los niveles de servicio acordados en los procesos de tecnología de información subcontratados, para asegurar su cumplimiento							
	7 - 049. Se monitorea el uso de las capacidades de procesamiento, y sus resultados se incorporan en los requerimientos de capacidad futuros.							
	8 - 050. Se ha implementado un proceso de certificación para el ingreso a producción de nuevos sistemas informáticos o actualizaciones.							
	9 - 051. Se han implementado controles para la prevención, detección y recuperación de ataques de código malicioso.							
	10 - 052. Se generan copias de respaldo de la información y software esenciales para el negocio, en concordancia con el Plan de recuperación de los servicios de							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÓN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	tecnología de información.							
	11 - 053. Se prueban regularmente las copias de respaldo generadas							
	12 - 054. Se han implementado procedimientos de administración y monitoreo de redes, y controles de seguridad para prevenir accesos externos no autorizados							
	13 - 055. Se han establecido acuerdos de niveles de servicio con los proveedores de servicios de red que incluyan criterios de seguridad de la información							
	14 - 056. Se han implementado procedimientos para la gestión de medios removibles de almacenamiento de información, incluyendo su eliminación cuando ya no son requeridos.							
	15 - 057. La documentación de los sistemas informáticos se encuentra protegida ante accesos no							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	autorizados.							
	16 - 058. Se han implementado procedimientos y controles para proteger el intercambio de información que se realice a través de medios electrónicos							
	17 - 059. Los servicios de banca electrónica implementados por la empresa cuentan con controles de autenticación, autorización, confidencialidad e integridad							
	18 - 060. Para operaciones de transferencia a terceros por Internet, ha implementado el uso de dos factores de autenticación, uno de los cuales es de generación o asignación dinámica.							
	19 - 061. Para operaciones de transferencia a terceros por canales electrónicos diferentes a Internet ha implementado el uso de dos factores de autenticación.							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	20 - 062. La integridad de la información accesible a través de redes públicas se encuentra protegida para prevenir modificaciones no autorizadas.							
	21 - 063. Se cuenta con registros estandarizados de auditoría, que incluyen las actividades de los usuarios, errores en el sistema y eventos de seguridad de la información, con el fin de utilizarlos periódicamente en el monitoreo y revisión de accesos.							
	22 - 064. Se han implementado procedimientos de monitoreo del uso de los recursos de procesamiento de información, así como de la revisión regular de sus resultados, según el nivel de riesgo asociado.							
	23 - 065. Los registros de auditoría, así como el hardware y software que soportan su generación y almacenamiento, son protegidos contra la manipulación y accesos no							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	autorizados.							
	24 - 066. Se han implementado procedimientos de respuesta ante errores reportados por usuarios o programas informáticos							
	25 - 067. Se realizan pruebas de intrusión y evaluaciones de vulnerabilidad orientadas a probar los controles de seguridad implementados en los sistemas informáticos.							
07. Seguridad en el desarrollo	1 - 068. Los requerimientos de nuevos sistemas informáticos o mejoras a sistemas existentes incluyen los requisitos y controles de seguridad a implementar.							
	2 - 069. Las aplicaciones críticas de la empresa validan los datos de entrada para asegurar que sean correctos y adecuados, de conformidad con la metodología y/o estándares de desarrollo de sistemas de la empresa.							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	3 - 070. Las aplicaciones críticas de la empresa realizan validaciones para evitar la pérdida de integridad de datos por errores de procesamiento o actos deliberados, de conformidad con la metodología y/o estándares de desarrollo de sistemas de la empresa.							
	4 - 071. Las aplicaciones validan los datos de salida para asegurar que el procesamiento de la información almacenada es correcto y apropiado, de conformidad con la metodología y/o estándares de desarrollo de sistemas de la empresa.							
	5 - 072. Se han implementado políticas para el uso de controles criptográficos, designando la responsabilidad de evaluar su aplicación y asegurar la implantación.							
	6 - 073. La empresa ha implementado procedimientos para la selección, protección y control de datos de prueba, en caso se utilice información de carácter confidencial.							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	7 - 074. El acceso a los programas fuente está controlado, siendo permitido previa autorización y de acuerdo a un procedimiento formal.							
	8 - 075. Se ha implementado un procedimiento de control de cambios en aplicaciones y en el ambiente operacional.							
	9 - 076. La empresa supervisa y monitorea el desarrollo de software encargado a terceros.							
08. Gestión de incidentes	1 - 077. Se ha implementado un procedimiento para reportar incidentes de seguridad de la información.							
	2 - 078. Se ha implementado un procedimiento para reportar las debilidades de seguridad de la información cuando son identificadas.							
	3 - 079. Se han establecido procedimientos para la atención de incidentes de seguridad de la información.							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÒN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	4 - 080. Se ha implementado un procedimiento de registro y revisión de los incidentes de seguridad de la información ocurridos							
09. Cumplimiento Normativo	1 - 081 Se han identificado los requerimientos legales, contractuales, o de regulación que la empresa debe cumplir.							
	2 - 082 Los requerimientos legales, contractuales, o de regulación se han incorporado en la lógica interna de las aplicaciones informáticas.							
10. Privacidad de la Información	1 - 083 Se han adoptado medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios.							
***Temas relacionados**	1 - La empresa ha contratado pólizas de seguros que les permiten cubrir las pérdidas asociadas a transacciones no autorizadas que se realicen con tarjetas de crédito, débito y banca por internet (a favor de la empresa).							

DOMINIO	PREGUNTA	IMPLEMENTADO	NO IMPLEMENTADO	NO APLICABLE	COMENTARIOS	ACCIONES	TIPO DE ACCIÓN (CORRECTIVA/PREVENTIVA)	RESPONSABLE
	2 - La empresa cuenta con fondos de cobertura propios (o similares) que le permite cubrir las pérdidas asociadas a transacciones no autorizadas que se realicen con tarjetas de crédito, débito y banca por internet (a favor de la empresa).							
	3 - La empresa pone a disposición de sus clientes seguros de empresas licenciadas en el país para la cobertura de riesgos asociados a transacciones no autorizadas que se realicen con tarjetas de crédito, débito y banca por internet.							
	4 - Se ha iniciado un proyecto de adecuación al estándar PCI DSS("Normas de Seguridad de Datos de la Industria de Tarjetas de Pago")							
	5 - Se ha iniciado un proyecto para la incorporación del uso de chips en las tarjetas de crédito y débito.							

ANEXO 39. INVENTARIO DE FUENTES DE INFORMACIÓN CLAVE

Proceso	Entidad externa o cliente	Entrega /Recepción	Descripción	Clasificación de la información	Medio de transmisión o intercambio	Periodicidad	Área responsable
Cierre contable	SBS	Se Entrega	Anexo 14 – archivo xls	Confidencial	FTP	Diario	Contabilidad
Captaciones	Proveedor A	Se Recibe		Uso Interno	Cinta	Semanal	Negocios
Créditos	Asbanc			Pública	Correo	Quincenal	
	BCR				CD	Anual	
					Internet	Ocasional	

ANEXO 40. PLANTILLA DE DEFINICIÓN DE LA ESTRUCTURA ORGANIZACIONAL

Tipo de Compañía	Banco/Financiera/Microfinanciera/Caja/Edpyme
Tamaño de la Compañía	N°Trabajadores:
	N°Sucursales:
Presupuesto	
Rol del Responsable de Seguridad	Funciones a desempeñar: a) b) c) d)
Benchmarking **¿Dónde está ubicada la SI en**	Entidad 1: Situación:

otras entidades?	
	Entidad 2: Situación:
	Entidad 3: Situación:
Otros factores a considerar	
Propuesta 1	

ANEXO 41. MATRIZ DE EVALUACIÓN DE PROCESOS

MATRIZ DE EVALUACION DE PROCESOS

			¿Se podría generar una estafa, operación fraudulenta o algún otro tipo de apropición indebida?.	¿Podrían se las relaciones con los socios de negocios, proveedores, etc. Impactadas negativamente?	¿Sería dañada la reputación antes los clientes?.	¿Podría perderse una ventaja competitiva y/o información propietaria sobre los procesos del negocio?.	¿Se podria producir un efecto directo de disminución de ingresos y/o aumento de costos?.	¿Se podría ver afectada la confidencialidad de otros activos de información?.	¿Podrían romperse o violarse obligaciones legales, regulatorias o contractuales?.	¿Podrían generase inexactitudes en los estados financieros u otros reportes relacionados al proceso?.	Cómo resultado de la modificación de la información ¿Podrían perderse relacionaciones comerciales, negocios, contratos de servicios, etc.?.	¿Podrían tomarse decisiones de negocios errradas?.	¿Podrían verse interrumpidas y/o demoradas las operaciones?.	¿Podría publicarse información errada (tasas y tarifarios, políticas, etc.)?.	¿Se podría afectar a un proceso crítico del negocio (que no puede ser demorado)?.	¿Podría afectarse la capacidad de proveer productos y servicios de tal manera que a lo largo del tiempo se vea deteriorada la base de datos?.	¿Se podría afectar el correcto funcionamiento de otros sistemas, procesos y/o provisión de otros productos y servicios?.	
Criterio de Seguridad de la Información -->			CONFIDENCIALIDAD						INTEGRIDAD						DISPONIBILIDAD			CRITICIDAD
P101	1.	**Macroproceso de Créditos**																
P102	1.1.	Proceso de Promoción	0	0	0	0	1	0	1	1	0	0	1	0	1	0	1	2.0
P103	1.2.	Proceso de Captación	0	0	1	1	0	1	0	0	1	1	1	0	0	0	0	2.0
P104	1.3.	Proceso de Evaluación	1	1	1	0	0	0	1	1	1	1	0	1	1	1	1	3.7
P105	1.4.	Proceso de Aprobación	1	1	1	0	1	0	0	0	0	0	1	1	1	0	0	2.3
P106	1.5.	Proceso de Desembolso	0	1	1	0	1	1	0	0	0	1	1	0	0	1	0	2.3
P108	2	**Macroproceso de...**																

Criticidad del Proceso	
1	Baja
2	Baja
3	Media
4	Alto
5	Alto

APENDICE: CIRCULAR G-140

Lima, 02 de abril de 2009

CIRCULAR Nº G-140-2009

Ref.: Gestión de la seguridad de la información

Señor
Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 del artículo 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley Nº 26702 y sus modificatorias en adelante Ley General, y por el inciso d) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones, aprobado por Decreto Supremo N° 054-97-EF, con la finalidad de establecer criterios mínimos para una adecuada gestión de la seguridad de la información, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones, las cuales toman como referencia estándares internacionales como el ISO 17799 e ISO 27001, disponiéndose su publicación en virtud de lo señalado en el Decreto Supremo N° 001-2009-JUS:

Alcance
Artículo 1º.- La presente Circular será de aplicación a las empresas señaladas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., y las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Definiciones
Artículo 2º.- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

a. Evento: Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

b. Factor de autenticación: Información utilizada para verificar la identidad de una persona. Pueden clasificarse de la siguiente manera:
   - Algo que el usuario conoce (por ejemplo: una clave de identificación)
   - Algo que el usuario posee (por ejemplo: una tarjeta)
   - Algo que el usuario es (por ejemplo: características biométricas)

c. Incidente de seguridad de información: Evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

d. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.

e. Ley General: Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus modificatorias.

f. Seguridad de la información: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad, definidos de la siguiente manera:

   I. Confidencialidad: La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
   II. Integridad: La información debe ser completa, exacta y válida.
   III. Disponibilidad: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

g. Subcontratación: Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizado por la empresa contratante.

h. Subcontratación significativa: Aquella subcontratación que, en caso de falla o suspensión del servicio, puede poner en riesgo importante a la empresa, al afectar sus ingresos, solvencia, o continuidad operativa.

Sistema de gestión de la seguridad de la información

Artículo 3º.- Las empresas deberán establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI).

Las actividades mínimas que deben desarrollarse para implementar el SGSI, son las siguientes:

a. Definición de una política de seguridad de información aprobada por el Directorio.
b. Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.
c. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

Estructura organizacional

Artículo 4°.- Las empresas deben contar con una estructura organizacional que les permita implementar y mantener el sistema de gestión de la seguridad de información señalado en el artículo anterior.

Asimismo, deben asegurarse que se desarrollen las siguientes funciones, ya sea a través de una unidad especializada o a través de alguna de las áreas de la empresa:

a. Asegurar el cumplimiento de la política de seguridad de información y de la metodología definida por la empresa.
b. Coordinar y monitorear la implementación de los controles de seguridad de información.
c. Desarrollar actividades de concientización y entrenamiento en seguridad de información.
d. Evaluar los incidentes de seguridad de información y recomendar acciones apropiadas.

La Superintendencia podrá requerir la creación de una unidad especializada en gestión de la seguridad de información en empresas que a su criterio resulten complejas, y cuando se observe en el ejercicio de las acciones de supervisión que no se cumple con los criterios previstos en la normativa vigente.

Controles de seguridad de información
Artículo 5°.- Como parte de su sistema de gestión de la seguridad de información, las empresas deberán considerar, como mínimo, la implementación de los controles generales que se indican en el presente artículo.

5.1 Seguridad lógica

a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.
b) Revisiones periódicas sobre los derechos concedidos a los usuarios.
c) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.
d) Controles especiales sobre utilidades del sistema y herramientas de auditoría.
e) Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.
f) Controles especiales sobre usuarios remotos y computación móvil.

5.2 Seguridad de personal

a) Definición de roles y responsabilidades establecidos sobre la seguridad de información.
b) Verificación de antecedentes, de conformidad con la legislación laboral vigente.
c) Concientización y entrenamiento.
d) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.
e) Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos.

5.3 Seguridad física y ambiental

a) Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.
b) Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales.

5.4 Inventario de activos y clasificación de la información

a) Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.
b) Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

5.5. Administración de las operaciones y comunicaciones

a) Procedimientos documentados para la operación de los sistemas.
b) Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.
c) Separación de funciones para reducir el riesgo de error o fraude.
d) Separación de los ambientes de desarrollo, pruebas y producción.
e) Monitoreo del servicio dado por terceras partes.
f) Administración de la capacidad de procesamiento.
g) Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.
h) Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.
i) Seguridad sobre el intercambio de la información, incluido el correo electrónico.
j) Seguridad sobre canales electrónicos.
k) Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.

5.6. Adquisición, desarrollo y mantenimiento de sistemas informáticos

Para la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.
b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.
c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.
d) Controlar el acceso a las librerías de programas fuente.
e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.
f) Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.

5.7. Procedimientos de respaldo

a) Procedimientos de respaldo regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad de negocios de la empresa.

b) Conservar la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación del centro principal de procesamiento.

5.8. Gestión de incidentes de seguridad de información

Para asegurar que los incidentes y vulnerabilidades de seguridad sean controlados de manera oportuna, las empresas deberán considerar los siguientes aspectos:

a) Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.
b) Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

5.9. Cumplimiento normativo

Las empresas deberán asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

5.10. Privacidad de la información

Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la normatividad vigente sobre la materia.

Seguridad en operaciones de transferencia de fondos por canales electrónicos
Artículo 6°.- En el caso de las operaciones de transferencia de fondos a terceros ofrecidas por las empresas para su realización a través de canales electrónicos, las empresas deberán implementar un esquema de autenticación de los clientes basado en dos factores como mínimo. Para el caso en que el canal electrónico sea Internet, uno de los factores de autenticación deberá ser de generación o asignación dinámica. Las empresas podrán utilizar otros factores de autenticación, en tanto éstos proporcionen un nivel de seguridad equivalente o superior respecto a los dos factores señalados, en particular cuando se trate de operaciones importantes según los límites que el banco determine de acuerdo a las características del producto o servicio ofrecido.

La empresa deberá tomar en cuenta los riesgos operacionales asociados, en el diseño de los procedimientos, las definiciones de límites y las consideraciones de seguridad e infraestructura requeridas para un funcionamiento seguro y apropiado en las operaciones de transferencia de fondos.

Subcontratación
Artículo 7º.- Las empresas son responsables y deben verificar que se mantengan las características de seguridad de la información contempladas en la presente norma, incluso cuando ciertas funciones o procesos puedan ser objeto de una subcontratación. Para ello se tendrá en cuenta lo dispuesto en el artículo 21° del Reglamento de la Gestión Integral de Riesgos. Asimismo, las empresas deben asegurarse que el procesamiento y la información objeto de la subcontratación, se encuentre efectivamente aislada en todo momento.

En caso que las empresas deseen realizar una subcontratación significativa de su procesamiento de datos, de tal manera que éste sea realizado en el exterior, requerirán de la autorización previa y expresa de la Superintendencia. Para ello, la empresa debe asegurar un adecuado cumplimiento de la presente Circular, en lo que sea aplicable al servicio de procesamiento contratado.

La Superintendencia podrá requerir cuando así lo considere apropiado que el proveedor del servicio en el exterior se encuentre sujeto a una supervisión efectiva por parte de la autoridad supervisora del país en el cual se brindará dicho servicio.

En el Anexo A que forma parte de la presente norma y se publica en el Portal electrónico institucional (www.sbs.gob.pe), conforme a lo dispuesto en el Decreto Supremo N° 001-2009-JUS, se detalla la información que debe remitir la empresa adjunta a su solicitud de autorización. Una vez recibida la documentación completa, dentro de un plazo que no excederá de sesenta (60) días útiles, la Superintendencia emitirá la resolución que autoriza o el oficio que deniega la solicitud presentada por la empresa.

Las empresas que obtengan la autorización para realizar su procesamiento de datos en el exterior, deberán asegurar, con una frecuencia anual, que el servicio subcontratado sea sometido a un examen de auditoría independiente, por una empresa auditora de prestigio, que guarde conformidad con el estándar SAS 70 emitido por el Instituto Americano de Contadores Públicos Certificados (AICPA). En tal sentido, las empresas deberán remitir a la Superintendencia el Reporte de Auditoría de Tipo II considerado en dicho estándar, el cual entre otros aspectos considera la evaluación de los controles implementados y las pruebas de su efectividad.

Información a la Superintendencia
Artículo 8°.- Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por el Reglamento para la gestión del riesgo operacional, emitido por la SBS, las empresas deberán incluir información sobre la gestión de la seguridad de la información.

Información adicional
Artículo 9°.- La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de la gestión de la seguridad de la información de la empresa.

Asimismo, la empresa deberá tener a disposición de la Superintendencia todos los documentos a que hace mención la presente Circular, así como la información de auditoría o revisiones realizadas por la casa matriz en caso de ser aplicable.

Sanciones
Artículo 10°.- En caso de incumplimiento de las disposiciones contenidas en la presente norma, la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Vigencia
Artículo 11°.- Las disposiciones de la presente Circular entran en vigencia al día siguiente de su publicación en el Diario Oficial "El Peruano", otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de marzo de 2010, fecha a partir de la cual quedará sin efecto la Circular SBS Nº G-105-2002.

Adecuación de las AFP
Artículo 12°.- En un plazo que no excederá de noventa (90) días calendario de haberse publicado la presente Circular, las AFP deberán remitir a la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

Dicho plan deberá incluir un diagnóstico de la situación existente en la AFP respecto al cumplimiento de cada uno de los artículos de la presente Circular, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Atentamente,

FELIPE TAM FOX
Superintendente de Banca, Seguros y

Administradoras Privadas de Fondos de Pensiones

ANEXO A

DOCUMENTACIÓN A REMITIR JUNTO CON LA SOLICITUD DE AUTORIZACIÓN PARA REALIZAR PROCESAMIENTO PRINCIPAL EN EL EXTERIOR

Documento	Contenido mínimo requerido
1. Información general del proveedor y del servicio	• Razón social del proveedor. • Giro del negocio y años de experiencia. Indicar a qué empresas brinda servicios actualmente. • Estados Financieros del proveedor correspondientes a los dos últimos años. • Relación de accionistas del proveedor y funcionarios principales. • Relación con la empresa supervisada (indicar si pertenecen al mismo grupo económico). • Servicios que serán provistos por el proveedor y el tipo de información a ser procesada. • Ubicación (país y ciudad) del centro de procesamiento principal. • Razones para seleccionar al proveedor.
2. Borrador del Contrato	Aspectos a considerar: • Acuerdos de niveles de servicio. • Procedimientos de monitoreo. • Procedimientos de contingencia. • Cumplimiento de las normas sobre secreto bancario y confidencialidad de la información. • Prestación del servicio en regímenes especiales (vigilancia, intervención, liquidación). El proveedor debe seguir brindando el servicio como mínimo un año después de que la empresa ha ingresado a un régimen especial. • Compromiso de cumplimiento de la normativa de la Superintendencia. • Aseguramiento del acceso adecuado a la información con fines de supervisión, en tiempos razonables y a solo requerimiento, por parte de la Superintendencia, Auditoría Interna y Externa, en condiciones normales de operación y en regímenes especiales. Este aspecto debe ser aplicable sobre cualquier otra empresa que el proveedor subcontrate para brindar servicios a la entidad supervisada. • Cláusulas que faciliten una adecuada revisión por parte de la Unidad de Auditoría Interna, la Sociedad de Auditoría Externa y la Superintendencia.
3. Informe de la Plataforma Tecnológica	Aspectos a considerar: (Señalar qué equipos y aplicaciones estarán a cargo del proveedor) • Inventario de equipos de cómputo. • Inventario de software base. • Herramientas y/o manejadores de base de datos. • Aplicaciones críticas. • Esquema de comunicaciones a ser implementado entre el proveedor y la empresa supervisada.
4. Informe de Comunicación con la	• Descripción de la forma de envío de información a la Superintendencia luego de que se implemente el servicio de procesamiento en el exterior. Asimismo, indicar los cambios que se aplicarán sobre los procedimientos asociados a la

Superintendencia (SUCAVE, RCD, otros)	generación, consolidación y reporte de dicha información.
5. Informe de Evaluación de Riesgos	• Evaluación de los riesgos de operación asociados con el esquema propuesto por la empresa, realizada por la Unidad de Riesgos.
6. Gestión de la seguridad de información	• Política de seguridad de información de la empresa. • Estructura organizativa para la gestión de la seguridad de información. • Asignación de responsabilidades asociadas con la seguridad de información en la entidad y el proveedor. • Forma en que se aislará el procesamiento y la información objeto de la subcontratación. • Procedimientos y controles a implementar, considerando el procesamiento en el exterior, en los siguientes aspectos: - Seguridad lógica. - Seguridad de personal. - Seguridad física y ambiental. - Administración de las operaciones y comunicaciones. - Desarrollo y mantenimiento de los sistemas informáticos. - Administración de las copias de respaldo.
7. Gestión de continuidad de negocios	• Plan de Contingencia del proveedor, para asegurar la continuidad del servicio de procesamiento informático. • Señalar la prioridad asignada al procesamiento de la información de la empresa supervisada respecto al resto de clientes del proveedor. • Señalar la forma en que se dará aviso a la empresa supervisada, y las acciones que deberá desarrollar la empresa en caso de una contingencia en el proveedor. • Frecuencia y alcance de las pruebas al Plan de Contingencia del proveedor.
8. Plan de Auditoría de Sistemas	• Señalar el alcance, forma y periodicidad de las revisiones de auditoría de sistemas considerando el nuevo esquema de procesamiento principal de la empresa.
9. Gestión del proyecto	• Cronograma de actividades, incluyendo plazos, responsables y principales hitos de control. • Costo estimado de implementación del proyecto.