Dirección General de los Estudios de Postgrado
Área de Ciencias Administrativas y de Gestión
Programa de Postgrado en Gerencia de Proyectos

UNIVERSIDAD CATOLICA ANDRES BELLO

VICERECTORADO ACADEMICO

ESTUDIOS DE POSTGRADO

AREA DE CIENCIAS ADMINISTRATIVAS Y DE GESTION

POSTGRADO EN GERENCIA DE PROYECTOS

TRABAJO ESPECIAL DE GRADO

DISEÑO DE UN MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27001 PARA ATENDER RIESGOS TECNOLÓGICOS EN LOS PROCESOS DE NEGOCIO DE BANDES

Presentado por

Raúl Antonio Hernández Chirinos

Para optar al título de:

Especialista en Gerencia de Proyectos

Asesor:

José Gregorio Durán Cáceres

Caracas, Enero de 2013

UNIVERSIDAD CATOLICA ANDRES BELLO
VICERECTORADO ACADEMICO
ESTUDIOS DE POSTGRADO
AREA DE CIENCIAS ADMINISTRATIVAS Y DE GESTION
POSTGRADO EN GERENCIA DE PROYECTOS

TRABAJO ESPECIAL DE GRADO

DISEÑO DE UN MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27001 PARA ATENDER RIESGOS TECNOLÓGICOS EN LOS PROCESOS DE NEGOCIO DE BANDES

Presentado por

Raúl Antonio Hernández Chirinos

Para optar al título de:

Especialista en Gerencia de Proyectos

Asesor:

José Gregorio Durán Cáceres

Caracas, Enero de 2013

CARTA DE ACEPTACION DEL ASESOR

Por la presente hago constar que he leído el Trabajo Especial de Grado, presentado por el ciudadano Raúl Antonio Hernández Chirinos, para optar al grado de Especialista en Gerencia de Proyectos, cuyo Título es: "**DISEÑO DE UN MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27001 PARA ATENDER RIESGOS TECNOLÓGICOS EN LOS PROCESOS DE NEGOCIO DE BANDES**"; y manifiesto que cumple con los requisitos exigidos por la Dirección General de los Estudios de Postgrado de la Universidad Católica Andrés Bello: y que, por lo tanto, lo considero apto para ser evaluado por el jurado que se decida designar a tal fin.

En la ciudad de Caracas a los 14 días del mes de Enero de 2013

José Gregorio Durán Cáceres
C.I.: 6.966.456

Gerencia Ejecutiva de Resguardo Institucional

Caracas, 14 de Enero de 2013

Sres.
UNIVERSIDAD CATOLICA ANDRES BELLO
Post grado de Gerencia de Proyectos
Caracas.-

Nos dirigimos a ustedes, para informarles, que hemos autorizado al Licenciado en Computación Raúl Antonio Hernández Chirinos; C.I.: V-15.395.013, quien labora en esta organización, a hacer uso de la información proveniente de esta institución, para documentar y soportar los elementos de los distintos análisis estrictamente académicos que conllevarán a la realización del Trabajo Especial de Grado "**DISEÑO DE UN MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ISO 27001 PARA ATENDER RIESGOS TECNOLÓGICOS EN LOS PROCESOS DE NEGOCIO DE BANDES**", como requisito para optar al título de Especialista en Gerencia de Proyectos, exigidos por la Dirección General de los estudios de post grado de la Universidad Católica Andrés Bello. Sin más a que hacer referencia, atentamente,

Leida Maribal Artigas León
Gerente Ejecutiva de Resguardo Institucional

Dirección General de los Estudios de Postgrado
Área de Ciencias Administrativas y de Gestión
Programa de Postgrado en Gerencia de Proyectos

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE CIENCIAS ADMINISTRATIVAS Y DE GESTIÓN
POSTGRADO EN GERENCIA DE PROYECTOS

Diseño de un modelo de Sistema de Gestión de Seguridad de la Información basado en ISO 27001 para atender Riesgos Tecnológicos en los procesos de Negocio de Bandes

Autor: Raúl A. Hernández Ch.
Tutor: José G. Durán C.
Año: 2013

RESUMEN

Los activos de información juegan un papel fundamental para el éxito y la continuidad en el mercado de cualquier organización. En la actualidad, los sistemas de información que soportan los procesos de negocio están expuestos a un número cada vez mayor de amenazas que, al ser explotadas, pueden ocasionar interrupciones en el modelo de negocio. Por lo antes expuesto, el establecimiento de metodologías, prácticas y procedimientos que resguarden los activos de información, y proporcionen seguridad a los Sistemas de Información que soportan los procesos del negocio, son cada vez más comunes en las organizaciones. Bandes no escapa a esta realidad, y mediante el establecimiento de políticas y controles de seguridad adecuados, busca asegurar la confidencialidad, integridad y disponibilidad de sus activos de información; estrategia que da origen a este TEG, el cual tuvo como objetivo diseñar un modelo de Sistema de Gestión de Seguridad de la Información basado en ISO 27001 para atender riesgos tecnológicos en los procesos de negocio de la Institución. Además de dar cumplimiento legal a las cada vez más numerosas leyes, reglamentos y normativas que tienen implicaciones en la gestión de seguridad de la información por parte de los entes reguladores de Bandes, la investigación presentada a través de éste Trabajo Especial de Grado aportó un modelo que contribuye al desarrollo de capacidades medulares, traduciéndolas en ventajas competitivas para la organización.

Palabras clave: Sistema de Gestión de Seguridad de la Información, ISO 27001, Activos de Información.
Línea de Trabajo: Gerencia del Riesgo en Proyectos

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

Los activos de información, junto a los sistemas y procesos que hacen uso de ella, juegan un papel fundamental para el éxito y la continuidad en el mercado de cualquier organización. En la actualidad, las organizaciones han comenzado a visualizar la necesidad imperante de gestionar la seguridad de sus activos de información, toda vez que han comprendido la importancia que estos tienen para el logro de sus objetivos. Particularmente han entendido la relación existente entre sus activos de información y sus activos de conocimiento, y cómo estos juegan un papel fundamental en su desempeño, por lo que el aseguramiento de dichos activos y de la tecnología que los soportan se ha convertido en un objetivo de primer nivel. Por esta razón, el establecimiento de metodologías, prácticas y procedimientos que busquen proteger la información como un activo valioso de la organización, proporcionando seguridad a las Tecnologías de Información que soportan los procesos del negocio, es cada vez más común en las organizaciones.

Para la Coordinación de Seguridad de la Información (CSI) del Banco de Desarrollo Económico y Social de Venezuela (Bandes), es determinante asegurar la confidencialidad, integridad y disponibilidad de los activos de información de la Institución mediante el establecimiento de políticas y controles de seguridad adecuados. Con la finalidad de apoyar la gestión de dicha coordinación, esta investigación está orientada a diseñar un modelo de calidad, documentado y conocido por todos los involucrados, basado en el estándar de Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información, de la Organización Internacional para la Estandarización (ISO27001), para la Gestión de Seguridad de la plataforma tecnológica, y principalmente a los sistemas de información que apoyan los procesos del negocio y se encuentran en la

plataforma tecnológica de Bandes, que permita conocer los riesgos a los que están expuestos y la forma de tratarlos.

Este modelo, pretende optimizar e incrementar la gestión de seguridad de la información aplicada a los activos y sistemas de información de la Institución, identificando oportunidades de mejora y orientando el esfuerzo de acuerdo a la relevancia del proceso de negocio al cual pertenecen.

El desarrollo de este trabajo de investigación ha sido contemplado en seis (6) capítulos, a saber:

Capítulo I. El problema de investigación. Aborda el planteamiento del problema, la justificación de la investigación, los objetivos generales y específicos, el alcance y limitaciones, con la finalidad de exponer y contextualizar el motivo que dio origen a este trabajo.

Capítulo II. Marco Teórico. Se presentan los antecedentes de la investigación, así como también, los diferentes conceptos que conforman el basamento teórico de la investigación.

Capítulo III. Marco Metodológico. Se exponen el tipo y diseño de la investigación, la población y muestra, la metodología utilizada para la recolección de la información, procesamiento y análisis de datos, el procedimiento de la investigación y las consideraciones éticas.

Capítulo IV. Marco Organizacional. Se presenta el contexto organizacional del Bandes, su visión, misión, valores y estructura organizativa.

Capitulo V. Desarrollo de la Investigación. Se desarrollan los cinco objetivos específicos del presente TEG.

Capítulo VI. Análisis de resultados. Se presentan los resultados obtenidos en la investigación.

Capitulo VII. Evaluación del proyecto. Se verifican los objetivos específicos planteados en base a los logros obtenidos.

Conclusiones y recomendaciones. Se presenta el cierre y sugerencias a tomar producto del desarrollo y evaluación de este TEG.

Por último, se presentan las Referencias Bibliográficas utilizadas en el desarrollo de este Proyecto de Trabajo Especial de Grado.

CAPITULO I

EL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

La ISO 27001 es un estándar de calidad internacional que especifica los requerimientos necesarios para establecer, implantar, monitorear, mantener y mejorar un sistema de Gestión de Seguridad de la Información. El propósito de este sistema de gestión es garantizar que los riesgos referentes a seguridad de la información sean conocidos, asumidos, gestionados y minimizados por organizaciones de una forma documentada, sistemática y estructurada.

El Banco de Desarrollo Económico y Social de Venezuela (Bandes), es un banco encargado de financiar proyectos que promuevan el desarrollo económico de la nación. Actúa como ente financiero del Estado Venezolano para atender proyectos orientados a la desconcentración económica y estimular la inversión privada en zonas deprimidas y de bajo rendimiento, apoyando financieramente proyectos especiales de desarrollo a nivel regional y en diversos países. Esta institución está facultada para ser el ente fiduciario de organismos del sector público; y para apoyar técnica y financieramente la expansión y diversificación de la infraestructura social y productiva de los sectores prioritarios, a fin de contribuir con el desarrollo equilibrado de las distintas regiones del país; e igualmente para administrar acuerdos financieros internacionales.

Para alcanzar los objetivos estratégicos mencionados anteriormente, los procesos de negocio de Bandes así como los recursos y servicios que los soportan son de vital importancia. Estos aseguran y mantienen los niveles de competitividad y rentabilidad necesarios para alcanzar las metas propuestas, además de asegurar el desempeño de la organización en el mercado en el que se desenvuelve.

En la actualidad, las organizaciones y sus sistemas de información, están expuestos a un número cada vez más elevado de amenazas que pueden comprometer la integridad y disponibilidad de la información que manejan. Bandes no escapa a esta realidad, y es por esta razón que en el marco del proceso de transformación integral que ha llevado a cabo la organización, se crea la Coordinación de Seguridad de la Información en Febrero de 2008, como una unidad adscrita a la Gerencia Ejecutiva de Resguardo Institucional.

Esta coordinación nace con el objetivo de establecer políticas y controles de seguridad, que aseguren la confidencialidad, integridad y disponibilidad de los activos de información, así como también la identificación temprana de problemas y el análisis continuo de riesgos a los que está expuesta la organización.

A pesar de esto, en la actualidad las prácticas de gestión de riesgos aplicadas a la implementación de servicios y aplicaciones que soportan los procesos de negocio de Bandes, no son eficaces; y se demuestra en los informes generados durante las auditorías realizadas por la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN 2011).

En informe de revisión especial de riesgo tecnológico remitido a Bandes, el cual contiene los resultados obtenidos en la visita efectuada entre el 11 de Julio y el 11 de Agosto, la SUDEBAN expresa lo siguiente:

> Es deficiente el modelo de Seguridad Lógica implementado por la Coordinación de Seguridad de la Información, lo cual no garantiza la protección de los activos informáticos y por consiguiente la integridad y confidencialidad de la información básica y financiera de los clientes. (pág. 4)

Esto refleja ciertamente, que la organización no conoce a cabalidad los riesgos a los que está sometida su información ni la manera en la que

debe tratarlos, así como también resalta el hecho que aún no se han implementado los controles necesarios en la plataforma tecnológica para detectar anomalías que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información de la organización.

La implementación de un modelo de calidad para la Gestión de Seguridad de la Información en Bandes, basado en mejores prácticas, representa sin duda una mejora en la gestión de los activos de información de la organización. A través de la identificación y estimación de riesgos, la implementación de controles, el desarrollo de medidas alineadas con el negocio y la definición de procedimientos operativos, se apoyará al personal involucrado a mejorar la seguridad de sus activos de información garantizando así las propiedades fundamentales que deben cumplir: Integridad, Disponibilidad y Confidencialidad.

El alcance de un Sistema de Gestión de Seguridad de la Información (SGSI) puede contemplar a toda la organización o no. En una organización como Bandes, la cual cuenta con presencia a nivel Internacional en 3 países y posee más de 800 empleados en su sede principal, la cantidad de actividades que deberán ser llevadas a cabo para alcanzar el conjunto de sedes, servicios, procesos, unidades organizativas, activos de información y recursos humanos; demandará indudablemente un largo período para su ejecución y aumentará considerablemente los riesgos asociados, lo cual traería como consecuencia el fracaso del proyecto. Adicionalmente, las áreas de conocimiento contempladas por un SGSI están acotadas en cuerpos de conocimiento y son altamente especializadas, por lo que es necesario identificar cuáles de estas áreas de conocimiento son relevantes para tratar la problemática aquí expuesta, de manera que sean incorporadas como practicas del proceso de gestión de riesgos de los sistemas de información que apoyan los procesos de negocio de Bandes.

Cano (2011), en su publicación electrónica *Definición del alcance del SGSI en la norma ISO 27001*, sostiene que "hay que tener en cuenta que un alcance reducido facilita la implantación, reduciendo en principio, la cantidad de trabajo, el coste total y la cantidad de documentación necesaria (...)". La definición del alcance de implementación del SGSI es el punto fundamental que puede alterar el resultado del proyecto.

Por todo lo antes expuesto, esta investigación está orientada a definir un modelo de calidad, documentado y conocido por todos los involucrados basado en el ISO 27001, para la Gestión de Seguridad de la plataforma tecnológica, y principalmente a los sistemas de información que apoyan los procesos de negocio y se encuentran en la plataforma tecnológica de Bandes en su sede principal, que permita conocer los riesgos a los que están expuestos y la forma de tratarlos.

INTERROGANTES DE LA INVESTIGACIÓN

En base a lo antes expuesto, se desprenden las siguientes Interrogantes:

1. ¿Qué aspectos deben ser considerados por el modelo de Sistema de Gestión de Seguridad de la información, en base a sus áreas de conocimiento, para atender la gestión de riesgos en los procesos de negocio de la plataforma tecnológica de Bandes?

2. ¿De qué manera serán identificados y clasificados los activos de información de los procesos de negocio de Bandes?

3. ¿De qué manera serán identificados los riesgos asociados a los activos de información de los procesos de negocio de Bandes?

4. ¿Qué controles y procedimientos deberá contemplar el modelo propuesto? ¿Cómo serán identificados?

5. ¿Qué políticas y estándares deberán ser definidos para soportar los controles identificados?

6. ¿Qué metodología de evaluación de riesgos será apropiada para el modelo de acuerdo a los requerimientos del negocio?

OBJETIVOS DE LA INVESTIGACIÓN

OBJETIVO GENERAL

Diseñar un modelo de Sistema de Gestión de Seguridad de la Información basado en ISO 27001 para atender la gestión de riesgos en los procesos de negocio de la plataforma tecnológica de Bandes.

OBJETIVOS ESPECÍFICOS

1. Inventariar los sistemas informáticos que soportan los procesos de negocio de Bandes, obteniendo información sobre la valoración del impacto que puede suponer la pérdida de los mismos.

2. Identificar los riesgos asociados a los activos de información de los procesos de negocio.

3. Analizar en función a la confidencialidad, integridad y disponibilidad, los activos de información de los procesos de negocio.

4. Consolidar las bases del modelo propuesto a través de la definición de políticas y estándares, así como los controles y procedimientos que definan las reglas generales para la interacción con los activos de información de los procesos de negocio.

5. Evaluar la metodología para la gestión de riesgos que será utilizada en el modelo propuesto, de acuerdo a los requerimientos del negocio.

JUSTIFICACION DE LA INVESTIGACIÓN

Los activos de información juegan un papel fundamental para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dichos activos y de la tecnología que los soportan debe ser, por tanto, un objetivo de primer nivel para Bandes.

Además de dar cumplimiento legal a las cada vez más numerosas leyes, reglamentos y normativas que tienen implicaciones en la gestión de seguridad de la información por parte de los entes reguladores de Bandes, el propósito de diseñar un modelo SGSI basado en ISO27001 es evitar interrupciones en el modelo de negocio, asegurando la disponibilidad, integridad y confidencialidad de los activos de información, garantizando que los riesgos asociados sean conocidos y gestionados de una forma documentada y estructurada, adaptada a los cambios que se produzcan en el entorno de Bandes, las tecnologías y la exposición a los riesgos.

La investigación presentada a través de éste Trabajo Especial de Grado aporta un modelo que sirve de herramienta para la Gestión de Seguridad de la Información en Bandes. Entre los beneficios que serán alcanzados con el desarrollo de este trabajo, podemos mencionar los siguientes:

a. Se adoptará una postura pro activa por parte de la organización en relación a la Seguridad, cambiando su forma de actuar, la cual se manifiesta reactiva ante los eventos en la actualidad.
b. Se definirán políticas que garanticen la seguridad de la información en los activos de información de los procesos de negocio de la organización.

c. Gestión de seguridad en los riesgos presentes en los activos de información de los procesos de negocio.
d. Inclusión de métricas e indicadores para determinar el desarrollo de la seguridad.
e. Implementación de controles de seguridad en las tecnologías que soportan los procesos de negocio.

Por todo esto, se desprende la importancia que tiene la realización del presente estudio como un mecanismo que puede contribuir al desarrollo de capacidades medulares que se traduzcan en ventajas competitivas para Bandes.

ALCANCE Y LIMITACIONES

La propuesta se limita a definir un modelo de calidad, documentado y conocido por todos los involucrados, basado en ISO27001, para la Gestión de Seguridad de la plataforma tecnológica, y principalmente a los sistemas de información que apoyan los procesos de negocio y se encuentran en la plataforma tecnológica de Bandes en su sede principal.

CAPITULO II
MARCO TEORICO Y CONCEPTUAL

Para fundamentar el planteamiento de una investigación, es necesario hacer explícito aquello que se propone conocer, e identificar lo que se sabe sobre el tema con la finalidad de definir claramente el problema a investigar. Este planteamiento, deberá necesariamente ser sustentado con datos empíricos y hallazgos realizados en estudios similares que permitan comprender la importancia que tiene el problema de estudio.

Es por ello que en este capítulo se desea fundamentar teóricamente la presente investigación, a través de la exposición y análisis de teorías que soporten al problema planteado. Esta sección, proporciona a la investigación un basamento teórico, coordinado y coherente que permite abordar el problema con la mayor claridad posible.

ANTECEDENTES DE LA INVESTIGACIÓN

La importancia que tiene la seguridad de la información y el poder que implica manejar información, es un tema muy delicado que en la actualidad está generando cambios en las organizaciones. El establecimiento de metodologías, prácticas y procedimientos que busquen proteger la información como un activo valioso, proporcionando seguridad a los procesos de los Sistemas de Información que soportan los procesos del negocio con la finalidad de resguardar los activos de información, son cada vez más comunes en las organizaciones.

Desde el inicio de este trabajo de investigación, fueron consultados varios trabajos especiales de grado (TEG), publicaciones e investigaciones en Internet, que guardan estrecha relación con el tema en cuestión y que han aportado información valiosa al mismo, con la finalidad de contar con una

base de estudios previos que sirvan de apoyo en la realización de este trabajo de grado.

Mendoza (2010), desarrolló como trabajo especial de grado para optar al título de Magíster Scientiarum en Ciencias de la Computación, una investigación titulada *Sistema de Gestión para la Seguridad de la Información Caso: Centro de Tecnología de Información y Comunicación del Decanato de Ciencias y Tecnología – UCLA.* Este trabajo especial de grado, propone un Sistema de Gestión de Seguridad de la Información (SGSI) para el tratamiento de riesgos informáticos en el Centro de Tecnología de Información y Comunicación (CTIC) del Decanato de Ciencias y Tecnología de la Universidad Centroccidental Lisandro Alvarado de acuerdo a lo establecido en el estándar internacional ISO/IEC 27001:2005.

Este trabajo de grado aporta información valiosa a la presente investigación, al desarrollar un análisis comparativo entre distintas metodologías para la gestión de riesgos compatibles con el estándar Internacional ISO 27001:2005, además de enfatizar la necesidad de orientar y adecuar los requerimientos reales de seguridad del CTIC para la gestión de riesgos, alcanzando de esta manera los objetivos empresariales.

En la misma línea de investigación, Pallas (2009), llevó a cabo una investigación titulada *Metodología de Implantación de un SGSI en un grupo empresarial jerárquico*, como trabajo especial de grado para optar por el título Magíster en Ingeniería en Computación. En esta investigación, se analizan diversos estándares que han sido desarrollados para gestionar la seguridad de la información, con el fin de proponer una metodología de implementación, gestión y mejora de un SGSI en un grupo empresarial jerárquico en Uruguay. Esta investigación presenta adicionalmente, algunas alternativas estratégicas y plantea diferentes métodos conocidos para el análisis y gestión de riesgos (serie ISO/IEC 27000), así como también,

incursiona en la aplicación de técnicas para la valoración de activos de información.

Este trabajo de grado aporta información valiosa a la presente investigación, al presentar una metodología adecuada al grupo empresarial objeto de estudio, que integra lo mejor de los enfoques analizados y enfatiza la necesidad de orientación y adecuación de los requerimientos reales de seguridad del negocio para la gestión de riesgos.

Matalobos (2009), en su trabajo especial de grado para optar al grado de Ingeniería Informática denominado *Análisis de Riesgos de Seguridad de la Información*, llevo a cabo un análisis de riesgos de seguridad de la información que permite cuantificar y comparar los requerimientos de seguridad de la información de la organización que fue objeto de estudio, con los controles implantados para asegurar su cumplimento, y en base a las diferencias encontradas, definir los controles adicionales necesarios para cumplir con todos los requerimientos de un SGSI.

Esta investigación, enfatiza la necesidad creciente de llevar a cabo evaluaciones de riesgos, y propone un marco de acción apropiado para gestionar riesgos de Seguridad de la Información, así como la implementación de controles apropiadamente seleccionados para proteger a la organización contra esos riesgos.

Freitas (2009), en su trabajo especial de grado para optar al título Magíster en Ingeniería de Sistemas denominado *Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar*, propone una metodología que permite conocer las fortalezas y debilidades a los que están sometidos los activos de información de la organización objeto de estudio, con el fin de sugerir estrategias que minimicen la ocurrencia de eventos adversos, ante posibles amenazas que pudiesen explotar las vulnerabilidades organizacionales.

Esta investigación enfatiza el propósito de la Seguridad de la Información, basándose en la norma ISO 27001, para asegurar la continuidad de los procesos organizacionales que soportan los activos de información, minimizando con ello el costo global de la ejecución de dichos procesos como las pérdidas de los recursos asignados para su funcionamiento.

Roos (2008), con la finalidad de obtener el título de Magíster en Tecnología de la Información y Negocios, llevó a cabo un trabajo de investigación en Holanda, denominado *Residual Risk Management – A Quantitative Approach to Information Security (Gestión de Riesgos Residuales – Una aproximación cuantitativa a Seguridad de Información)*, en el cual plantea que el manejo de riesgos informáticos no sólo es cuestión de implementar "mejores prácticas". El autor expone que en muchas oportunidades, a pesar de las medidas implementadas para gestionar riesgos informáticos y llevarlos a los niveles aceptables de la organización, no es tomado en consideración la gestión del riesgo residual, por lo que propone una aproximación cuantitativa para su tratamiento.

Castañeda y Quesada (2007), en su trabajo especial de grado para optar al título Tecnólogo en Análisis de Sistemas Informáticos denominado *Aplicación de la Norma Técnica ISO 27001:2005, para la Gestión de la Seguridad de la Información en la Dirección de Desarrollo Institucional (DDI) del Instituto Ecuatoriano de Seguridad Social (IESS),* plantean un estudio de la norma ISO antes mencionada con la finalidad de definir políticas de Seguridad de la Información que permitan minimizar las amenazas a las que pueda estar expuesto el Centro de Datos del IESS. Estos autores proponen en su investigación, un análisis previo con la finalidad de identificar los activos de información relevantes para la institución así como los riesgos y controles que están asociados a cada uno de ellos.

Esta investigación aporta información valiosa en cuanto a la definición de políticas y controles de Seguridad de la Información acorde a la norma técnica ISO 27001:2005 para proteger los activos de información de la institución, garantizando de esta forma su disponibilidad, integridad y confidencialidad.

Mayol (2006), llevo a cabo una investigación titulada *Modelo para la auditoría de la Seguridad Informática en la red de datos de la Universidad de los Andes*, como trabajo especial de grado para optar por el título Magíster en Computación. Esta investigación propone un modelo de auditoría completo, equilibrado, extensible a cualquier entidad de características similares a la red de datos de la Universidad de los Andes.

El modelo propuesto en esta investigación ofrece una visión general sobre el procedimiento que debe ser llevado a cabo para ejecutar una auditoría de seguridad, tomando en cuenta las peculiaridades de la organización objeto de estudio, e incluyendo reglas que guiarán aspectos importantes como lo son las políticas de seguridad, condiciones de seguridad física y controles a ser aplicados.

Corletti (2006), en su artículo de Seguridad Informática denominado *Análisis ISO-27001:2005*, presenta un breve resumen de los aspectos más importantes que deben ser tomados en consideración para la aplicación de estándar internacional ISO-27001:2005. Sostiene que su propuesta está orientada a aspectos netamente organizativos, y propone toda una secuencia de acciones para establecer, implementar, operar, monitorizar, revisar y mantener un Sistema de Gestión de Seguridad de la Información, lo cual es el punto fuerte de este estándar.

Este artículo, propone una síntesis de los aspectos que deben ser tomados en consideración en la implementación de un SGSI, por cualquier

empresa o particular, detallando claramente los aspectos de compatibilidad entre cada uno de ellos.

BASES TEÓRICAS

ISO 27001

Es un estándar internacional adaptable a cualquier organización, que permite, a través del análisis de riesgos y de la implementación de controles, políticas y procedimientos, preservar la confidencialidad, la integridad y la disponibilidad de los activos de información. La Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), sostienen lo siguiente:

> Este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, operar, monitorear, revisar, mantener, y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). (…) El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización (…). (Pág. 5)

Sistema de Gestión de Seguridad de la Información

Es el concepto central bajo el cual se construye el Estándar Internacional ISO 27001, y forma parte del sistema gerencial general de una organización. Es un proceso sistemático y documentado que ayuda a establecer políticas y procedimientos con la finalidad de preservar los activos de información de la organización, basándose en un enfoque de riesgo comercial y manteniendo un nivel de exposición siempre menor al nivel de riesgo que se ha decidido asumir. Este proceso permite identificar y reducir riesgos vitales de seguridad latentes en los activos de información, y enfoca todo el esfuerzo de la organización para mitigarlos.

Gestión-Calidad Consulting (2011), en su publicación electrónica denominada *Seguridad de la Información (SI) y orígenes de los estándares ISO 27000* afirma lo siguiente:

> Un Sistema de Gestión de la Seguridad de la Información (SGSI) debe constituir un modelo de gestión que establezca unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos. (http://www.gestion-calidad.com/seguridad-informacion.html)

Bajo el enfoque del Estándar Internacional ISO 27001, el SGSI adopta el modelo Plan-Do-Check-Act (Planear-Hacer-Chequear-Actuar), el cual es aplicable a todos sus procesos. A continuación se detalla como un SGSI toma como insumos los requerimientos y expectativas de seguridad que tiene la organización, y a través de acciones y procesos necesarios enfoca todo el esfuerzo para satisfacerlos.

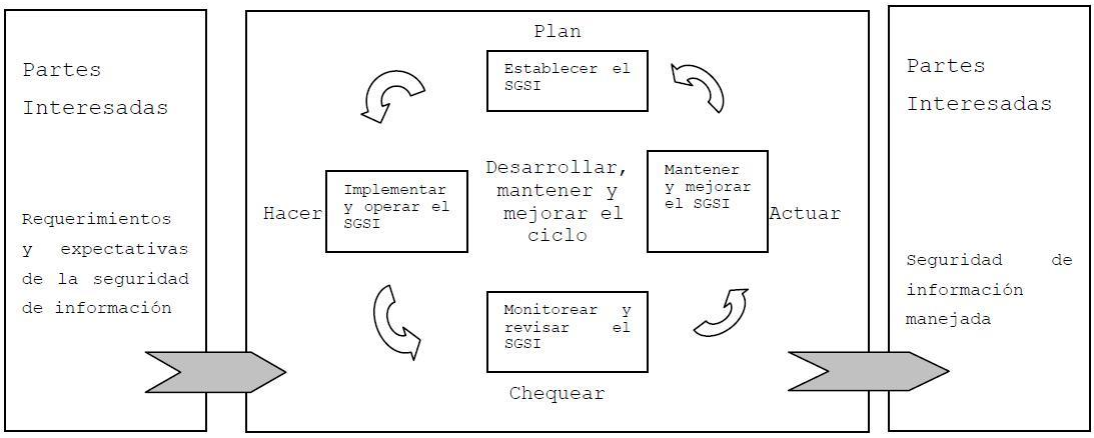


Figura N°1: Modelo *Plan-Do-Check-Act* aplicado a los procesos de un SGSI

Fuente: ISO / IEC 27001:2005

Modelo Plan-Do-Check-Act (PDCA)

Es una estrategia que permite la mejora continua de la calidad en los procesos a los que es aplicado, y es conocido también como el espiral de la

mejora continua. Este modelo está conformado por cuatro pasos que La Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), en su Estándar Internacional ISO/IEC 27001 definen de la siguiente forma:

> **Planear (establecer el SGSI)**: Establecer políticas, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización. **Hacer (implementar y operar el SGSI)**: Implementar y operar las políticas, controles, procesos y procedimientos SGSI. **Chequear (monitorear y revisar el SGSI)**: Evaluar y (…) medir el desempeño del proceso (…). **Actuar (mantener y mejorar el SGSI)**: Tomar acciones correctivas (…) basadas en los resultados de la auditoría Interna SGSI y la revisión gerencial (…) para lograr el mejoramiento continuo (…). (Pág. 7)

Riesgos

Espiñeira y Asociados (2008), en su *Boletín Digital No. 12*, exponen el siguiente concepto de riesgo presentado en un informe promulgado por el *Comité COSO* en su *Marco de Gestión Integral de Riesgos*: “Los riesgos son futuros eventos inciertos, los cuales pueden influir en el cumplimiento de los objetivos de las organizaciones, incluyendo sus objetivos estratégicos, operacionales, financieros, y de cumplimiento”.

Gestión de Riesgos

Es un enfoque estructurado para manejar la incertidumbre relativa a eventos o condiciones a las que pueden estar expuestos los activos de información de una organización. Este enfoque incluye procesos relacionados a la planificación de gestión de riesgos, identificación y análisis de riesgos, respuestas a los riesgos, y el seguimiento y control de riesgos. El objetivo de la gestión de riesgos es la canalización y tratamiento de los

riesgos asociados a los activos de información hasta alcanzar el nivel aceptado por la organización.

Planificación de la Gestión de Riesgos

La Guía de los Fundamentos de la Dirección de Proyectos, en su cuarta edición, sostiene lo siguiente:

> (…) La planificación de la Gestión de Riesgos es el proceso de decidir cómo abordar y llevar a cabo las actividades de gestión de riesgos (…). La planificación de los procesos de gestión de riesgos es importante para garantizar que el nivel, tipo y la visibilidad de la gestión de riesgos sean acordes con el riesgo y la importancia (…) para la organización (…). (Pág. 242)

En la siguiente figura, se detallan las entradas, herramientas y técnicas, así como las salidas del proceso de planificación de riesgos en proyectos según la Guía de los Fundamentos de la Dirección de Proyectos:

Figura N°2: Proceso de la Planificación de la Gestión de Riesgos en proyectos

Fuente: PMI (2008)

Identificación de Riesgos

Es un proceso iterativo en el cual se determinan los riesgos a los que puede estar expuesta una organización. En este proceso iterativo, se pueden identificar nuevos riesgos durante la implementación del SGSI. Los interesados proporcionan información para el proceso de identificación de riesgos, así como las acciones asociadas a las respuestas.

A continuación se detallan las entradas, herramientas y técnicas, así como las salidas del proceso de identificación de riesgos en proyectos según la Guía de los Fundamentos de la Dirección de Proyectos:

Figura N°3: Proceso de Identificación de Riesgos en proyectos

Fuente: PMI (2008)

Análisis de Riesgos

El análisis de riesgos es un proceso sistemático para estimar la magnitud e impacto de los riesgos a los que está expuesta una organización. Existen dos enfoques para llevar a cabo el análisis de los riesgos: cualitativo y cuantitativo.

En cuanto al análisis cualitativo de riesgos, la Guía de Fundamentos de la Dirección de Proyectos sostiene que “el Análisis Cualitativo de Riesgos

evalúa la prioridad de los riesgos identificados usando la probabilidad de ocurrencia, el impacto correspondiente sobre los objetivos del proyecto si los riesgos efectivamente ocurren" (Pág. 249).

Este tipo de análisis es utilizado normalmente como una forma rápida y rentable para las organizaciones para establecer prioridades en la planificación de respuestas a los riesgos, y sienta las bases para llevar a cabo el análisis cuantitativo si ese fuera el caso.

En cuanto al análisis cuantitativo, la Guía de Fundamentos de la Dirección de Proyectos sostiene que:

> (…) Se realiza respecto a los riesgos priorizados en el proceso Análisis Cualitativo de Riesgos por tener un posible impacto significativo sobre las demandas concurrentes del proyecto. El proceso Análisis Cuantitativo de Riesgos analiza el efecto de esos riesgos y les asigna una calificación numérica. También presenta un método cuantitativo para tomar decisiones en caso de incertidumbre (…). (Pág. 254)

Este tipo de análisis no se utiliza comúnmente ya que en muchos casos implica la ejecución de cálculos complejos, datos difíciles de estimar, o el acceso a la fuente de información detallada que permita realizar dichos cálculos.

Planificación de Respuestas a los riesgos

Es el proceso en el cual se define el tratamiento de selección e implementación de medidas para manejar los riesgos que fueron identificados y analizados previamente. Es aquí donde se definen los objetivos de control y los respectivos controles a ser implementados con la finalidad de reducir las amenazas a las que está expuesta la organización.

Controles de Seguridad

Los controles de seguridad, son mecanismos que permiten garantizar que cada uno de los aspectos que fue considerado en la planificación para asegurar los activos de información de una organización, se esté cumpliendo de acuerdo a lo establecido. Estos controles están diseñados para proteger los activos de información y generar confianza a las partes interesadas.

Microsoft (2005), en su Guía de Administración de Riesgos de Seguridad, afirma lo siguiente:

> Los controles, que en ocasiones se denominan contramedidas o protecciones, son medios organizativos, de procedimiento o técnicos para administrar los riesgos. Los responsables de mitigación, con el apoyo del equipo de administración de riesgos de seguridad, identifican todos los posibles controles, (…) y evalúan la reducción del nivel de riesgo posible con cada control. (…) Los controles que reduzcan con más eficacia el riesgo para los activos clave a un costo razonable para la organización son los controles cuya implementación el equipo recomendará con más entusiasmo.

CAPITULO III
MARCO METODOLOGICO

Hernández y otros (2007), en su libro *Metodología de la Investigación*, sostienen que “La investigación científica es en esencia como cualquier tipo de investigación, sólo que más rigurosa, organizada y se lleva a cabo cuidadosamente”. Este tipo de investigación, es la que se propone para dar solución a problemas o interrogantes de carácter científico y se caracteriza por ser un proceso único, sistemático, organizado y objetivo.

Este capítulo tiene como finalidad, desde una perspectiva teórica y conceptual, describir los procedimientos y técnicas aplicados para el desarrollo del presente trabajo de investigación. En este sentido, se presenta el tipo y diseño de investigación, población, muestra, e instrumentos y técnicas aplicadas para la recolección de datos.

TIPO Y DISEÑO DE LA INVESTIGACION

Por las características del estudio propuesto, el presente trabajo de investigación se identificó en un hibrido entre tres modalidades: *el proyecto factible*, ya que propone un modelo viable para atender riesgos tecnológicos en los procesos de negocio de la institución; *la investigación documental*, ya que, con la finalidad de profundizar el conocimiento, el autor interpretó datos secundarios de investigaciones previas, como referencias bibliográficas, referencias electrónicas, entre otros; para formar criterios y generar conclusiones que permitieron diseñar el modelo; y *la investigación de campo,* ya que los datos de interés fueron recolectados en forma directa de la realidad de la organización y el investigador participó en dicha recolección.

Según el Manual de trabajos de Especialización y Maestría y Tesis Doctorales, publicado por la Universidad Experimental Pedagógica Libertador (UPEL), (2011), estas modalidades se definen de la siguiente forma:

> El proyecto factible consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. (Pág. 21)
>
> Se entiende por Investigación Documental, el estudio de problemas con el propósito de ampliar y profundizar el conocimiento de su naturaleza, con apoyo, principalmente, en trabajos previos, información y datos divulgados por medios impresos, audiovisuales o electrónicos. La originalidad del estudio se refleja en el enfoque, criterios, (…) y en general, en el pensamiento del autor. (Pág. 20)
>
> Se entiende por Investigación de Campo, el análisis sistemático de problemas en la realidad, con el propósito bien sea de describirlos, interpretarlos, entender su naturaleza y factores constituyentes, explicar sus causas y efectos, o predecir su ocurrencia, haciendo uso de métodos característicos de cualquiera de los paradigmas o enfoques de investigación conocidos o en desarrollo. (Pág. 18)

El diseño de la investigación será de tipo No Experimental, transeccional y descriptivo, ya que, durante el desarrollo del trabajo de investigación, no podrán controlarse las variables de estudio, y se les dará carácter transversal y descriptivo, a razón de diagnosticar la problemática a un máximo nivel de detalle. Según Hernández y otros (2007), una investigación no experimental, se define como: “observar fenómenos tal como se dan en su contexto natural, para después analizarlos” (Pág. 205). Estos autores, también sostienen lo siguiente en relación a los estudios no experimentales:

> En un estudio no experimental no se construye ninguna situación, si no que se observan situaciones ya existentes no provocadas intencionalmente en la investigación por quien la realiza. En la investigación no experimental las variables independientes ocurren y no es posible manipularlas, no se tiene control directo sobre dichas variables ni se puede influir sobre ellas, porque ya sucedieron, al igual que sus efectos. (Pág. 206)

POBLACION Y MUESTRA

Hernández y otros (2007), definen población como: “Conjunto de todos los casos que concuerdan con determinadas especificaciones”; también definen muestra como: “Sub grupo de la población del cual se recolectan los datos y debe ser representativo de dicha población”.

La población definida para la presente investigación está conformada por las cuatro (4) personas que constituyen la Coordinación de Seguridad de la Información, así como las diez (10) personas que constituyen la Gerencia de Infraestructura y servicios tecnológicos perteneciente a la Gerencia Ejecutiva de Tecnología de la Información, quienes poseen experiencia en la implementación de servicios tecnológicos que soporten los procesos de negocio de la institución, y en el trato de riesgos asociados. Debido a que la población es pequeña, finita y manejable para un desarrollo objetivo, se tomó como muestra la misma población.

TECNICAS E INSTRUMENTOS DE RECOPILACION DE LA INFORMACION

La recolección de datos se obtuvo mediante dos (2) grandes fuentes: el análisis documental, en donde se seleccionaron y analizaron los informes de revisión especial de riesgo tecnológico remitidos a Bandes por SUDEBAN, así como un conjunto de factores que sirvieron de marco de referencia para diseñar el modelo de Gestión de Seguridad de la Información, y las entrevistas realizadas a personas expertas en la materia y

de quienes se obtuvo información útil, la cual fue utilizada en el desarrollo de esta investigación.

Kendall y Kendall (2005), en la sexta edición de su libro denominado *Análisis y Diseño de Sistemas*, plantean lo siguiente en relación a las entrevistas:

> (…) Es una conversación dirigida con un propósito específico que utiliza un formato de preguntas y respuestas. En la entrevista usted necesita obtener las opiniones de los entrevistados y su parecer acerca del estado actual del sistema, metas organizacionales y personales y procedimientos informales. (Pág. 90)

En su publicación, Kendall y Kendall (2005) plantea cinco pasos que deben ser tomados en consideración al preparar una entrevista:

1. *Leer los antecedentes:* Leer y entender tanto como sea posible los antecedentes de los entrevistados y su organización. (…)El propósito es crear un vocabulario común que en un futuro le permita expresar preguntas de la entrevista de una manera comprensible para su entrevistado. (…)

2. *Establecer los objetivos de la entrevista:* Utilice los antecedentes que haya recopilado así como su propia experiencia para establecer los objetivos de la entrevista. (…)

3. *Decidir a quién entrevistar:* Cuando tenga que decidir a quién entrevistar, incluya a gente clave de todos los niveles que vayan a ser afectadas por el sistema de alguna manera. Esfuércese por conseguir el equilibrio de tal manera que atienda las necesidades de tantos usuarios como sea posible. (…)

4. *Preparar al entrevistado:* Prepare a la persona que va a ser entrevistada hablándole por anticipado o enviándole un mensaje de correo electrónico y dándole tiempo para pensar en la entrevista. (…) Las entrevistas se deben llevar a cabo en 45 minutos o una hora a lo mucho. (…)

5. *Decidir el tipo de preguntas y la estructura*: Escriba preguntas que abarquen las áreas clave de la toma de decisiones que haya descubierto al determinar los objetivos de la entrevista. Las técnicas apropiadas para preguntar son el corazón de la entrevista. Las preguntas tienen algunas formas básicas que usted debe conocer. Los dos tipos básicos de preguntas son las abiertas y las cerradas. Cada tipo de pregunta puede lograr resultados un poco diferentes a los de la otra, y cada una tiene ventajas y desventajas. Es necesario que usted piense en el efecto que tendrá cada tipo de pregunta. (…). (Pág. 91)

PROCEDIMIENTO

Para la recolección de información, debido a la naturaleza de la investigación, se utilizó el tipo de entrevista no estructurada con preguntas abiertas. Este tipo de entrevista le permitió al entrevistado, desarrollar sus ideas con claridad y confianza y con un alto nivel de detalle, pudiendo revelar líneas de preguntas que pudieron haber pasado desapercibidas por el entrevistador.

Recolectados los datos, fue necesario analizarlos con la finalidad de descubrir su significado y relación en función a los objetivos planteados en la investigación. El tipo de análisis utilizado para tratar los datos en la presente investigación fue de tipo cualitativo, el cual se refiere a la interpretación no matemática de los datos en función a los aspectos de calidad. El registro, clasificación y organización de la información recolectada se realizó mediante la implementación de técnicas lógicas de análisis, como lo son la síntesis, la inducción y la deducción.

FASES DE LA INVESTIGACION

Para lograr los objetivos específicos planteados en este trabajo de investigación, fueron llevadas a cabo las siguientes fases:

- Fase de planificación del estudio.

- Fase de búsqueda de información.
- Fase de análisis de la información recolectada.
- Fase de diseño del modelo de Sistema de Gestión de Seguridad de la Información.
- Fase de evaluación del cumplimiento de los objetivos.

La fase de planificación estuvo constituida por la elaboración de la propuesta del Trabajo Especial de Grado, el cual incluye el planteamiento del problema, el marco teórico, la metodología para la investigación y el marco organizacional.

La fase de búsqueda de información, recabo las bases teóricas que sustentan el modelo de Sistema de Gestión de Seguridad de la Información propuesto.

La fase de análisis de la información recolectada, abarcó el estudio y la interpretación de la información obtenida, lo cual permitió el diseño del plan propuesto y derivó las conclusiones del trabajo de investigación.

En la fase de diseño, se elaboró el modelo de Sistema de Gestión de Seguridad de la Información para atender riesgos tecnológicos en los procesos de negocio de Bandes, el cual fue revisado y aprobado por el tutor de la tesis y el jurado designado por la Dirección de Postgrado de la Universidad Católica Andrés Bello.

Finalmente, en la fase de evaluación del cumplimiento de los objetivos, se valoró y determinó el grado de culminación de los objetivos operacionalizados.

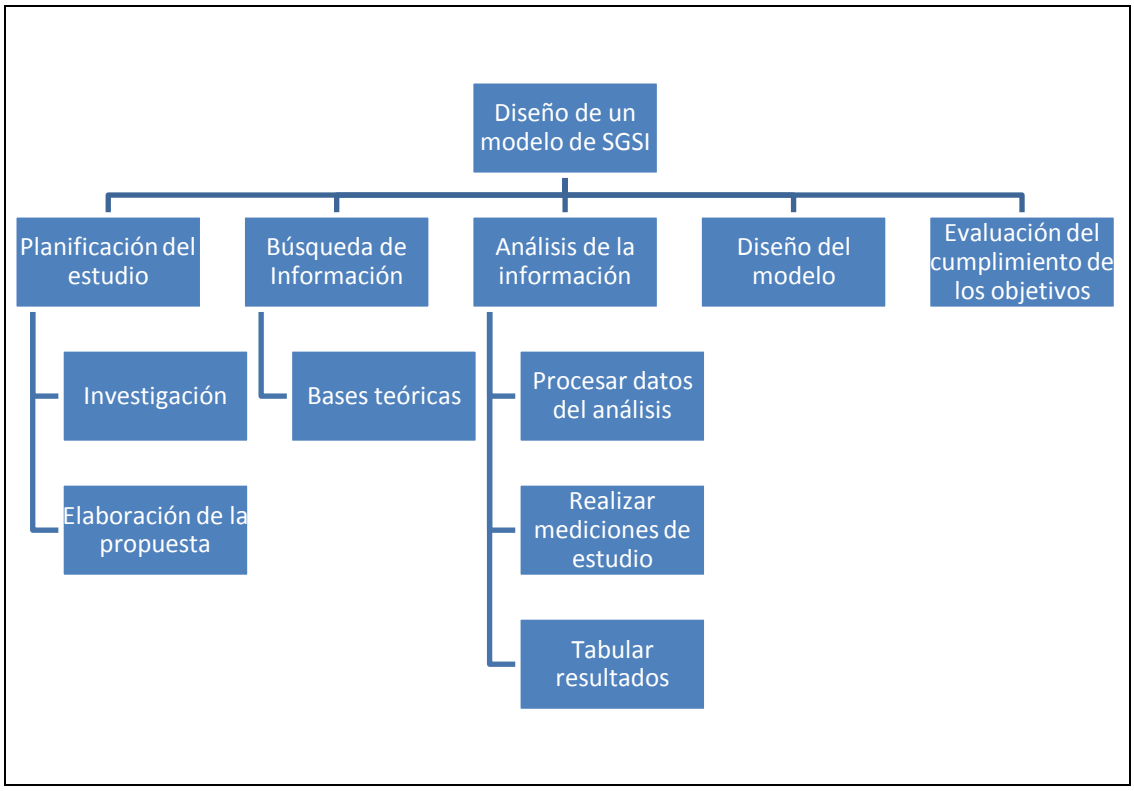


Figura N°4. EDT del trabajo de investigación

OPERACIONALIZACION DE LOS OBJETIVOS

Para completar el marco metodológico, se estableció la operacionalización de los objetivos, lo cual no es más que definir una relación entre los objetivos específicos definidos en el capítulo I con las variables de la investigación. Estas variables forman parte del estudio y pueden medirse (cualitativamente / cuantitativamente) para proporcionar información. Para ello, fue necesario precisar los fenómenos, eventos, hechos, características, procesos y situaciones objeto de estudio; y definirlos conceptualmente para determinar la manera en la que serían medidos.

A continuación se expone la operacionalización de los objetivos específicos del presente trabajo de investigación:

Tabla N°1. Operacionalización de objetivos específicos

Objetivo General. Diseñar un modelo de Sistema de Gestión de Seguridad de la Información basado en ISO 27001 para atender la gestión de riesgos en los procesos de negocio de la plataforma tecnológica de Bandes.		
Objetivo específico N° 1. Inventariar los sistemas informáticos que soportan los procesos de negocio de Bandes, obteniendo información sobre la valoración del impacto que puede suponer la pérdida de los mismos.		
Variables	**Definición operacional**	**Indicadores**
Sistemas informáticos	Todos aquellos elementos (hardware y software) que interactúan entre sí, con el fin de apoyar las actividades de la Institución.	- Soporten procesos de negocio de la Institución - Alta valoración de impacto en caso de pérdida
Objetivo especifico N° 2. Identificar los riesgos asociados a los activos de información de los procesos de negocio		
Variables	**Definición operacional**	**Indicadores**
Riesgos asociados a activos de información.	- Probabilidad de ocurrencia de eventos que afecten la integridad, disponibilidad o confidencialidad de los activos de información de los procesos de negocio.	- Amenazas - Vulnerabilidades

Objetivo especifico N° 3. Analizar en función a la confidencialidad, integridad, disponibilidad y uso, los activos de información de los procesos de negocio.		
Variables	**Definición operacional**	**Indicadores**
Propiedades de los Activos de Información	Propiedades que deben cumplir todos aquellos activos que tienen valor para los procesos de negocio, y que sin ellos, no pudiesen llevar a cabo las actividades inmersas en el proceso.	- Necesidades, requisitos y expectativas para los procesos de negocio
Objetivo especifico N° 4. Consolidar las bases del modelo propuesto a través de la definición de políticas y estándares, así como los controles y procedimientos que definan las reglas generales para la interacción con los activos de información de los procesos de negocio.		
Variables	**Definición operacional**	**Indicadores**
Políticas	Instrumentos referenciales que definen las reglas generales de comportamiento para la interacción entre usuarios y activos de información.	Necesidades, requisitos y expectativas para los procesos de negocio
Estándares	Especificaciones técnicas que definen y describen aspectos que deberán ser contemplados por los activos de	Necesidades, requisitos y expectativas para los procesos de negocio

	información.	
Procedimientos	Sucesión cronológica de eventos para la ejecución de actividades que involucren a los activos de información de los procesos de negocio.	Necesidades, requisitos y expectativas para los procesos de negocio
Objetivo especifico N° 5. Evaluar la metodología para la gestión de riesgos que será utilizada en el modelo propuesto, de acuerdo a los requerimientos del negocio.		
Variables	**Definición operacional**	**Indicadores**
Metodología para la gestión de riesgos	Conjunto de métodos bajo los cuales se regirá el proceso de gestión de riesgos asociados a los activos de información.	Necesidades, requisitos y expectativas de los involucrados.

CONSIDERACIONES ETICAS

Las consideraciones éticas tomadas para la realización de este Trabajo Especial de Grado, se basan en el acuerdo de confidencialidad para el manejo de información de Bandes, así como también en el código de ética y conducta profesional del PMI.

Acuerdo de confidencialidad para el manejo de información de Bandes:

Bandes, expresa en su acuerdo de confidencialidad para el manejo de la información lo siguiente:

> **Segunda:** Información Confidencial: será toda aquella información y/o material que contenga información relativa a los empleados, contratistas, tecnologías de información y de seguridad, relacionados de Bandes, o cualquier otra información cuya naturaleza indique su carácter confidencial.
>
> **Tercera:** Confidencialidad: No se podrá divulgar en forma alguna, toda aquella información relacionada con el trabajo realizado, ni entregar a terceros, originales o copias de los documentos que forman parte del mismo, sin la previa autorización por escrito de Bandes.
>
> **Cuarta:** Incumplimiento: El incumplimiento del presente acuerdo, será considerado una violación y dará derecho a Bandes como parte afectada a exigir la indemnización correspondiente por el daño causado, sin perjuicio de otras responsabilidades a la que se contrae la legislación venezolana.

Código de ética y conducta profesional del PMI:

- Capítulo II: Responsabilidad
- Capítulo III: Respeto
- Capítulo IV: Equidad
- Capítulo V: Honestidad

CAPITULO IV
CONTEXTO ORGANIZACIONAL

El Banco de Desarrollo Económico y Social de Venezuela (Bandes), fue creado mediante el Decreto N° 1.274 con Rango y Fuerza de Ley de Transformación del Fondo de Inversiones de Venezuela en el Banco de Desarrollo Económico y Social de Venezuela. Desde su inicio, Bandes ha experimentado cambios significativos en su rol como banca de desarrollo, posicionándose como una pieza fundamental en la ejecución de las políticas económicas y sociales del Estado Venezolano, a través del apoyo técnico y financiero a las inversiones sociales y productivas nacionales e internacionales, siguiendo los lineamientos del Plan de Desarrollo Económico y Social de la Nación y del Plan de Desarrollo Regional.

En la actualidad, Bandes es el organismo del estado encargado de financiar proyectos que promuevan el desarrollo económico de la nación. Actúa como ente financiero del Estado Venezolano para atender proyectos orientados a la desconcentración económica y estimular la inversión privada en zonas deprimidas y de bajo rendimiento de la nación, apoyando financieramente proyectos especiales de desarrollo a nivel regional y en diversos países. Está facultado para ser el ente fiduciario de organismos del sector público; y para apoyar técnica y financieramente la expansión y diversificación de la infraestructura social y productiva de los sectores prioritarios, a fin de contribuir con el desarrollo equilibrado de las distintas regiones del país.

Dentro del sistema financiero público nacional, Bandes se ha convertido en líder al desarrollar su integración con participación accionaria en la banca del Estado, ampliando sus capacidades y apalancando el apoyo financiero al país.

En el ámbito internacional, Bandes realiza operaciones de financiamiento internacional con recursos propios o provenientes de terceros, participa en programas bilaterales y cualquier otro acuerdo financiero internacional que establezca el Ejecutivo Nacional, siempre dirigido al bienestar de los pueblos, en el marco de las políticas de Cooperación Internacional para promover la multipolaridad.

MISIÓN

Somos el Banco dirigido a promover el desarrollo económico y social a través del apoyo técnico y financiero a la inversión social y productiva en el ámbito nacional e internacional bajo los principios de justicia, equidad y solidaridad.

VISIÓN

Ser el Banco de desarrollo líder de la inversión social y productiva, modelo en calidad de servicio y talento humano orientado a la excelencia.

VALORES INSTITUCIONALES

- Honestidad
- Humildad y sencillez
- Lealtad
- Solidaridad
- Respeto
- Compromiso
- Transparencia
- Responsabilidad
- Cooperación

ESTRUCTURA ORGANIZATIVA

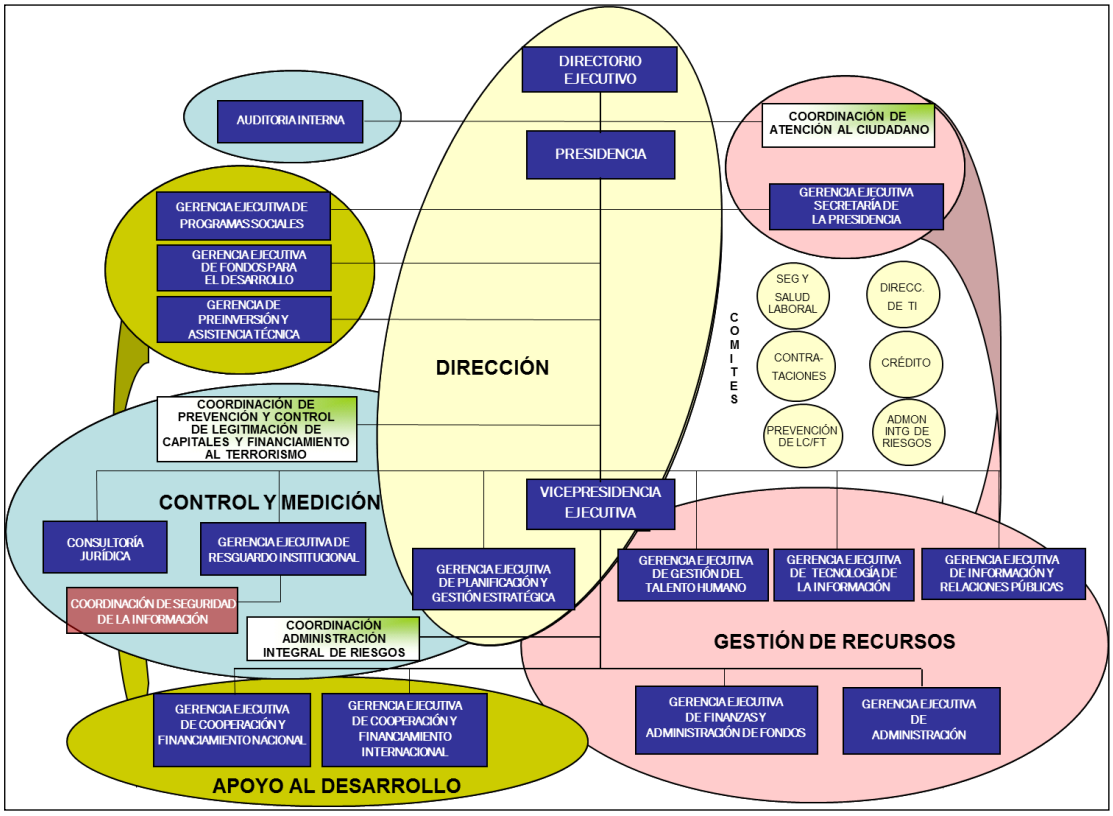


Figura Nº5. Estructura organizativa macro de Bandes

Fuente: Banco de Desarrollo Económico y Social de Venezuela (http://www.bandes.gob.ve)

CAPITULO V
DESARROLLO DE LA INVESTIGACIÓN

Este capítulo constituye el eje central de la investigación. Es aquí donde se analiza el proceso que se llevó a cabo para diseñar un modelo de SGSI que atienda la gestión de riesgos asociados a los procesos de negocio en la plataforma tecnológica de Bandes.

En primer lugar, se identifican las áreas de conocimiento de un SGSI relevantes a la investigación, y que han sido contempladas por el modelo:

Figura Nº6. Áreas de conocimiento contempladas por el modelo de SGSI diseñado

Del análisis de éstas áreas de conocimiento, se propone un modelo de SGSI, bajo el cual se desarrolla la investigación. El mismo esta compuesto por cuatro fases, a saber:

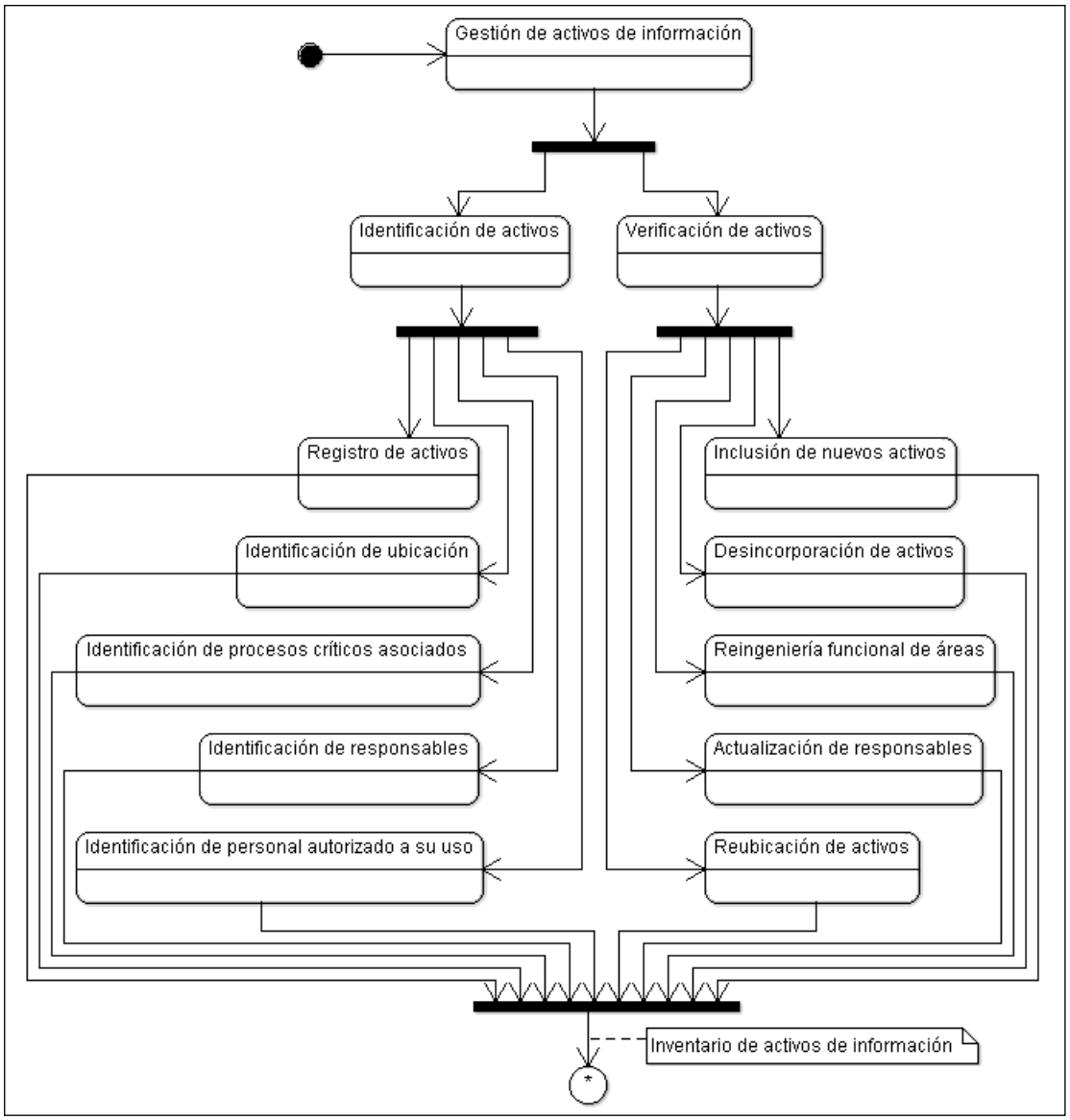


Figura Nº7. Fase I: Gestión de activos de información

Esta primera fase, contempla todo lo referente a la Gestión de los Activos de Información, y persigue establecer los criterios y procedimientos a ser utilizados para la realización y el mantenimiento del inventario de activos

de información de Bandes. Contempla la definición de roles y la consciente asunción de responsabilidades y tareas, lo cual es requisito indispensable para el logro de los objetivos propuestos en la investigación.

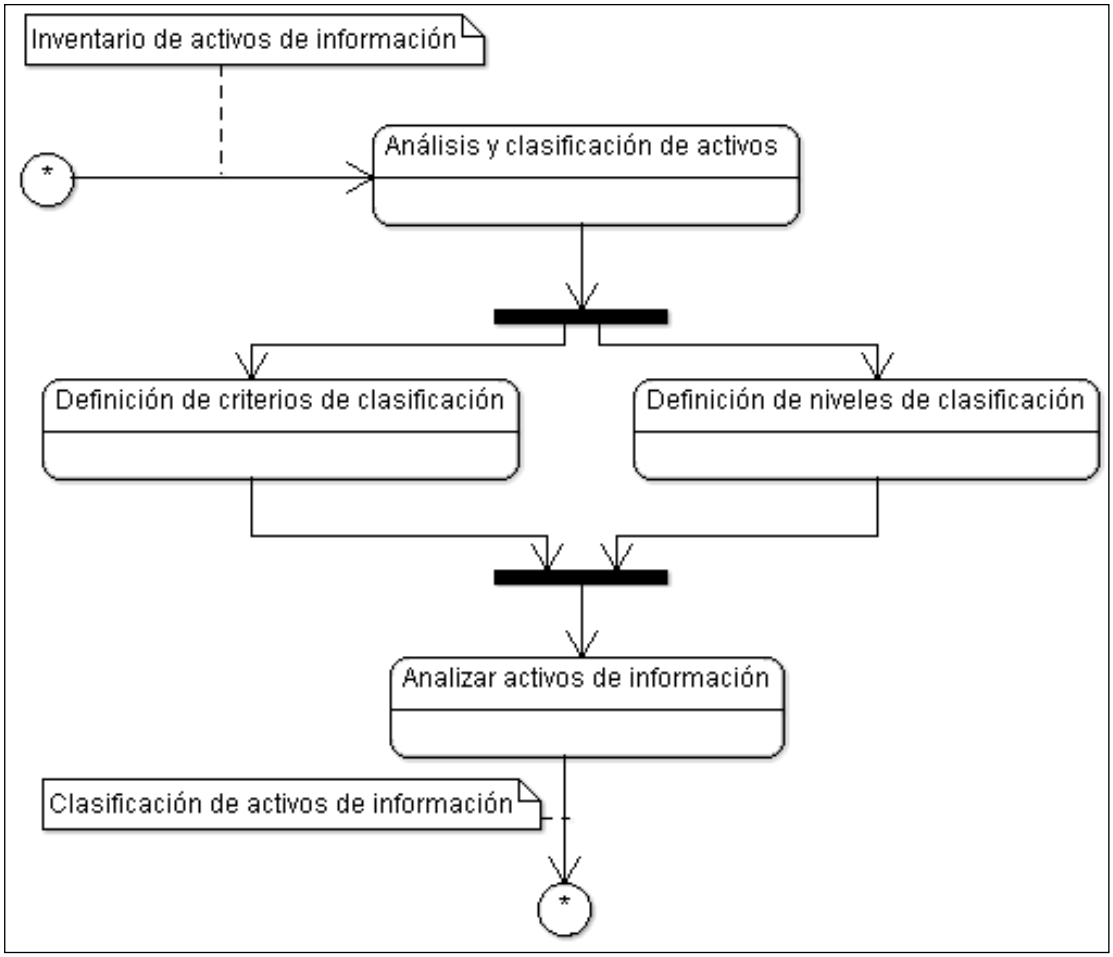


Figura Nº8. Fase II: Clasificación de activos de información

La fase de clasificación de activos de información, persigue asegurar un nivel de protección adecuado sobre los activos de información de Bandes, minimizando así la pérdida de confidencialidad e integridad en ellos. La información deberá clasificarse para indicar la necesidad, prioridad y grado de protección a la cual deberán ser sometidos los activos de información.

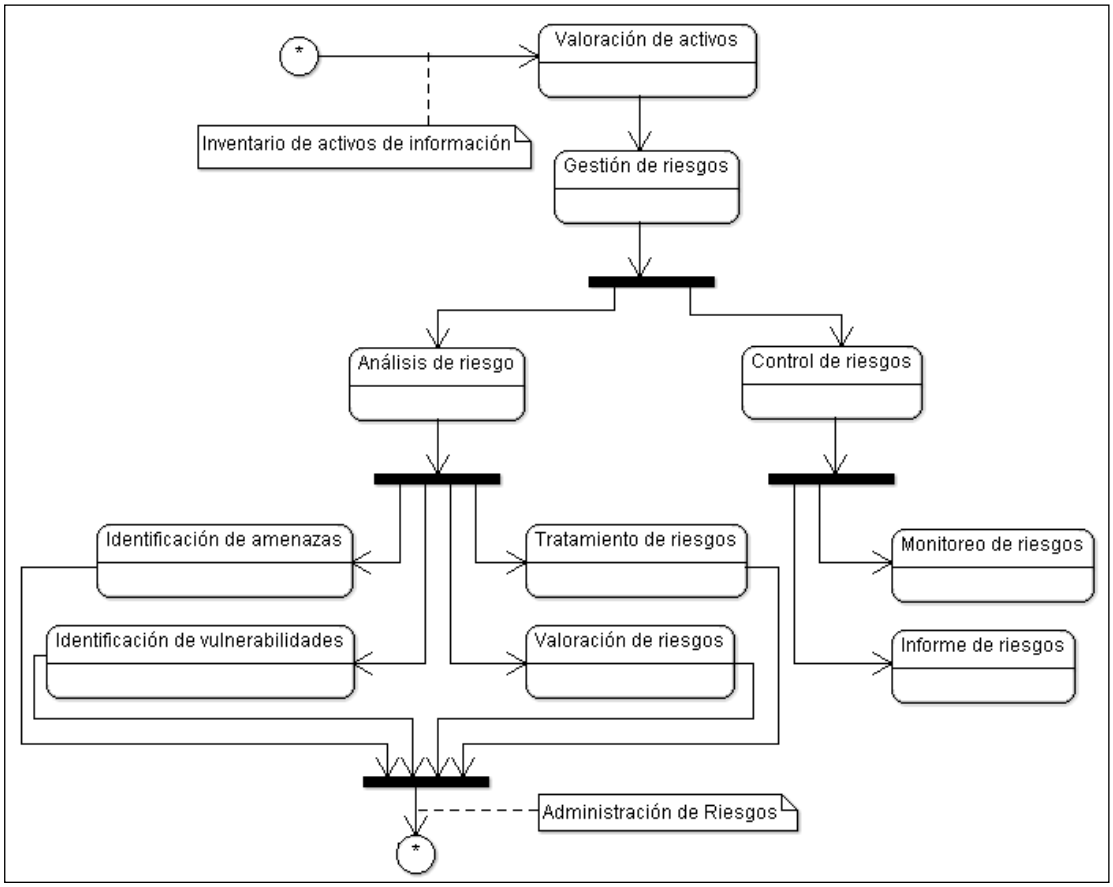


Figura Nº9. Fase III: Gestión de riesgos

La fase de Gestión de riesgos, proporciona un enfoque estructurado que permite reducir y controlar permanente los riesgos a los cuales pueden estar expuestos los activos de información de la Institución, a través de la identificación y valoración de eventos adversos que puedan materializarse sobre dichos activos. Esta fase justifica razonablemente las acciones correctivas o de control que serán llevadas a cabo en fases posteriores del modelo para resguardar adecuadamente los activos de información de Bandes.

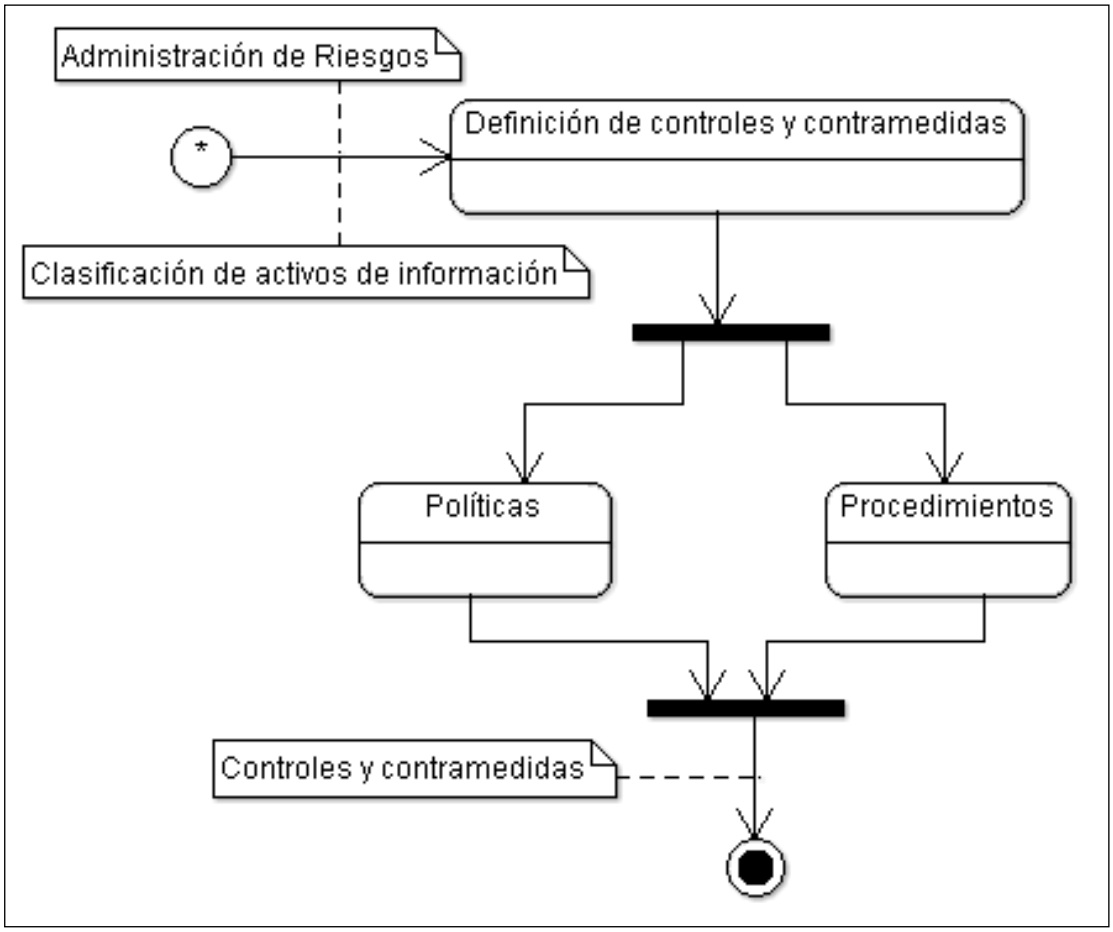


Figura Nº10. Fase IV: Definición de controles y contramedidas

La fase de definición de controles y contramedidas, persigue el diseño de medidas que coadyuvarán en la mejora y conservación de la seguridad y disponibilidad de los activos de información.

Objetivo Específico N° 1**. Inventariar los sistemas informáticos que soportan los procesos de negocio de Bandes, obteniendo información sobre la valoración del impacto que puede suponer la pérdida de los mismos.**

El manual de Políticas Operativas para la Seguridad de la Información de Bandes; la Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes sometidos al Control, Regulación y Supervisión de la Superintendencia de las Instituciones del Sector Bancario, emanada de la SUDEBAN; la Providencia Administrativa Nº 009.10 del 21 de diciembre de 2010, referente a la normas de Clasificación y Tratamiento de la Información dictada por la Superintendencia de Servicios de Certificación Electrónica, SUSCERTE; así como las mejores prácticas en la implementación de un SGSI basado en ISO 27001, recomiendan de manera imperativa la elaboración de un inventario y la subsiguiente clasificación de los activos de información, con la finalidad de determinar cómo deben ser utilizados en los procesos del negocio, definir los roles y las responsabilidades que tendrá el personal sobre ellos, reconociendo adicionalmente los niveles de confidencialidad que a cada activo debe otorgársele.

Con la finalidad de minimizar los riesgos de exposición y/o accesos indebidos a dichos activos, y definir criterios de valoración y protección que den cumplimiento a las normativas vigentes, la Coordinación de Seguridad de la Información, con el apoyo de una empresa externa con la experiencia apropiada, determinó y estableció el marco metodológico asociado a la fase de gestión de activos de información, el cual fue utilizado por la Institución para la realización y el mantenimiento del inventario.

El inventario desarrollado, contempla todos los activos de información contenidos en la plataforma tecnológica de Bandes (hardware, software,

aplicaciones, datos, etc.), que soportan los procesos de negocios de la Institución. Para el proceso de identificación y verificación de la información sobre estos bienes informáticos, de acuerdo al marco metodológico establecido, fueron contempladas las siguientes actividades:

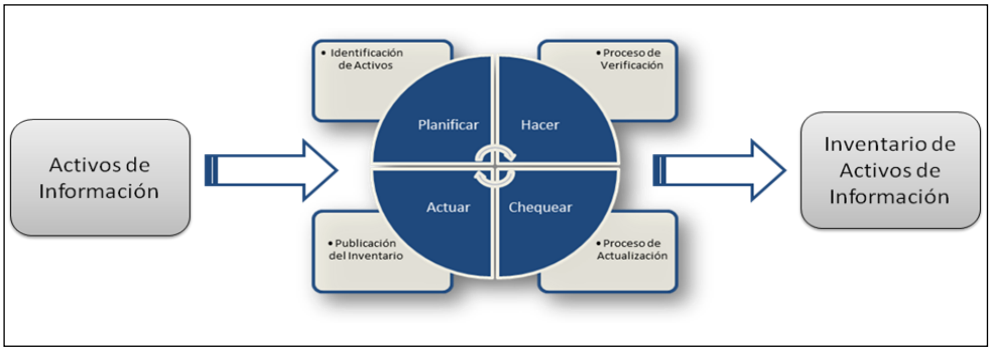


Figura Nº11. Ciclo del procedimiento de Inventario.

Fuente: Metodología para la gestión de Activos. Durán y Asociados, Consultores de Riesgo, C.A.

La actividad relativa a la identificación de activos determinó los componentes de información que forman parte del inventario. Esta identificación, fue realizada a nivel departamental y por procesos de negocios, y se ejecutó de la siguiente manera:

a. Para cada proceso de negocio, se aplicó el procedimiento para la identificación de activos, haciendo uso del formato *"Identificación y Registro de los Activos de Información"*. El responsable del proceso reportó y garantizó que todos sus activos de información fueron identificados y valorados.

b. La Coordinación de Seguridad de la Información, fue la unidad encargada de solicitar a los responsables de cada área, la ejecución del procedimiento para la identificación y registro de los activos, así como del monitoreo de la actividad.

c. Una vez identificados los activos, los responsables del proceso solicitaron al propietario de la Información[1] del área, la validación del levantamiento realizado. Culminado el proceso de validación, se entregó a la Coordinación de Seguridad de la Información, el formulario con los datos de los activos identificados y autenticados con la firma de ambos funcionarios.

La actividad referente al proceso de verificación, determinó que los componentes de información identificados, continuaran formando parte o no del inventario. La ejecución de esta actividad, permitió constatar adicionalmente si los datos o valores asignados inicialmente debían ser actualizados. Este proceso se llevó a cabo a demanda y por solicitud del responsable, del custodio o de la Coordinación de Seguridad de la Información. Las razones que dieron inicio al proceso de verificación se detallan a continuación:

a. Actualización del inventario.

b. Inclusión de nuevos activos.

c. Desincorporación de activos.

d. Reingeniería funcional de algunas de las áreas.

e. Remoción, promoción o sustitución del responsable o del custodio de los activos por reubicación física del área.

f. Reubicación de alguno de los activos hacia otras áreas.

[1] **Propietario de la Información**: parte designada de la organización, cargo, proceso o grupo de trabajo que tiene como responsabilidad definir quienes tienen acceso a qué información y que pueden hacer con ella. También, es responsable de determinar cuáles son los requisitos para que los activos se salvaguarden ante accesos no autorizados, posibles modificaciones, pérdida de confidencialidad o destrucción deliberada y, al mismo tiempo, definir lo que se hará con el activo cuando ya no sea útil.

El proceso de actualización, le permitió al personal de la Coordinación de Seguridad de la Información, integrar la información recibida y previamente validada al Inventario y Clasificación de Activos de Información de Bandes, con lo cual pudo ser generado y publicado dicho inventario. Una vez concluido el proceso, se realizó una presentación formal del mismo a todos los propietarios y custodios de áreas[2], resaltando su importancia y vigencia a la vez que fueron informadas las responsabilidades asociadas.

El inventario publicado, es resguardado y mantenido por la Coordinación de Seguridad de la Información, a través de un control de versiones de dicho documento.

Instrumento de campo utilizado para la recolección de información

Este instrumento de campo, fue diseñado para realizar y registrar el inventario inicial de los activos de información de Bandes así como su clasificación de acuerdo a los criterios previamente establecidos. También fue utilizado para el levantamiento de los inventarios que fueron programados periódicamente para dar cumplimiento a las normativas vigentes. El producto resultante de la aplicación de este instrumento de campo es el Inventario y Clasificación de Activos de Información de Bandes.

Su desarrollo es consistente con los estándares y mejores prácticas consideradas para el manejo de la seguridad de la información; así como de la normativa y leyes vigentes para el tratamiento de la información digital y activos de información, regulación bancaria y uso y costumbres aplicados a

[2] **Custodio:** Es una parte designada de la organización, un cargo, un proceso o un grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (toma de copias de seguridad, asignar privilegios de: acceso, modificaciones, borrado) que el propietario de la información haya definido, con base en los controles de seguridad disponibles en la organización.

las organizaciones gubernamentales de la República Bolivariana de Venezuela. El instrumento de campo denominado “Identificación y Registro de los Activos de Información”, se detalla a continuación:

Tabla N°2. Instrumento de campo. Identificación del área inventariada

Objetivo del Instrumento:	**Levantar el inventario de activos de información de la Institución Bandes, asignarle un Centro de Costos por área de pertenencia, clasificarlos según la norma (Clasificación y tratamiento de la información en la administración pública - Gaceta Oficial: 39578) y determinar el nivel de riesgo de todos y cada uno de los activos identificados.**
Alcance	**Para este levantamiento solo se tomarán en cuenta aquellos activos de información que representan un valor para la organización, bien sea por su valor intrínseco o porque son contenedores de otros activos de valor.**

Identificación del área inventariada			
			Código
Nombre de la Unidad		—	
Unidad de Adscripción		—	

Tabla N°3. Instrumento de campo. Ficha de activos de información

Ficha de Activos de Información													
Criterios a tomar en consideración ==>						Validar, el nivel de automatización de los procesos para actualizar el BIA							
Código				Nombre	Descripción	Proceso Crítico Asociado	Propietario		Custodio		Ubicación		Personal Autorizado a su uso
Área	Tipo	Clase	Núm.				Nombre	Cargo	Nombre	Cargo	Física	Lógica	

Tabla N°4. Instrumento de campo. Clasificación de activos de información

Clasificación de Activos de Información									
Código				Nombre	Descripción	Valoración Cualitativa			Clasificación
Área	Tipo	Clase	Núm.			Confidencialidad	Integridad	Disponibilidad	

Tabla N°5. Instrumento de campo. Amenazas y Vulnerabilidades asociadas a los activos de información (Parte I)

Amenazas y Vulnerabilidades asociadas (Primera parte)																													
Código				[D]							[I]											[C]							
Área	Tipo	Clase	Núm.	E.1	E.2	E.4	E.24	A.4	A.7	A.24	E.1	E.2	E.4	E.9	E.10	A.4	A.5	A.6	A.9	A.10	A.11	E.2	E.4	E.9	A.4	A.5	A.6	A.9	A.11

Tabla N°6. Instrumento de campo. Amenazas y Vulnerabilidades asociadas a los activos de información (Parte II)

Amenazas y Vulnerabilidades asociadas (Segunda parte)																	
Código				[A_*]							[T_*]						Otras amenazas / vulnerabilidades
Área	Tipo	Clase	Núm.	E.2	E.4	E.9	A.4	A.5	A.9	A.11	E.2	E.3	E.4	E.9	A.9	A.13	

Tabla N°7. Instrumento de campo. Formulario de identificación y registro de activos de información

Formulario de identificación y Registro de los Activos de Información										
Identificación del área					Actualización		Propietario		Custodio	
					Incorporación		Nombre:		Nombre:	
					Desincorporación		Cargo:		Cargo:	
Código				Nombre	Descripción	Proceso Crítico Asociado	Ubicación		Personal Autorizado a su Uso	
Área	Tipo	Clase	Núm.				Física	Lógica		

Firma del propietario:	
Firma del custodio:	

Tipo		Clase	
D	Datos / Info.	VR	Registros Vitales
S	Servicios	COM	Comerciales
A	Aplicaciones / Software	INT	Gestión Interna
H	Hardware	ADM	Administrativos
R	Redes	CONF	Configuración
E	Equipos Aux.	PER	Personales
L	Instalaciones	FAC	Facility

Inventario de activos de información

De la aplicación del instrumento de campo, de acuerdo a lo establecido en el marco metodológico definido, se obtuvo el inventario de activos de información contenidos en la plataforma tecnológica de Bandes y que soportan los procesos de negocios de la Institución. El inventario derivado de este modelo, se encuentra en el anexo N°1 de este trabajo especial de grado, y se denomina **"Inventario de activos de información de Bandes"**.

Objetivo Específico N° 2. **Analizar en función de la confidencialidad, integridad y disponibilidad, los activos de Información de los procesos de negocio.**

Una vez que los activos de información han sido convenientemente identificados e inventariados, el modelo propuesto contempla el análisis y clasificación de los mismos, con el propósito de asegurar que reciban los niveles de protección adecuados en función de la naturaleza y contexto operativo en el que se desempeñan, basándose en la información levantada y en criterios de clasificación previamente definidos.

Este proceso de clasificación fue llevado a cabo empleando el mismo instrumento y procedimientos utilizados para realizar el inventario de activos de información, específicamente la sección del instrumento referente a "***Clasificación de activos de información***" (ver figura 14).

La Coordinación de Seguridad de la Información fue responsable de la asignación de los niveles de clasificación de acuerdo a la información consignada durante la elaboración del inventario. En este sentido, en función al análisis realizado y de acuerdo a los criterios de clasificación establecidos, se asignó el valor de clasificación. Los criterios propuestos en el modelo, y considerados para el análisis y clasificación de los activos de información se detallan a continuación:

Figura Nº12. Criterios de la Información desde un enfoque de seguridad.

Estos criterios se refieren específicamente a lo siguiente:

Confidencialidad: La información debe ser accedida únicamente por personas, procesos o entes debidamente autorizados.

Integridad: La información debe estar actualizada, completa y sólo cambios autorizados deben ser aplicados a la misma.

Disponibilidad: Los usuarios deben tener acceso a la información para utilizarla cuando la misma sea requerida.

La clasificación definida en el presente modelo, es consistente a las necesidades de uso y tratamiento que da la Institución a su información. Del resultado de este análisis, se obtuvieron hasta cuatro niveles de clasificación; los cuales fueron aplicados a los activos de información en Bandes, a saber:

Pública: La información pública estará disponible a todos los empleados fijos, contratados y terceros. Se refiere a toda aquella información que ha sido declarada de conocimiento público.

Protegida: Información que es sensible a estar fuera de la institución. Esta información incluye información sobre el personal, datos financieros o detalles sobre el funcionamiento eficaz de la Institución. El acceso debe estar disponible únicamente a empleados y entes autorizados, cuyos productos o servicios dependen del conocimiento de la misma.

Confidencial: Información sensible cuyo uso no autorizado podría afectar moderadamente la reputación de la Institución, la calidad de sus procesos o sus operaciones. Sólo está disponible a funciones específicas, grupos de trabajo o roles.

Restringida: Información cuyo conocimiento debe estar limitado en términos generales. En caso de ser conocida por personas no autorizadas, podría afectar en forma severa la competitividad de la Institución, sus procesos o su reputación. Información que debe estar disponible sólo a roles o personalidades específicas en la organización.

A continuación se presenta la guía de clasificación de los activos de información establecida y definida en la metodología de gestión de riesgos evaluada:

Tabla N°8. Guía para clasificación de activos de información en función a los criterios establecidos

Niveles de Clasificación			
Confidencialidad	**Integridad**	**Disponibilidad**	**Clasificación**
Muy alta	Muy alta / Alta / Media / Baja / Despreciable	Muy alta / Alta / Media / Baja / Despreciable	Restringida
Alta	Muy alta / Alta / Media / Baja / Despreciable	Muy alta / Alta / Media / Baja / Despreciable	Confidencial
Media	Muy alta / Alta / Media / Baja / Despreciable	Muy alta / Alta / Media / Baja / Despreciable	Protegida
Baja	Muy alta / Alta	Muy alta / Alta / Media / Baja / Despreciable	Protegida
Baja	Media / Baja / Despreciable	Muy alta / Alta / Media / Baja / Despreciable	Pública
Muy baja	Muy alta / Alta / Media / Baja / Despreciable	Muy alta / Alta / Media / Baja / Despreciable	Pública

Cada activo de información inventariado, ha sido analizado en función de los criterios definidos, y se le ha asociado un único nivel de clasificación. Cada nivel de clasificación posee características propias de protección, manejo y tratamiento en cuanto a sus niveles de acceso, métodos de distribución, restricciones, almacenamiento, disposición y destrucción. Para cada activo de información fueron asignados atributos de clasificación, los cuales indican propiedades adicionales y específicas que cada activo posee, permitiendo identificar el nivel de riesgo inherente a cada uno.

De la aplicación del instrumento de campo, y los procedimientos establecidos en el marco metodológico definido, se obtuvo la clasificación de los activos de información contenidos en la plataforma tecnológica de Bandes y que soportan los procesos de negocios de la Institución. La

clasificación derivada de este modelo, se encuentra en el anexo N°2 de este trabajo especial de grado, y se denomina **"Clasificación de los activos de información Bandes"**.

Objetivo Específico N° 3**. Identificar los riesgos asociados a los activos de información de los procesos de negocio.**

El objetivo de la fase de gestión de riesgos de este modelo, es realizar el análisis de las amenazas[3] y vulnerabilidades[4] a las cuales están expuestos los activos de información de la Institución que forman parte del inventario producto de la fase de gestión de activos, con la finalidad de seleccionar luego los controles adecuados para mitigarlos. El riesgo se define como la probabilidad de que una amenaza pueda sacar provecho de una vulnerabilidad, por lo que el proceso de identificación de vulnerabilidades y amenazas a las que están expuestos los activos de información de acuerdo al contexto operativo en el que se desempeñan, es imprescindible para poder gestionarlos.

Este proceso de identificación de riesgos, fue llevado a cabo mediante la aplicación del instrumento de campo para el levantamiento del inventario de los activos de información, específicamente las secciones referentes a "***Amenazas y Vulnerabilidades asociadas a los activos de información***" (figuras 15 y 16 respectivamente); lo cual permitió establecer en conjunto con el propietario del activo, la exposición a las amenazas y vulnerabilidades de acuerdo a su contexto operativo; y en virtud de ello, se otorgó el nivel de clasificación para su administración y en consecuencia, fueron definidos los controles y medidas que debieron ser adoptadas para su debida protección. El equipo de trabajo tuvo la tarea de realizar entrevistas a los empleados que participan en los diferentes procesos de negocio con la finalidad de, entre otras cosas, recabar la información a nivel gerencial, operacional y de usuario final, que permitió la identificación de riesgos.

[3] **Amenaza:** es la posibilidad de ocurrencia de cualquier tipo de evento o acción que pueda comprometer las propiedades de confidencialidad, integridad y disponibilidad de los activos de información.

[4] **Vulnerabilidad:** capacidad, condición o característica que poseen los activos de información, que los hace susceptible a amenazas.

Figura Nº13. Identificación de amenazas y vulnerabilidades

El proceso de identificación de amenazas y vulnerabilidades definido en este modelo, toma en consideración la valoración[5] otorgada al activo de acuerdo a la relevancia del proceso de negocio al cual pertenece. Esta valoración permite tener una idea del impacto que un incidente puede causar al proceso de negocio, al tomar en consideración el valor estratégico que posee para la organización como un todo; con lo que se permite la elaboración de acciones de correctivas en función a la prioridad determinada en el momento del análisis, pues son parte de procesos de negocio de alta relevancia.

El modelo propuesto en esta investigación, con la finalidad de hacer simple y factible la práctica de identificación de riesgos, está conformado por las siguientes actividades:

[5] **Valoración de activos de información:** estimación del valor que tienen los activos de información para la Institución, de acuerdo a su importancia en los procesos de negocio.

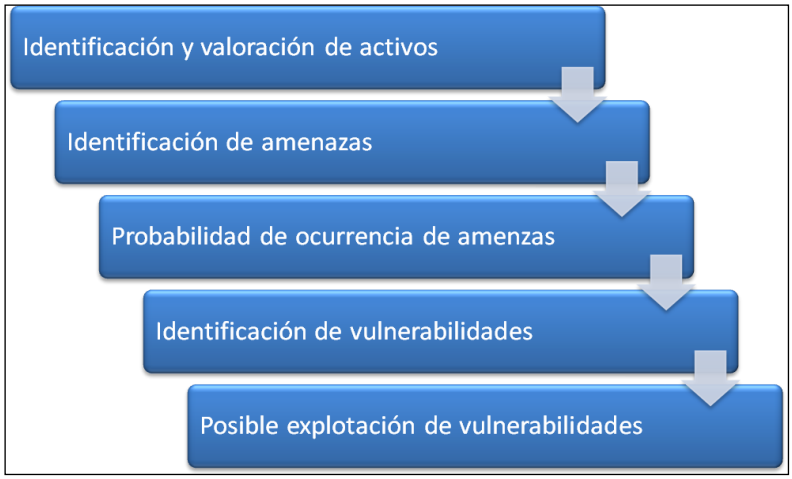


Figura Nº14. Actividades del proceso de identificación de riesgos propuesto

Identificación y valoración de activos: Permitió la caracterización de elementos que tienen valor para la Institución y por lo tanto deben ser protegidos, creando la cultura y el enfoque proactivo para gestionarlos. En esta actividad fueron enumerados los activos existentes y se les asignó un valor en función a la importancia que tienen para la institución.

Para realizar el cálculo de valor, fue considerado el daño que supone para la Institución que cualquiera de las propiedades del activo se vean afectadas: disponibilidad, integridad y confidencialidad. Esta actividad, permitió abocar el esfuerzo a resguardar aquellos activos de información que generen valor al negocio.

La valoración de los activos se realizó en función a la siguiente escala cualitativa: bajo, medio, alto. Los aspectos que fueron considerados en la valoración de activos se detallan a continuación:

- Reducción en el rendimiento de actividades
- Efecto negativo en la reputación de la Institución y/o unidades funcionales
- Pérdidas económicas

- Trastornos en el negocio

Identificación de amenazas: Esta actividad permitió la identificación a través de información generada en distintos niveles, como se muestra en la figura 13, de todas aquellas amenazas a las que estaban expuestos aquellos activos de información que generan valor al negocio.

La valoración de amenazas se realizó en función a la siguiente escala cualitativa: baja, moderada, severa. Una calificación pudo presentarse cuando la amenaza tuvo poca o ninguna capacidad o motivación. Una calificación alta se presentó en aquellas amenazas que son muy capaces y altamente motivadas.

Probabilidad de ocurrencia de amenazas: Permitió identificar la probabilidad de materialización de una, la cual fue realizada en función a la siguiente escala cualitativa: baja, media, alta.

Para calcular la probabilidad de ocurrencia de una amenaza, se utilizó el método de probabilidad subjetiva, en el cual, en base a la experiencia y a la evidencia disponible, el especialista en Seguridad de la Información, asignó la escala correspondiente. En el modelo propuesto, la probabilidad subjetiva puede tener forma de frecuencia relativa de ocurrencia anterior de eventos o simplemente puede consistir en una conjetura inteligente, es decir, puede ser definida en base a experiencia de eventos en función al juicio de los involucrados en el proceso de análisis.

Identificación de vulnerabilidades: Esta actividad contempló la identificación de aquellas debilidades que presentaba un activo de información, a través de la información recolectada en los diferentes niveles, lo cual permitió estimar el grado de afectación al que está expuesto para poder reforzarlos y evitar daños, permitiendo luego la implementación medidas de mitigación que disminuyan la vulnerabilidad y permitan reducir el

riesgo, garantizando de esta manera la sostenibilidad de los mismos en el tiempo.

La valoración de vulnerabilidades se realizó en función a la siguiente escala cualitativa: baja, moderada, severa.

Posible explotación de vulnerabilidades: Esta actividad permitió determinar el grado en que una amenaza puede explotar cada vulnerabilidad detectada. La valoración de explotación de vulnerabilidades se realizó en función a la siguiente escala cualitativa: baja, media, alta.

Como resultado de la ejecución de esta fase del modelo, se generó un informe denominado **"Informe de evaluación de riesgos asociados a los activos de información"**, el cual se encuentra en el anexo N°3 de este trabajo especial de grado.

Objetivo Específico N° 4. **Consolidar las bases del modelo propuesto a través de la definición de políticas y estándares, así como los controles y procedimientos que definan las reglas generales para la interacción con los activos de información de los procesos de negocio.**

La aplicación del modelo propuesto se sustentará en la definición de políticas, normas y estándares, los cuales tienen como finalidad consolidar y engranar las reglas o contramedidas de seguridad de la información para el establecimiento de un sistema de gestión robusto y a su vez flexible para adaptarlo a cualquier organización. Estos instrumentos referenciales, permitirán el desarrollo de controles y procedimientos con criterios específicos para abordar situaciones concretas a posteriori.

Una vez definidos y aprobados estos instrumentos, resultan de obligatorio cumplimiento, ya que establecen las reglas y los procedimientos que regulan la forma en que una organización protege sus activos de información, manejando una estrategia para mitigar los riesgos asociados a estos activos. A través de ellos se constituye una forma de comunicación con el personal (empleados fijos, terceros, contratistas, entre otros) que forman parte y laboran en la institución, indicándoles los lineamientos para el buen uso de los recursos y servicios con los que cuenta la organización.

El objetivo de esta fase dentro del modelo propuesto, es lograr que todos los empleados y contratistas estén conscientes de los límites que existen con respecto al uso de la información en la Institución, por lo que se han desprendido un compendio de políticas que buscan proporcionar una guía y apoyo legal a la Coordinación de Seguridad de la Información en relación al manejo de los activos de información de la Institución en función a los requisitos del negocio. Estas políticas se encuentran organizadas en tres (3) capítulos, y cada una de ellas cuenta con su declaración, objetivos, alcance y responsabilidades del personal.

El documento de políticas derivado de este modelo, se encuentra en el anexo N°4 de este trabajo especial de grado denominado **"Políticas Operativas del Sistema de Gestión de Seguridad de la Información del Banco de Desarrollo Económico y Social de Venezuela (Bandes)"**. El mismo ha sido desarrollado para este modelo y adaptado a las normas de la Gerencia de Gestión de la Calidad de Bandes.

De este modelo, también se desprenden normas y procedimientos para la interacción con los activos de información de la Institución, identificación de amenazas y vulnerabilidades e implementación de controles, los cuales son instrumentos de vital importancia ya que contienen una serie de directrices, pautas y lineamientos para guiar el curso de acción en el desenvolvimiento de las actividades que aquí se contemplan. Este manual de Normas y Procedimientos, se encuentra en el anexo N°5 de este trabajo de grado denominado "**Manual de Normas y procedimientos para el Sistema de Gestión de Seguridad de la Información del Banco de Desarrollo Económico y Social de Venezuela (Bandes)**"

Objetivo Específico N° 5. **Evaluar la metodología para la gestión de riesgos que será utilizada en el modelo propuesto, de acuerdo a los requerimientos del negocio.**

Bandes cuenta en la actualidad con una unidad responsable de la administración integral de riesgo institucional, la cual fundamenta la gestión de riesgos en la Resolución Número 136-03, "*Normas para una adecuada Administración Integral de Riesgos*", emanada de la SUDEBAN el 29 de Mayo de 2003.

La metodología evaluada y propuesta en este modelo, no sustituye la metodología de gestión integral de riesgos de la Institución. Su objetivo fue desarrollar un complemento sobre la práctica ya existente, con el objetivo de fortalecer el modelo de SGSI propuesto en este trabajo especial de grado, mediante la definición de una metodología para la estimación cualitativa de la exposición de riesgos de los activos de información de la Institución.

Esta metodología para la valoración cualitativa de exposición de riesgos, se basó en un estándar de aceptación general identificado como el ISO/IEC 31000:2009, el cual tiene su origen en el estándar AS/NZS 4360[6], referente a la práctica de gestión de riesgos. Éste estándar proporciona principios y directrices para gestionar riesgos de todo tipo, de una forma sistemática y transparente, aplicable en cualquier contexto, estimando cualitativamente el grado de exposición de los activos de información a riesgos.

Elementos del marco de gestión de riesgos:

El Modelo fue basado en la siguiente estructura establecida por las mejores prácticas ya adoptadas por Bandes:

[6] **AS/NZ 4360:2004** Gerencia de Riesgos, Estándar Australiano y Estándar de Nueva Zelanda. ISBN 0 7337 5904 1.

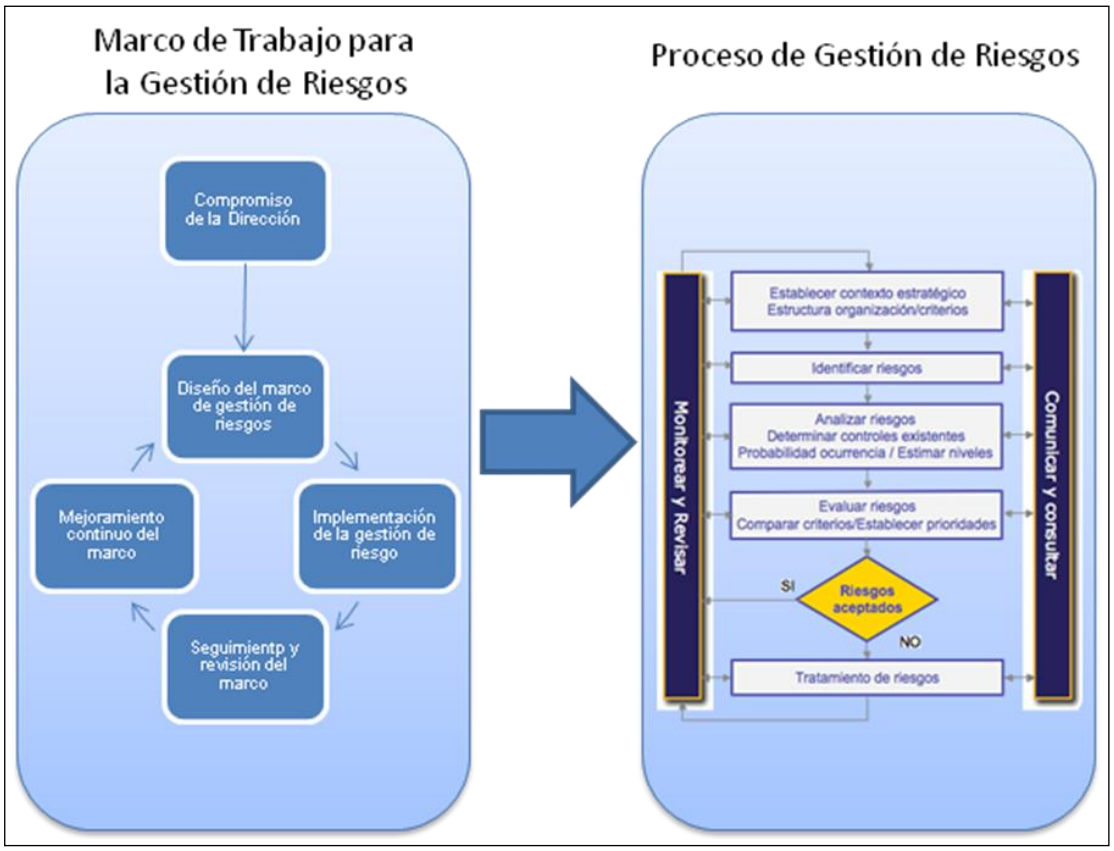


Figura Nº15. Modelo general de Gestión de Riesgos AS/NZS 4360, el cual se integra al ISO/IEC 31000.
Fuente: Marco de Evaluación de Riesgos. Durán y Asociados, Consultores de Riesgo, C.A.

El concepto de riesgo que se aplica a este modelo, es la combinación de la probabilidad de un suceso y de la consecuencia de su materialización, cuyo efecto puede desviar el propósito original esperado de los procesos de la Institución.

La metodología evaluada y propuesta en este modelo, se basa en la identificación del contexto (procesos y áreas de negocio) en el que se utilizan los activos de información, con la finalidad de calcular el grado de exposición a eventos que puedan poner en riesgo o peligro dichos activos en función a

la importancia que tengan para la Institución; mediante la identificación y análisis de amenazas y vulnerabilidades.

Los elementos claves en el proceso de evaluación de riesgos propuesto, son la frecuencia y el impacto. La frecuencia se refiere a la ocurrencia relativa a largo plazo de un suceso. Para un alto grado de frecuencia, la probabilidad se acerca a 1; es decir: 100%. La frecuencia en la metodología evaluada, se mide de acuerdo a lo expresado en la siguiente tabla:

Tabla Nº9. Frecuencia relativa de materialización de eventos definida para el modelo propuesto.

Frecuencia	Descripción
Casi cierto	Sucesos que tienen una probabilidad de ocurrencia extremadamente alta, y se aproxima a 1.
Frecuente	Sucesos que tienen una probabilidad de ocurrencia igual o superior a 6 en 12 meses.
Posible	Sucesos que tienen una probabilidad de ocurrencia mayor o igual a 3, y menor a 6 en 12 meses.
Poco frecuente	Sucesos que tienen una probabilidad de ocurrencia mayor a 1 y menor o igual a 3 en 12 meses.
Raro	Un suceso que tiene una probabilidad de ocurrencia extremadamente baja que se aproxima (entre 0 y 1) en el lapso de operación determinado.

Por otro lado, el impacto se refiere a la magnitud de la consecuencia de la materialización de eventos expresada en forma cualitativa; las cuales, por lo general, generan un daño o afectación de los objetivos del proceso de negocio. El impacto en la metodología evaluada, se mide de acuerdo a lo expresado en la siguiente tabla:

Tabla Nº10. Clasificación de Impacto en la materialización de eventos definida en el modelo propuesto.

Impacto	Descripción
Catastrófico	Afecta negativamente al Estado, a la Institución y a sus relacionados. La pérdida financiera es considerable, y la afectación de imagen corporativa conlleva a la pérdida de confianza.
Mayor	Afecta negativamente a la Institución y a sus relacionados. La pérdida financiera es considerable, la afectación de imagen corporativa conlleva a la pérdida de confianza.
Moderado	Afecta negativamente los procesos de la Institución y relacionados. La pérdida financiera es apreciable, y la afectación de imagen es probable debido a que puede impactar negativamente los servicios y la continuidad regular de las operaciones.
Menor	Afecta negativamente a los procesos de la Institución. La pérdida financiera es mínima, y la afectación de imagen es poco probable, pudiendo impactar algunos servicios de la institución.
Mínimo	La afectación de los activos no conlleva a que ocurra ningún tipo de pérdida ni afectación de imagen, sin embargo algunos aspectos de soporte regular a la operación pudieran estar siendo impactados.

Esta evaluación indica el valor que tiene el activo de información para la Institución, desde el punto de vista cualitativo en cada uno de los criterios definidos: Integridad, Disponibilidad y Confidencialidad. Para establecer la valoración adecuada entre la frecuencia probable del suceso y el impacto a la que el activo pudiera estar expuesto, fueron utilizados los siguientes valores:

Tabla Nº11. Valoración adecuada entre frecuencia e impacto del riesgo del modelo propuesto

	Impacto				
Frecuencia	**Mínimo**	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
Casi cierto	Bajo	Medio	Alto	Muy Alto	Muy Alto
Frecuente	Bajo	Bajo	Medio	Alto	Muy Alto
Posible	Muy Bajo	Bajo	Medio	Alto	Alto
Poco frecuente	Muy Bajo	Muy Bajo	Bajo	Medio	Alto
Raro	Muy Bajo	Muy Bajo	Muy Bajo	Medio	Medio

Para cada uno de los criterios definidos por el modelo, fue calculado el impacto de la evaluación de riesgo. El resultado del proceso de evaluación otorgó un nivel de clasificación de riesgo en forma consistente con los criterios de clasificación del activo. Los niveles de clasificación de acuerdo a la evaluación general del activo, se detallan a continuación:

Tabla Nº12. Nivel de clasificación según evaluación general de activos.

Criterios de SI			Valor	Descripción	Criterio
Confidencialidad	Integridad	Disponibilidad			
Muy Alto	Alto	Alto	Muy Alto	Información que de ser impactada adversamente puede afectar en forma severa la vida, la organización, los procesos, la reputación de la organización y está disponible sólo a roles o personalidades específicas en la organización.	Restringida
Medio	Alto	Alto	Alto	Información que de ser impactada adversamente, puede afectar moderadamente la reputación, la calidad y las operaciones de la organización. Sólo está disponible a funciones específicas, grupos de trabajo o roles	Confidencial
Bajo	Alto	Alto	Medio	Información que es sensible a estar fuera de la institución. El acceso debe ser autorizado a los empleados fijos, contratados y terceros, los cuales requieren el acceso a los activos de información basados en la necesidad de conocer para generar sus productos o servicios	Protegida

Criterios de SI			Valor	Descripción	Criterio
Confidencialidad	Integridad	Disponibilidad			
Bajo	Medio	Medio	Bajo	La información pública estará la disponible a todos los empleados fijos, contratados y terceros.	Pública

La valoración de riesgos establece la selección y puesta en práctica de las medidas necesarias para contrarrestar los riesgos a los que están expuestos los activos de información. Esto puede derivar en múltiples acciones que conlleven a reducir los riesgos u optimizar los riesgos.

CAPITULO VI
ANÁLISIS DE RESULTADOS

Este capítulo está enfocado a presentar los resultados obtenidos en la investigación. Para ello, ha sido necesario validar la precisión y validez del modelo propuesto con la finalidad de medir su eficiencia, y determinar que las expectativas hayan sido cubiertas en su totalidad.

Las pruebas realizadas para validar la precisión del modelo propuesto, son conocidas como pruebas de "bondad de ajuste estadístico basado en la distribución empírica de datos". Esta prueba es aplicada a diseños de investigación en los que es necesario probar modelos o hipótesis, mediante el estudio de la relación que existe entre las variables estudiadas y el modelo propuesto, permitiendo determinar si la distribución empírica de dichas variables se ajusta o no al modelo.

Para la ejecución de estas pruebas, fueron recolectados datos de eventos recientes en cuanto a la gestión de activos de información y el análisis de riesgos, los cuales fueron sometidos luego a las estrategias que contempla el modelo propuesto con el fin de comparar la distribución de las frecuencias observadas en las variables estudiadas, con la distribución de frecuencias de las mismas variables medidas en el modelo propuesto. El personal de la Coordinación de Seguridad de la Información de Bandes, participó activamente en la ejecución de dichas pruebas.

Estas pruebas fueron llevadas a cabo con el propósito de validar que existen diferencias estadísticamente significativas entre la distribución de la frecuencia observada de las variables en eventos recientes y la distribución de frecuencia esperada al someterlas al modelo propuesto, lo cual indicaría que existe una fuerte relación entre las variables y lo que el modelo intenta captar.

En relación al proceso de gestión de activos de información, fue tomada en consideración una muestra de 80 activos de información. Las variables tomadas en consideración en la prueba, así como la distribución de frecuencias observadas en los datos recolectados se detallan a continuación:

Tabla Nº13. Frecuencia de distribución de variables utilizadas como referencia observada.

Variables estudiadas	Cantidad	Porcentaje
Identificación de procesos críticos asociados.	27	33.75%
Identificación del responsable del activo	41	51.25%
Valoración del activo de información	19	23.75%
Identificación de ubicación del activo (física / lógica)	39	48.75%
Identificación del personal autorizado para su uso	9	11.25%
Esfuerzos adecuados para protección del activo	20	25%
Clasificación de activo	12	15%

La distribución de frecuencia al someter estas variables a las estrategias que contempla el modelo propuesto, se detalla a continuación:

Tabla Nº14. Frecuencia de distribución de variables aplicadas al modelo observada.

Variables estudiadas	Cantidad	Porcentaje
Identificación de procesos críticos asociados.	80	100%
Identificación del responsable del activo	80	100%
Valoración del activo de información	73	91.25%
Identificación de ubicación del activo (física / lógica)	78	97.5%
Identificación del personal autorizado para su uso	75	93.75%
Esfuerzos adecuados para protección del activo	70	87.75%
Clasificación de activo	80	100%

Como complemento a esta técnica analítica y con la finalidad de validar el modelo propuesto, a continuación se presentan gráficos comparativos que permiten mostrar en forma descriptiva la diferencia significativa entre ambas distribuciones, a la vez que contribuyen en la validación y aceptación del modelo propuesto.

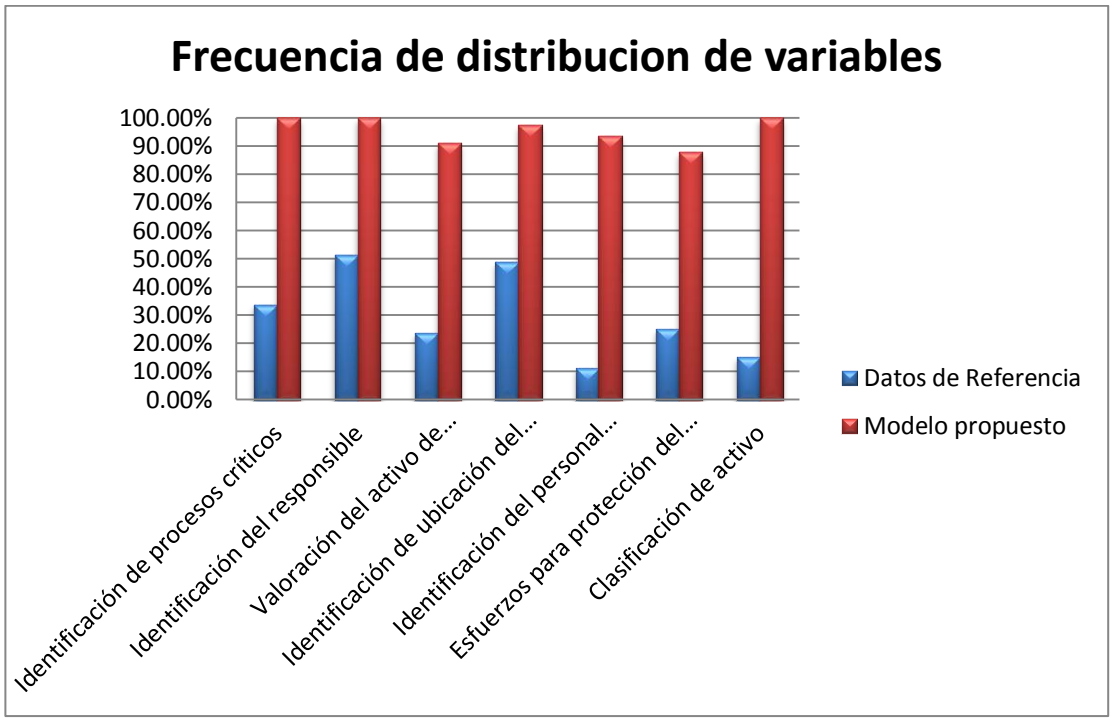


Figura Nº16. Diferencias entre frecuencias de distribución de variables expresada en columnas.

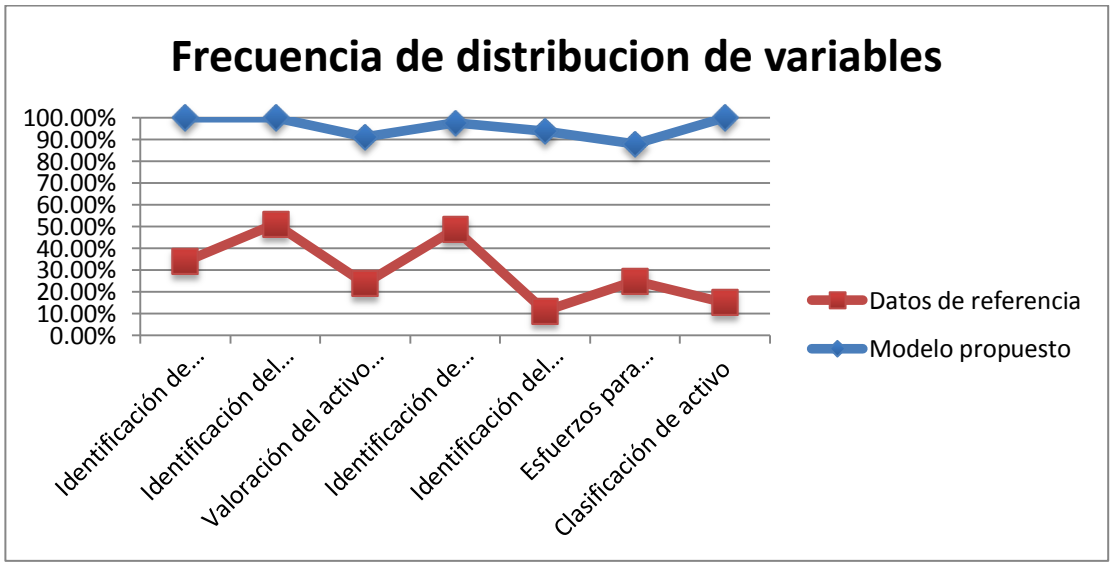


Figura Nº17. Diferencias entre frecuencias de distribución de variables expresada en líneas.

Como se puede observar, la diferencia significativa entre las distribuciones de frecuencia evidencia una mejora considerable en la gestión de activos de información con la aplicación del modelo.

En cuanto al proceso de gestión de riesgos, fue tomada en consideración una muestra de 40 activos de información. Las variables tomadas en consideración en la prueba, así como la distribución de frecuencias observadas en los datos recolectados para este proceso, se detallan a continuación:

Tabla Nº15. Frecuencia de distribución de variables utilizadas como referencia observada.

Variables estudiadas	Cantidad	Porcentaje
Identificación de amenazas y vulnerabilidades asociadas	12	30%
Contempla información a nivel gerencial, operacional y funcional en el análisis	4	10%
Toma en cuenta la valoración del activo de información en el análisis	3	7.5%
Identificación del contexto estratégico donde se utiliza el activo de información	18	45%
Establecimiento de prioridades y comparación de criterios para el análisis	5	12.5%
Frecuencia en la revisión y análisis de riesgos asociados	10	55%
Tratamiento de riesgos asociados	11	27.5%

La distribución de frecuencia al someter estas variables a las estrategias que contempla el modelo propuesto, se detalla a continuación:

Tabla Nº16. Frecuencia de distribución de variables aplicadas al modelo observada.

Variables estudiadas	Cantidad	Porcentaje
Identificación de amenazas y vulnerabilidades asociadas	40	100%
Contempla información a nivel gerencial, operacional y funcional en el análisis	40	100%
Toma en cuenta la valoración del activo de información en el análisis	40	100%
Identificación del contexto estratégico donde se utiliza el activo de información	40	100%
Establecimiento de prioridades y comparación de criterios para el análisis	30	75%
Frecuencia en la revisión y análisis de riesgos asociados	32	80%
Tratamiento de riesgos asociados	35	87.5%

Al igual que el proceso anterior, como complemento a esta técnica analítica y con la finalidad de validar el modelo propuesto, a continuación se presentan gráficos comparativos que permiten mostrar en forma descriptiva la diferencia significativa entre ambas distribuciones:

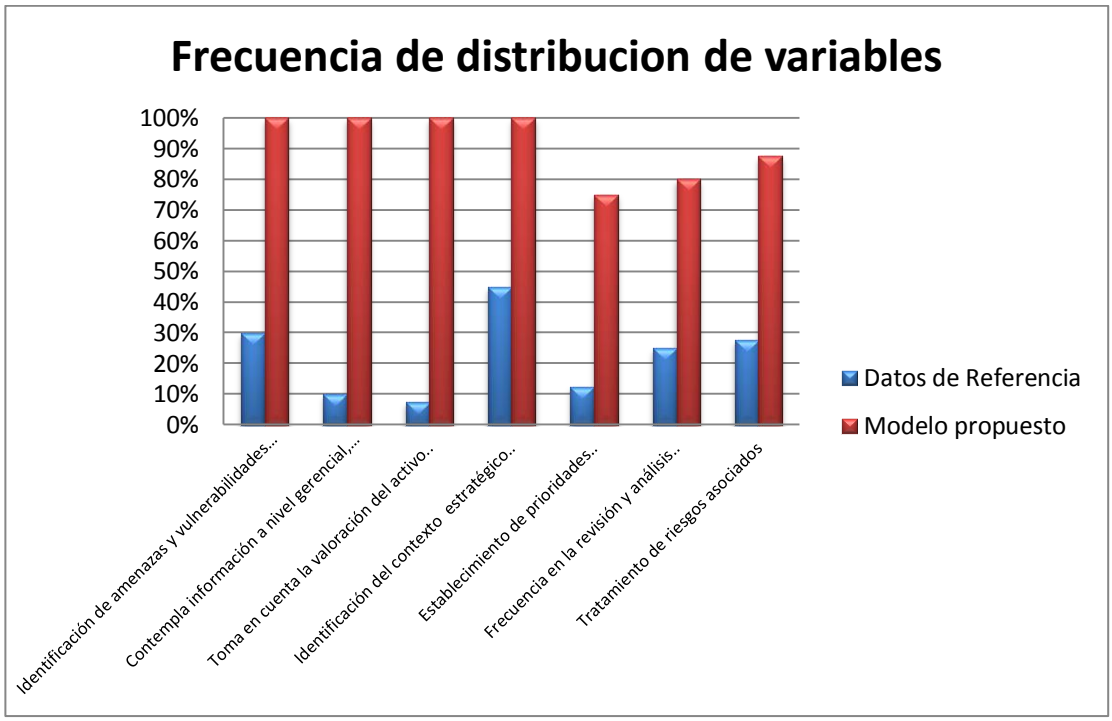


Figura Nº18. Diferencias entre frecuencias de distribución de variables expresada en columnas.

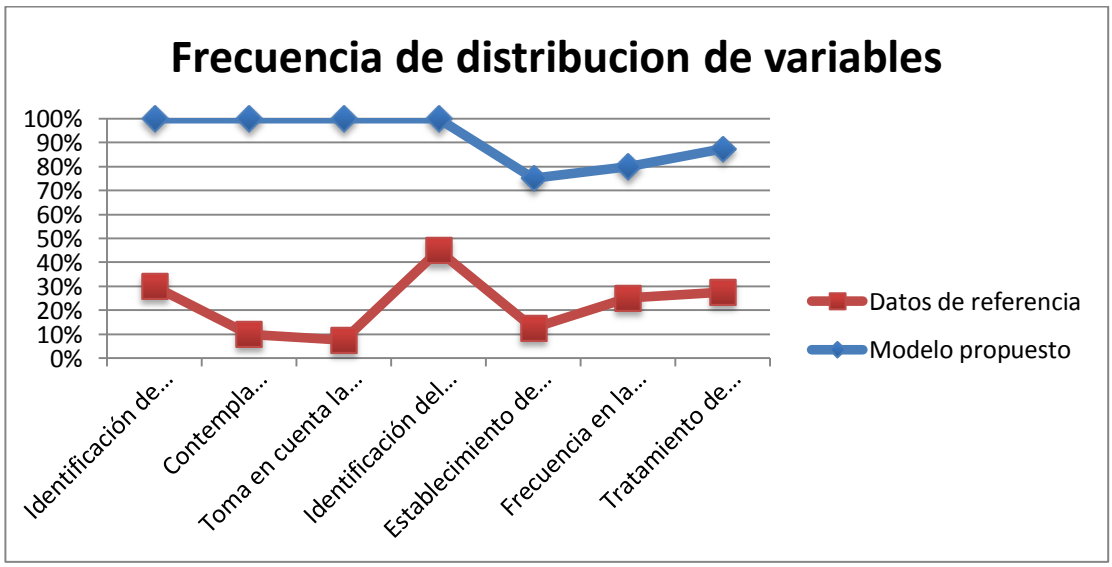


Figura Nº19. Diferencias entre frecuencias de distribución de variables expresada en líneas.

Al igual que ocurre en el proceso probado anteriormente, se puede observar la diferencia significativa entre las distribuciones de frecuencia, lo

cual evidencia una mejora considerable en la gestión de riesgos asociados a los activos de información con la aplicación del modelo. Los resultados obtenidos en las pruebas valida la precisión y eficiencia del modelo propuesto.

CAPITULO VII
EVALUACIÓN DEL PROYECTO

En el desarrollo de este TEG, fueron considerados los objetivos definidos en el Capítulo I, los cuales permitieron diseñar un modelo de gestión de seguridad de la información basado en ISO27001 para atender riesgos tecnológicos asociados a los activos y sistemas de información de los procesos de negocio de Bandes.

Si se realiza una verificación de los objetivos específicos planteados con los logros obtenidos, tenemos lo siguiente:

Objetivo específico N°1. Inventariar los sistemas informáticos que soportan los procesos de negocio de Bandes, obteniendo información sobre la valoración del impacto que puede suponer la pérdida de los mismos.

Este objetivo se cumplió mediante el desarrollo, consistentemente con los estándares y mejores prácticas consideradas para el manejo de la seguridad de la información, de un procedimiento para llevar a cabo el proceso de identificación y verificación de la información sobre los bienes informáticos contenidos en la plataforma tecnológica que soportan los procesos de negocios de Bandes; el cual al ser aplicado, permitió generar el inventario de los activos de información que allí residen, contemplando a su vez procedimientos para mantenerlo actualizado.

Objetivo específico N°2. Analizar en función a la confidencialidad, integridad, disponibilidad y uso, los activos de información de los procesos de negocio.

Este objetivo fue alcanzado satisfactoriamente mediante el desarrollo de un procedimiento que permite realizar la clasificación de los activos de información considerando las necesidades de negocios y operacionales, y

toma en cuenta la evaluación de amenazas, análisis de riesgos y análisis de impacto al negocio.

El procedimiento fue desarrollado consistentemente con los estándares y mejores prácticas consideradas para el manejo de la seguridad de la información; así como las normativas y leyes vigentes para el tratamiento de la información digital y activos de información, regulación bancaria y uso y costumbres aplicados a las organizaciones gubernamentales de la República Bolivariana de Venezuela. Al aplicar este procedimiento, se generó el documento de clasificación de activos de información asociados a los procesos de negocio de la institución.

Objetivo específico N°3. Identificar los riesgos asociados a los activos de información de los procesos de negocio.

Este objetivo fue cubierto satisfactoriamente mediante el desarrollo y aprobación de un proceso que permite el establecimiento efectivo de prácticas de seguridad de la información para la identificación de riesgos asociados a los activos y sistemas de información, el cual toma en consideración la valoración otorgada a los mismos de acuerdo a la relevancia del proceso de negocio al cual pertenecen. Esta valoración le permite al personal involucrado, tener una idea del impacto que un incidente puede causar a un proceso de negocio, al tomar en consideración el valor estratégico que posee para la organización como un todo. Al aplicar este procedimiento, se obtuvo el Informe de evaluación de riesgos asociados a los activos de información.

Objetivo específico N°4. Consolidar las bases del modelo propuesto a través de la definición de políticas y estándares, así como los controles y procedimientos que definan las reglas generales para la interacción con los activos de información de los procesos de negocio.

Este objetivo fue cubierto con el desarrollo y definición de documentos de políticas, normas y procedimientos que sustentan el modelo propuesto y tienen como finalidad consolidar y engranar las reglas o contramedidas de seguridad de la información para el establecimiento de un sistema de gestión robusto y a su vez flexible que se adapta a la organización y permiten el desarrollo de controles y procedimientos con criterios específicos para abordar situaciones concretas.

Objetivo específico N°5. Evaluar la metodología para la gestión de riesgos que será utilizada en el modelo propuesto, de acuerdo a los requerimientos del negocio.

Este objetivo fue alcanzado satisfactoriamente, mediante el desarrollo de un complemento a la metodología de gestión de riesgos adoptada por la organización previamente, con el objetivo de fortalecer el modelo de SGSI propuesto, mediante la estimación cualitativa de la exposición de riesgos de los activos de información de la Institución, basada en el estándar de aceptación general ISO/IEC 31000:2009.

CAPITULO VIII

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

De este Trabajo Especial de Grado, se pueden desprender un conjunto de conclusiones que se presentarán a continuación.

Se realizó un trabajo de investigación de campo, bibliográfica y documental de envergadura, para lograr los objetivos propuestos con la calidad requerida.

La implementación de un modelo que establece un Sistema de Gestión de Seguridad de la Información, permite que la Institución establezca y reordene la seguridad de los activos y sistemas de información de acuerdo a la relevancia del proceso de negocio al cual pertenecen, conforme a un procedimiento desarrollado consistentemente con los estándares y mejores prácticas consideradas para el manejo de la seguridad de la información; así como las normativas y leyes vigentes para el tratamiento de la información digital y activos de información, regulación bancaria, así como uso y costumbres aplicados a las organizaciones gubernamentales de la República Bolivariana de Venezuela.

Permite que los procesos de negocio de la Institución sean controlados mediante la identificación de riesgos asociados y la salvaguarda de sus activos críticos, a través de una metodología y basamento legal que permiten ordenar, sintetizar y simplificar de manera continua el esfuerzo que ya se realiza en cuanto a seguridad de la información se refiere.

Desde el punto de vista del análisis de riesgos que propone el modelo, estos se reducen notablemente a un nivel aceptado por la Institución, siempre en relación a sus objetivos de negocio.

Este modelo transforma el esfuerzo del personal de la Coordinación de Seguridad de la Información en una actividad de gestión, dejando a un lado la ejecución de actividades técnicas organizadas, para transformarse en un ciclo metódico y controlado, conocido por todos los involucrados, creando a su vez conciencia y compromiso de seguridad en todos los niveles donde sea aplicado.

Asegura el cumplimiento de todas las regulaciones vigentes para el tratamiento de la información digital y activos de información, aplicados a las organizaciones gubernamentales de la República Bolivariana de Venezuela, verificando su debida adecuación.

Con el desarrollo de este trabajo especial de grado, se logró generar conciencia en los usuarios, sobre la importancia de resguardar y aplicar los niveles de protección adecuados a los activos y sistemas de información asociados a los procesos de negocio, debido al entendimiento de la relación existente entre dichos activos y sistemas de información, y los activos de conocimiento para lograr los resultados esperados.

En base a la experiencia del trabajo realizado y a la disposición de la adopción del instrumento demostrada por el personal de la Coordinación de Seguridad de la Información, se puede concluir que la implementación del producto resultante de este trabajo de grado, es el comienzo de la gestión exitosa de seguridad.

Recomendaciones

Para el éxito de la gestión de riesgo tecnológico por el personal de la Coordinación de Seguridad de la Información, es necesario aplicar las oportunidades de mejora identificadas en este TEG.

Es conveniente que comiencen a dictarse talleres de adiestramiento al personal de las áreas involucradas en el proceso, sobre la aplicación del modelo y el análisis de los resultados que se obtendrán, para que al momento de implementar dicho instrumento a nivel general, el personal tenga claras las reglas y pueda dar mantenimiento, así como el debido cumplimiento de los controles que serán implementados, dándoles los argumentos necesarios en cada uno de los procesos de la gestión de riesgo.

Es necesario profundizar el desarrollo de políticas, normas y procedimientos que den basamento legal a este modelo.

REFERENCIAS BIBLIOGRÁFICAS

Arias, F. (2006). El proyecto de investigación. Introducción a la metodología científica. Quinta edición. Caracas: Editorial Episteme.

Banco de Desarrollo Económico y Social de Venezuela. (http://www.bandes.gob.ve 08/01/2012)

Banco de Desarrollo Económico y Social de Venezuela. Acuerdo de confidencialidad para el manejo de información. (http://intranet.bandes.gob.ve/instructivos/index.html)

Cano, F. (2011). Definición del alcance del SGSI en la norma ISO 27001. Publicación Online. Consultada por última vez el 05 de Febrero de 2012. Disponible en: http://www.seinhe.com/es/posts/16

Castañeda, L. y Quesada, W. (2007). Aplicación de la Norma Técnica ISO 27001:2005, para la Gestión de la Seguridad de la Información en la Dirección de Desarrollo Institucional (DDI) del Instituto Ecuatoriano de Seguridad Social (IESS). Escuela Politécnica Nacional, Ecuador.

Castro, C. (2007). Tests de Bondad de Ajuste basados en la distribución empírica para datos con y sin censura. Tesis de Maestría en Estadística Matemática. Universidad de Buenos Aires, Argentina.

CLUSIF (Club de la Sécurité de l'Information Français). (2009). [Online]. Risk Management – Concepts and Methods. Consultada por última vez el 02 de Agosto de 2012. http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-risk-management.pdf

Corletti, A. (2006). Análisis ISO-27001:2005. [Online]. Consultada por última vez el 22 de Octubre de 2011.

http://www.delitosinformaticos.com/11/2006/seguridad-informatica/analisis-iso-270012005

Duran & Asociados, Consultores de Riesgo. Criterios para la Clasificación de los Activos de Información. Octubre 28, 2011.

Duran & Asociados, Consultores de Riesgo. Definición de Normas: Clasificación de los Activos de Información. Octubre 28, 2011.

Duran & Asociados, Consultores de Riesgo. Instrumento para inventario de activos de información. Octubre 28, 2011.

Duran & Asociados, Consultores de Riesgo. Marco de Evaluación de Riesgos. Octubre 17, 2011.

Duran & Asociados, Consultores de Riesgo. Metodología para la Gestión de los Activos de Información de Bandes. Octubre 17, 2011.

Espiñeira, S. y Asociados. (2008). [Online]. Boletín Digital No. 12. Asesoría Gerencial. Consultado por última vez el 03 de Noviembre de 2011. http://www.pwc.com/ve/es/asesoria-gerencial/boletin/assets/boletin-advisory-edicion-12-2008.pdf

Estructura Organizativa del Banco de Desarrollo Económico y Social de Venezuela (Resolución Nº 348.2-11). (2011, Diciembre 21) Directorio Ejecutivo Nº 348, Marzo 15, 2009.

Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Tesis de Maestría en Ingeniería de Sistemas. Universidad Simón Bolívar, Venezuela.

Gestión-Calidad Consulting. (2011). [Online]. Seguridad de la Información (SI) y orígenes de los estándares ISO 27000. Consultado por última vez el 02

de Agosto de 2012. http://www.gestion-calidad.com/seguridad-informacion.html

Hernández, R., Fernández, C. y Baptista, P. (2007). Metodología de la Investigación. Cuarta Edición. McGraw-Hill: México.

Higson, C. y Waltho, D. (2010). [Online]. Valuing Information as an Asset. Consultado por última vez el 02 de Agosto de 2012. http://www.eurim.org.uk/activities/ig/InformationAsset.pdf

ISO/IEC. (2005). Estándar Internacional ISO/IEC 27001. Primera Edición.

ISO/IEC 31010:2009. (2009). Risk Management - Risk Assessment Techniques. Primera Edición.

Kendall, K. y Kendall, J. (2005). Análisis y Diseño de Sistemas. Sexta Edición. Pearson Educación: México.

MAGERIT. Metodología de Análisis y Sesión de Riesgos de los Sistemas de Información. Versión 2.0.

Manual de Políticas Operativas de Seguridad de la Información del Banco de Desarrollo Económico y Social de Venezuela. Código B_REI_SEI_PO001, (Resolución Nº 373.1-12). (2012, Agosto 23).

Matalobos, J. (2009). Análisis de Riesgos de Seguridad de la Información. Universidad Politécnica de Madrid, España.

Mayol, R. (2006). Modelo para la auditoria de la Seguridad Informática en la red de datos de la Universidad de los Andes. Tesis de Maestría en Computación. Universidad de los Andes, Venezuela.

Mendoza, R. (2010). Sistema de Gestión para la Seguridad de la Información – Caso: Centro de Tecnología de Información y Comunicación del Decanato

de Ciencias y Tecnología – UCLA. Tesis de Maestría en Ciencias de la Computación. Universidad Centroccidental Lisandro Alvarado, Venezuela.

Microsoft. (2005). [Online]. Guía de Administración de Riesgos de Seguridad. Consultado por última vez el 02 de Diciembre de 2011. http://www.microsoft.com/spain/technet/recursos/articulos/srsgch05.mspx

Monsalve, A. (2011). [Online]. Test de Bondad de Ajuste para modelos de tipo de interés: Un enfoque basado en procesos empíricos. Departamento de Estadística e Investigación Operativa, Universidad de Santiago de Compostela. Santiago de Compostela, España. Consultado por última vez el 03 de Agosto de 2012. http://dspace.usc.es/bitstream/10347/3651/1/9788498878349.pdf

Pallas, G. (2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Tesis de Maestría en Ingeniería en Computación, Universidad de la Republica, Uruguay.

Project Management Institute. (2008). Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK). Cuarta edición. Pennsylvania: Project Management Institute, Inc.

Reynaga, J. (2012). [Online]. Prueba de Bondad de Ajuste. Consultado por última vez el 05 de Agosto de 2012. http://www.facmed.unam.mx/deptos/salud/censenanza/planunico/spii/antologia2012/3.pdf

Ross, J. (2008). Residual Risk Management – A Quantitative approach to Information Security. Tesis de Maestría en Tecnología de Información y Negocios. University of Twente, Holanda.

SANS Institute. (2011). [Online]. Scoping Security Assessments - A Project Management Approach. Consultado por última vez el 03 de Agosto de 2012.

http://www.sans.org/reading_room/whitepapers/auditing/scoping-security-assessments-project-management-approach_33673

Superintendencia de las Instituciones del Sector Bancario. (2011). Informe de revisión especial de riesgo tecnológico – Bandes.

Superintendencia de las Instituciones del Sector Bancario. (2007). Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes sometidos al Control, Regulación y Supervisión de la Superintendencia de las Instituciones del Sector Bancario. Venezuela.

Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). (2010). Normas de Clasificación y Tratamiento de la Información. Providencia Administrativa Nº 009.10 del 21 de diciembre de 2010. Venezuela.

Transformación del Fondo de Inversiones de Venezuela en el Banco de Desarrollo Económico y Social de Venezuela (Decreto No. 1.274). (2001, Mayo 10) Gaceta Oficial de la República Bolivariana de Venezuela, 37.194 (Extraordinario), Abril 9, 2002.

Transformación del Fondo de Inversiones de Venezuela en el Banco de Desarrollo Económico y Social de Venezuela, reimpresión por error del ente emisor (Decreto No. 1.274). (2001, Junio 27) Gaceta Oficial de la República Bolivariana de Venezuela, 37.228 (Extraordinario), Abril 9, 2002.

Universidad Pedagógica Experimental Libertador. (2011). Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales. Cuarta edición. Caracas: UPEL.

Velazco, L. (Comp.) (2010). Instructivo Integrado para Trabajos Especiales de Grado (TEG). Caracas: Universidad Católica Andrés Bello, Copyright.

Zubcoff, J. (2008). [Online]. Introducción a la Inferencia Estadística. Universidad de Alicante, España. Consultado por última vez el 05 de Agosto de 2012. http://rua.ua.es/dspace/bitstream/10045/3893/1/1%20-%20Contraste%20de%20bondad%20de%20ajuste.pdf

ANEXOS

NOTA DE CONFIDENCIALIDAD

Los documentos contenidos en los anexos de este trabajo de investigación son de carácter confidencial, ya que contienen información relativa de empleados, contratistas, tecnologías de información y de seguridad, relacionada a Bandes. Dicha información ha sido destinada a demostrar las acciones realizadas durante el desarrollo de la presente investigación, y deberá ser mantenida en estricto secreto. No se podrá divulgar en forma alguna, la información producto de la aplicación del modelo de SGSI en Bandes, ni entregar a terceros, originales o copias de los documentos que forman parte del mismo, sin la previa autorización por escrito de Bandes.

Debido a la naturaleza de la información, tanto el "***Inventario de Activos de Información de Bandes***" como el documento de "***Clasificación de los activos de información de Bandes***", son un extracto de los documentos originales. Estos documentos, poseen información suficiente para demostrar el resultado de la aplicación del modelo propuesto en la Institución.

ANEXO N° 1

INVENTARIO DE ACTIVOS DE INFORMACIÓN DE BANDES

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
71500501	A	app	00001	LA SISTEMAS	Aplicativo para control de Fideicomisos	Registros de aportes, desembolsos, Control de inversiones y documentacion (Contratos de Fideicomiso)	Rafael Galanton	Coordinador	Nick Ramirez	Especlista Financ II	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor S01wp-app3	Confidencial	Francisco Albarran, Joani Hernandez, Nancy Pimentel, Jesue Medina, Dainy Ojeda, Jean Hernandez, Herber Vizcaya, Mariana Cuervo, Roberto Marcano, Victor Giron, Thais Arrechadera, Daniel Leonard, Maryorie Sanchez
71500502	A	app	00001	Oracle Financials	Aplicativo para control de Requisiciones	Control de los fideicomisos	Douglas Castro	Gerente	Yanine Rodriguez	Especialista Financiero	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor blade11	Protegida	Shirley Torres, Betzabeth Landaeta, Sonia Cortes, Carlos Fernandez, Linardo Rios, Noel Arteaga, Naya Salas, Laura Mora, Jose Osorio, Armando Bastardo, Erika Espinoza

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
71500502	A	app	00002	LA SISTEMAS	Aplicativo para elaboracion de reportes y contabilidad	Reportes y elaboracion de contabilidad	Douglas Castro	Gerente	Yanine Rodriguez	Especialista Financiero	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor S01wp-app3	Protegida	Shirley Torres, Betzabeth Landaeta, Sonia Cortes, Carlos Fernandez, Linardo Rios, Noel Arteaga, Naya Salas, Laura Mora, Jose Osorio, Armando Bastardo, Erika Espinoza
71000002	A	app	00001	SISCOPRO	Registro y control de proyectos financiados por el Fondo Conjunto Chino-Venezolano	Informes de Proyectos	Dennys Camejo	Especialista en Proyectos	Luis Almeida	Coordinador	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor appbandes	Confidencial	Leonardo Bermudez, Ayarit Rodriguez, Adela Salgado, Aroldo Souto
71000001	A	app	00001	RT (Request Tracker)	Sistema de seguimiento de tickets para coordinar tareas y solicitudes de una comunidad de usuarios. También se usará para control de la correspondencia	Recepción y emision de correspondencia	Cesar Cortissoz	Coordinador	Moira Viso	Abogado II	Piso 3, Torre Bandes. Centro de Datos Principal	Servidorrt	Protegida	Maria Gabriela Dona, Javier Gonzalez
71000300	A	app	00001	Trusstee	Aplicativo para control de Fideicomisos	Registros de aportes, desembolsos, Control de inversiones y documentacion (Contratos de Fideicomiso)	Javier Briceño	Gerente	Javier Briceño	Gerente	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor S01wp-app3	Confidencial	Personal de la Gerencia de Operaciones del Fondo Chino

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
71000300	A	app	00002	Siscopro	Registro y control de proyectos financiados	Registros de aportes, desembolsos, Control de inversiones y documentacion (Contratos de Fideicomiso)	Javier Briceño	Gerente	Javier Briceño	Gerente	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor appbandes	Confidencial	Personal de la Gerencia de Operaciones del Fondo Chino
71000300	A	app	00003	Oracle	Requisiciones de Ordenes Administrativa	Solicitudes de Ordenes Administrativas (Proveduria)	Gladys Ramirez	Especialista Banca II	Javier Briceño	Gerente	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor blade11	Protegida	Gladys Ramirez, Javier Briceño
71300200	A	app	00001	Gebos	Sistema que maneja toda la ruta crediticia	Sistema que maneja toda la ruta crediticia	Horacio Plaza	Gte de Analisis de Creditos	Ellen Moreno	Gte de la unidad	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor Gebos	Confidencial	Personal de la Gcia. de Análisis de Financiamiento
71300200	A	app	00002	Request Tracker	Sistema de seguimiento de tickets para coordinar tareas y solicitudes de una comunidad de usuarios. También se usará para control de la correspondencia	Gestion de requerimientos	Ellen Moreno	Gerente	Ellen Moreno	Gte de la unidad	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor app.intranet	Protegida	Personal de la Gcia. de Análisis de Financiamiento

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
71300101	A	app	00001	Request Tracker	Sistema de seguimiento de tickets para coordinar tareas y solicitudes de una comunidad de usuarios. También se usará para control de la correspondencia	Gestion de requerimientos	Joksi Badillo	Coordinador	Joksi Badillo	Coordinador	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor app.intranet	Confidencial	Personal de la Coord. de Seguimiento y Control
71300101	A	app	00002	Gebos	Sistema que maneja toda la ruta crediticia	Nuevos creditos que se incorporan a la ruta crediticia	Joksi Badillo	Coordinador	Joksi Badillo	Coordinador	Piso 3, Torre Bandes. Centro de Datos Principal	ServidorGebos	Confidencial	Personal de la Coord. de Seguimiento y Control
71300100	A	app	00001	Oracle Financial	Aplicativo para control de Requisiciones	Desembolso	Francisco Contreras	Coordinador	Francisco Contreras	Coordinador	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor blade11	Confidencial	Personal de la Gcia. de Administración de Contratos
70800001	A	app	00001	Oracle Aplication Manager	Control presupuestario	Control presupuestario	Vilma Parra	Coordinador	Vilma Parra	Coordinador	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor blade11	Confidencial	Eloy Lopez, Nancy Rodriguez, Vilma Parra, Raiza Rojas,Angie Gonzalez
71300302	A	app	00001	Gebos	Sistema de Crédito	Control de gestion crediticia/ (aprobado, liquidado y cobrado) Políticas de financiamiento/ Presupuesto.	Ellen Karina Moreno	Gerente Ejecutiva	Arturo Gutierrez	Gerente Proyecto	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor Gebos	Restringida	Toda la ruta crediticia

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
70300201	A	app	00001	Sistema de Nómina y Personal TIACA	Manejo de los Recursos Humanos y la Nómina de BANDES	Manejo de los Recursos Humanos y la Nómina de BANDES	Andy Jimenez	Especialista	Tecnologia		Piso 3, Torre Bandes. Centro de Datos Principal	Servidor tiaca.dca	Confidencial	Andy Jimenez, Hugo Laffe, Eggle Rizquez, Alicia Alaya, Nayari Bandes, Juan Gonzalez, Pablo Marquez, Aaron Moncada
70300201	A	app	00002	FORMULARIOS RRHH	Generación de Formularios de Ley tipo 14- (se entrega a personal que trabajo para organismos cuya custodia la tiene BANDES, como Viasa)	Custodia de expedientes de personal activo y relacionado / emision de certificados de constancias	Aaron Moncada	Especialista	Pablo Marquez	Especialista	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor ccsbandesdat2	Protegida	Andy Jimenez
70300201	A	app	00003	Recibos Electrónicos de Pago de Nomina	Generación en formato .pdf de los recibos de pago de la Nómina	Generacion de Recibos de pagos de nómina	Andy Jimenez	Especialista	Tecnologia		Piso 3, Torre Bandes. Centro de Datos Principal	Servidor aplicaciones	Confidencial	Andy Jimenez, Hugo Laffe, Eggle Rizquez, Alicia Alaya, Nayari Bandes, Juan Gonzalez, Pablo Marquez, Aaron Moncada
71400100	A	app	00001	Control de proyectos de Cooperación Internacional	Sistema para el control y manejo de los proyectos de cooperacion internacional	Control de proyectos: solicitud y evaluación y contratos.	María Ledesma	Gerente	María Ledesma	Gerente	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor aplicaciones	Confidencial	Personal de la Gerencia de Cooperacion Internacional

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
71500000	A	app	00001	LA Sistemas - Módulo Portafolio (Push trust)	Módulo que controla el portafolio de inversiones de los contratos de fideicomisos en forma centralizada	Control y creacion de portafolios	Marcos Silva	Gerente	Marcos Silva	Gerente	Piso 3, Torre Bandes. Centro de Datos Principal	Servidors01 wp-app3	Confidencial	Todos
71500000	A	app	00002	CUSTODIA DE TITULOS VALORES (ULTRAFU ERTE)	Registro y control de la custodia de Titulos Valores de la cartera propia	Registro y control de custodia de títulos valores de cartera propia	Marcos Silva	Gerente	Marcos Silva	Gerente	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor s01wp-app3	Confidencial	Janeth Gallo , Marcos Silva y Francisco Dáscoli
71500000	A	app	00003	ULTRASEC	Manejo de operaciones en mercado monetario y renta fija	Aperturas, cancelacion y renovaciones	Marcos Silva	Gerente	Marcos Silva	Gerente	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor s01wp-app3	Confidencial	Todos
71500000	A	app	00004	ULTRAFLO W	Flujo de cada una de las cuentas corresponsales de BANDES	Movimientos de cuentas por dia (mercado monetario, desembolsos y operaciones)	Marcos Silva	Gerente	Marcos Silva	Gerente	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor s01wp-app3	Confidencial	Todos
71500100	A	app	00001	TESORERI A (ULTRASE C, ULTRAFLO W de LA Sistemas)	Registro y manejo de las Operaciones de Tesorería de BANDES (Tradding, Flujo de Caja (Consulta)	Registro y manejo de las Operaciones de Tesorería de BANDES (Tradding, Flujo de Caja (Consulta) / Operaciones diarias de Tesoreria	Hilmer Cardenas	Especialista Integral	Adolfo Cardenas	Gerente	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor s01wp-app3	Restringida	Nelson Perdomo, David Perez, Jose Luis Rodriguez, Ernesto Tellez

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
71500100	S	ext	00001	Bloomberg	Terminal de consulta	Precios de mercados (bonos, confirmaciones, chats con bancos del exterior)	David Perez	Especialista Financiero	Nelson Perdomo	Especialista Financiero	Proveedor Externo	Proveedor Externo	Protegida	Jose Luis Rodriguez, Adolfo Maldonado, Hilmer Cardenas, Ernesto Tellez
71500100	S	ext	00001	Reuters	Modulo de Consulta	Chequeo de información	Nelson Perdomo	Especialista Financiero	David Perez	Especialista Financiero	Proveedor Externo	Proveedor Externo	Protegida	Jose Luis Rodriguez, Adolfo Maldonado, Hilmer Cardenas, Ernesto Tellez
70400002	D	int	00001	Carpetas Compartidas	Carpetas Compartidas	Ayudas de Salud a personas de escasos recursos / Información del Solicitante / Información del Beneficiario	Saray Chang	Coordinadora	Miriam Garcia	Gerente Ejecutiva	Piso 3, Torre Bandes. Centro de Datos Principal	Servidores ccsbandesdat ccsbandesdat2	Confidencial	Auxiliadora Valera, Renny Valderrama, Isbelia Lobo
71500501	D	Int	00001	Carpetas compartidas (4)	Carpetas compartidas de los procesos	Registros de aportes, registro de las solicitudes de desembolsos	Rafael Galanton	Coordinador	Maryorie Sanchez	Especialista Financ III	Piso 3, Torre Bandes. Centro de Datos Principal	Servidorescsbandesdatccsbandesdat2	Confidencial	Francisco Albarran, Joani Hernandez, Nancy Pimentel, Jesue Medina, Dainy Ojeda, Jean Hernandez, Herber Vizcaya, Mariana Cuervo, Roberto Marcano, Victor Giron, Thais Arrechadera, Daniel Leonard, Nick Ramirez

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
71500502	D	int	00001	Carpetas Compartidas (4)	Carpetas compartidas	Estados de cuenta y estados financieros / informacion de reporteria del cliente (saldos de fondos fiduciarios)	Douglas Castro	Coordinador	Yanine Rodriguez	Especialista Financ III	Piso 3, Torre Bandes. Centro de Datos Principal	Servidores ccsbandesdat ccsbandesdat2	Protegida	Shirley Torres, Betzabeth Landaeta, Sonia Cortes, Carlos Fernandez, Linardo Rios, Noel Arteaga, Naya Salas, Laura Mora, Jose Osorio, Armando Bastardo, Erika Espinoza
71000002	D	int	00001	Carpeta Compartidas	Carpetas compartidas	Informes de Inspeccion	Dennys Camejo	Especialista de Proyectos	Luis Almeida	Coordinador	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor ccsbandesdat	Confidencial	Leonardo Bermudez, Ayarit Rodriguez, Adela Salgado, Aroldo Souto
71000002	D	int	00002	Archivos en PC (no compartidos)	Archivos que se encuentran en la pc de los usuarios	Cronogramas / Memoria Fotográfica / Solicitud de Viaticos / Etiquetado de Carpetas	Dennys Camejo	Especialista de Proyectos	Luis Almeida	Coordinador	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor ccsbandesdat	Confidencial	Leonardo Bermudez, Ayarit Rodriguez, Adela Salgado, Aroldo Souto
71000001	D	int	00001	Carpeta Compartidas	Carpetas Compartidas	Desembolsos a cada proyecto / Convenios interinstitucionales / Puntos de Cuentas	Cesar Cortissoz	Coordinador	Moira Viso	Abogado II	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor ccsbandesdat	Confidencial	Javier Gonzalez, Maria Gabriela Dona
71000300	D	int	00001	Carpeta Compartidas	Estados de cuenta de Bancos Externos,	Estados de cuenta de Bancos Externos,	Desiree Gomez	Especialista Banca I	Ana Carolina Quero	Especialista Banca II	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor ccsbandesdat	Confidencial	Hugo Hersen, Gladis Ramirez, Ana Karina Quero, Alexander Bello, Angel Daniel Davila

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
71000300	D	int	00002	Carpeta Compartidas	Estados de cuentas que emite la unidad	Estados de cuentas que emite la unidad (movimientos generados por la unidad)	Javier Briceño	Gerente	Hugo Hersen	Especialista Integral	Piso 3, Torre Bandes. Centro de Datos Principal	Servidorccsbandesdat	Confidencial	Hugo Hersen, Gladis Ramirez, Ana Karina Quero, Alexander Bello, Angel Daniel Davila
71400100	D	int	00005	Desembolsos Bandes	Archivo Digital: Informes de Desembolsos Bandes	Desembolsos	Johana Martínes, Victor Quiñonez, Diomara Rondón, Anabel Becerra, Frank García, Ciro Uzcátegui	Especialista en banca de desarrollo III	Mario Rodriguez	Archivista	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor ccsbandesdat	Protegida	Johana Martínes, Victor Quiñonez, Diomara Rondón, Anabel Becerra, Frank García, Ciro Uzcátegui
71400100	D	int	00006	Desembolsos Fondos Administrados	Archivi Digital: Informes de Desembolsos Fondos Administrados	Desembolsos	Johana Martinez, Victor Quiñonez, Diomara Rondón	Especialista en banca de desarrollo III	Mario Rodriguez	Archivista	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor ccsbandesdat	Protegida	Johana Martínez, Victor Quiñonez, Diomara Rondón
71400100	S	int	00001	Desembolsos	Procesos de Desembolsos	Desembolsos	Todos	Especialista	Todos	Especialista	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor ccsbandesdat	Confidencial	Todos
71400100	S	int	00002	Cierres financieros Bandes	Cierres financieros Bandes	Cierres financieros Bandes	Juan Carlos Camacho, Victor Quiñonez, Diomara Rondón	Especialista	Juan Carlos Camacho, Victor Quiñonez, Diomara Rondón	Especialista	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor ccsbandesdat	Confidencial	Juan Carlos Camacho, Victor Quiñonez, Diomara Rondón
71400100	S	int	00003	Cierres financieros fondos administrados a terceros	Cierres financieros fondos administrados a terceros	Cierres financieros fondos administrados a terceros	Johana Martinez, Victor Quiñonez, Diomara Rondón	Especialista	Johana Martinez, Victor Quiñonez, Diomara Rondón	Especialista	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor ccsbandesdat	Confidencial	Johana Martinez, Victor Quiñonez, Diomara Rondón

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
71500000	D	int	00001	Administración de Fondos: Soporte Operaciones financieras	Ubicación de todas las carpetas de la unidad	Liquidez de moneda para los procesos operativos (Control) y chequeo de disponibilidad de esos recursos	Marcos Silva	Gerente de operaciones Financieras	Marcos Silva	Gerente de operaciones Financieras	Piso 3, Torre Bandes. Centro de Datos Principal	Servidores ccsbandesdat ccsbandesdat2	Confidencial	Todos
71500100	D	int	00001	Carpeta Compartida	Carpeta compartida donde se almacenan los procesos	Informes de Tesoreria / Cierre diario de Carteras / Gestiones Semanales de Tesoreria / Flujos de efectivo	Hilmer Cardenas	Especialista Integral	Ernesto Tellez	Especialista Financiero II	Piso 3, Torre Bandes. Centro de Datos Principal	Servidores ccsbandesdat ccsbandesdat2	Confidencial	Nelson Perdomo, David Perez, Jose Luis Rodriguez, Adolfo Maldonado
70000000	D	int	00001	Carpetas Compartidas	Carpetas Compartidas del Directorio	Actas del Directorio / Agendas de Reuniones	Fabiola Juarez	Abogado I	Thairi Moya	Gerente Encargada	Piso 3, Torre Bandes. Centro de Datos Principal	Servidores ccsbandesdat ccsbandesdat2	Restringida	Marjorie Sanchez
70000000	D	int	00002	Carpetas Compartidas	Carpetas Compartidas del Directorio	Correspondencia Interna	Fabiola Juarez	Abogado I	Thairi Moya	Gerente Encargada	Piso 3, Torre Bandes. Centro de Datos Principal	Servidorescsbandesdatccsbandesdat2	Restringida	Marjorie Sanchez
70000000	D	int	00003	Carpetas Compartidas	Carpetas Compartidas del Directorio	Correspondencia Externa	Fabiola Juarez	Abogado I	Thairi Moya	Gerente Encargada	Piso 3, Torre Bandes. Centro de Datos Principal	Servidores ccsbandesdat ccsbandesdat2	Restringida	Marjorie Sanchez
70000000	D	int	00004	Carpetas Compartidas	Carpetas Compartidas del Directorio	Archivo Presidencia	Fabiola Juarez	Abogado I	Thairi Moya	Gerente Encargada	Piso 3, Torre Bandes. Centro de Datos Principal	Servidores ccsbandesdat ccsbandesdat2	Restringida	Marjorie Sanchez

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
70400002	I	printed	00001	Expedientes de casos de ayudas sociales	Casos de ayudas otorgadas	Casos de ayuda	El que realiza la carga es el responsable		Miriam Garcia	Gerente Ejecutiva	MZ 1		Confidencial	Auxiliadora Valera, Saray Chang, Ysvelia Lobo
71500501	I	printed	00001	Expedientes en Fisico	Expedientes	Expedientes de Fideicomisos y Pagos	Rafael Garanton	Coordinador	Maryorie Sanchez	Especialista	Piso 5		Confidencial	Francisco Albarran, Joani Hernandez, Nancy Pimentel, Jesue Medina, Dainy Ojeda, Jean Hernandez, Herber Vizcaya, Mariana Cuervo, Roberto Marcano, Victor Giron, Thais Arrechadera, Daniel Leonard, Nick Ramirez
71500502	I	printed	00001	Expedientes	Expendientes físicos	Expedientes de desembolsos	Douglas Castro	Coordinador	Yanine Rodriguez	Especialista Financiero	Piso 6		Protegida	Shirley Torres, Betzabeth Landaeta, Sonia Cortes, Carlos Fernandez, Linardo Rios, Noel Arteaga, Naya Salas, Laura Mora, Jose Osorio, Armando Bastardo, Erika Espinoza
71000002	I	printed	00001	Informe de Inspeccion	Informe de Inspeccion	Informes de Inspeccion	Dennys Camejo	Especialista en Proy	Luis Almeida	Coordinador	CFL Piso 23		Confidencial	Leonardo Bermudez, Ayarit Rodriguez, Adela Salgado, Aroldo Souto

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
71000001	I	printed	00001	Expediente	Expedientes de Requerimientos	Soportes de convenios / soportes desembolsos	Abogado que maneja el caso		Cesar Cortissoz	Coordinador	CFL Piso 23		Confidencial	Moira Viso, Javier Gonzalez, Maria Gabriela Dona
71000300	I	printed	00001	Expediente	Expedientes de Clientes	Elaboracion de estados de cuentas	Especialista que tenga el caso		Hugo Hersen	Especialista	CFL Piso 23		Confidencial	Desiree Gomez, Gladis Ramirez, Ana Karina Quero, Alexander Bello, Angel Daniel Davila
71300200	I	printed	00001	Expedientes	Expedientes	Analisis de Financiamiento	Cada usuario		Cada Usuario		Mezanina Veroes		Pública	Cada Analista
71300101	I	printed	00001	Expediente	Expediente de Credito	Expediente de Credito		Gcia de Credito	Nilza Perez	Archivo	Veroes Sotano		Confidencial	Todos
70300201	I	printed	00001	Expedientes	Expedientes de nomina y personal	Expedientes de nomina y personal	Aaron Moncada	Especialista	Pablo Marquez	Especialista	Piso 5		Confidencial	Andy Gimenez
60900200	D	bd	00004	ORACLE_FINANZAS	Base de datos relacionados a los procesos financieros, conectada al aplicativo LA SISTEMAS	Procesos de manejo de Tesorería e Inversiones financieras, incluyendo fideicomisos	Gerente Ejecutivo de Finanzas y Administración de Fondos	Gerente Ejecutivo María de los Angeles	America Delima / Yoxaide Jimenez	Especialista Tecnológico	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor orafin	Confidencial	Gcia. Ejecutiva de Finanzas; America Delima
60900200	D	bd	00005	ORACLEPROD	Base de datos administrativa (app oracle financial)	Procesos administrativos de Bandes (presupuesto, compras, pagos, contabilidad, activo fijo)	Gerente Ejecutivo de Administración	Gerente María Eugenia Jardín	America Delima / Yoxaide Jimenez	Especialista Tecnológico III	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor oraprod	Protegida	Gerentes, Coordinadores, Asistentes; Gcia. Ejecutiva de Administración
60900200	D	bd	00006	ORACLE_RRHH	BD conectada a Aplicativo Tiaca	Procesos RRHH y Procesos de Pago (Nómina)	Gerente Ejecutivo Gestión Talento Humano	Gerente: Marianela Veitia	America Delima / Yoxaide Jimenez	Especialista Tecnológico II	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor oraadinrh	Confidencial	Gcia. Ejecutiva Gestión Talento Humano

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
60900200	D	bd	00007	ORACLE_ADIN (POA)	Base de datos de aplicaciones desarrolladas internamente (Plan Operativo Anual)	Proceso de control y seguimiento del Plan Operativo Anual hasta el cierre el proceso de formulación	Gerente de Planificación y Gestión Estratégica	Gerente José Herrera Rodríguez	America Delima / Yoxaide Jimenez	Especialista Tecnológico III	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor oraadinrh	Confidencial	Coordinadores; Gerentes y especialistas integrales
60900200	D	bd	00008	ORACLE_ADIN (PPL)	Base de datos de aplicaciones desarrolladas internamente (PPL: Plan de Participación Laboral-Bandes)	Control y seguimineto de la cobranza producto de la venta de las acciones de los diferentes PPL a los trabajadores elegibles de las empresas privatizadas	Gerente Ejecutivo de Finanzas y Administración de Fondos	Gerente María de los Angeles González	America Delima / Yoxaide Jimenez	Especialista Tecnológico III	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor oraadinrh	Restringida	Supervisor Jonathan Hernandez, Violeta Silva.
60900200	D	bd	00009	ORACLE_ADIN (SRC)	Base de datos de aplicaciones desarrolladas internamente (Sistema de Registro de Consultores)	Registro y control de consultores de Bandes	Gerente Ejecutivo de Administración	Gerente María Eugenia Jardín	America Delima / Yoxaide Jimenez	Especialista Tecnológico III	Piso 3, Torre Bandes. Centro de Datos Principal	Servidorora adinrh	Confidencial	Unidad de Registro de Consultores, Proveedores y Contratistas: Demetrio Arenare, Noraima Oropeza, Antonio Rodríguez
60900200	D	bd	00010	ORACLE_ADIN (ARCHIVO)	Registro de Microcreditos otorgados durante los años 2002-2005	Utilizado para Consulta de Microcreditos otorgados durante los años 2002-2005	Gerente Ejecutivo de Cooperación y Financiamiento Nacional	Gerente Karina Moreno	America Delima / Yoxaide Jimenez	Especialista Tecnológico III	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor oraadinrh	Confidencial	Coord. de Prevención y Control del Legitimación de Capitales y Financiamiento al Terrorismo
60900200	D	bd	00012	POSTGRESQL_ADIN (AYUDASOCIAL)	Base de datos de aplicativo de registro y control ayudas sociales	Procesos programas sociales	Gcia. de Infraestructura y Servicios Tecnológicos	Gerente Ferdinando Soares	America Delima / Yoxaide Jimenez	Especialista Tecnológico III	Piso 3, Torre Bandes. Centro de Datos	Servidor cachapa	Confidencial	Coord. de Programación Social

Área	Tipo	Clase	Núm.	Nombre	Descripción	Proceso critico asociado	Propietario	Cargo	Custodio	Cargo	Ubic. Física	Ubic. Lógica	Clasificación	Personal Autorizado
											Principal			
60900200	D	bd	00019	POSTGRESQL_ADIN (PRESUPUESTO)	Base de datos sistema de presupuesto	Formulación del presupuesto	Gerente de Planificación y Gestión Estratégica	Gerente José Herrera Rodríguez	America Delima / Yoxaide Jimenez	Especialista Tecnológico III	Piso 3, Torre Bandes. Centro de Datos Principal	Servidor cachapa	Restringida	Belkys Castillo Eduardo Caraballo Rosa Chirinos

ANEXO N° 2

CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN DE BANDES

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71500501	A	app	00001	LA SISTEMAS	Modulo completo	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71500502	A	app	00001	Oracle Financials	Aplicativo para control de Fideicomisos	Protegida	M	A	A	MAA	El control de acceso para los activos de información es requerido. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71500502	A	app	00002	LA SISTEMAS	Aplicativo para elaboracion de reportes y contabilidad	Protegida	M	A	A	MAA	El control de acceso para los activos de información es requerido. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71000002	A	app	00001	SISCOPRO	Registro y control de proyectos financiados por el Fondo Conjunto Chino-Venezolano	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71000001	A	app	00001	RT (Request Tracker)	Actividades muy puntuales	Protegida	M	M	M	MMM	El control de acceso para los activos de información requiere autenticación robusta. El proceso de integridad está basado en la protección a los accesos y a la restauración vía respaldos. La disponibilidad puede ser soportada con base a recuperación vía respaldos o de la alta disponibilidad.
71000300	A	app	00001	Trusstee	En Desarrollo	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71000300	A	app	00002	Siscopro	En Desarrollo	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71000300	A	app	00003	Oracle	Requisiciones de Ordenes Administrativa	Protegida	M	A	A	MAA	El control de acceso para los activos de información es requerido. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71300200	A	app	00001	Gebos	Sistema que maneja toda la ruta crediticia	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71300200	A	app	00002	Request Tracker	Sistema de seguimiento de tickets para coordinar tareas y solicitudes de una comunidad de usuarios. También se usará para control de la correspondencia	Protegida	M	A	A	MAA	El control de acceso para los activos de información es requerido. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71300101	A	app	00001	Request Tracker	Sistema de seguimiento de tickets para coordinar tareas y solicitudes de una comunidad de usuarios. También se usará para control de la correspondencia	Confidencial	A	A	M	AAM	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad no es requerida como una condición importante.
71300101	A	app	00002	Gebos	Sistema que maneja toda la ruta crediticia	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71300100	A	app	00001	Oracle Financial		Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
70800001	A	app	00001	Oracle Aplication Manager	Control presupuestario	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71300302	A	app	00001	Gebos	Sistema de Crédito (En proceso de implementación)	Restringida	MA	A	A	MAAA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
70300201	A	app	00001	Sistema de Nómina y Personal TIACA (Tecnología de Información Abierta C.A.)	Manejo de los Recursos Humanos y la Nómina de BANDES	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
70300201	A	app	00002	FORMULARIOS RRHH (egresados)	Generación de Formularios de Ley tipo 14- (se entrega a personal que trabajo para organismos cuya custodia la tiene BANDES, como Viasa)	Protegida	M	A	M	MAM	El control de acceso para los activos de información requiere autenticación robusta. La integridad es importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad puede ser soportada con base a recuperación vía respaldos o de la alta disponibilidad.
70300201	A	app	00003	Recibos Electrónicos de Pago de Nomina	Generación en formato .pdf de los recibos de pago de la Nómina	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71400100	A	app	00001	Control de proyectos de Cooperación Internacional	Sistema para el control y manejo de los proyectos de cooperacion internacional	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71500000	A	app	00001	LA Sistemas - Módulo Portafolio (Push trust)	Módulo que controla el portafolio de inversiones de los contratos de fideicomisos en forma centralizada	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71500000	A	app	00002	CUSTODIA DE TITULOS VALORES (ULTRAFUERTE)	Registro y control de la custodia de Titulos Valores de la cartera propia	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71500000	A	app	00003	ULTRASEC	Manejo de operaciones en mercado monetario y renta fija	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71500000	A	app	00004	ULTRAFLOW	Flujo de cada una de las cuentas corresponsales de BANDES	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71500100	A	app	00001	TESORERIA (ULTRASEC, ULTRAFLOW de LA Sistemas)	Registro y manejo de las Operaciones de Tesorería de BANDES (Tradding, Flujo de Caja (Consulta)	Restringida	MA	A	A	MAAA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71500100	S	ext	00001	Bloomberg	Terminal de consulta	Protegida	M	A	A	MAA	El control de acceso para los activos de información es requerido. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71500100	S	ext	00001	Reuters	Modulo de Consulta	Protegida	M	A	A	MAA	El control de acceso para los activos de información es requerido. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
70400002	D	int	00001	Carpetas Compartidas	Carpetas Compartidas	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71500501	D	Int	00001	Carpetas compartidas (4)	Carpetas compartidas de los procesos	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71500502	D	int	00001	Carpetas Compartidas (4)	Carpetas compartidas	Protegida	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71000002	D	int	00001	Carpeta Compartidas	Carpetas compartidas	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71000002	D	int	00002	Archivos en PC (no compartidos)	Archivos que se encuentran en la pc de los usuarios	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71000001	D	int	00001	Carpeta Compartidas	Carpetas Compartidas	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71000300	D	int	00001	Carpeta Compartidas	Estados de cuentas que emite la unidad	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71000300	D	int	00002	Carpeta Compartidas	Estados de cuenta de Bancos Externos,	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71400100	D	int	00005	Desembolsos Bandes	Archivo Digital: Informes de Desembolsos Bandes	Protegida	M	A	A	MAA	El control de acceso para los activos de información es requerido. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71400100	D	int	00006	Desembolsos Fondos Administrados	Archivi Digital: Informes de Desembolsos Fondos Administrados	Protegida	M	A	A	MAA	El control de acceso para los activos de información es requerido. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71400100	S	int	00001	Desembolsos	Procesos de Desembolsos	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71400100	S	int	00002	Cierres financieros Bandes	Cierres financieros Bandes	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71400100	S	int	00003	Cierres financieros fondos administrados a terceros	Cierres financieros fondos administrados a terceros	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71500000	D	int	00001	Administración de Fondos: Soporte Operaciones financieras	Ubicación de todas las carpetas de la unidad	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71500100	D	int	00001	Carpeta Compartida	Carpeta compartida donde se almacenan los procesos	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
70000000	D	int	00001	Carpetas Compartidas	Carpetas Compartidas del Directorio	Restringida	MA	A	A	MAAA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
70000000	D	int	00002	Carpetas Compartidas	Carpetas Compartidas del Directorio	Restringida	MA	A	A	MAAA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
70000000	D	int	00003	Carpetas Compartidas	Carpetas Compartidas del Directorio	Restringida	MA	A	A	MAAA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
70000000	D	int	00004	Carpetas Compartidas	Carpetas Compartidas del Directorio	Restringida	MA	A	A	MAAA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
70400002	I	printed	00001	Expedientes de casos de ayudas sociales	Casos de ayudas otorgadas	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71500501	I	printed	00001	Expedientes en Fisico	Expedientes	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71500502	I	printed	00001	Expedientes	Expendientes físicos	Protegida	M	A	M	MAM	El control de acceso para los activos de información requiere autenticación robusta. La integridad es importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad puede ser soportada con base a recuperación vía respaldos o de la alta disponibilidad.
71000002	I	printed	00001	Informe de Inspeccion	Informe de Inspeccion	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71000001	I	printed	00001	Expediente	Expedientes de Requerimientos	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71000300	I	printed	00001	Expediente	Expedientes de Clientes	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
71300200	I	printed	00001	Expedientes	Expedientes	Pública	B	B	B	BBB	El acceso al servicio, sistemas, información o área no requiere autenticación. Es posible que la afectación de la integridad no represente mayor necesidad, así como el acceso al servicio en forma constante.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
71300101	I	printed	00001	Expediente	Expediente de Credito	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
70300201	I	printed	00001	Expedientes	Expedientes de nomina y personal	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
60900200	D	bd	00004	ORACLE_FINANZAS	Base de datos relacionados a los procesos financieros, conectada al aplicativo LA SISTEMAS	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
60900200	D	bd	00005	ORACLEPROD	Base de datos administrativa (app oracle financial)	Protegida	M	A	A	MAA	El control de acceso para los activos de información es requerido. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
60900200	D	bd	00006	ORACLE_RRHH	BD conectada a Aplicativo Tiaca	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
60900200	D	bd	00007	ORACLE_ADIN (POA)	Base de datos de aplicaciones desarrolladas internamente (Plan Operativo Anual)	Confidencial	A	A	A	AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.
60900200	D	bd	00008	ORACLE_ADIN (PPL)	Base de datos de aplicaciones desarrolladas internamente (PPL: Plan de Participación Laboral-Bandes)	Restringida	MA	A	A	MAAA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Área	Tipo	Clase	Núm.	Nombre	Descripción	Clasificación	Criterios				Contramedidas
							C	I	D	Total	
60900200	D	bd	00009	ORACLE_ADIN (SRC)	Base de datos de aplicaciones desarrolladas internamente (Sistema de Registro de Consultores)	Confidencial	A	A	M	AAM	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad no es requerida como una condición importante.
60900200	D	bd	00010	ORACLE_ADIN (ARCHIVO)	Registro de Microcreditos otorgados durante los años 2002-2005	Confidencial	A	A	B	AAB	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad no es requerida como una condición importante.
60900200	D	bd	00012	POSTGRESQL_ADIN (AYUDASOCIAL)	Base de datos de aplicaciones desarrolladas internamente (Directorio Telefónico)	Pública	B	A	M	B AM	El control de acceso para los activos de información requiere autenticación robusta. El proceso de integridad está basado en la protección a los accesos y a la restauración vía respaldos. La disponibilidad puede ser soportada con base a recuperación vía respaldos o de la alta disponibilidad.
60900200	D	bd	00019	POSTGRESQL_ADIN (PRESUPUESTO)	Base de datos sistema de presupuesto	Restringida	MA	A	A	MAAA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.

Definición de criterios de clasificación de activos de información y acciones de protección

Criterios	Acción de Protección	Clasificación (Leyenda)
AAA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.	**Confidencialidad:** Alta **Integridad:** Alta **Disponibilidad:** Alta := AAA
AAB	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad no es requerida como una condición importante.	**Confidencialidad:** Alta **Integridad:** Alta **Disponibilidad:** Baja := AAB

Criterios	Acción de Protección	Clasificación (Leyenda)
AAM	El acceso a la información requiere autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad puede ser soportada con base de recuperación vía respaldos o de la alta disponibilidad.	**Confidencialidad:** Alta **Integridad:** Alta **Disponibilidad:** Media := AAM
AAMA	El acceso a la información requiere autenticación robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente.La disponibilidad apropiada para no permitir la interrumpción del acceso al activo o reestablecer su disponibilidad del activo de información en forma inmediata es requerida.	**Confidencialidad:** Alta **Integridad:** Alta **Disponibilidad:** Muy Alta := AAMA

Criterios	Acción de Protección	Clasificación (Leyenda)
ABA	El acceso a los activos de información requiere de autenticación robusta. Es posible que la afectación de la integridad no represente mayor necesidad, así como el acceso al servicio en forma constante. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.	**Confidencialidad:** Alta **Integridad:** Baja **Disponibilidad:** Alta := ABA
ABB	El acceso a los activos de información requiere de autenticación robusta. Es posible que la afectación de la integridad no represente mayor necesidad. La disponibilidad no es requerida como una condición importante.	**Confidencialidad:** Alta **Integridad:** Baja **Disponibilidad:** Baja := ABB
AMAA	El acceso a los activos de información requiere de autenticación. La integridad es considerablemente importante por tanto acciones para proteger los datos como cripografía y práctica de respaldo deben ser robustas.La disponibilidad apropiada para restablecer su disponibilidd del activo de información en forma inmediate es requerida.	**Confidencialidad:** Alta **Integridad:** Muy Alta **Disponibilidad:** Alta := AMAA

Criterios	Acción de Protección	Clasificación (Leyenda)
AMAMA	El acceso a los activos de información requiere de autenticación robusta. La integridad es considerablemente importante por tanto acciones para proteger los datos como criptografía y práctica de respaldo deben ser robustas y la disponibilidad apropiada para no permitir la interrumpción del acceso al activo o reestablecer su disponibilidad del activo de información en forma inmediata es requerida.	**Confidencialidad:** Alta **Integridad:** Muy Alta **Disponibilidad:** Muy Alta := AMAMA
AMM	El control de acceso para los activos de información requiere autenticación robusta. El proceso de integridad está basado en la protección a los accesos y a la restauración vía respaldos. La disponibilidad puede ser soportada con base a recuperación vía respaldos o de la alta disponibilidad.	**Confidencialidad**: Alta Integridad: Media **Disponibilidad:** Media := AMM

Criterios	Acción de Protección	Clasificación (Leyenda)
BAA	El acceso al servicio, sistemas, información o área no requiere autenticación. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.	**Confidencialidad:** Baja **Integridad:** Alta **Disponibilidad:** Alta := BAA
BAB	El acceso a los activos de información requiere de autenticación. La integridad es consideblemente importante por tanto acciones para proteger los activos de información como las prácticas de respaldo. La disponibilidad no es requerida como una condición importante.	**Confidencialidad:** Baja **Integridad:** Alta **Disponibilidad:** Baja := BAB

Criterios	Acción de Protección	Clasificación (Leyenda)
BBA	El acceso al servicio, sistemas, información o área no requiere autenticación. Es posible que la afectación de la integridad no represente mayor necesidad, sin embargo debe haber condiciones apropiadas para reestablecer el servicio o disponibilidad del activo de información en lapsos muy breves.	**Confidencialidad:** Baja **Integridad:** Baja **Disponibilidad:** Alta := BBA
BBB	El acceso al servicio, sistemas, información o área no requiere autenticación. Es posible que la afectación de la integridad no represente mayor necesidad, así como el acceso al servicio en forma constante.	**Confidencialidad:** Baja **Integridad:** Baja **Disponibilidad:** Baja := BBB
BBM	El acceso al servicio, sistemas, información o área no requiere autenticación. Es posible que la afectación de la integridad no represente mayor necesidad. La disponibilidad puede ser soportada con base a recuperación vía respaldos o de la alta disponibilidad	**Confidencialidad:** Baja **Integridad:** Baja **Disponibilidad:** Media := BBM

Criterios	Acción de Protección	Clasificación (Leyenda)
BBMA	El acceso al servicio, sistemas, información o área no requiere autenticación. Es posible que la afectación de la integridad no represente mayor necesidad, sin embargo debe haber condiciones apropiadas para no permitir la interrupción del acceso al activo o reestablecer su disponibilidad del activo de información en forma inmediata.	**Confidencialidad:** Baja **Integridad:** Baja **Disponibilidad:** Muy Alta := BBMA
BMAB	El acceso al servicio, sistemas, información o área no requiere autenticación. La integridad es considerablemente importante por tanto acciones para proteger los activos de información como la criptografía y las prácticas de respaldo deben ser robustas.	**Confidencialidad:** Baja **Integridad:** Muy Alta **Disponibilidad:** Baja := BMAB

Criterios	Acción de Protección	Clasificación (Leyenda)
BMAMA	El acceso al servicio, sistemas, información o área no requiere autenticación. La integridad es considerablemente importante por tanto acciones para proteger los datos como criptografía y práctica de respaldo deben ser robustas y la disponibilidad apropiada para no permitir la interrumpción del acceso al activo o reestablecer su disponibilidad del activo de información en forma inmediata es requerida.	**Confidencialidad:** Baja **Integridad:** Muy Alta **Disponibilidad:** Muy Alta := BMAMA
BMM	El acceso al servicio, sistemas, información o área no requiere autenticación. El proceso de integridad está basado en la protección a los accesos y a la restauración vía respaldos. La disponibilidad puede ser soportada con base a recuperación vía respaldos o de la alta disponibilidad.	**Confidencialidad:** Baja **Integridad:** **Medi**a **Disponibilidad:** Media := BMM

Criterios	Acción de Protección	Clasificación (Leyenda)
MAA	El control de acceso para los activos de información es requerido. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.	**Confidencialidad:** Media **Integridad:** Alta **Disponibilidad:** Alta := MAA
MAAA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerada importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.	**Confidencialidad**: Muy Alta **Integridad:** Alta **Disponibilidad** Alta := MAAA

Criterios	Acción de Protección	Clasificación (Leyenda)
MAAMA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad apropiada para no permitir la interrumpción del acceso al activo o reestablecer su disponibilidad del activo de información en forma inmediata es requerida.	**Confidencialidad:** Muy Alta **Integridad:** Alta **Disponibilidad** Muy Alta := MAAMA
MABB	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. Es posible que la afectación de la integridad no represente mayor necesidad, así como el acceso al servicio en forma constante.	**Confidencialidad:** Muy Alta **Integridad:** Baja **Disponibilidad** Baja := MABB

Criterios	Acción de Protección	Clasificación (Leyenda)
MABMA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad no es muy importante por tanto acciones para proteger los datos como criptografía y práctica de respaldo no es requerida. La disponibilidad apropiada para no permitir la interrumpción del acceso al activo o reestablecer su disponibilidad del activo de información en forma inmediata es requerida.	**Confidencialidad**: Muy Alta **Integridad:** Baja **Disponibilidad** Muy Alta := MABMA
MAM	El control de acceso para los activos de información requiere autenticación robusta. La integridad es importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad puede ser soportada con base a recuperación vía respaldos o de la alta disponibilidad.	**Confidencialidad:** Media **Integridad: Alta Disponibilidad: Media** := MAM

Criterios	Acción de Protección	Clasificación (Leyenda)
MAMAA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerablemente importante por tanto acciones para proteger los datos como criptografía y práctica de respaldo deben ser robustas y disponibilidad debe procurar que se recupere en lapsos muy breves.	**Confidencialidad:** Muy Alta **Integridad:** Muy Alta **Disponibilidad** Alta := MAMAA
MAMAB	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerablemente importante por tanto acciones para proteger los datos como criptografía y práctica de respaldo deben ser robustas. La disponibilidad no es requerida como una condición importante.	**Confidencialidad:** Muy Alta **Integridad:** Muy Alta **Disponibilidad Baja** := MAMAB

Criterios	Acción de Protección	Clasificación (Leyenda)
MAMAM	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerablemente importante por tanto acciones para proteger los datos como criptografía y práctica de respaldo deben ser robustas. La disponibilidad puede ser soportada con base de recuperación vía respaldos o de la alta disponibilidad.	**Confidencialidad:** Muy Alta **Integridad:** Muy Alta **Disponibilidad:** Media := MAMAM
MAMAMA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. La integridad es considerablemente importante por tanto acciones para proteger los datos como criptografía y práctica de respaldo deben ser robustas. La disponibilidad es constante y debe procurar el acceso permanente al servicio o su recuperación en lapsos muy breves.	**Confidencialidad:** Muy Alta **Integridad:** Muy Alta **Disponibilidad Muy Alta** := MAMAMA

Criterios	Acción de Protección	Clasificación (Leyenda)
MAMMA	El acceso al servicio, sistemas, información o área requiere autenticación extremadamente robusta. El proceso de integridad está basado en la protección a los accesos y a la restauración vía respaldos. La disponbilidad es constante y debe procurar el acceso permanente o su recuperación el lapsos muy breves.	**Confidencialidad:** Muy Alta **Integridad:** Media **Disponibilidad:** Muy Alta := MAMMA
MBB	El control de acceso para los activos de información es requerido. La integridad es importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantementeLa disponibilidad no es requerida como una condición importante.	**Confidencialidad:** Muy Alta **Integridad:** Muy Alta **Disponibilidad:** Media := MAMAM

Criterios	Acción de Protección	Clasificación (Leyenda)
MBM	El control de acceso para los activos de información requiere autenticación robusta. La integridad es importante por tanto acciones para proteger los datos como la práctica de respaldo deben ser aplicadas constantemente. La disponibilidad puede ser soportada con base a recuperación vía respaldos o de la alta disponibilidad.	**Confidencialidad:** Media **Integridad:** Baja **Disponibilidad:** Media := MBM
MMA	El control de acceso para los activos de información requiere autenticación robusta. El proceso de integridad está basado en la protección a los accesos y a la restauración vía respaldos. La disponibilidad apropiada para reestablecer su disponibilidad del activo de información en forma inmediata es requerida.	**Confidencialidad:** Media **Integridad:** Media **Disponibilidad: Alt**a := MMA

Criterios	Acción de Protección	Clasificación (Leyenda)
MMAMA	El control de acceso para los activos de información es requerido. La integridad es considerablemente importante por tanto acciones para proteger los datos como criptografía y práctica de respaldo deben ser robustas. La disponbilidad es constante y debe procurar el acceso permanente o su recuperación el lapsos muy breves.	**Confidencialidad:** Media **Integridad:** Muy Alta **Disponibilidad: Muy Alt**a := MMAMA
MMB	El control de acceso para los activos de información requiere autenticación robusta. El proceso de integridad está basado en la protección a los accesos y a la restauración vía respaldos. La disponibilidad no es requerida como una condición importante.	**Confidencialidad:** Media **Integridad:** Media **Disponibilidad: Baja** := MMB
MMM	El control de acceso para los activos de información requiere autenticación robusta. El proceso de integridad está basado en la protección a los accesos y a la restauración vía respaldos. La disponibilidad puede ser soportada con base a recuperación vía respaldos o de la alta disponibilidad.	**Confidencialidad:** Media **Integridad:** Media **Disponibilidad: Media** := MMM

ANEXO N° 3

INFORME DE EVALUACIÓN DE RIESGOS ASOCIADOS A LOS ACTIVOS DE INFORMACIÓN DE BANDES

Caracas, 03 de Agosto de 2012

1. ASUNTO

Informe de Evaluación de riesgos asociados a los Activos de Información que soportan los procesos de negocio de la institución.

Dirigido a:

- Gerencia Ejecutiva de Tecnología de la Información

2. OBJETIVOS

- Informar los resultados sobre la evaluación realizada a los activos de información que soportan los procesos de negocio de la Institución, y que residen en la Gerencia Ejecutiva de Tecnología de la Información para su administración y custodia; como parte de las funciones de servicios que ofrece dicha Gerencia Ejecutiva a las diferentes unidades de la Institución, garantizando de esta forma la disponibilidad, integridad y confidencialidad que deben tener según el área y las unidades relacionadas dentro del banco.
- Generar las recomendaciones a ser aplicadas de acuerdo a los hallazgos y brechas que han podido observarse con respecto a las normativas establecidas para la gestión de activos de información y estándares relacionados.

3. PLANTEAMIENTO

La evaluación de los activos de información, está basada en los criterios de exposición de la confidencialidad, integridad y disponibilidad, así como en el nivel de clasificación que debe aplicarse a los mismos, a través

del procedimiento de análisis, validando esta información con las entrevistas realizadas a los propietarios de dichos activos.

Las acciones consideradas en esta evaluación son aplicadas a todos los activos que, de alguna forma, puedan impactar la gestión normal de los procesos de negocio, con posibles afectaciones a toda la Institución, abarcando desde las estructuras de datos hasta las instalaciones o localizaciones físicas en donde se opera.

Los criterios adoptados para el análisis de vulnerabilidades y amenazas de dichos activos de información, son la combinación de estándares especializados en materia de seguridad de la información como lo son ISO, Magerit, entre otros, que persiguen generar buenas prácticas en materia de los objetivos de control y seguridad de la información.

A su vez, la aplicación del instrumento de campo, para el levantamiento del inventario de los activos de información, permitió establecer la exposición a las amenazas y vulnerabilidades de estos, de acuerdo a su contexto operativo, tomando en cuenta el tipo de uso de cada activo, su ubicación, si mantiene algún tipo de datos, bien sea de usuarios o de configuración para enrutar mensajes o facilitar la entrega o procesamiento de datos. En virtud de ello, se otorga el nivel de clasificación para su administración y en consecuencia las medidas que han de adoptarse para su debida protección.

4. RESULTADOS DE LA EVALUACIÓN DE LOS ACTIVOS DE INFORMACIÓN

A continuación se describe y presenta en forma gráfica, un resumen del resultado obtenido durante la evaluación referente a los activos de información que soportan los procesos de negocio de la Institución y la

Gerencia Ejecutiva de Tecnología de la Información tiene la responsabilidad de administración y/o control.

Debido a las funciones que desempeña y los recursos que administra, le es conferida a la Gerencia Ejecutiva de Tecnología de la Información, la custodia de los activos de información de la organización, específicamente aquellos en medios electrónicos.

Igualmente, maneja información que es generada en las unidades funcionales y administra otros activos que son contenedores de la información que se almacena y procesa de las diferentes procesos de negocio, estando restringidos al personal especializado en mantenerlo disponible y funcional para cumplir con la misión encomendada. Dadas estas características, se debe utilizar, criterios que consideren los puntos expuestos para ejecutar el proceso de clasificación y etiquetado.

- **IDENTIFICACIÓN DE AMENAZAS GENÉRICAS EN EL CONTEXTO DE BANDES**

  Análisis sobre los Activos: Datos/Información

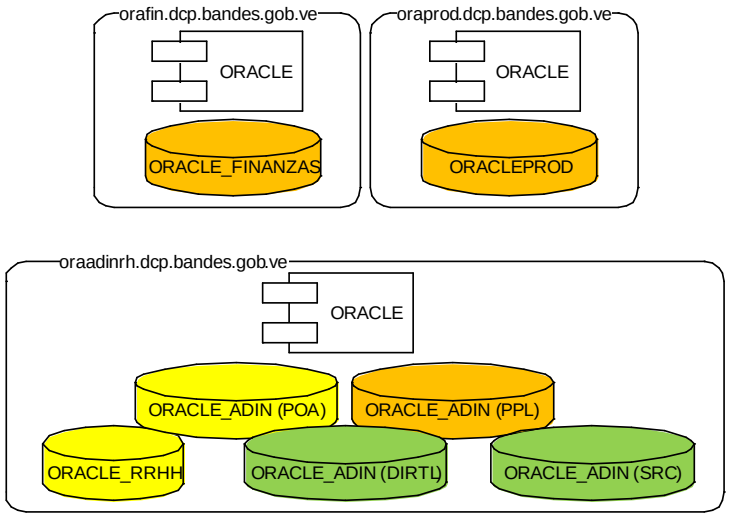
  Fueron identificados repositorios de datos, para la actividad operativa de las unidades de negocio, inventariando al mismo tiempo bases de datos relacionadas a diferentes sistemas de información utilizadas en los diferentes procesos de negocio.

  Se reportan registros vitales, relacionados con los inventarios de los equipos activos en centro principal de datos y alterno, los cuales están ubicados en los equipos asignados a los especialistas.

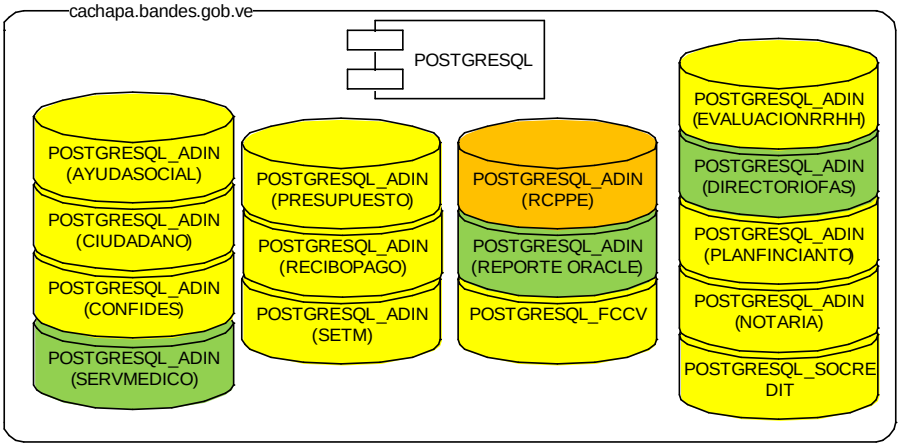
  Se determino en muchos casos, la existencia de niveles de encapsulamientos para llegar a los datos finales. La mayor parte de las bases de datos identificadas, han sido catalogadas como confidenciales.

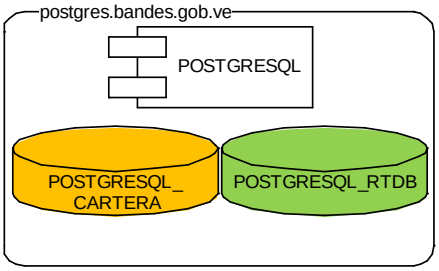
En el caso de las bases de datos, existe una composición de contenedores de datos. Las protecciones y contramedidas para lograr la mitigación de riesgos relacionados a los factores evaluados, deberá considerar esta estructuración.

Se refleja en forma gráfica el encapsulamiento que conforman las capas de la estructura de acceso y manejo de los datos finales. Se reflejan en tres niveles de colores como un mapa de calor[7], la criticidad de cada base de datos, según el tipo de uso, clasificación y sensibilidad de los datos que aloja.



[7] Naranja: Mayor relevancia / Criticidad -→ Verde Criticidad Normal Uso Común





El sistema de almacenamiento en red (SAN), alberga todas las base de datos de la entidad, estas se concentran en los subsistemas de almacenamiento DS8000 / DS8300.

Estos dispositivos fueron clasificados como restringidos, por lo tanto se requerirá el establecimiento de mecanismos para su administración y autorizaciones acordes al nivel de sensibilidad de la información allí resguardada.

Descripción de las Amenazas sobre los activos: Datos/Información

Las amenazas que presentan un grado de significación importante y que requieren de seguimiento cercano y un alto grado de

responsabilidad, por parte de las Unidades con responsabilidad sobre estos componentes, son las siguientes:

- *Destrucción no intencional de información*
- *Errores de ingreso de datos de usuarios e introducción no intencional de información incorrecta*
- *Acceso no autorizado a los datos*
- *Errores del administrador*
- *Errores no intencionales de configuración*

Análisis sobre los Activos: Servicios

Descripción de las Amenazas sobre los activos: Servicios

No se reportaron elementos para valorar en este rubro.

Análisis sobre los Activos: Redes

Se realizó una síntesis agrupada por clase de activo, los cuales fueron reducidos a lo siguiente:

✓ Virtual Private Nertworks (VPN's)

Las redes VPN establecidas en Bandes están definidas con dos objetivos:

- Acceso externo a empleados para teletrabajo y a proveedores
- Para crear segmentos seguros entre equipos específicos

- ✓ Redes WAN
- ✓ Redes LAN (definición de redes lógicas VLAN's)

  Este segmento, corresponde a la definición lógica de las VLAN's que están establecidas, la segregación de las VLAN's obedece a diferentes necesidades; segmentación más eficiente de subredes para evitar colisiones, separar tráfico sobre segmentos de características de los datos que se transportan de condición sensible (en estos casos, la clasificación correcta de estas redes virtuales permitirá establecer los parámetros de operaciones y protección acordes con su nivel de criticidad). Existe un tipo de ataque que hace factible para una persona hacer que un equipo viole la política de asignación y salte de una VLAN a otra, el método se llama VLAN hopping, por lo general se utiliza un esquema de doble etiquetado para lograr el acceso. El tener cuales VLAN's manejan tráfico muy sensible permitirá el establecimiento de políticas y mecanismos para mitigar estas violaciones.

- ✓ Internet

  En este caso hay dos tipos básicos de tráfico, el público a los empleados para consultar los recursos disponibles en la nube y aquel que corresponda a tráfico especial (VPN's y otro tráfico que pueda ser intercambiada por protocolos como SSL).

Descripción de las Amenazas sobre los activos: Redes

Los posibles factores de exposición se concentran en fallos en los dispositivos, errores de configuración y cambios, así como fallas

eléctricas. La posibilidad de verse afectada la confiabilidad del activo, motivado a problemas de re-enrutamiento y escucha son menores pero con alguna posibilidad, motivado esencialmente en alguna vulnerabilidad presente en el no ejecutar en el mantenimiento, análisis de impacto en dependencias al agregar o reconfigurar conexiones de redes o comunicaciones lógicas y punto a punto encapsuladas.

Análisis sobre los Activos: Aplicaciones/Software

Fueron identificados distintos habilitadores que la Gerencia Ejecutiva de Tecnología e la Información, utiliza para prestar la administración y soporte en telecomunicaciones, bases de datos y virtualización.

Descripción de las Amenazas sobre los activos: Aplicaciones/Software

Con la excepción de la exposición a la amenaza de *Errores de Configuración* y *Actualizaciones Erradas*, no se identifican exposiciones a riesgos significativos para la organización. Estos son factibles en el ámbito de mantenimiento de configuración de componentes y sus dependencias, motivado a que no se evidencia un robusto ciclo de administración de la configuración de los servicios y de los activos asociados.

Lo anterior puede traer como consecuencia, que por el ajuste de parámetros de los sistemas de base datos o software de soporte a la operación de sistemas operativos se pueda afectar la disponibilidad o confiabilidad de los servicios y aplicaciones en uso.

Se recomienda establecer en conjunto con la clasificación de los activos de información, un proyecto de desarrollo de gestión de

configuración, el cual complementaría la gestión de activos y control de cambios.

Análisis sobre los Activos: Hardware

Fueron considerados aquellos bienes tangibles utilizados para el procesamiento, almacenamiento, transmisión y resguardo; relacionados a las operaciones y/o seguridad en el soporte de los servicios que integran la tecnología subyacente que da soporte a los servicios que se ejecutan los procesos de negocio.

Descripción de las Amenazas sobre los activos: Hardware

El centro de datos de Bandes ha sido adecuado para cumplir con las exigencias de las prácticas para centros de datos y de la normativa local. Aunque se pudo apreciar algunos materiales que no habían sido desalojados del área de comunicaciones, por otra parte, existen elementos de mejora para garantizar un sistema de enfriamiento continuo.

Son posibles los factores de *manipulación no intencional de configuraciones*, *modificaciones de configuración*, *errores de administrador y acceso no autorizado*, esto se debe como elemento causal a vulnerabilidades expuestas y que son comunes para los otros tipos de activos indicados. En resumen: Vulnerabilidades en el control de activos, administración de configuración, establecimiento de la función de custodia y las necesidades de controlar la trazabilidad en algunas plataformas, en especial en aquellas de mayor criticidad, con la aplicación de las políticas de seguridad establecidas.

Es relevante para el establecimiento de las medidas de protección y mitigación de riesgos sobre los activos, el conocimiento exacto de

cuales están en uso, conectados y activos, con el fin de establecer las responsabilidades de administración y custodia, uso, tipo de datos que procesará, con el fin de que las medidas y controles sean efectivos.

Existen varios componentes de hardware en los centros principal y alterno de datos inactivos.

Análisis sobre los Activos: Repositorio de Datos (Carpetas Compartidas)

Dentro del esquema de evaluación de los activos de información se considera la catalogación por los tipos de documentos que son manejados en los distintos procesos de negocio en las carpetas compartidas, las cuales están sujetas al procedimiento habitual de respaldo.

Existen, en distintos servidores, directorios compartidas en la red, separadas para las diferentes unidades de negocio.

Con los directorios compartidos, se catalogaron 3.930 directorios de trabajo, lo cual representa una estructura de información que se puede considerar extremadamente extendida para ser administrada de forma conveniente. Esto considerando que segregadas en dicho número de carpetas, se encuentran distribuidos 34.196 archivos de diferente índole. En estas carpetas coexisten archivos de paquetes de instalación, así como, documentos y hojas de trabajo.

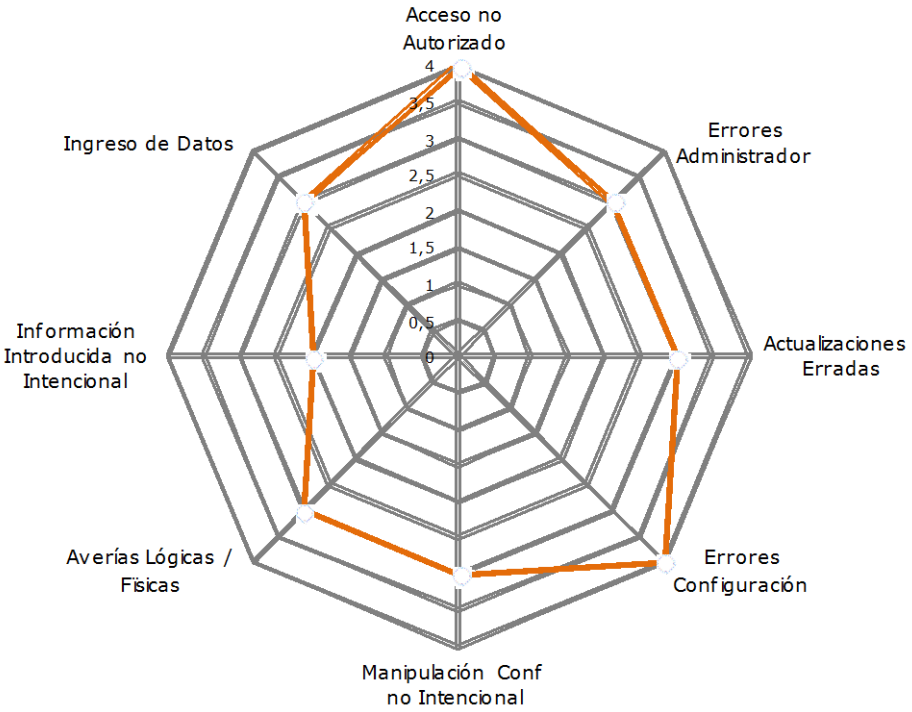
El volumen de documentos gestionados, archivos de trabajo, hojas de cálculo de control se encuentra en forma similar en otras unidades de Bandes, por lo que se hace razonable valorar la utilización de un habilitador tecnológico (gestor documental), que permita administrar de forma lógica esta diversidad documental y ser organizada en un

esquema que no requiera una expansión que se haga inmanejable de estructura de directorios, así como, implementar políticas generales aceptadas para el ciclo de vida de información, manejos de versiones, desincorporación de documentos y resguardo de aquellos de valor como soporte institucional.

- El Resumen de Amenazas sobre los Activos de Información

A continuación se representa el nivel de exposición a las amenazas de los activos de información que soportan los procesos de negocio de Bandes, y son custodiados por la Gerencia Ejecutiva de Tecnología de la Información. Los riesgos expuestos en este gráfico son los considerados como los más representativos, producto de las inferencias en las sesiones realizadas con las personas entrevistadas.

Este criterio se establece cualitativamente con valores comprendidos entre el 0 y 5. Siendo 0 el nivel de inexistente severidad y el 5 el de mayor severidad en lo referido a la afectación de los servicios y plataformas tecnológicas del banco.



Mapa radial con las amenazas de riesgo más representativas de Activos Administrados por la GETI

Entre un conjunto aproximado de 104 tipos de riesgos, distribuidos en las clases de activos de información relacionados con los procesos de negocio, los que mayor exposición representan con base a la conjunción de amenazas y vulnerabilidades, se encuentra la configuración errónea de componentes, actualizaciones erradas, acceso no autorizado, Averías lógicas y físicas por el uso intensivo, así como los errores de administrador.

Otras amenazas perceptibles sobre los activos de información (en especial base de datos), se encuentran correlacionadas con el acceso no

autorizado que, en virtud de la vulnerabilidad del control de acceso sobre algunos sistemas con uso único de cuenta y cuyos usuarios están restringidos a nivel de aplicación pero no de base de datos, podrían generarse la divulgación no autorizada, fuga de información, así como la no repudiación (Se entiende como no repudiación, la condición de poder establecer la responsabilidad de haber emitido o recibido información en forma física o electrónica). Aunque en la mayoría de estos sistemas existe una cuenta única con privilegios sobre todas las estructuras de datos que puede ser monitoreada, algunas operaciones no podrían ser categorizadas si fueron error de la aplicación o del administrador, en otros casos, es posible que no exista traza de seguimiento, lo que generaría igualmente brechas de cumplimiento normativo, particularmente con el título VII de la Norma de Tecnología de la SUDEBAN

5. RECOMENDACIONES

A continuación se resaltan algunas recomendaciones sobre las observaciones de mayor pertinencia encontradas en la Gerencia Ejecutiva de Tecnología, con la finalidad de que las mismas sean corregidas o minimizadas para mitigar los riesgos implícitos:

- Los equipos de seguridad y control de tráfico, así como de monitoreo y trazas, se recomienda realizar una instrumentación o política de asignación de dueño y custodio que evite posibles ambigüedades en su control, entre la Gerencia Ejecutiva de Tecnología y Seguridad de la Información.Igualmente, la administración de aquellas cuentas especiales de los sistemas de información que utilizan un usuario definido único para todas las interacciones con el sistema de base de datos y el sistema operativo.

- Establecer un esquema que sea auditable de administración de configuración de componentes y activos informáticos, esto con la finalidad de lograr un marco integrable con las actividades de administración de accesos, clasificación de activos y gestión de cambios. Esto incluye el desarrollo de un análisis de dependencias, que permita inferir los componentes subyacentes que pueden afectar las protecciones y acciones de control según la clasificación de ciertos tipos de activos y el impacto en la organización bajo escenarios de afectación de disponibilidad, integridad o confiabilidad.

- Un proceso de gestión de activos informáticos debe ser asignado a un único responsable funcional y contar con el apoyo de habilitadores tecnológicos que ofrezcan confiabilidad sobre el registro de estos. Se

sugiere establecer una política sobre el responsable de administración y custodia de los equipos auxiliares de protección del centro de datos.

- Existen elementos evidenciados en este proceso de clasificación de activos de información que tanto para el objetivo final de establecer los resguardos adecuados, como para el correcto manejo de los activos y los datos contenidos en estos, el desarrollo de un proyecto de gestión de ciclo de vida de la información, esto motivado a las siguientes premisas identificadas en Bandes:

    a. Crecimiento vegetativo de Información. Documentos temporales se mantienen en el tiempo, papeles de trabajo, versiones intermedias.

    b. Uso no eficiente del Almacenamiento.

    c. Posibles vulnerabilidades en la administración de las operaciones de respaldo y restauración.

    d. Posible crecimiento exponencial de la Base de Datos de correo.

    e. Manejo de Documentos.

ANEXO N° 4

POLÍTICAS OPERATIVAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE BANDES

Manual de Políticas Operativas del Sistema de Gestión de Seguridad de la Información del Banco de Desarrollo Económico y Social de Venezuela (Bandes)

Código: B_REI _SEI_PO001
Versión N° 1
Para aprobación del Directorio Ejecutivo de Bandes

APROBACIÓN

El presente manual, contiene las Políticas Operativas del Sistema de Gestión de Seguridad de la Información a implementar por la Coordinación de Seguridad de la Información del Banco de Desarrollo Económico y Social de Venezuela Bandes, el cual fue debidamente visto, analizado y aprobado por los siguientes niveles de decisión:

EDMÉE BETANCOURT DE GARCÍA
Presidenta

INDICE

Aprobado:

INTRODUCCIÓN

El presente manual ha sido desarrollado con la finalidad de contar con un instrumento que sirva de base legal para consolidar y engranar las reglas o contramedidas de seguridad de la información para el establecimiento de un sistema de gestión de seguridad de la información robusto, que defina una estrategia global de seguridad de la información y se convierta en un sistema práctico de defensa contra posibles incidentes, estableciendo las directrices, procedimientos y requisitos necesarios para asegurar la integridad, disponibilidad y confidencialidad de la Información en Bandes.

Objetivo General:

Establecer las directrices y lineamientos que regirán la implementación del Sistema de Gestión de Seguridad de la Información, para asegurar la integridad, disponibilidad y confidencialidad de la Información en el Banco de Desarrollo Económico y Social de Venezuela (Bandes).

Objetivos Específicos:

1. Proveer un marco para el diseño y desarrollo de los controles lógicos y físicos de acceso, a fin de proteger la integridad de la información y de las aplicaciones.
2. Garantizar la protección de la información en las redes y de la infraestructura de soporte.
3. Conservar la integridad y disponibilidad del procesamiento y transmisión de la información.
4. Asegurar el cumplimiento de las leyes, regulaciones estándares y normas aplicables en el Instituto.
5. Minimizar el riesgo de fallas en los sistemas, a fin de evitar daños a los recursos o activos de información e interrupciones en las actividades del Instituto.

Aprobado:

6. Proporcionar una orientación general sobre la asignación de funciones y responsabilidades en el Instituto, así como también, la orientación sobre los sitios específicos, activos, servicios y procesos de seguridad relacionados, tales como la planificación de la recuperación y continuidad del negocio.

Ámbito de Aplicación

Toda la infraestructura tecnológica del Instituto, incluyendo los medios físicos y lógicos, comunicaciones electrónicas, información, procesos, procedimientos y medidas de control que directamente impacten a la operación y sean de vital importancia para el buen desarrollo de las operaciones de Bandes, estarán sujetas a la aplicación de estas políticas operativas.

En ningún caso, ningún factor de producción, sistema administrativo o proceso que afecte la continuidad de las Operaciones del Instituto y sus objetivos, estará exento de la aplicación de estas políticas.

Específicamente, estas políticas aplican a:

- La infraestructura tecnológica de Bandes, que ofrece servicios a los usuarios (internos y externos).
- La red interna y el Centro de Cómputo, incluyendo hardware, software y activos de información de Bandes.
- Todos los empleados de Bandes, que tengan acceso físico a las instalaciones y lógico a la infraestructura tecnológica del Instituto.

En general las políticas aquí descritas aplican a todos los empleados y personal temporal (pasantes, comisión de servicio, proveedores, entre otros) del Instituto, la participación de las áreas de Control en materia de seguridad de la Información, como lo son el área de Seguridad de la Información encargada de elaborar y actualizar las mismas. El contenido de este manual debe ser actualizado constantemente, puede expandirse su alcance y la utilidad en el tiempo del mismo.

Aprobado:

RESPONSABILIDAD Y CUMPLIMIENTO DEL MANUAL

1. Es responsabilidad del área de Seguridad de la Información así como de los Supervisores de las Unidades involucradas en este proceso, asegurar que las Políticas Operativas establecidas en el presente documento sean de estricto cumplimiento haciéndolas de conocimiento a sus supervisados
2. Mantener actualizado el proceso en cuestión, con una periodicidad anual.
3. Solicitar la revisión o corrección de este manual enviando un memorando o correo electrónico (cuenta: Gestión Calidad), según el nivel jerárquico de Unidad, de acuerdo a:
   - Gerencias Ejecutivas a la Gerencia Ejecutiva de Planificación y Gestión Estratégica
   - Gerencias y Coordinaciones a la Gerencia de Gestión de la Calidad.

   La solicitud debe contener los siguientes datos: a) Nombre del Funcionario que hace la sugerencia, b) Denominación del cargo que ocupa, c) Objeto de la revisión, corrección o eliminación: título(s), o texto(s), d) Justificación del cambio.

PUBLICACIÓN DEL MANUAL

El manual se mantendrá como material de consulta en la Intranet de Bandes, para todos los usuarios involucrados en el proceso.

Aprobado:

MARCO LEGAL

- Cumplir con la Normativa de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes Sometidos al Control, Regulación y Supervisión de la Superintendencia de la Instituciones del Sector Bancario (SUDEBAN)", prevista en el Decreto Nº 6.287 con Fuerza de Ley de Reforma de la Ley General de Bancos y Otras Instituciones Financieras, de fecha 30 de julio de 2008.

Aprobado:

GLOSARIO DE TÉRMINOS

A los fines de la interpretación y aplicación de este Manual, se definen los siguientes términos:

1. **Activo:** es el conjunto de bienes y derechos tangibles e intangibles propiedad de una persona natural o jurídica, que por lo general son generadores de renta o fuente de beneficios.
2. **Activo de Información:** se refiere a los bienes de información y procesamiento, que posee la institución. Son recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos. El verdadero valor del activo lo proporciona el valor de la información en él contenida. Estos activos de información pueden existir en muchas formas, tales como:
    a. Impresa o escrita en papel.
    b. Almacenada electrónicamente.
    c. Transmitida por correo o utilizando medios electrónicos.
    d. Presentada en imágenes.
    e. Expuesta en una conversación.
3. **Activo Físico:** se caracteriza por tener un valor intrínseco.
4. **Activos de información informáticos:** son todas las formas actuales y futuras de hardware, software y productos relacionados que se utilizan para el negocio de procesamiento de datos y automatización de las oficinas que tienen la capacidad de conectarse, ya sea directamente o a través de una red de área local.
5. **Amenaza:** evento que puede desencadenar un incidente en el Instituto, produciendo daños o pérdidas materiales o inmateriales en sus activos.

Aprobado:

6. **Áreas Restringidas:** son aquellas en que se concentran bienes informáticos de alto valor e importancia crítica cuya afectación pueda paralizar o afectar severamente la gestión de ramas o sectores de la economía o de la sociedad; territorios o entidades.
7. **Arquitectura de Información:** es la disciplina y arte encargada del estudio, análisis, organización, disposición y estructuración de la información en espacios de información, y de la selección y presentación de los datos en los sistemas de información interactivos y no interactivos.
8. **Autorización:** es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.
9. **Clasificación de los activos de información:** es el ejercicio mediante el cual se determina el nivel de pertenencia del activo, según una taxonomía previamente establecida. Tiene como objetivo asegurar que el activo de información reciba una protección adecuada. Los activos de información deben clasificarse en términos de su sensibilidad e importancia para la organización.
10. **Clasificación de la información:** procedimiento mediante el cual se determina que la información, sea cual sea su estado, pertenece a un nivel de clasificación estipulado por políticas de Bandes y tiene como propósito fundamental asegurar que recibe el nivel de protección adecuado.
11. **Confiabilidad:** es el nivel de veracidad y exactitud de los datos contenidos en los sistemas de información.
12. **Confidencialidad:** se define como la protección de la información sensible contra la divulgación no autorizada.

Aprobado:

13. **Control:** práctica, procedimiento o mecanismo que reduce el nivel de riesgo de acceso a plataformas, sistemas o aplicaciones.
14. **Control de Acceso:** es un mecanismo que en función de la identificación ya autentificada, permite acceder a datos o recursos. Una vez identificado un usuario debe validarse qué puede hacer en la red y a que áreas está autorizado llegar. Algunas técnicas asociadas a la autorización y control de acceso son la definición de roles, conocida como RBAC (Role Based Access Control o Control de Acceso Basado en Roles) y el filtrado de paquetes.
15. **Controles de Seguridad:** es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, entre otros, que se utiliza para disminuir la probabilidad que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que se explote la misma.
16. **Criticidad:** el término es usado para determinar la importancia de un activo de la información en el proceso productivo de una organización. Esta "importancia", es típicamente basada en una evaluación de las consecuencias que implicaría la falla del equipo o sistema en servicio.
17. **Cumplimiento:** se refiere al acatamiento de las leyes y reglamentaciones a las que están sujetas las Instituciones sometidas a la supervisión, control, fiscalización y regulación de la Superintendencia de Bancos y Otras Instituciones Financieras.
18. **Custodio:** es una parte designada de la organización, un cargo, un proceso o un grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (toma de copias de seguridad, asignar privilegios de: acceso, modificaciones, borrado) que el propietario de la información haya definido, con base en los controles de seguridad disponibles en la organización.
19. **Datos sensibles:** son aquellos datos de carácter confidencial e importante que sería problemático divulgar sin protección.

Aprobado:

20. **Disponibilidad:** accesibilidad a la información en el tiempo y la forma cuando esta sea requerida.
21. **Gestión de Activos de Información**: se refiere a la gestión o administración sobre los activos de información del Instituto, a fin de garantizar que estos sean efectivamente controlados a través de su identificación, valoración y clasificación, así como la asignación de sus propietarios y custodios.
22. **Hardware:** son todos los componentes materiales de los computadores y sus periféricos (discos, memoria, impresoras, entre otros).
23. **Impacto:** consecuencia sobre un activo de la materialización de una amenaza.
24. **Integridad:** es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas, a fin de preservar la precisión y suficiencia de la información, así como, su validez acorde con las pauta s fijadas por la Institución y regulaciones externas.
25. **Infraestructura Tecnológica:** agrupación de equipos, aplicaciones y sistemas destinados a ofrecer productos y servicios a través del uso de los recursos tecnológicos disponibles, a una comunidad de usuarios, públicos y privados, tanto a nivel local, regional como nacional.
26. **Perfil de acceso:** también llamados permisos o privilegios, son los derechos otorgados a los usuarios por el administrador o el supervisor. Determinan las acciones que los usuarios pueden realizar (por ejemplo, leer, escribir, ejecutar, crear y eliminar) en los archivos compartidos en el servidor.
27. **Periféricos:** elementos de un sistema de tratamiento de la información distinto de la unidad central que sirve para memorizar datos o comunicar con el exterior.
28. **Perímetro de Seguridad:** delimitación de un espacio físico por medio

de una barrera (pared, puerta de acceso controlado, entre otros). El emplazamiento y la fortaleza de cada barrera dependerá de los resultados de evaluación de riesgo realizada.

29. **Privilegio:** es la asignación del tipo de transacción que puede ejecutar el Usuario de un sistema de información (consultar, incluir, eliminar, modificar).
30. **Propietario de la Información:** Es la persona designada por la organización el cual tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y determinar cuáles son los requerimientos para que la misma este salvaguardada ante el acceso no autorizado, modificación, pérdida de la confidencialidad o destrucción adrede. Esta persona es responsable de indicar cuando la información ha de ser desincorporada, una vez que esta no sea necesaria mantenerla o requerirla.
31. **Propietario del Sistema:** las personas, usualmente gerentes ejecutivos, gerentes de línea o coordinadores, que son responsables de la integridad, el reporte y el uso correcto de los sistemas de información.
32. **Riesgo:** posibilidad de que se produzca un acontecimiento que conlleve a pérdidas materiales en el resultado de las operaciones y actividades que desarrollen las Instituciones Financieras.
33. **Riesgo Tecnológico:** se define como la posible pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en los equipos, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información en la prestación de servicios bancarios o financieros con los clientes.
34. **Riesgos inherentes:** es el riesgo de que pueda ocurrir un error material, asumiendo que no existen controles relacionados para prevenir o para detectar el error.
35. **Seguridad de la información:** se define como la preservación de

integridad, disponibilidad y confidencialidad de la información en todas sus formas, impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios removibles, presentada en imágenes, expuesta en una conversación entre otras, también se puede decir que consiste en proteger la información y los recursos del sistema de información de una organización para que sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

36. **Servidor:** es una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de un ordenador y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un computador cumpla simultáneamente las funciones de cliente y de servidor.
37. **Sin acceso:** condición que impide a los Usuarios ingresar a un sistema de información.
38. **Sistema de Alto Riesgo:** son aquellas aplicaciones, sistemas, procesos, operaciones, equipos y cableado que en caso de falla o paralización parcial o total pueden ocasionar pérdidas incalculables o severas que afecten la continuidad operativa del negocio.
39. **Software:** es un conjunto de programas, documentos, procedimientos y rutinas asociados con la operación de un sistema de cómputo.
40. **Trazas de Auditoría:** archivo protegido contra escritura que almacena información en forma secuencial de las transacciones u operaciones que son ejecutadas por los usuarios de los sistemas de información.
41. **Usuario:** Es cualquier persona en la organización que genera, obtenga, transforme, retenga o use en papel o medios digitales,

físicamente o a través de las redes y sistemas de información de la organización. Estos utilizan la información para propósitos de los objetivos de la cadena de valor de Bandes y tendrán el derecho formal del uso dentro del inventario de los activos de información.

42. **Vulnerabilidad:** susceptibilidad de una unidad de obtener un resultado negativo derivado de un choque externo.

DIRECTRICES GENERALES

Capitulo 01: Inventario de Activos de Información

1. Identificación del propietario de los activos de Información

Declaración de la Política:

El Gerente o Coordinador de cada área, será el propietario de los activos de información en su departamento, permitiendo así la asignación de la responsabilidad cuanto al mantenimiento de los controles adecuados para protección de los activos.

Objetivo:

Mantener una protección adecuada de los activos de la Institución, alineada a los criterios definidos en la clasificación realizada a los activos de información.

Alcance:

Esta política va dirigida a todas las áreas de la Institución, las cuales son las responsables de identificar y clasificar los activos de información.

Responsabilidades:

- Cualquier Gerente o Supervisor que tenga a su cargo personal, es responsable de asegurar que el mismo conozca y le dé cumplimiento

a esta política.

- La máxima autoridad de cada área fungirá como propietario de los activos de información manejados, inventariados y almacenados en su departamento.
- El propietario de los activos de información, es responsable de nombrar al responsable o custodio de los activos de información de su departamento.
- La Coordinación de Seguridad de la Información, es responsable de velar por el cumplimiento de esta política, así como también será responsable de proporcionar orientación y apoyo, a las áreas funcionales, sobre las normas y los procedimientos de seguridad sobre los activos de información.

2. Identificación de los responsables de los Activos de Información

Declaración de la Política:

Cada área debe tener un responsable para el manejo, custodia y salvaguarda de los activos de información asignados. Este responsable está en la obligación de realizar periódicamente un inventario de dichos activos.

Aprobado:

Objetivo:

Mantener una protección adecuada de los activos de información de la Institución.

Alcance:

Esta política va dirigida a todas las áreas de la Institución, las cuales son las responsables de identificar y clasificar los activos de información.

Responsabilidades:

- Cualquier Gerente o Supervisor que tenga a su cargo personal, es responsable de asegurar que el mismo conozca y le dé cumplimiento a esta política.
- La Gerencia Ejecutiva, es responsable de llevar a cabo las acciones necesarias para cumplir esta política.
- La Coordinación de Seguridad de la Información, es responsable de velar por el cumplimiento de esta política, así como también será responsable de proporcionar orientación y apoyo, a las áreas funcionales, sobre las normas y los procedimientos de seguridad sobre los activos de información.

Aprobado:

3. Elaboración del Inventario de los Activos de Información

Declaración de la Política:

Todos los activos deben estar claramente identificados. Cada área está en la obligación de elaborar y mantener un inventario con los activos más importantes, según el nivel de criticidad para la organización.

Objetivo:

Elaborar y mantener un inventario con los activos más importantes, según el nivel de criticidad para la organización.

Alcance:

Esta política va dirigida a todas las áreas de la Organización, las cuales son las responsables de identificar y clasificar los activos de información.

Responsabilidades:

- Cualquier Gerente o Supervisor que tenga a su cargo personal, es responsable de asegurar que el mismo conozca y le dé cumplimiento a esta política.
- La Coordinación de Seguridad de la Información, es responsable de velar por el cumplimiento de esta política, además de proporcionar orientación y apoyo, a las áreas funcionales, sobre las normas y los procedimientos de seguridad sobre los activos de información.

Capitulo 02: Clasificación de los Activos de Información

1. Naturaleza de los Activos de Información

Declaración de la Política:

El personal que conforma el área, está obligado a entender la naturaleza y la clasificación adecuada de los activos que generan, usan y/o almacenan.

Objetivo:

Gestionar adecuadamente los activos de Información de la Institución, resguardando las propiedades que deben cumplir los mismos.

Alcance:

Esta política está dirigida a todos los propietarios, responsables, operadores y usuarios de los activos de información de la Institución.

Responsabilidades:

- Cualquier Gerente o Supervisor que tenga a su cargo personal, es responsable de asegurar que el mismo conozca y le dé cumplimiento a esta política.
- La Gerencia Ejecutiva, es responsable de llevar a cabo las acciones necesarias para cumplir esta política.
- La Coordinación de Seguridad de la Información, es responsable de velar por el cumplimiento de esta política, así como también será responsable de proporcionar orientación y apoyo a las áreas

funcionales, sobre el procedimiento e instrumentos definidos para la clasificación de los activos de información.

2. Responsables de la Clasificación

Declaración de la Política:

De forma individual, cada área es responsable de clasificar los activos de información allí inventariados, de acuerdo a los Criterios de Clasificación de Activos de Información establecidos.

Objetivo:

Asegurar que los activos de información, reciban un nivel de protección adecuado en función a su sensibilidad e importancia para la organización.

Alcance:

Esta política está dirigida al responsable de los activos de información y al personal de la Coordinación de Seguridad de la Información, quienes son los responsables del proceso de Clasificación de Activos de Información.

Responsabilidades:

- Los responsables de los activos de información deben conocer y dar cumplimiento a esta política.
- La Gerencia Ejecutiva, es responsable de llevar a cabo las acciones necesarias para dar cumplimiento a esta política.
- La Coordinación de Seguridad de la Información, es responsable de

velar por el cumplimiento de esta política, así como también será responsable de participar en el proceso de clasificación y proporcionar orientación y apoyo a los responsables de los activos, sobre el procedimiento e instrumentos definidos para su clasificación.

3. Niveles de protección y salvaguarda

Declaración de la Política:

Cada activo de información tendrá asociado un nivel único de clasificación, el cual posee características propias de protección y salvaguarda, manejo y tratamiento en cuanto a sus niveles de acceso, métodos de distribución, restricciones, almacenamiento, disposición y destrucción.

Objetivo:

Asegurar que los activos de información reciban un nivel de protección y salvaguarda adecuado en función a su sensibilidad e importancia.

Alcance:

Esta política está dirigida a los responsables del proceso de clasificación de los Activos de Información de la Institución.

Responsabilidades:

- Los responsables de los activos de información deben conocer y dar cumplimiento a esta política.
- La Coordinación de Seguridad de la Información, es responsable de velar por el cumplimiento de esta política, así como también será

responsable de definir el procedimiento y los niveles de protección y salvaguarda para los activos de información.

Aprobado:

Capitulo 03: Protección de los Activos de Información

1. Protección de las estaciones de trabajo

Declaración de la Política:

El usuario será responsable de la protección de su estación de trabajo, evitando así que personas ajenas puedan tener acceso a la información allí almacenada.

Objetivo:

Reforzar la cultura de resguardo y protección de los activos de información en el personal de la Institución, asegurando de esta forma que reciban un nivel de protección y salvaguarda adecuado en función a su sensibilidad e importancia.

Alcance:

Esta política está dirigida al personal de la Coordinación de Seguridad de la Información así como al resto del personal, quienes deben asegurar la aplicación y cumplimiento de los estándares definidos para la protección de los activos de información.

Responsabilidades:

- Cualquier Gerente o Supervisor que tenga a su cargo personal, es responsable de asegurar que el mismo conozca y le dé cumplimiento a esta política.
- La Coordinación de Seguridad de la Información, es responsable de

velar por el cumplimiento de esta política, así como también será responsable de mantener actualizados los estándares de seguridad de la información y protección de activos de información.

2. Administración de estándares para el control de acceso

Declaración de la Política:

Es importante el establecimiento de estándares para el control de acceso a las instalaciones y sistemas de información, contemplando un balance entre las restricciones para prevenir el acceso no autorizado y la necesidad de acceso de acuerdo a las actividades a desempeñar en la Institución.

Objetivo:

Aplicar estándares para el control de acceso a las instalaciones y sistemas de información. Estos estándares, deben ser apropiados a las necesidades de la Institución y los requisitos de seguridad establecidos en función a la clasificación de activos de información.

Alcance:

Esta política está dirigida al personal de la Coordinación de Seguridad de la Información así como al resto del personal, quienes deben asegurar la aplicación y cumplimiento de los estándares definidos para la protección de los activos de información.

Responsabilidades:

- Cualquier Gerente o Supervisor que tenga a su cargo personal, es

responsable de asegurar que el mismo conozca y le dé cumplimiento a esta política.

- La Coordinación de Seguridad de la Información, es responsable de velar por el cumplimiento de esta política, así como también será responsable de mantener actualizados los estándares de seguridad de la información y protección de activos de información.

3. Administración del acceso a usuarios a los activos de información

Declaración de la Política:

El acceso a los activos de información, así como los derechos de acceso o privilegios, deberán estar autorizados por el propietario de los mismos.

Objetivo:

Establecer controles robustos para la identificación de posibles brechas de seguridad en los estándares de control de acceso definidos, a través de la adecuada administración de acceso a los activos de información de la Institución.

Alcance:

Esta política va dirigida al personal de la Coordinación de Seguridad de la Información, quien es responsable de definir y proporcionar orientación y apoyo a las áreas funcionales, sobre las normas y los procedimientos de seguridad sobre los activos de información; así como también a los responsables de los activos quienes son garantes de los mismos.

Aprobado:

Responsabilidades:

- Cualquier Gerente o Supervisor que tenga a su cargo personal, es responsable de asegurar que el mismo conozca y le dé cumplimiento a esta política.
- La Coordinación de Seguridad de la Información, es responsable de velar por el cumplimiento de esta política, así como también será responsable de mantener actualizados los estándares de seguridad de la información y protección de activos de información.

4. Salvaguarda de los activos de Información

Declaración de la Política:

El personal responsable de los activos de cada unidad funcional o área de trabajo, velará por la salvaguarda de los activos de información dados para su funcionamiento.

Objetivo:

Asegurar que los activos de información reciban un nivel de protección y salvaguarda adecuado en función a su sensibilidad e importancia.

Alcance:

Esta política está dirigida a todo el personal de la Institución.

Responsabilidades:

- Cualquier Gerente o Supervisor que tenga a su cargo personal, es responsable de asegurar que el mismo conozca y le dé cumplimiento

a esta política.

- La Coordinación de Seguridad de la Información, es responsable de velar por el cumplimiento de esta política.

5. Administración de controles de acceso a la red Institucional

Declaración de la Política:

Los acceso a los recursos de la red, deben ser controlados estrictamente para prevenir el acceso no autorizado. El acceso a todo equipo de la infraestructura tecnológica y sistemas de información, debe estar restringido a menos que el mismo sea autorizado explícitamente.

Objetivo:

Asegurar que solo los dispositivos y personas autorizadas se conecten a la red interna, administrando apropiadamente las conexiones de red.

Alcance:

Esta política va dirigida al personal de la Coordinación de Seguridad de la Información, quien es responsable de definir y administrar los niveles de acceso a los recursos de la red.

Responsabilidades:

- La Coordinación de Seguridad de la Información es responsable de administrar los niveles de acceso a los recursos de la red, asegurar que su personal conozca y le dé cumplimiento a esta política.

Aprobado:

- El personal de la Coordinación de Seguridad de la Información es responsable de mantener actualizada esta política, y de existir algún cambio, solicitar la actualización al documento de políticas.

6. Restricción del acceso a la información

Declaración de la Política:

Los controles de acceso a la información deben ser fijados a un nivel apropiado, que reduzca al mínimo los riesgos de seguridad y permitan la realización de las actividades de los funcionarios de la Institución sin obstáculo alguno, resguardando las propiedades de la información.

Objetivo:

Restringir el acceso a los activos de información de una forma adecuada, con el objeto de asegurar que estén disponibles únicamente a usuarios autorizados.

Alcance:

Esta política está dirigida al personal de la Coordinación de Seguridad de la Información, quien es responsable de la administración del control de acceso.

Responsabilidades:

- La Coordinación de Seguridad de la Información es la unidad responsable de cumplir y hacer cumplir la política de acceso restringido a la información, de acuerdo a los requerimientos y

funcionalidades indicadas.

7. Monitorización de los Activos de Información digitales y sistemas que los soportan

Declaración de la Política:

Las trazas de auditoría que generan los sistemas que soportan a los activos de información digitales, deben ser registradas, controladas y monitorizadas, con la finalidad de identificar el uso inadecuado de los mismos.

Objetivo:

Monitorizar constantemente el acceso a los sistemas de información, con la finalidad de frustrar accesos no autorizados y corroborar que los estándares de control de acceso sean eficaces.

Alcance:

Esta política va dirigida al personal de la Coordinación de Seguridad de la Información y a la Gerencia Ejecutiva de Tecnología de la Información.

Responsabilidades:

- El personal de la Gerencia Ejecutiva de Tecnología de Información, es responsable de mantener activas las trazas de auditoría de los sistemas de información.
- El personal de la Coordinación de Seguridad de la Información, es responsable de la monitorización de las trazas de auditoría de los sistemas de información, así como sugerir controles eficaces para

resguardarlos.

- La Coordinación de Seguridad de la Información es responsable de velar por el cumplimiento de esta política.
- Cualquier Gerente o Supervisor que tenga a su cargo personal, es responsable de asegurar que el mismo conozca y le dé cumplimiento a esta política.

8. Administración de Acceso a los Sistemas Críticos

Declaración de la Política:

Los controles de acceso para los sistemas de información altamente sensibles para la Institución, deben ser definidos de acuerdo con el valor y la clasificación de los activos de información.

Objetivo:

Administrar el control de acceso a los sistemas críticos que requieren protección debido al nivel de confidencialidad de la información que procesa.

Alcance:

Esta política va dirigida al personal de la Coordinación de Seguridad de la Información, quien es responsable de definir y proporcionar orientación y apoyo a las áreas funcionales, sobre las normas y los procedimientos de seguridad sobre los activos de información; así como también a los responsables de los activos quienes son garantes de los mismos.

Aprobado:

Responsabilidades:

- Cualquier Gerente o Supervisor que tenga a su cargo personal, es responsable de asegurar que el mismo conozca y le dé cumplimiento a esta política.
- La Coordinación de Seguridad de la Información es responsable de velar por el cumplimiento de esta política.

Aprobado:

Bandes	CONTROL DE ☐ Lectura ☐ Revisión
Unidad Organizativa	Nombre del Documento

Ley Orgánica de la Contraloría General de la República y del Sistema Nacional de Control Fiscal

Artículo 82. Los Funcionarios, empleados y obreros que presten servicios en los entes de la Administración Pública, responden penal, civil y administrativamente de los actos, hechos u omisiones contrarios a norma expresa en que incurran con ocasión del desempeño de sus funciones.

Código Civil

Artículo 2. La ignorancia de la Ley no excusa de su cumplimiento.

Los Abajo firmantes nos comprometemos a cumplir con lo establecido en el mencionado documento, para lo cual dejamos constancia a través de nuestra firma.

Apellido y Nombre	Cédula de Identidad	Cargo	Fecha	Firma

Firma y Sello del Gerente Ejecutivo:

Firma y Sello del Supervisor Inmediato

FORM B_CLR_54_10

Pag

Aprobado:

ANEXO N° 5

NORMAS Y PROCEDIMIENTOS PARA EL SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN DE BANDES

Manual de Normas y Procedimientos para el Sistema de Gestión de Seguridad de la Información del Banco de Desarrollo Económico y Social de Venezuela (Bandes)

Código: B_REI _SEI_PR_001
Versión N° 1
Para aprobación del Directorio Ejecutivo de Bandes

APROBACIÓN

El presente manual, contentivo de las Normas y Procedimientos para el Sistema de Gestión de Seguridad de la Información, fue debidamente visto, analizado y aprobado en su contenido por la Gerencia Ejecutiva de Resguardo Institucional / Coordinación de Seguridad de la Información, como usuarios principales del proceso:

LEIDA MARIBAL ARTIGAS LEÓN
Gerente Ejecutiva de Resguardo Institucional

INDICE

Aprobado:

INTRODUCCIÓN

La información tiene una importancia fundamental para el funcionamiento, y quizás incluso sea decisiva para la supervivencia de la organización. De allí la importancia de contar con un Sistema de Gestión de Seguridad de la Información, el cual permitirá tratar y minimizar efectivamente los riesgos de exposición y/o accesos indebidos a dichos activos, y definir criterios de valoración y protección que den cumplimiento a las normativas vigentes, la Coordinación de Seguridad de la Información. Consciente de esta realidad, la Gerencia de Gestión de la Calidad, en un esfuerzo conjunto con la Coordinación de Seguridad de la Información, procedió a documentar el manual de normas y procedimientos que rigen este Sistema de Gestión.

En el contenido de este documento, se proveen lineamientos necesarios para la identificación, valoración y clasificación de los activos de información, así como los lineamientos para identificar sus dueños y establecer adecuados niveles de salvaguarda, que ayuden a evitar posibles daños que puedan afectar significativamente el funcionamiento de la organización.

RESPONSABILIDAD Y CUMPLIMIENTO DEL MANUAL

Es responsabilidad de la Coordinación de Seguridad de la Información, así como de los supervisores de las Unidades involucradas en este proceso, asegurar que las Normas y Procedimientos establecidos en el presente documento sean de estricto complimiento, y de mantener actualizadas las instrucciones de trabajo existentes relacionadas con el proceso en cuestión, solicitando a la Gerencia de Calidad la actualización del presente manual.

Para solicitar cualquier revisión o corrección de este manual, se enviará un Memorando o Correo Electrónico, según el nivel jerárquico de la unidad:

- **De Gerencias Ejecutivas:** a la Gerencia Ejecutiva de Planificación y Gestión Estratégica.
- **De Gerencias y Coordinaciones:** a la Gerencia de Gestión de la Calidad.

Aprobado:

La comunicación deberá contener los siguientes datos: **a)** Nombre del Funcionario que hace la sugerencia, **b)** Denominación del cargo que ocupa, **c)** Objeto de la revisión, corrección o eliminación, **d)** Justificación del cambio.

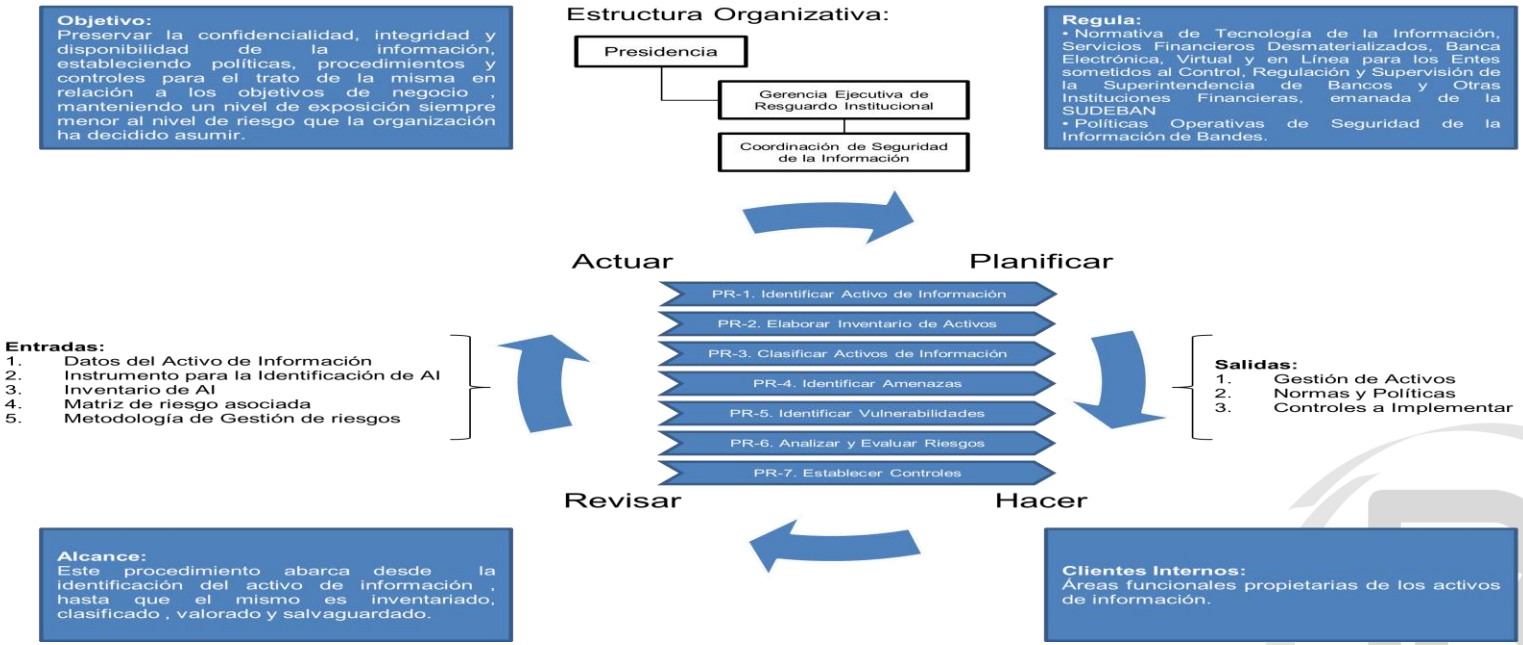
PUBLICACIÓN DEL MANUAL

El manual se mantendrá como material de consulta en la Intranet de Bandes, para todos los usuarios involucrados en el proceso.

Aprobado:

Manual de Normas y Procedimientos: Sistema de Gestión de Seguridad de la Información COD. B_REI _SEI_PR_001		
Función Organizacional: Control y Medición	**Línea de Acción:** Estratégico	**Macro-proceso:** Resguardo Institucional
Proceso: Seguridad de la Información	**Subproceso:** Gestión de Seguridad de la Información	

MAPA GENERAL DEL PROCESO:



Aprobado:

GLOSARIO DE TÉRMINOS

A los fines de la interpretación y aplicación de este Manual, se definen los siguientes términos:

43. **Activo:** es el conjunto de bienes y derechos tangibles e intangibles propiedad de una persona natural o jurídica, que por lo general son generadores de renta o fuente de beneficios.
44. **Activo de Información:** se refiere a los bienes de información y procesamiento, que posee la institución. Son recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos. El verdadero valor del activo lo proporciona el valor de la información en él contenida. Estos activos de información pueden existir en muchas formas, tales como:
    a. **Impresa o escrita en papel.**
    b. **Almacenada electrónicamente.**
    c. **Transmitida por correo o utilizando medios electrónicos.**
    d. **Presentada en imágenes.**
    e. **Expuesta en una conversación.**
45. **Activo Físico:** se caracteriza por tener un valor intrínseco.
46. **Activos de información informáticos:** son todas las formas actuales y futuras de hardware, software y productos relacionados que se utilizan para el negocio de procesamiento de datos y automatización de las oficinas que tienen la capacidad de conectarse, ya sea directamente o a través de una red de área local.
47. **Amenaza:** evento que puede desencadenar un incidente en el Instituto, produciendo daños o pérdidas materiales o inmateriales en sus activos.
48. **Análisis de Riesgos:** proceso de identificar riesgos de seguridad, determinar su magnitud e identificar áreas que necesiten controles.
49. **Áreas Restringidas:** son aquellas en que se concentran bienes

informáticos de alto valor e importancia crítica cuya afectación pueda paralizar o afectar severamente la gestión de ramas o sectores de la economía o de la sociedad; territorios o entidades.

50. **Arquitectura de Información:** es la disciplina y arte encargada del estudio, análisis, organización, disposición y estructuración de la información en espacios de información, y de la selección y presentación de los datos en los sistemas de información interactivos y no interactivos.
51. **Autorización:** es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.
52. **Clasificación de los activos de información:** es el ejercicio mediante el cual se determina el nivel de pertenencia del activo, según una taxonomía previamente establecida. Tiene como objetivo asegurar que el activo de información reciba una protección adecuada. Los activos de información deben clasificarse en términos de su sensibilidad e importancia para la organización.
53. **Clasificación de la información:** procedimiento mediante el cual se determina que la información, sea cual sea su estado, pertenece a un nivel de clasificación estipulado por políticas de Bandes y tiene como propósito fundamental asegurar que recibe el nivel de protección adecuado.
54. **Confiabilidad:** es el nivel de veracidad y exactitud de los datos contenidos en los sistemas de información.
55. **Confidencialidad:** se define como la protección de la información sensible contra la divulgación no autorizada.
56. **Control:** práctica, procedimiento o mecanismo que reduce el nivel de riesgo de acceso a plataformas, sistemas o aplicaciones.
57. **Control de Acceso:** es un mecanismo que en función de la identificación ya autentificada, permite acceder a datos o recursos. Una vez identificado un usuario debe validarse qué puede hacer en la

red y a que áreas está autorizado llegar. Algunas técnicas asociadas a la autorización y control de acceso son la definición de roles, conocida como RBAC (Role Based Access Control o Control de Acceso Basado en Roles) y el filtrado de paquetes.

58. **Controles de Seguridad:** es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, entre otros, que se utiliza para disminuir la probabilidad que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que se explote la misma.
59. **Criticidad:** el término es usado para determinar la importancia de un activo de la información en el proceso productivo de una organización. Esta "importancia", es típicamente basada en una evaluación de las consecuencias que implicaría la falla del equipo o sistema en servicio.
60. **Cumplimiento:** se refiere al acatamiento de las leyes y reglamentaciones a las que están sujetas las Instituciones sometidas a la supervisión, control, fiscalización y regulación de la Superintendencia de Bancos y Otras Instituciones Financieras.
61. **Custodio:** es una parte designada de la organización, un cargo, un proceso o un grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (toma de copias de seguridad, asignar privilegios de: acceso, modificaciones, borrado) que el propietario de la información haya definido, con base en los controles de seguridad disponibles en la organización.
62. **Datos sensibles:** son aquellos datos de carácter confidencial e importante que sería problemático divulgar sin protección.
63. **Disponibilidad:** accesibilidad a la información en el tiempo y la forma cuando esta sea requerida.
64. **Gestión de Activos de Información**: se refiere a la gestión o administración sobre los activos de información del Instituto, a fin de garantizar que estos sean efectivamente controlados a través de su identificación, valoración y clasificación, así como la asignación de sus propietarios y custodios.
65. **Hardware:** son todos los componentes materiales de los

computadores y sus periféricos (discos, memoria, impresoras, entre otros).

66. **Impacto:** consecuencia sobre un activo de la materialización de una amenaza.
67. **Integridad:** es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas, a fin de preservar la precisión y suficiencia de la información, así como, su validez acorde con las pauta s fijadas por la Institución y regulaciones externas.
68. **Infraestructura Tecnológica:** agrupación de equipos, aplicaciones y sistemas destinados a ofrecer productos y servicios a través del uso de los recursos tecnológicos disponibles, a una comunidad de usuarios, públicos y privados, tanto a nivel local, regional como nacional.
69. **Perfil de acceso:** también llamados permisos o privilegios, son los derechos otorgados a los usuarios por el administrador o el supervisor. Determinan las acciones que los usuarios pueden realizar (por ejemplo, leer, escribir, ejecutar, crear y eliminar) en los archivos compartidos en el servidor.
70. **Periféricos:** elementos de un sistema de tratamiento de la información distinto de la unidad central que sirve para memorizar datos o comunicar con el exterior.
71. **Perímetro de Seguridad:** delimitación de un espacio físico por medio de una barrera (pared, puerta de acceso controlado, entre otros). El emplazamiento y la fortaleza de cada barrera dependerá de los resultados de evaluación de riesgo realizada.
72. **Privilegio:** es la asignación del tipo de transacción que puede ejecutar el Usuario de un sistema de información (consultar, incluir, eliminar, modificar).
73. **Propietario de la Información:** Es la persona designada por la organización el cual tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y determinar cuáles son los requerimientos para que la misma este salvaguardada ante el acceso no autorizado, modificación, pérdida de la confidencialidad o

destrucción adrede. Esta persona es responsable de indicar cuando la información ha de ser desincorporada, una vez que esta no sea necesaria mantenerla o requerirla.

74. **Propietario del Sistema:** las personas, usualmente gerentes ejecutivos, gerentes de línea o coordinadores, que son responsables de la integridad, el reporte y el uso correcto de los sistemas de información.

75. **Riesgo:** posibilidad de que se produzca un acontecimiento que conlleve a pérdidas materiales en el resultado de las operaciones y actividades que desarrollen las Instituciones Financieras.

76. **Riesgo Tecnológico:** se define como la posible pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en los equipos, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información en la prestación de servicios bancarios o financieros con los clientes.

77. **Riesgos inherentes:** es el riesgo de que pueda ocurrir un error material, asumiendo que no existen controles relacionados para prevenir o para detectar el error.

78. **Seguridad de la información:** se define como la preservación de integridad, disponibilidad y confidencialidad de la información en todas sus formas, impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios removibles, presentada en imágenes, expuesta en una conversación entre otras, también se puede decir que consiste en proteger la información y los recursos del sistema de información de una organización para que sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

79. **Servidor:** es una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de un ordenador y los servicios de aplicaciones, que realizan tareas en

beneficio directo del usuario final. Este es el significado original del término. Es posible que un computador cumpla simultáneamente las funciones de cliente y de servidor.

80. **Sin acceso:** condición que impide a los Usuarios ingresar a un sistema de información.
81. **Sistema de Alto Riesgo:** son aquellas aplicaciones, sistemas, procesos, operaciones, equipos y cableado que en caso de falla o paralización parcial o total pueden ocasionar pérdidas incalculables o severas que afecten la continuidad operativa del negocio.
82. **Software:** es un conjunto de programas, documentos, procedimientos y rutinas asociados con la operación de un sistema de cómputo.
83. **Trazas de Auditoría:** archivo protegido contra escritura que almacena información en forma secuencial de las transacciones u operaciones que son ejecutadas por los usuarios de los sistemas de información.
84. **Usuario:** Es cualquier persona en la organización que genera, obtenga, transforme, retenga o use en papel o medios digitales, físicamente o a través de las redes y sistemas de información de la organización. Estos utilizan la información para propósitos de los objetivos de la cadena de valor de Bandes y tendrán el derecho formal del uso dentro del inventario de los activos de información.
85. **Vulnerabilidad:** susceptibilidad de una unidad de obtener un resultado negativo derivado de un choque externo.

RESPONSABILIDADES Y NORMATIVAS

Responsabilidades relacionadas con el procedimiento

Coordinación de Seguridad de la Información	Propietarios de los Activos de Información
✓ Definir los niveles de clasificación de los activos de información en base a los siguientes criterios: confidencialidad, integridad, disponibilidad, uso. ✓ Elaborar y mantener actualizado un inventario de activos de información. ✓ Diseñar los controles de protección necesarios, que den respuesta a las necesidades del Instituto, con respecto a la distribución o restricción de la información, en base al análisis de amenazas y vulnerabilidades realizado. ✓ Gestionar riesgos tecnológicos. Realizar evaluaciones, a fin de determinar los puntos de criticidad de los activos de información y generar informes que permitan el establecimiento de controles de seguridad necesarios para la protección de los activos de información.	✓ Cumplir con las políticas operativas y controles establecidos para el uso y resguardo de los activos de información que están bajo su responsabilidad. ✓ Mantener los criterios de confidencialidad, integridad, disponibilidad y uso, que correspondan a los activos de información que están bajo su responsabilidad. ✓ Participar activamente en el proceso de definición y clasificación de los activos de información. ✓ Definir y revisar periódicamente, en conjunto con el personal de la Coordinación de Seguridad de la Información, las restricciones y clasificaciones de acceso, tomando en consideración las políticas operativas que rigen el proceso.

Aprobado:

NORMAS RELACIONADAS CON EL PROCEDIMIENTO

De la incorporación/desincorporación de activos de información

1. De manera individual, las distintas unidades de Bandes, son responsables por la incorporación al inventario, de todo nuevo activo de información que entre en funcionamiento en sus dependencias. Para tal fin, deberán notificar de inmediato a la Coordinación de Seguridad de la Información, para que proceda a su pronta inclusión y clasificación.
2. De manera individual, las distintas unidades de Bandes, deben notificar a la Coordinación de Seguridad de la Información sobre todo activo de información que haya cumplido su acometido o su vida útil y que deba ser desincorporado. Esto con la finalidad de que sea legalmente desincorporado del inventario de activos de información.
3. Tanto la incorporación como la desincorporación de cualquier activo de información digital, debe ser autorizada y ejecutado por el personal de la Gerencia Ejecutiva de Tecnología.

Del etiquetamiento de los activos de información

1. Se deben implementar medidas de control de inventarios, tales como etiquetas de activos u otras marcas de identificación que permitan el seguimiento y la contabilidad de los activos de información.
2. Toda información sensible que haya sido impresa, debe ser apropiadamente etiquetada para indicar su grado de confidencialidad. Para tales efectos se proporcionará un diseño de etiqueta para ser usado en las carátulas, encabezados y pié de página, según lo establecido en los criterios de clasificación.

Aprobado:

3. Todo mecanismo intercambiable que almacene información sensible, debe ser etiquetada de forma apropiada para indicar su grado de confidencialidad y de acuerdo a la información que contenga. Para tales efectos se proporcionará un diseño de etiqueta externa y electrónica para ser usado en dichos.

Del almacenamiento de los activos de información

1. Se deben mantener procedimientos para realizar copias periódicas de seguridad de todos los datos y archivos de sistema, necesarios para su recuperación.
2. Todo medio de almacenamiento con información crítica será resguardado bajo llave en una caja fuerte o área especial a la cual tendrá acceso únicamente, el gestor de seguridad o la unidad responsable.
3. Se establecerá un esquema de respaldo de la información, de acuerdo a su criticidad o importancia, con la finalidad de poder hacer frente a cualquier incidente de seguridad que amerite la recuperación de la instalación.
4. En principio, los equipos portátiles o cualquier otro dispositivo móvil no deben ser utilizados para almacenar información restringida. En todo caso y mediante previa autorización del custodio, aquellas computadoras o dispositivos portátiles que contenga información restringida, deberán mantenerse bajo estricta seguridad y con acceso permitido solo a las personas autorizadas y la información deberá ser eliminada de dichos dispositivos tan pronto como deje de ser necesaria.

De la transmisión de los activos de información

1. Toda transmisión de datos confidenciales o restringidos debe utilizar un protocolo de transporte seguro y/o un sistema de cifrado, utilizando los estándares establecidos.

Aprobado:

2. La información restringida, incluyendo los respaldos, solo puede ser transmitida vía protocolos de cifrados tales como HTTPS, SSH, SFTP, TLS, etc.
3. Las capacidades de cifrado y los protocolos de seguridad deben estar disponibles para los sistemas que contienen, envían o reciben datos restringidos o confidenciales.
4. Las computadoras, máquinas de fax e impresoras que puedan ser utilizadas para el manejo de información restringida, deberán ser colocadas en áreas seguras con acceso solo a aquellas personas autorizadas a manejar información restringida.
5. Cuando se requiera enviar por fax información restringida, se deben verificar que sean correctos los números del mismo y usar siempre una carátula de confidencialidad. Si por el contrario se recibe un fax no deseado que contiene información restringida, deberá informarse de inmediato al remitente y asegurar o destruir la información.
6. La transmisión de archivos de vídeo, de audio o de música, el almacenamiento de imágenes y cualquier otra función de ancho de banda o de almacenamiento intensivo debe ser utilizado con prudencia y con la estricta justificación del negocio.

Del acceso y divulgación de los activos de información

1. Las medidas de control requeridas para establecer el acceso de los usuarios a cualquier activo de información, deben ser proporcionales a la naturaleza funcional y al grado de criticidad de los recursos involucrados:

   1.1. Es responsabilidad de todos los propietarios, usuarios y custodios de los activos, asegurar que sus sistemas estén debidamente protegidos.

Aprobado:

1.2. Los activos de información deben contar con un mecanismo técnico de control de acceso.

1.3. Se requiere que todos los activos de información tengan la capacidad de registrar información básica sobre el acceso de los usuarios, sobre los eventos y errores del sistema y generar informes de violación de acceso.

1.4. Todas las cuentas de acceso al sistema deben estar basadas en un identificador único.

1.5. No se permitirán cuentas compartidas o genéricas.

1.6. Todos los accesos de los usuarios estarán basados en el "principio de mínimo privilegio" y en el "principio de separación de funciones".

1.7. Deben existir procedimientos documentados para emitir, modificar y revocar privilegios de acceso a los activos compartidos.

1.8. Toda estación de trabajo que tenga cinco (05) minutos de inactividad debe entrar, de forma automática, en modo protegido por contraseña (bloqueo).

2. Son usuarios de la red institucional todos los empleados de Bandes que tengan contacto directo y utilicen sus servicios. A éstos se les asignará una cuenta de acceso, siempre y cuando sea convenientemente identificado, autenticado y autorizado por su supervisor.

3. La Coordinación de Seguridad de la Información proporcionará, a los usuarios de los activos de información, toda la instrumentación necesaria para agilizar la utilización y garantizar la seguridad de los activos informáticos de la institución.

Aprobado:

4. Todo usuario de la red empresarial, está en la obligación de leer, firmar y acatar un "Acuerdo de Confidencialidad".
5. Toda solicitud de información, servicio o acción proveniente de un determinado usuario o departamento, deberá efectuarse siguiendo los canales de gestión formalmente establecidos por la institución.
6. Todo usuario está en la obligación de no buscar información restringida relativa a sí mismo o a cualquier otra persona sin estar autorizado para hacerlo.

De la auditabilidad de los activos de información.

1. Se deben establecer registros electrónicos de pistas de auditoría para vigilar el acceso de los empleados y terceros a los registros con información restringida.
2. Todos los sistemas deben tener la capacidad de registrar la información básica sobre la actividad de acceso de los usuarios, de cambios en el sistema y de eventos. Todos los registros de eventos deben ser convertidos a formato syslog para permitir su recolección y monitoreo centralizado. Las aplicaciones Web deben crear y enviar los registros del sistema a un servidor de registro centralizado. Los Firewalls y los sensores de detección de intrusos deben encaminar las alertas hacia un dispositivo de Gestión de Incidente de Seguridad (GIS).
3. Se deben implementar procedimientos electrónicos de seguimiento de auditoría para controlar qué tipo información se accede y por quién.

Del monitoreo de los sistemas de información

1. Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad de los sistemas de información. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación de sesión, la identidad o

ubicación de la estación de trabajo, un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.

2. Se implementarán procedimientos para monitorear el uso y procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.
3. Los propietarios de la información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para los procesos que se encuentran bajo su responsabilidad.
4. Se implementará un sistema de información para centralizar el registro, correlación y revisión de eventos de seguridad producidos en los sistemas de información.

De la seguridad Organizacional

1. La Coordinación de Seguridad de la Información de Bandes, debe proporcionar la visión estratégica, la dirección y la coordinación del programa de seguridad de los activos de información para toda la organización.
2. Los propietarios de los activos de información deben administrar y proteger los activos que están bajo su responsabilidad. Para eso deben garantizar el cumplimiento de las normas de seguridad y todos los requisitos legales y reglamentarios establecidos. También deben garantizar su confidencialidad, su integridad y su disponibilidad, así como apoyar al usuario en el cumplimiento de todas las políticas, normas y procedimientos de seguridad.
3. El custodio debe proporcionar la autoridad directa y el control sobre el manejo y uso de los activos de información bajo su responsabilidad. Esta persona puede ser un supervisor, un gerente, un jefe de departamento o un profesional designado. Puede tener doble papel como propietario/operador de un sistema, así como el de custodio de

los datos. Por lo general no lo pueden ejercer los técnicos (administradores del sistema) que le dan soporte a los sistemas informáticos o las aplicaciones relacionadas. Los custodios son responsables de seguir todas las normas, políticas y las directrices de seguridad para proteger y garantizar la confidencialidad de los activos sensibles que controlan.

4. Los usuarios (empleados y terceros) de los recursos informáticos de Bandes deben cumplir con todas las políticas, normas y procedimientos de seguridad establecidas. Están obligados a asistir y completar al menos una clase de sensibilización sobre seguridad de la información y presentar un comprobante de asistencia a su dirección de personal, para que sea incluido en su expediente.

De la seguridad de la red

1. Todas las medidas de seguridad de los activos de información y muy específicamente de los que se encuentran en la red, deben estar basadas en la naturaleza funcional y el grado de criticidad de dichos y de los activos involucrados:

   1.1. Es responsabilidad de todos los propietarios y operadores garantizar que se han implementado todas las medidas de seguridad necesarias.

   1.2. Los sistemas operativos deben ser mantenidos con la aplicación oportuna de todas las actualizaciones relacionadas y emitidas por el vendedor.

   1.3. Donde sea apropiado, los sistemas deben tener un software antivirus y mantener los procedimientos para las actualizaciones regulares.

   1.4. Todos los sistemas deben mantener en funcionamiento un sistema de medición del tiempo (clock) exacto.

Aprobado:

1.5. Los propietarios/operadores debe asegurarse que ninguna función, aplicación o proceso informático sea ejecutado en su sistema (s) utilizando una cantidad excesivamente grande de ancho de banda.

1.6. No se permite que existan dispositivos de almacenamiento masivo conectados a los sistemas de Bandes, a menos que y hasta que una solicitud de excepción que indique una razón legítima de negocio, sea recibida y aceptada por la Coordinación de Seguridad de la Información.

1.7. No se permite, bajo ninguna circunstancia y en ningún momento, la conexión a nuestros sistemas de dispositivos de red, no gestionados o autorizados por Bandes.

1.8. No se permite que ningún dispositivo que contenga un módem o una conexión externa que contenga un sistema operativo, esté conectado a los sistemas Bandes sin una aprobación de excepción, emanada por escrito de la Coordinación de Información de Seguridad. Las solicitudes de excepción no se concederán a menos que estas se adhieran a estrictas directrices de configuración.

1.9. Los propietarios/operadores deben desplegar (en el monitor) una advertencia de seguridad, antes de permitir que el proceso de apertura de sesión sea iniciado por los usuarios.

1.10. Todos los servidores considerados críticos a las funciones de negocios y/o que contengan datos confidenciales o restringidos, deberán contar con un sistema de detección/prevención de intrusos instalado, con alertas que se envían a un dispositivo de Gestión de Incidente de Seguridad (GIS).

Aprobado:

De la exposición a vulnerabilidades y amenazas de los Activos de Información

1. Para el proceso de evaluación de riesgos de los activos de información en Bandes, se considerarán amenazas que podrán ser causadas por uno o más eventos de tipo deliberado (D), accidental (A) o ambientales (M).
2. Para la evaluación de posibles vulnerabilidades, serán considerados aspectos ambientales y de infraestructura, hardware, software, documentos y personas.
3. A través de la recopilación de información a nivel gerencial, operacional y a nivel de usuarios, será realizado el proceso de identificación de amenazas y vulnerabilidades a los que están expuestos los activos de información.
4. Se deberá evidenciar la existencia de análisis de riesgos formalmente realizados y documentados sobre los sistemas de información, la tecnología informática y sus recursos asociados.
5. El resultado del análisis de riesgo debe ser formalmente reportado a la Gerencia Ejecutiva de Tecnología de la Información.

De los controles para salvaguardar los Activos de Información

1. La Coordinación de Seguridad de la Información será responsable de determinar y planificar la implementación de mecanismos de control para mitigar los riesgos asociados a los activos de información. Serán a la vez los responsables primarios de observar su continua ejecución.
2. Los mecanismos de control planificados, deberán ser notificados a la unidad correspondiente para su implementación.

Aprobado:
