UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

IMPLEMENTACIÓN DE UNA SOLUCIÓN DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS EN UNA ENTIDAD FINANCIERA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PRESENTADO POR:

CARLOS ENRIQUE SOTO LIMO

LIMA – PERÚ

2013

ÍNDICE

RESUMEN EJECUTIVO

El informe describe la implementación de una solución para la auditoría y seguridad en las bases de datos de una empresa financiera peruana, como respuesta a un conjunto de iniciativas internas y requerimientos de los organismos reguladores; presentando una metodología para la evaluación e implementación de las soluciones.

Se realizó una evaluación de las soluciones de seguridad en base de datos IBM InfoSphere Guardium e IMPERVA SecureSphere Database Security, considerando un análisis cualitativo, un análisis financiero y un análisis FODA, para determinar la alternativa que sería implementada. Como resultado de la evaluación de soluciones se decidió adquirir y desplegar la herramienta IMPERVA SecureSphere Database Security.

Luego del proceso de evaluación de soluciones se realizó una fase piloto inicial donde se desplegó la herramienta en un ambiente reducido y se identificaron los requerimientos para la planificación del proyecto. Posteriormente se procedió con la instalación básica de los componentes de acuerdo con las indicaciones del fabricante, para luego proceder con la configuración de la funcionalidad de monitoreo y las políticas de protección; y finalmente realizar la transferencia de conocimiento y la documentación.

DESCRIPTORES TEMÁTICOS

- Seguridad de la información
- Riesgo Operacional
- Auditoría de sistemas
- Gestión de logs
- Segregación de funciones
- Firewall de base de datos

INTRODUCCIÓN

En la actualidad los entornos empresariales se encuentran fuertemente regulados y se obliga a las empresas a cumplir con una serie de requerimientos, incluyendo el gobierno y la protección de datos. La mayoría de regulaciones requieren el cumplimento de los criterios de Integridad de Datos (regulaciones diseñadas para prevenir el fraude) o Confidencialidad de Datos (regulaciones diseñadas para proteger de robo o exposición de información personal, médica o financiera), criterios indispensables para mantener la seguridad de la información en las organizaciones.

Por ejemplo, podemos encontrar entre las regulaciones internacionales más importantes: las *Normas de Seguridad de Datos de la Industria de Tarjetas de Pago* (PCI DSS), cuyo objetivo es asegurar la integridad de las transacciones realizadas con Tarjetas de Crédito; la *Ley Sarbanes-Oxley* (SOX Act), publicada a raíz de una serie de escándalos de fraude financiero donde la integridad de la información financiera estuvo comprometida; y la *Ley de Responsabilidad y Portabilidad de Seguros Médicos* (HIPAA Act), con el objetivo de asegurar la privacidad y confidencialidad de la información médica personal. Sin embargo, el mercado peruano no es ajeno a esta tendencia dado que también existen regulaciones locales, como el caso del Sistema Financiero peruano que se encuentra fuertemente regulado por la Superintendencia de Banca, Seguros y AFP, en materia de la Gestión Integral de Riesgos, considerando también la seguridad de la información.

Por tanto, para mantener la competitividad y la rentabilidad de las organizaciones no sólo basta con identificar las necesidades y

requerimientos internos, sino también se hace necesario identificar las regulaciones de la industria, externas a la compañía. Sin embargo, existe una gran dificultad al momento de alinear estas necesidades internas y los requerimientos externos con los objetivos estratégicos del negocio.

En este sentido, el presente documento expone la implementación de una solución de auditoría y seguridad en bases de datos, como respuesta a una serie de necesidades internas y requerimientos regulatorios, pero sin desviarse del cumplimiento de los objetivos estratégicos del negocio y el retorno de la inversión.

El Capítulo 1 presenta una descripción general sobre el negocio de la Empresa Financiera, los productos ofrecidos, los principales clientes, la organización y sus principales procesos; así como un diagnóstico general de la estrategia, realizada a través de un análisis interno y externo, considerando la visión, misión y objetivos estratégicos.

El Capítulo 2 presenta un marco teórico y metodológico con los principales aspectos normativos locales e internacionales que son aplicables para el sistema financiero y se encuentran asociados con la preservación de la seguridad de la información.

El Capítulo 3 presenta los requerimientos externos que tiene que cumplir la organización y además las necesidades internas que impulsan la implementación de las soluciones de seguridad escogidas.

Y por último, se presentan los resultados obtenidos luego de la implementación de las soluciones de seguridad, así como también se describen las conclusiones y se brinda una serie de recomendaciones a tomar en cuenta.

CAPÍTULO I: PENSAMIENTO ESTRATÉGICO

1.1. DIAGNÓSTICO FUNCIONAL

1.1.1. Productos y Servicios

En el año 2008 la Superintendencia de Banca, Seguros y AFP aprobó el nuevo *Reglamento para la Evaluación y Clasificación del Deudor y la Exigencia de Provisiones*, el cual entró en vigencia a partir del 01 de Julio de 2010. En este reglamento se establecen las siguientes ocho categorías para la clasificación de los créditos que pueden ofrecer las instituciones financieras: Créditos Corporativos, Créditos a Grandes Empresas, Créditos a Medianas Empresas, Créditos a Pequeñas Empresas, Créditos a Micro Empresas, Créditos de Consumo Revolvente, Créditos de Consumo No-Revolvente, Créditos Hipotecarios para Vivienda.

Con respecto a la EMPRESA, los principales productos que ofrece son:

- Créditos a Micro Empresas: *"Son aquellos créditos destinados a financiar actividades de producción, comercialización o prestación de servicios, otorgados a personas naturales o jurídicas, cuyo endeudamiento total en el sistema financiero (sin incluir los créditos hipotecarios para vivienda) es no mayor a S/. 20,000 en los últimos seis (6) meses."* [1]

- Créditos a Pequeñas Empresas: *"Son aquellos créditos destinados a financiar actividades de producción, comercialización o prestación de*

servicios, otorgados a personas naturales o jurídicas, cuyo endeudamiento total en el sistema financiero (sin incluir los créditos hipotecarios para vivienda) es superior a S/. 20,000 pero no mayor a S/. 300,000 en los últimos seis (6) meses." [1]

- Créditos de Consumo: *"Son aquellos créditos revolventes o no revolventes otorgados a personas naturales, con la finalidad de atender el pago de bienes, servicios o gastos no relacionados con la actividad empresarial."* [1]

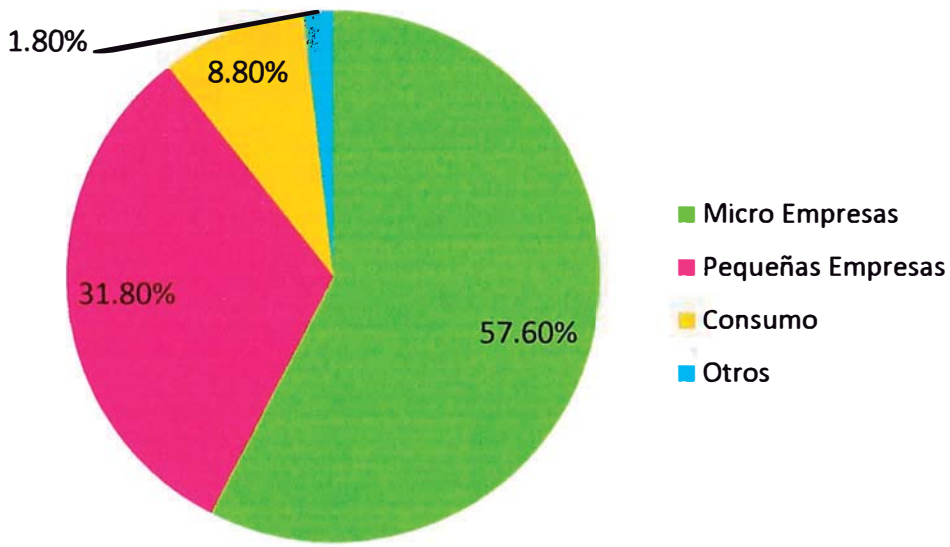


Gráfico 1: Composición productos de crédito

Fuente: Elaboración propia

Es importante mencionar que anteriormente la EMPRESA ha ofrecido productos de ahorro (depósitos a plazo fijo); sin embargo en la actualidad estos productos ya no son ofrecidos.

1.1.2. Clientes

Los clientes de la EMPRESA son los propietarios de negocios que pertenecen al sector de la pequeña y micro empresa, clasificándose de acuerdo con el volumen de los créditos que son ofrecidos (Créditos Micro Empresa, Créditos Pequeña Empresa y Créditos de Consumo). La EMPRESA busca que sus clientes no sólo puedan cumplir con sus compromisos contraídos, sino que también puedan seguir una trayectoria que los ayude a incrementar sus ingresos y sus activos.

A diciembre de 2012, la EMPRESA registraba aproximadamente unos 435,000 clientes de créditos [2] y ha presentado un incremento sostenido en los últimos 5 años. [3]

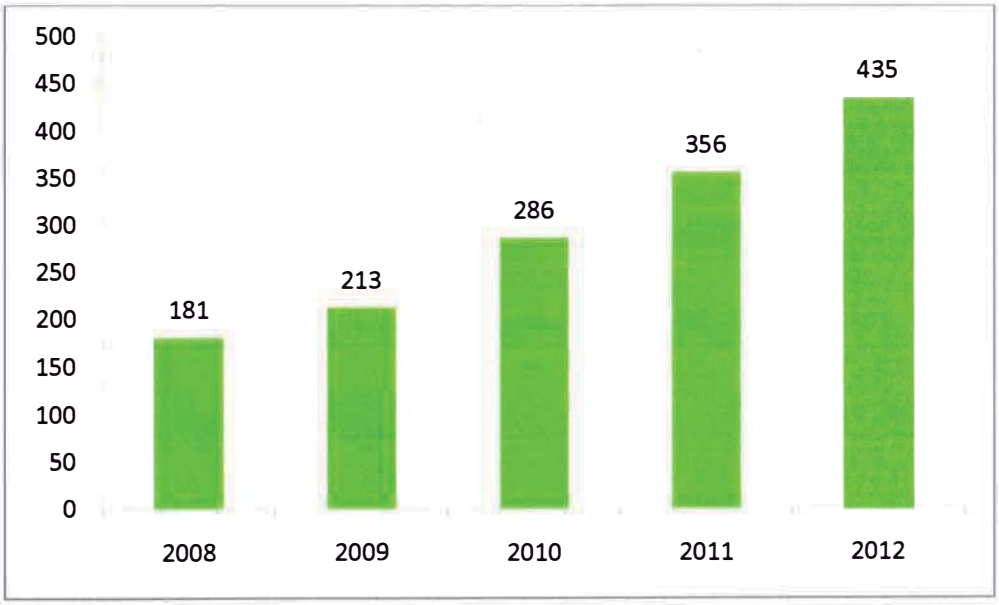


Gráfico 2: Evolución del número de clientes (en miles)

Fuente: Elaboración propia

1.1.3. Proveedores

Para soportar sus principales funciones y actividades, la EMPRESA tiene proveedores para sus siguientes servicios críticos:

Tabla 1: Proveedores

Servicio	# de proveedores
Vigilancia privada y seguridad física	1
Administración y custodia de documentos	1
Administración y custodia de cintas magnéticas	1
Adquisición y mantenimiento de software que soporta los procesos críticos	5
Adquisición, arrendamiento y mantenimiento de infraestructura tecnológica	2
Transporte y custodia de valores	2
Comunicaciones de datos	2

Fuente: Elaboración propia

1.1.4. Procesos

Los procesos en la empresa se clasifican en Procesos de Dirección, Procesos Clave y Procesos de Soporte, como se describen a continuación:

Tabla 2: Procesos

Proceso	Subproceso
Mercadeo	Investigación de Mercado
	Promoción y Publicidad
	Fortalecimiento de imagen institucional

Proceso	Subproceso
Colocación de fondos	Atención de Solicitudes de préstamos
	Evaluación
	Aprobación
	Desembolso
Gestión post venta	Atención al usuario
	Seguimiento
	Cobranza Extrajudicial
	Cobranza Judicial
	Recuperación de cartera
	Gestión de Seguros
	Operaciones Especiales
	Regularizaciones
	Gestión de documentos
Gestión de Bienes y Servicios	Adquisiciones y Contrataciones
	Proyectos de Infraestructura
	Distribución
	Gestión documentaria
	Gestión de Activos
Gestión Tecnológica	Planificación y Organización
	Adquisición e Implementación
	Entrega y Soporte de Servicios de TI
	Adquisición e Implementación
Gestión Financiera	Recaudación de ingresos
	Administración de Recursos Financieros
	Egresos de fondos
	Gestión Contable
	Movimiento de fondos
	Generación de Información para ente regulador

Fuente: Elaboración propia

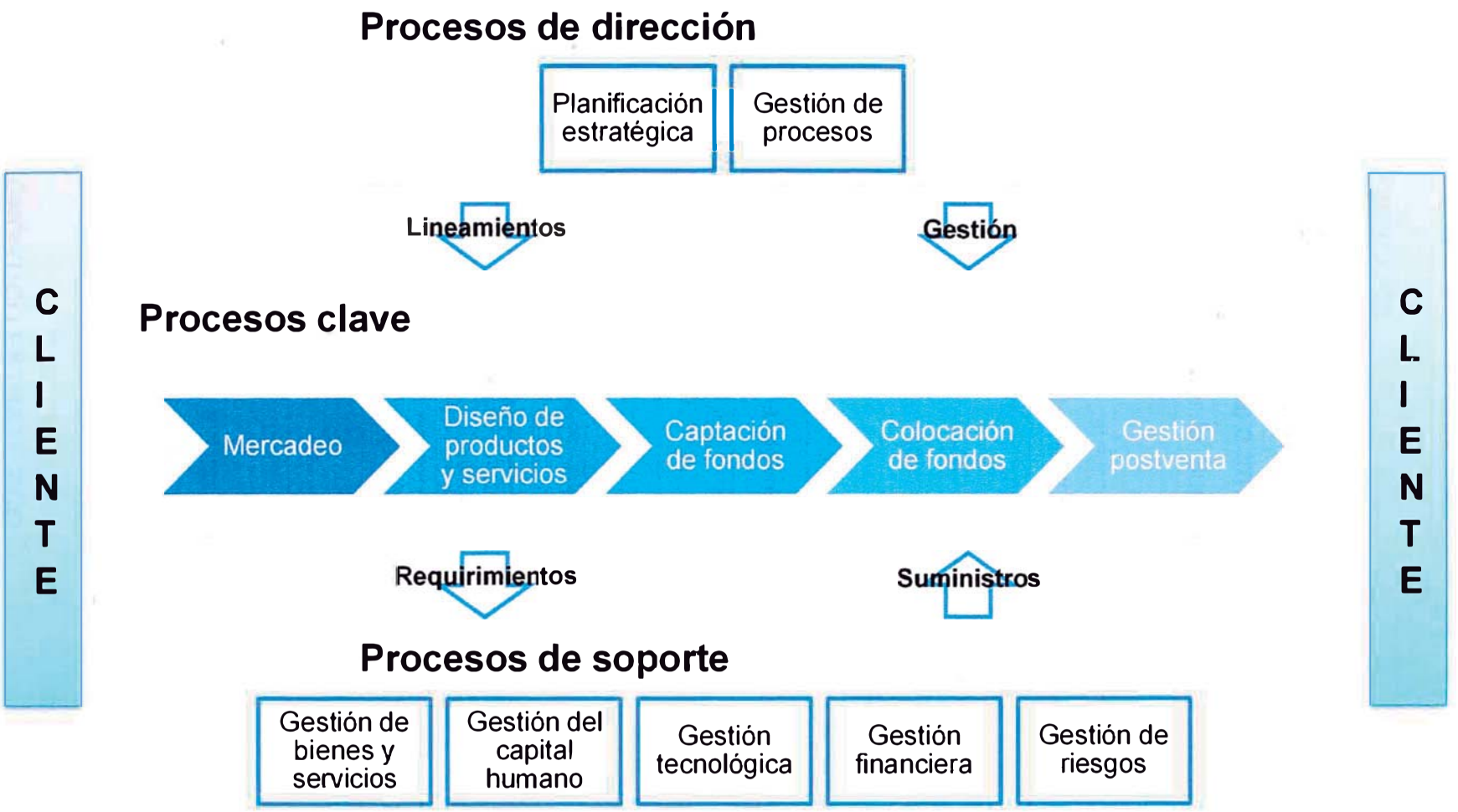


Gráfico 3: Macroprocesos

Fuente: Elaboración propia

1.1.5. Organización

La EMPRESA es una entidad financiera con más de 15 años apoyando al sector de la micro empresa, a través de servicios financieros. La EMPRESA se encuentra regulada por la Superintendencia de Banca, Seguros y AFP (SBS).

A diciembre de 2012, la EMPRESA contaba con alrededor de 160 sucursales, distribuidas a nivel nacional; de esta manera estaba presente en Lima, Ancash, Apurímac, Arequipa, Ayacucho, Cajamarca, Cusco, Huánuco, Ica, Junín, La Libertad, Lambayeque, Moquegua, Piura, Puno, San Martín, Tacna, Tumbes y Ucayali.

La EMPRESA cuenta con la siguiente estructura organizacional:

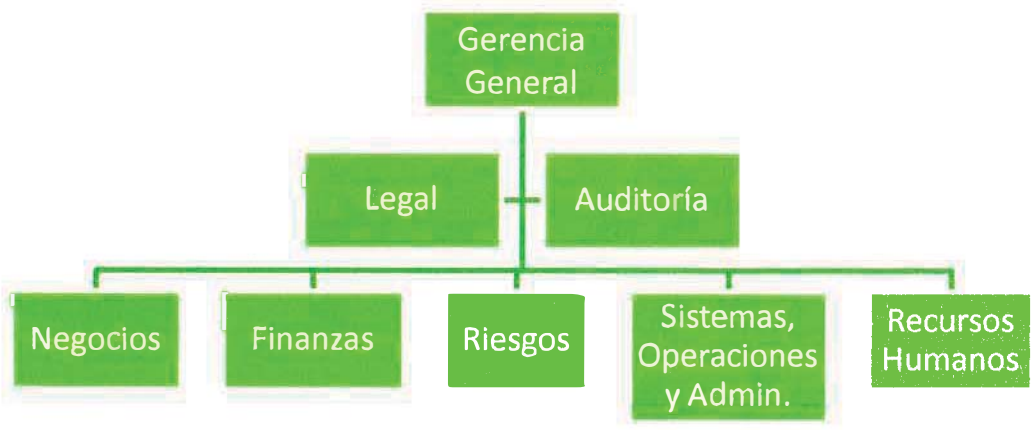


Gráfico 4: Organigrama de la EMPRESA

Fuente: Elaboración propia basado en información de la EMPRESA

1.2. DIAGNÓSTICO ESTRATÉGICO

1.2.1. Visión y Misión de la Empresa

"Promovemos la inclusión social, liderando el acceso al sistema financiero, y somos el mejor socio para el crecimiento de nuestros *clientes." – Visión de la EMPRESA* [3]

"Damos acceso y proveemos servicios financieros a personas de menores recursos económicos, preferentemente a empresarios y empresarias de la micro y pequeña empresa, contribuyendo a la mejora de su calidad de vida." – Misión de la EMPRESA [3]

Asimismo, la EMPRESA ha definido los siguientes valores organizacionales para ser difundidos en toda la organización:

- Pasión por nuestro Cliente
- Compañerismo y trabajo en equipo
- Creatividad y adaptación al cambio
- Integridad sin concesiones
- Compromiso con la inclusión Financiera

1.2.2. Objetivos Estratégicos

Como parte del proceso de planificación estratégica, luego del desarrollo de la estrategia, es necesario que sea traducida en Objetivos Estratégicos, que se encuentren alineados con la Misión y Visión de la organización.

Estos objetivos estratégicos son:

- Incrementar considerablemente el número de clientes.
- Aumentar considerablemente la participación del mercado.
- Extender la red de sucursales.

1.2.3. Fortalezas y Debilidades

Para la definición de las Fortalezas y Debilidades de la EMPRESA, se ha realizado un análisis exhaustivo basado en los últimos informes de las clasificadoras de riesgo:

Fortalezas

- Buenos resultados financieros y un adecuado margen.
- Muchos años de experiencia en el sector.
- Amplia red de sucursales a nivel nacional.

Debilidades

- Altos niveles de gastos operativos.
- Existente crecimiento en los niveles de morosidad.
- Alta rotación entre el personal de la empresa.

1.2.4. Oportunidades y Amenazas

Para la definición de las Oportunidades y Amenazas de la EMPRESA, se ha realizado un análisis exhaustivo basado en los últimos informes de las clasificadoras de riesgo y en la información del sector de servicios micro financieros:

Oportunidades

- Ventajas corporativas con la incorporación de su importante socio estratégico.
- Crecimiento de sucursales en nuevos mercados geográficos.
- Brindar productos crediticios para nuevos segmentos no atendidos.

Amenazas

- Alto crecimiento de la competencia en el sector de servicios micro financieros (Bancos, Empresas Financieras, Cajas Municipales de Ahorro y Crédito (CMAC), Cajas Rurales de Ahorro y Crédito (CRAC), y Entidades de Desarrollo para la Pequeña y Microempresa (EDPYMES)).
- Incremento en el sobreendeudamiento de los clientes.
- Fluctuaciones en algunos sectores económicos que podrían afectar la calidad de su cartera.

1.2.5. Matriz FODA

CAPÍTULO II: MARCO TEÓRICO Y METODOLÓGICO

2.1. ASPECTOS NORMATIVOS LOCALES

2.1.1. Resolución SBS N° 2115-2009

Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo Operacional

La resolución SBS N° 2115-2009 aprueba el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo Operacional, aplicable a todas las empresas reguladas del sistema financiero. Este documento indica en su Artículo 3° Requerimiento de patrimonio efectivo por riesgo operacional (actualizado con la Resolución SBS N° 3127-2012):

"Las empresas deberán destinar patrimonio efectivo para cubrir el riesgo operacional que enfrentan. Para el cálculo de dicho requerimiento patrimonial, las empresas deberán aplicar uno de los siguientes métodos:

a. Método del indicador básico
b. Método estándar alternativo
c. Métodos avanzados

El uso del método estándar alternativo o de los métodos avanzados requiere la autorización expresa de la Superintendencia.

En tanto no cuenten con la autorización señalada en el párrafo anterior, las empresas deberán aplicar el método del indicador básico.

El requerimiento de patrimonio efectivo por riesgo operacional no será mayor al 20% del requerimiento de patrimonio efectivo total (por riesgo de crédito, riesgo de mercado y riesgo operacional). Para calcular el límite de 20%, las empresas usarán la siguiente fórmula:

Requerimiento de patrimonio efectivo por riesgo operacional	≤	0.25 x (Patrimonio Mín. R. Crédito + Patrimonio Mín. R. Mercado)

Donde:

Patrimonio Mín. R. Crédito: Es el requerimiento mínimo de patrimonio efectivo según el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo de Crédito.

Patrimonio Mín. R. Mercado: Es el requerimiento mínimo de patrimonio efectivo según el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo de Mercado.

Las empresas que obtengan un requerimiento de patrimonio efectivo por riesgo operacional superior a este límite al usar cualquiera de los métodos establecidos en el presente artículo, no tendrán que destinar patrimonio por el monto que exceda al mismo.

Para hallar el equivalente a los activos ponderados por riesgo (APR) en el caso de riesgo operacional, se multiplicará el requerimiento patrimonial calculado según los métodos señalados al inicio de este artículo, por la inversa del límite global que establece la Ley General en el artículo 199°.

Adicionalmente, el APR por riesgo operacional deberá ser multiplicado por un factor, cuyo valor corresponderá al indicado en la siguiente tabla:" [4]

Periodo	Factor de ajuste
Julio de 2009 - Junio de 2010	0,40
Julio de 2010 - Junio de 2011	0,40
Julio de 2011 – Junio de 2012	0,50
Julio de 2012 – Junio de 2013	0,60
Julio de 2013 – Junio de 2014	0,80
Julio de 2014 – En adelante	1,00

Asimismo, la resolución indica en su Artículo 8° Requisitos mínimos para el uso del método estándar alternativo, literal k):

> *"La empresa deberá contar con un sistema de gestión de la seguridad de la información conforme a la normativa vigente, orientado a garantizar la integridad, confidencialidad y disponibilidad de su información."*

2.1.2. Resolución SBS N° 2116-2009
Reglamento para la Gestión del Riesgo Operacional

El riesgo operacional se define como la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

El riesgo operacional puede ser originado por los siguientes factores:

- Procesos internos: Las empresas deben gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el

desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

- Personal: Las empresas deben gestionar apropiadamente los riesgos asociados al personal de la empresa, relacionados a la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, entre otros.

- Tecnología de información: Las empresas deben gestionar los riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.

- Eventos externos: Las empresas deberán gestionar los riesgos asociados a eventos externos ajenos al control de la empresa, relacionados por ejemplo a fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores.

Además, la resolución SBS N° 2116-2009 aprueba el Reglamento para la Gestión del Riesgo Operacional, aplicable a todas las empresas reguladas del sistema financiero. Este documento indica en su Artículo 13° Gestión de la continuidad del negocio y de la seguridad de la información:

"Como parte de una adecuada gestión del riesgo operacional, las empresas deben implementar un sistema de gestión de la continuidad del negocio que tendrá como objetivo implementar respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable,

ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

Asimismo, las empresas deben contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

Para ello, las empresas deberán aplicar las disposiciones que se establezcan en las normas específicas sobre estos temas." [5]

2.1.3. Circular SBS N° G-140-2009
Gestión de la Seguridad de la Información

La circular SBS N° G-140-2009, con la finalidad de establecer criterios mínimos para una adecuada gestión de la seguridad de la información (tomando como referencia los estándares internacionales como ISO 17799 e ISO 27001), establece en su Artículo N° 3 Sistema de gestión de seguridad de la información, lo siguiente:

"Las empresas deberán establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI).

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

a. *Definición de una política de seguridad de información aprobada por el Directorio.*
b. *Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.*

c. *Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría."* [6]

Asimismo, la circular indica en su Artículo 5° "Controles de seguridad de información", una lista de controles generales que deben ser implementados.

2.2. ASPECTOS NORMATIVOS INTERNACIONALES

2.2.1. Ley Sarbanes-Oxley (SOX)

La Ley Sarbanes-Oxley (Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745), es una ley de Estados Unidos que regula las funciones financieras contables y de auditoría, y penaliza en una forma severa, el crimen corporativo y de cuello blanco. Esta ley se aprueba como producto de los múltiples fraudes, actos de corrupción administrativa, conflictos de interés, negligencia y malas prácticas de algunos profesionales y ejecutivos que conociendo los códigos de ética, realizaron actividades fraudulentas en sus organizaciones, engañando a los accionistas, a los empleados y distintos grupos de interés, entre ellos sus clientes y proveedores.

Esta ley considera en su sección 404, requerimientos para la evaluación gerencial de los controles internos, de modo que se requiere que el informe anual contenga "un informe de control interno", que deberá:

- (1) indicar la responsabilidad de la gerencia para establecer y mantener una estructura de control interno adecuado y procedimientos para informes financieros, y

- (2) tener una evaluación, a la fecha del cierre del año fiscal, de la efectividad de la estructura de control interno y de los procedimientos de los informes financieros.

Esta evaluación de la efectividad de la estructura de control interno debe considerar los controles de Tecnologías de Información implementados para asegurar la integridad de datos financieros y la emisión de reportes periódicos para evidenciar la implementación de estos controles.

2.2.2. Normas de Seguridad de Datos de la Industria de Tarjetas Payment Card Industry Data Security Standard (PCI DSS)

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas. Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos.

A continuación, se muestra una descripción general de los 12 requisitos de las PCI DSS [7]:

Tabla 3: Requisitos PCI DSS

Normas de Seguridad de Datos de la PCI	
Desarrollar y mantener una red segura	1. Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta. 2. No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.
Proteger los datos del titular de la tarjeta	3. Proteja los datos del titular de la tarjeta que fueron almacenados. 4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidades	5. Utilice y actualice con regularidad los programas o software antivirus. 6. Desarrolle y mantenga sistemas y aplicaciones seguras.
Implementar medidas sólidas de control de acceso	7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa. 8. Asignar una ID exclusiva a cada persona que tenga acceso por computador. 9. Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	10. Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de tarjetas. 11. Prueba con regularidad los sistemas y procesos de seguridad
Mantener una política de seguridad de información	12. Mantenga una política que aborde la seguridad de la información para todo el personal

Fuente: Elaboración propia basado en PCI DSS

2.3. SEGURIDAD DE DATOS Y CUMPLIMIENTO

2.3.1. Amenazas de seguridad en base de datos

Las amenazas de seguridad en base de datos incluyen amenazas de hacking externo, como las Amenazas Persistentes Avanzadas (Advanced

Persistent Threats APT), ataques de inyección SQL, gusanos y malware. Los ataques internos o "Amenazas Internas" también poseen un riesgo significativo para la seguridad en base de datos [8].

Amenazas externas:

- Amenazas Persistentes Avanzadas: El término APT (Advanced Persistent Threats) se refiere a un patrón a largo plazo de sofisticados ataques de hacking dirigidos a objetivos políticos o empresas. Las APT se componen típicamente de una serie de ataques que utilizan diferentes técnicas para eludir las defensas corporativas y acceder a recursos internos.
- Ataques de inyección SQL: Estos ataques explotan las vulnerabilidades en las aplicaciones Web. El atacante aprovecha las vulnerabilidades en la validación de ingreso de datos en las aplicaciones Web para inyectar consultas SQL no autorizadas en las bases de datos. Utilizando esta técnica un hacker puede obtener accesos sin restricciones al contenido de una base de datos completa.
- Gusanos y Malware: La existencia de vulnerabilidades permite la proliferación de malware que expone las bases de datos a los hackers. Los gusanos también han sido utilizados para explotar vulnerabilidades existentes en las bases de datos. Por ejemplo, el gusano "SQL Slammer" apareció a inicios de 2003, explotando una vulnerabilidad conocida de desbordamiento de buffer en el motor de base de datos SQL Server 2000, a pesar que Microsoft publicó a mediados de 2002 el parche de seguridad para remover esta vulnerabilidad, no todas las compañías lo aplicaron y este gusano estuvo comprometiendo muchas bases de datos hasta finales de 2010.

Amenazas internas:

Los usuarios maliciosos tienen numerosas oportunidades para robar o alterar los datos alojados en las bases de datos. Ya sea abusando de la confianza depositada en los usuarios o explotando una debilidad conocida en las bases de datos, los usuarios maliciosos a menudo son capaces de acceder a los datos sensibles. Los siguientes ejemplos ilustran técnicas de ataque de bases de datos comunes que pueden conducir a quebrantamientos costosos de base de datos:

- Abuso de privilegios de base de datos: Cuando los usuarios reciben privilegios de acceso de base de datos que exceden los requerimientos de sus funciones o responsabilidades, pueden abusar de estos privilegios para acceder a los datos con fines maliciosos, por ejemplo, el robo de datos.
- Elevación de privilegios de base de datos: Un atacante interno puede aprovecharse de las vulnerabilidades de la plataforma de base de datos para convertir los privilegios de acceso común en los privilegios de administrador. Las vulnerabilidades se pueden encontrar en los procedimientos almacenados, funciones integradas, las implementaciones del protocolo e incluso en las consultas SQL.
- Débiles controles de auditoría: Los controles de auditoría débiles permiten a los atacantes internos eludir el proceso de auditoría o borrar toda prueba de su fechoría en la pista de auditoría. Como resultado, la brecha no se puede detectar de manera oportuna y los investigadores tendrán que luchar para entender la causa y efecto del ataque.

2.3.2. Marco de trabajo para el cumplimiento de estándares

Considerando la existencia de distintas regulaciones, estándares y marcos de trabajo, se pueden observar temas comunes a través de cada esfuerzo de gobierno, independientemente del estándar o reglamento. Con estas consideraciones, podemos definir un conjunto de acciones concretas de pasos que se extrae de los puntos fuertes de cada marco de gestión de TI y que al mismo tiempo permite un esfuerzo de cumplimiento manejable [9].

Este proceso iterativo incluye los siguientes cuatro pasos:

- Paso 1: Evaluar
  Recopilar información de riesgos y el uso de los datos.

- Paso 2: Establecer controles y políticas
  Definir patrón de uso aceptable.

- Paso 3: Vigilar y hacer cumplir
  Capturar la actividad y evitar acciones no autorizadas.

- Paso 4: Medir
  Informar sobre la actividad y recomendar mejoras cuando sea necesario.

Mediante este proceso, se podrán satisfacer los requisitos de cumplimiento de los auditores y directores de empresas, así como para asegurar el alineamiento del negocio, un control satisfactorio, niveles de seguridad robustos y eficiencia de las operaciones en la organización de TI.

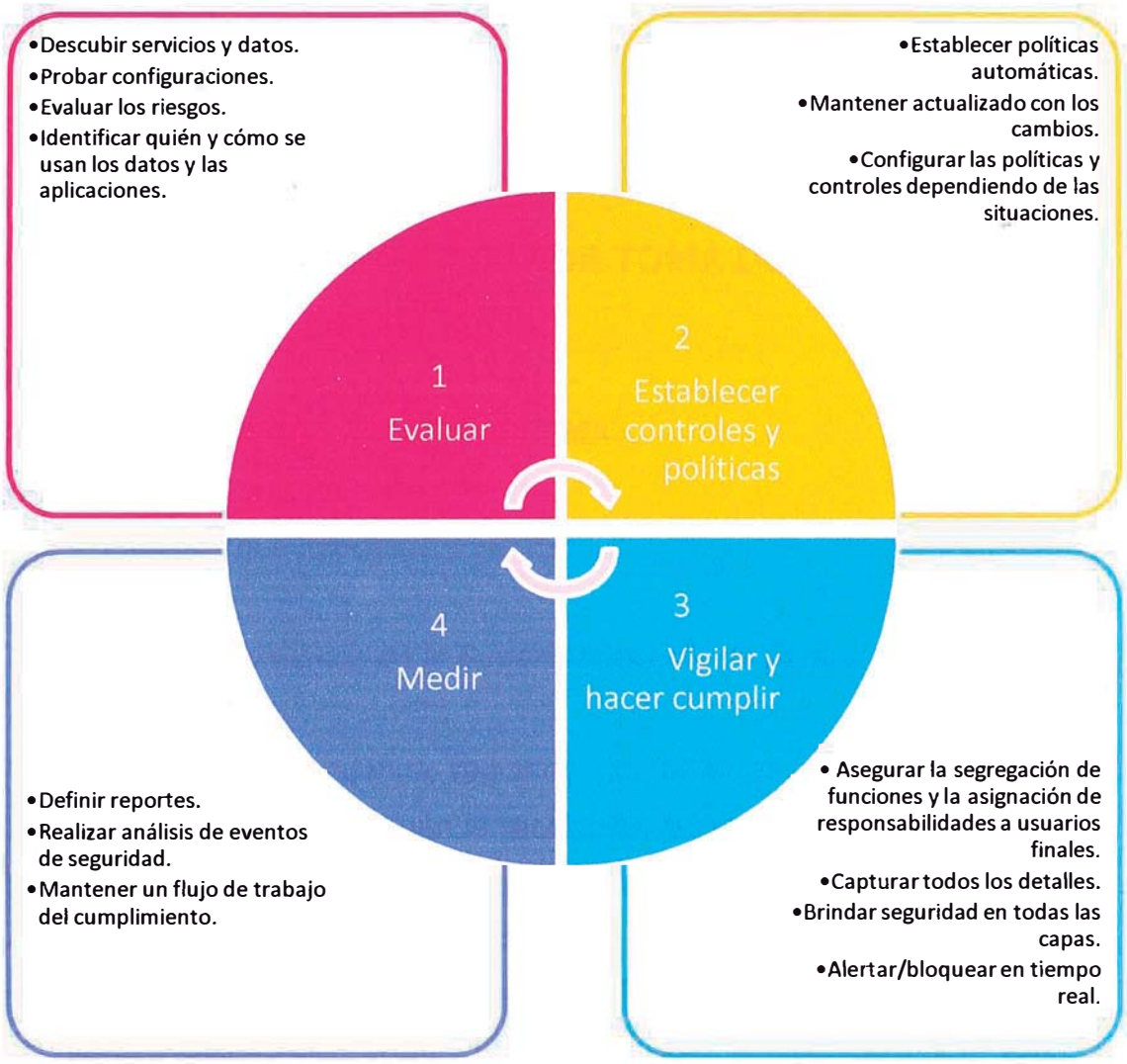


Gráfico 5: Marco de trabajo

Fuente: Elaboración propia

CAPÍTULO III: PROCESO DE TOMA DE DECISIONES

3.1. PLANTEAMIENTO DEL PROBLEMA

3.1.1. Factores que impulsan el cambio

3.1.1.1. Requerimientos de la Superintendencia de Banca, Seguros y AFP

La EMPRESA se encuentra regulada por la Superintendencia de banca Seguros y AFP (SBS) y según la resolución N° 2115-2009 se debe destinar patrimonio efectivo para cubrir el riesgo operacional que enfrenta. Actualmente el cálculo de este requerimiento patrimonial se realiza utilizando el Método del Indicador Básico que considera como indicador de exposición el "margen operacional bruto" de la EMPRESA, el cual se define como la suma de los ingresos financieros y los ingresos por servicios menos los gastos financieros y los gastos por servicios. Se deberá utilizar la siguiente fórmula:

$$R = \sum_{i=1} (MO_i \times \alpha) / n$$

Donde:

R : Requerimiento patrimonial por riesgo operacional
MOi : Saldo anualizado del margen operacional bruto correspondiente al año i, en los casos que sea positivo
α : Factor fijo igual a 15%
n : Número de años en los que el saldo anualizado del margen operacional bruto fue positivo, considerando los 3 últimos años.

Por tanto, si consideramos los siguientes montos aproximados para los periodos 2009, 2010 y 2011:

Tabla 4: Margen operacional bruto

En miles de NS	2009	2010	2011
Margen Operacional Bruto	166,000	239,000	314,000

Fuente: Elaboración propia basado en información de la EMPRESA

$$R = \frac{(166{,}000 + 239{,}000 + 314{,}000) \times (15\%)}{3}$$

$$R = 35{,}950$$

Obtendremos para 2011 cerca de 36 Millones de Nuevos Soles como requerimiento de patrimonio efectivo para cubrir el Riesgo Operacional.

Sin embargo, realizando los cálculos necesarios para el mismo periodo según el método estándar alternativo, que requiere considerar los saldos de créditos e inversiones durante los últimos 12 meses, conforme a la siguiente fórmula:

$$IE = m \times \sum_{i=1}^{12} Ci / 12$$

Donde:

IE : Indicador de exposición anual para la línea de negocio banca comercial o banca minorista
m : 0,035 (Factor fijo)
Ci : Monto del saldo de créditos e inversiones para el mes i para Banca Comercial o Banca Minorista, según corresponda.

Obtendremos para 2011 cerca de 11 Millones de Nuevos Soles como requerimiento de patrimonio efectivo para cubrir el Riesgo Operacional.

En conclusión, obtener la autorización para la utilización del método estándar alternativo en el cálculo de los requerimientos de patrimonio efectivo por riesgo operacional, brinda una disminución de aproximadamente 25 Millones de Nuevos Soles en requerimientos patrimoniales.

Luego, para que la EMPRESA obtenga la autorización del uso del método estándar alternativo requiere la autorización expresa de la Superintendencia de Banca, Seguros y AFP. Esta autorización requiere que la EMPRESA cuente con un sistema de gestión de la seguridad de la información conforme a la normativa vigente, orientado a garantizar la integridad, confidencialidad y disponibilidad de su información. Con respecto a este sistema de gestión, la Superintendencia ha indicado que la EMPRESA debe aplicar técnicas para asegurar la integridad y confidencialidad de los datos almacenados en sus bases de datos, además debe restringir el acceso a información sensible por parte de usuarios privilegiados.

3.1.1.2. Cumplimiento de regulaciones

Las bases de datos de la EMPRESA son el activo de información más estratégico que tiene ya que estas almacenan datos extraordinariamente valiosos, como información personal, datos de tarjetas de crédito, datos de clientes, datos financieros y más. En los últimos años una serie de normas y leyes de privacidad se han promulgado para garantizar que la EMPRESA proteja estos datos contra el robo y el abuso.

Como la EMPRESA debe cumplir con la ley SOX y con la Circular SBS N° G-140-2009, debe considerar:

- Administrar y monitorear el acceso de usuarios a información sensible.
- Proteger las bases de datos y la información que almacenan de los ataques y accesos no autorizados.
- Evaluar las vulnerabilidades y mitigar los riesgos de las brechas de seguridad.
- Mantener una completa pista de auditoría de las actividades de base de datos.
- Reportes periódicos para validar la implementación de los controles.

3.1.1.3. Requerimientos internos de la EMPRESA

Considerando que las bases de datos contienen la información más valiosa y sensible de la EMPRESA, es necesario proteger las bases de datos a través de una estrategia que considere:

- Evaluación de vulnerabilidades: La EMPRESA debe evaluar sus bases de datos para determinar configuraciones erróneas y las vulnerabilidades que pueden aumentar el riesgo de una fuga de datos.
- Administración de privilegios de usuarios: La EMPRESA debe limitar los derechos de acceso a los datos a la "necesidad de saber" del negocio. Esto ayudará a reducir y controlar mejor el riesgo de una fuga de datos.
- Prevención de ataques de aplicaciones y base de datos: Para proteger los datos de sus bases de datos, las EMPRESA debe identificar y bloquear ataques en tiempo real.

3.2. ALTERNATIVAS DE SOLUCIÓN

Para satisfacer los requerimientos regulatorios y de negocio, se presentan 2 alternativas para la implementación de una solución de auditoría y monitoreo de base de datos:

Alternativa 1: IBM InfoSphere Guardium
Alternativa 2: IMPERVA SecureSphere Database Security

A continuación describiremos ambas soluciones.

3.2.1. IBM InfoSphere Guardium

Los productos IBM InfoSphere Guardium garantizan la seguridad, la privacidad y la integridad de la información de las bases de datos. Estos productos de seguridad de datos admiten entornos heterogéneos de bases de datos y uso compartido de archivos para aplicaciones empaquetadas y personalizadas en todas las plataformas operativas líderes. [10]

3.2.1.1. IBM InfoSphere Guardium Activity Monitor

La solución impide que se realicen actividades no autorizadas por parte de usuarios internos privilegiados o de hackers y, al mismo tiempo, supervisa los usuarios finales a fin de detectar posibles fraudes, sin realizar cambios en las bases de datos ni en las aplicaciones y sin que ello afecte al rendimiento. Esta la solución ofrece [10]:

- 100% de visibilidad de todas las transacciones de bases de datos, en todas las plataformas y protocolos, incluidas las de los

administradores de bases de datos, los desarrolladores y el personal subcontratado.

- Supervisión e imposición de políticas para acceso a datos confidenciales, acciones de usuarios privilegiados, control de cambios, actividades de usuarios de aplicaciones y excepciones de seguridad.
- Agregación y normalización centralizadas de datos de auditoría de toda la infraestructura de bases de datos para realizar auditorías, informes, correlación y análisis forenses conformes a las normas a nivel de empresa.
- Seguimiento seguro a prueba de manipulaciones que permite la separación de tareas que requieren los auditores.

3.2.1.2. IBM InfoSphere Guardium Vulnerability Assessment

La solución permite eliminar el enorme riesgo generado por las configuraciones de bases de datos no seguras, la falta de parches, un débil sistema de contraseñas y otras vulnerabilidades, y ofrece [10]:

- Pruebas de vulnerabilidad preconfiguradas, que incluyen prácticas recomendadas, que se actualizan de forma regular a través de la base de conocimiento de IBM.
- Pruebas estáticas específicas de plataforma que detectan configuraciones no seguras de la base de datos concreta que se está evaluando.
- Pruebas dinámicas, lo que permite la detección de vulnerabilidades de comportamiento, como la compartición de cuentas, el exceso de inicios de sesión de administración y la actividad inusual fuera de horas.
- Un resumen de la evaluación de seguridad, además de detalles, ordenados según prioridades, que recomiendan medidas correctivas.

- El más amplio soporte heterogéneo, que incluye plataformas de bases de datos en los principales sistemas operativos.
- Pruebas exhaustivas de vulnerabilidad que no se basan en aprovechamientos intrusivos ni en pruebas que puedan afectar a la disponibilidad del sistema, así como información de consulta sobre vulnerabilidades externas, como identificadores de CVE.

3.2.2. IMPERVA SecureSphere Database Security

Los productos SecureSphere Database Security de Imperva automatizan las auditorías de las bases de datos, e identifican de inmediato los ataques, las actividades malintencionadas y el fraude. En combinación con las soluciones Web Application Security y File Security de Imperva, SecureSphere es la primera opción para la protección de la información empresarial restringida.

3.2.2.1. IMPERVA SecureSphere Database Firewall

El producto SecureSphere Database Firewall (DBF) proporciona una solución de seguridad y cumplimiento para aplicaciones y bases de datos entregando una automatizada y transparente aproximación para monitoreo y protección de datos en la medida que estos son accedidos y modificados a través de aplicaciones y bases de datos. DBF adiciona capacidades de aplicación de políticas y protección para bloquear actividades no autorizadas y ataques a bases de datos.

SecureSphere Database Firewall incluye lo siguiente:

- Monitoreo de actividad y auditoría con total visibilidad en el uso de datos por usuarios finales desde la aplicación hasta la base de datos.

- Modelo de defensa Multi-capa incluyendo detección y prevención de ataques.

- Capacidades automatizadas para alcanzar, mantener y documentar cumplimiento regulatorio.

Los beneficios de la solución son:

- Auditoría continua del uso de la información restringida: SecureSphere monitoriza de forma continua y en tiempo real todas las operaciones de las bases de datos, proporcionando cadenas detalladas de auditoría que indican el 'quién, qué, cuándo, dónde y cómo de todas las transacciones. SecureSphere hace auditorías de los usuarios con privilegios que tienen acceso directo a los servidores de bases de datos, así como a los usuarios sin privilegios que tienen acceso a las bases de datos a través de diversas aplicaciones. SecureSphere también monitoriza las respuestas de las bases de datos a fin de alertar y detener las fugas de información restringida.

- Detección de accesos no autorizados y de actividades fraudulentas: SecureSphere identifica los patrones normales de acceso de los usuarios a la información, mediante la tecnología de perfiles dinámicos.

- Bloqueo en tiempo real de las inyecciones SQL, de los ataques DoS y de otros: A la vez que hace auditorías selectivas de la información restringida, SecureSphere monitoriza en tiempo real toda la actividad de las bases de datos a fin de detectar fugas desconocidas de información, transacciones SQL no autorizadas, y ataques a los protocolos y a los sistemas.

- Cumplimiento de directivas e informes ágiles de la conformidad: SecureSphere incluye un conjunto completo de directivas de seguridad y auditoría predefinidas y personalizables.

- Clasificación del alcance de la información a efectos de la conformidad y de la seguridad: SecureSphere detecta todos los sistemas de bases de datos a fin de determinar el alcance de los proyectos de seguridad y de conformidad, a través del descubrimiento y la clasificación automáticas de la información restringida.

- Control eficaz de los derechos de usuario en todas las bases de datos: SecureSphere agrega automáticamente los derechos de usuario, aún entre bases de datos heterogéneas.

3.3. METODOLOGÍA DE EVALUACIÓN DE SOLUCIONES

3.3.1. Evaluación cualitativa

Se realizará la comparación de las funcionalidades que brindan ambas alternativas, los estándares que son soportados por las herramientas, las características de la arquitectura y las configuraciones de seguridad (ver detalle en el Anexo 3).

Tabla 5: Evaluación cualitativa

Categoría	Ponderación	IMPERVA SecureSphere		IBM InfoSphere Guardium	
		% Alcanzado	% Ponderado	% Alcanzado	% Ponderado
Funcionalidades	60%	89%	53%	89%	53%
Estándares	10%	100%	10%	100%	10%
Arquitectura	15%	89%	13%	89%	13%
Seguridad	15%	67%	10%	100%	15%
	TOTAL	**87%**		**92%**	

Fuente: Elaboración propia

3.3.2. Evaluación financiera

Se realizará la comparación de las propuestas económicas enviadas por los proveedores de ambas alternativas; se evaluarán los precios de las licencias, el mantenimiento, los servicios de implementación y capacitación.

Tabla 6: Evaluación financiera

En US$	IMPERVA SecureSphere	IBM InfoSphere Guardium
Licencias HW y SW	40,000	54,000
Mantenimiento	8,000	8,000
Consultoría y capacitación	10,000	8,000
Total (sin impuestos)	**58,000**	**70,000**
IGV (18%)	10,440	12,600
TOTAL (con impuestos)	**68,440.00**	**82,600.00**

Fuente: Elaboración propia

3.3.3. Análisis FODA

En base a la información obtenida, se ha realizado un análisis FODA para ambas alternativas:

Tabla 7: Análisis FODA

	IMPERVA SecureSphere	IBM InfoSphere Guardium
Fortalezas	• Solución no intrusiva en las bases de datos. • División de la carga de trabajo entre agente (tráfico local)y appliance (tráfico de red).	• Experiencia previa del partner local en implementaciones de la solución. En Chile, Argentina y Bolivia. • Solución basada en agentes con 5 años de experiencia previa y mejoras continúas.
Amenazas	N/A	N/A
Oportunidades	• Habilitación posterior de la funcionalidad de Web Application Firewall y File Server Security utilizando los mismos equipo.	
Debilidades	• Solución basada en appliance con poca experiencia en instalaciones locales.	
Semáforo		

Fuente: Elaboración propia

3.4. TOMA DE DECISIÓN

Considerando las evaluaciones cualitativas y económicas, además de la evaluación de las Fortalezas, Oportunidades, Debilidades y Amenazas de cada alterativa, se decidió por la solución IMPERVA SecureSphere Database Security.

Esta solución se implementará a través de lo siguiente:

- Consola de administración:
  Realiza monitoreo de bases de datos y aplicaciones proporcionando total visibilidad en como los datos son usados en la organización sin importar si estos son accesados de manera directa o indirecta por la aplicación.
- Firewall de base de datos:
  Realiza tareas de monitoreo y bloqueo de tráfico malicioso
- Agentes locales:
  Los agentes instalados sobre los servidores de bases de datos monitorean la actividad local en la base de datos ya sea que se use una consola o una sesión SSH sobre la red. Los agentes registran tráfico de la base de datos y envían este a la consola de administración para el almacenamiento y análisis.

3.5. DESARROLLO DE LA SOLUCIÓN ELEGIDA

3.5.1. Gestión del proyecto

Se definió la siguiente estructura de desglose del trabajo para detallar el alcance del proyecto:

Gráfico 6: Estructura de Desglose de Trabajo (EDT)

Fuente: Elaboración propia

Asimismo, se definió el siguiente cronograma con las principales actividades e hitos:

Tabla 8: Cronograma

No	Actividad	Inicio	Fin
Fase 0			
1.1	Preparación	May-12	May-12
1.2	Pruebas	May-12	May-12
1.3	Conclusiones	May-12	May-12
Fase 1 - Requerimientos			
2.1	Revisión de requerimientos del proyecto	Jun-12	Jun-12
2.2	Levantamiento de información	Jun-12	Jun-12

No	Actividad	Inicio	Fin
Fase 2. Instalación básica de componentes			
2.1	Instalación física de componentes	Jul-12	Jul-12
2.2	Instalación de Firmware	Jul-12	Jul-12
2.3	Configuración de parámetros de red	Jul-12	Jul-12
Fase 3. Configuración de funcionalidad de monitoreo			
3.1	Definición de grupo de servers	Ago-12	Ago-12
3.2	Definición de reglas de auditoría	Ago-12	Ago-12
3.3	Creación de reportes	Set-12	Set-12
3.4	Definición de acciones	Oct-12	Oct-12
Fase 4. Configuración de políticas de protección			
5.1	Gestión de perfiles	Nov-12	Nov-12
5.2	Revisión y monitoreo de alertas	Nov-12	Nov-12
5.3	Revisión de logs de eventos del sistema	Dic-12	Dic-12
5.4	Definición de políticas de protección	Dic-12	Dic-12
Fase 5. Transferencia de conocimiento y documentación			
6.1	Documentación	Ene-13	Ene-13
6.2	Capacitación presencial	Ene-13	Ene-13

Fuente: Elaboración propia

3.5.2. Fase 0. Prueba piloto

Para verificar la correcta funcionalidad de la solución IMPERVA SecureSphere Database Security se programó una prueba piloto en un ambiente controlado con características similares a las del ambiente de producción. Esta prueba consideró 3 actividades:

- Preparación: Se prepararon los servidores para generar un ambiente similar al ambiente de producción, con las siguientes características:

    - Servidor: IBM POWER 750
    - Base de datos: Oracle 11g R2
    - Sistema operativo: AIX 7.1

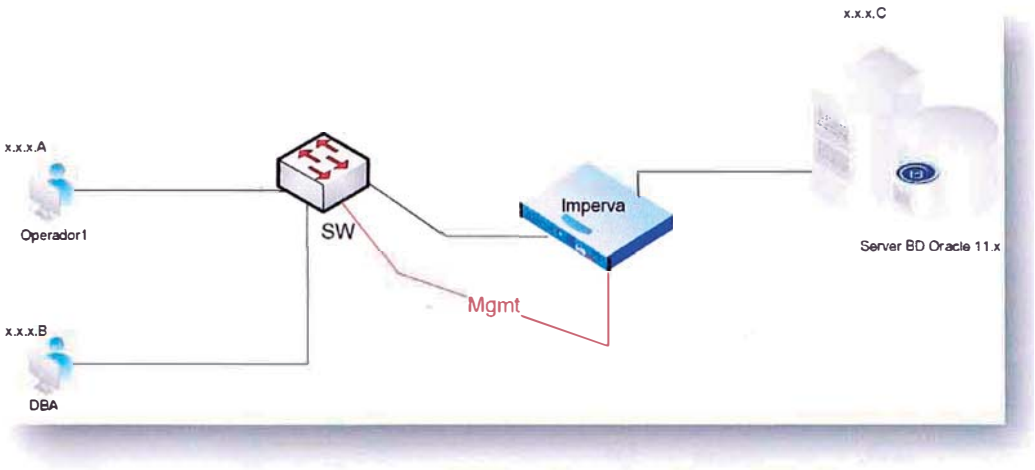


Gráfico 7: Diagrama de red propuesto

Fuente: Elaboración propia

Se realizaron las configuraciones de red como se muestra en la imagen anterior. Luego se instalaron los agentes en el servidor de base de datos y se creó la cuenta "consulta_".

Se realizaron consultas hacia la base de datos para generar tráfico y se identificó que la herramienta ha detectado dicho tráfico, como se muestra en la imagen siguiente:

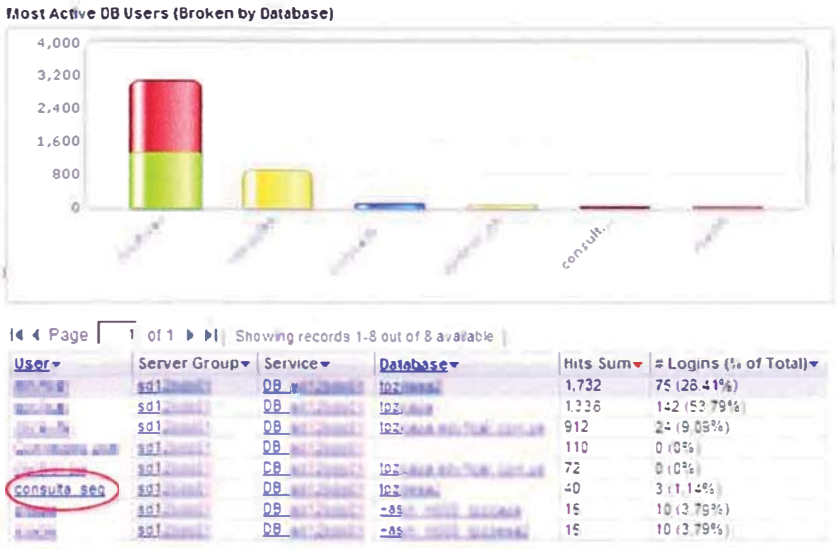


Gráfico 8: Actividad de la cuenta "consulta_seg"

Fuente: Elaboración propia basado en el dashboard de IMPERVA SecureSphere

En la consola de la herramienta se configuró la política "policy_block_tabla" para la cuenta "consulta_seg", estableciendo restricciones sobre las tablas "sl_balance", "sl_solicitudcreditopersona" y "usuarios".

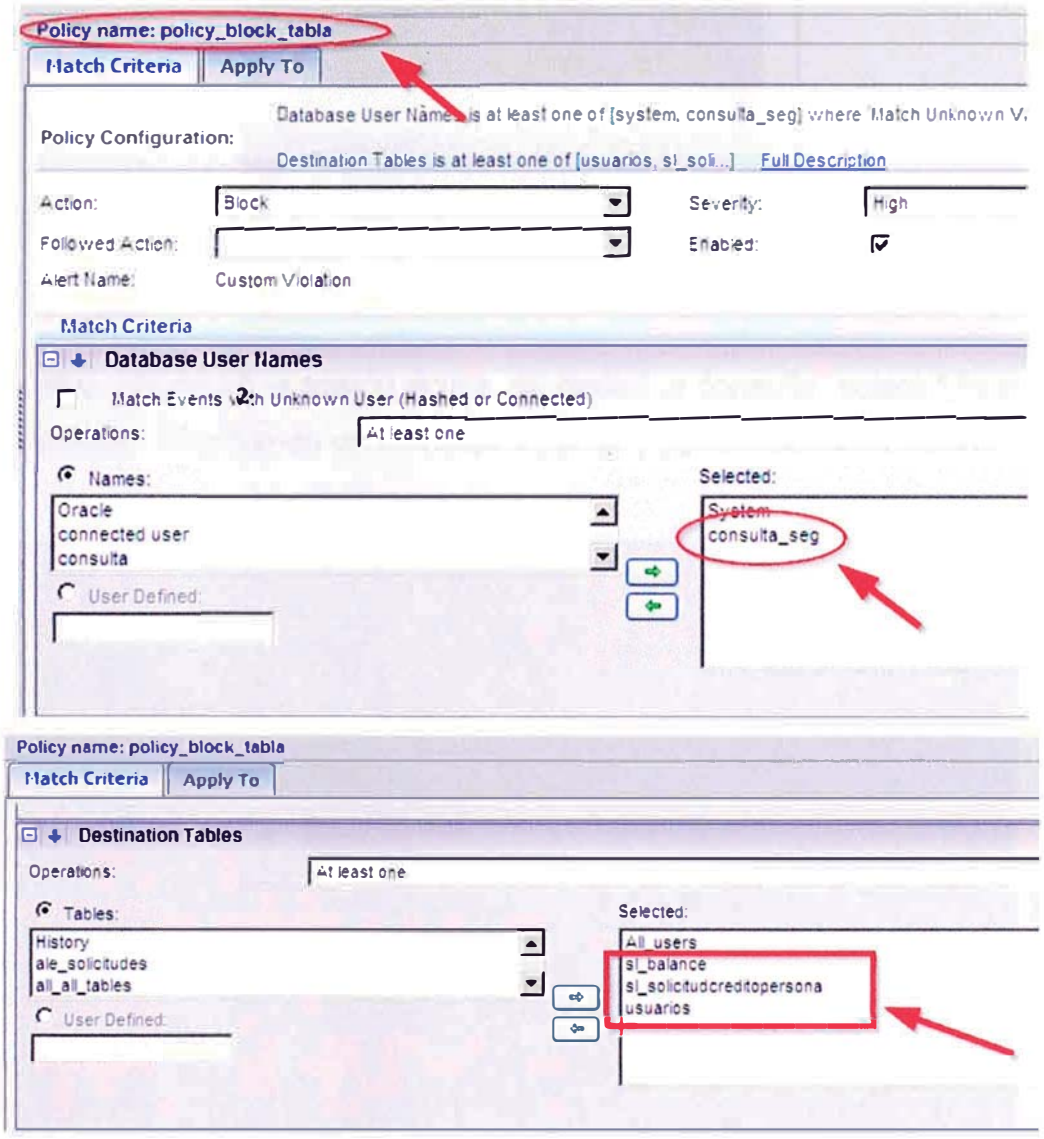


Gráfico 9: Configuración de la política "policy_block_tabla"

Fuente: Elaboración propia basado en el dashboard de IMPERVA SecureSphere

- Prueba de conexión directa (SSH):

  El Administrador de Base de Datos, se conectó al servidor de base de datos "10.2.X.X" utilizando la cuenta local "oracle" de modo que se

puedan hacer consultas locales utilizando el usuario de base de datos “consulta_seg”.

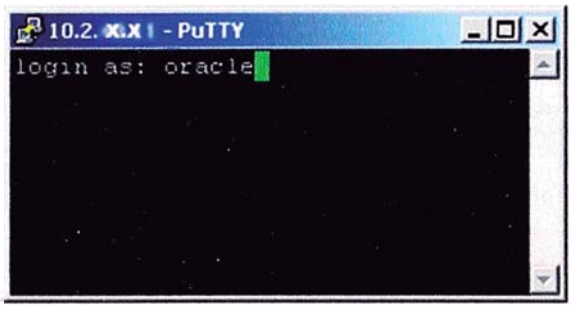


Gráfico 10: Login servidor de base de datos

Fuente: Elaboración propia basado el inicio de sesión del servidor AIX

Luego, utilizando la sesión activa, se realizó la consulta “select * from usuarios”, obteniendo un mensaje de error y cerrándose la conexión.

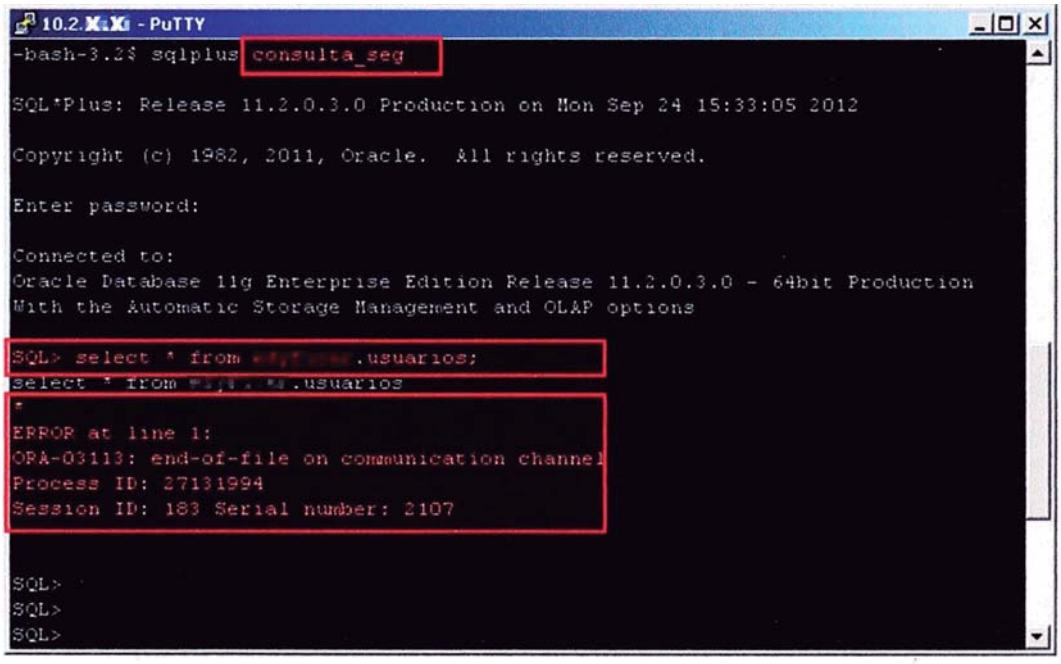


Gráfico 11: Consulta a la tabla “usuarios”

Fuente: Elaboración propia basado el inicio de sesión del servidor AIX

Revisando el historial de alertas, se verificó que el mensaje de error mostrado en la actividad anterior fue generado por la activación de la política “policy_block_tabla” que considera el bloqueo para los

accesos locales del usuario “consulta_seg” al servidor “10.2.X.X” (sd12XXX) utilizando la herramienta “sqlplus”. Además, se puede observar la consulta que lanzó ejecución de la política.

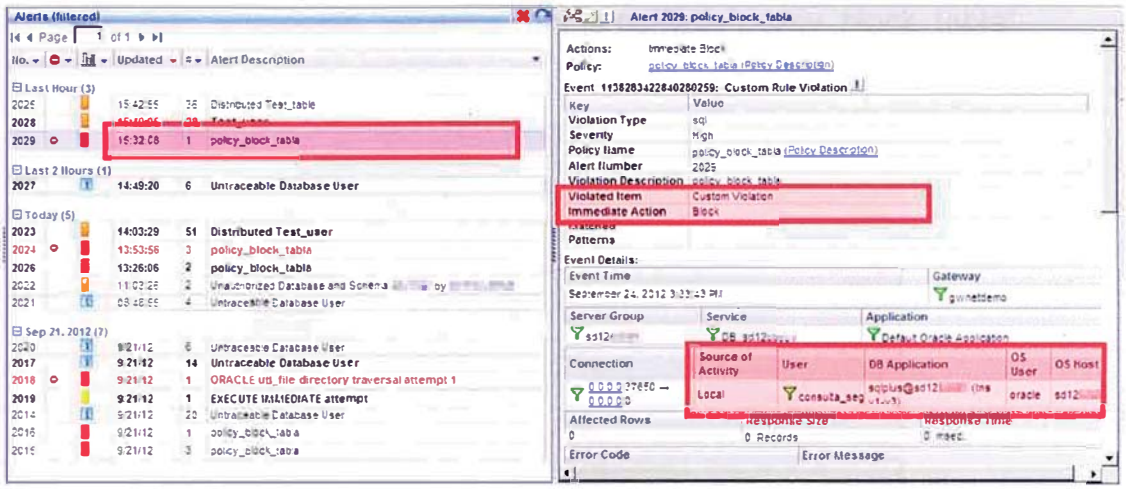


Gráfico 12: Historial de alertas

Fuente: Elaboración propia basado en el dashboard de IMPERVA SecureSphere

Luego, se realizó una consulta a la tabla “operaciones” que no fue considerada en la política “policy_block_tabla” para verificar el acceso, obteniendo resultados satisfactorios.

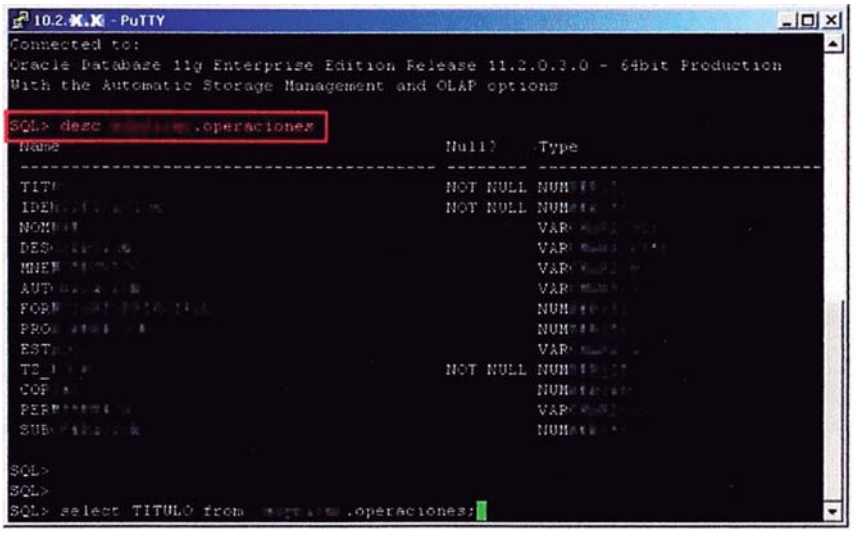


Gráfico 13: Consulta a la tabla “operaciones”

Fuente: Elaboración propia basado el SQLplus

- Prueba de conexión de red:

  Las pruebas de conexión a través de la red utilizando el cliente "PL/SQL Developer" con la cuenta "consulta_seg" no fueron completamente satisfactorias ya que se pudo consultar el contenido de la tabla restringida "usuarios" por la política "policy_block_tabla".

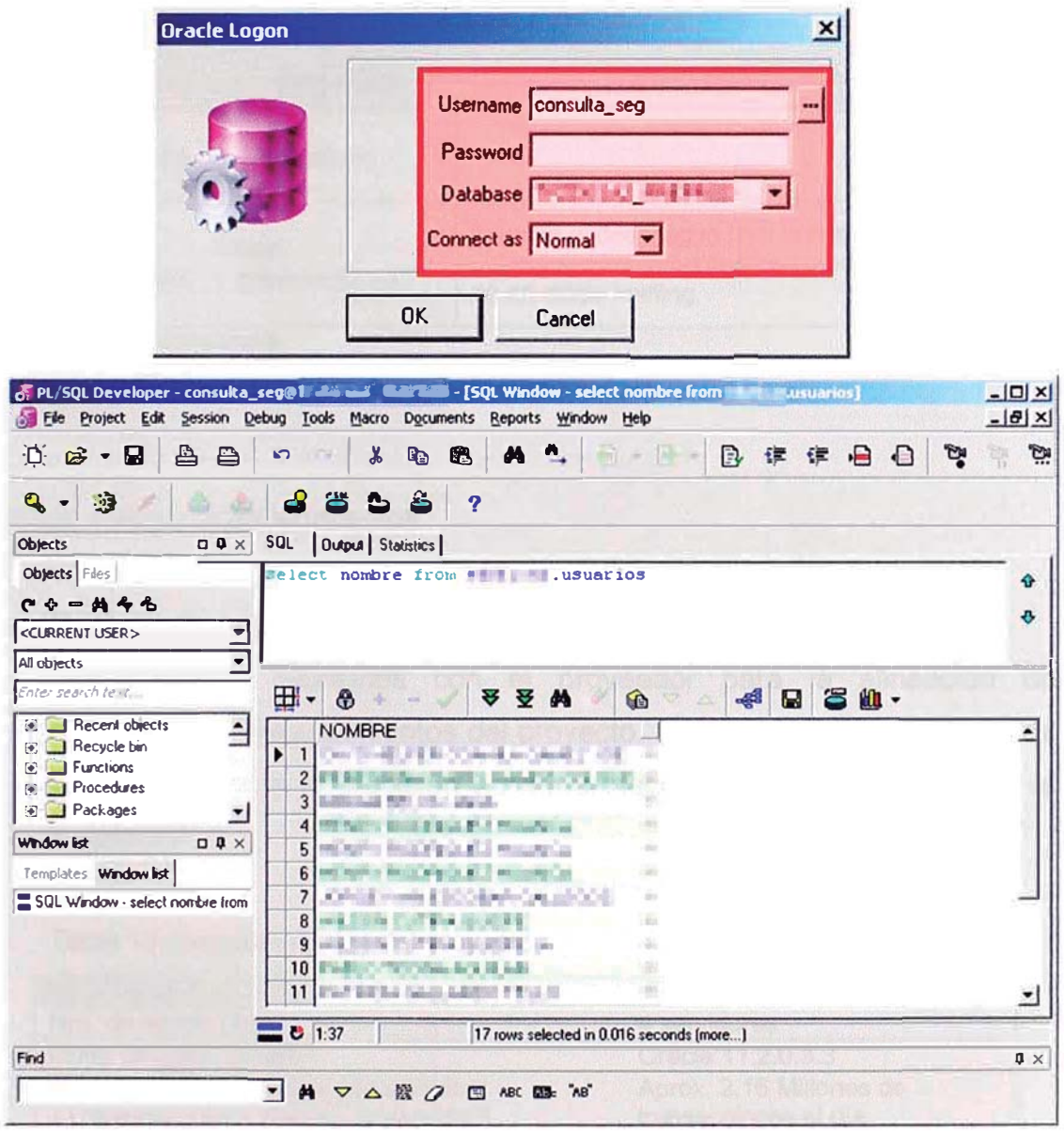


Gráfico 14: PL/SQL Developer

Fuente: Elaboración propia basado en PL/SQL Developer

Esto se presenta porque para la prueba piloto la herramienta no está siendo implementada en modo in-line, sino en modo sniffing para garantizar la disponibilidad de los servicios de base de datos.

- Conclusiones:

Tabla 9: Conclusiones

Tipo de conexión	Resultado	Planes de acción
Prueba de conexión directa (SSH)	Satisfactorio	-
Prueba de conexión de red	Con observaciones	Durante el despliegue final la herramienta deberá ser implementada en modo "in-line" y no en modo sniffing.

Fuente: Elaboración propia

3.5.3. Fase 1. Requerimientos

- Revisión de requerimientos del proyecto

Se realizaron reuniones con el proveedor para la alineación de expectativas y requerimientos del proyecto. Se revisó la disponibilidad de los recursos y la información adicional necesaria para llevar a cabo la instalación.

Tabla 10: Requerimientos del proyecto

Requerimientos	Respuesta
Nro. de servidores	4 servidores
Motor de base de datos	Oracle 11.2.0.3.3
¿Tráfico (MB x segundo) por servidor? ¿Transacciones x segundo x servidor? ¿Procesadores x servidor?	Aprox. 2.16 Millones de transacciones al día 1500 transacciones por minuto.
¿En cuántos segmentos se encuentran los servidores?	Los servidores se encuentran en un solo segmento, es el mismo segmento donde se encuentra el File Server.
¿Monitoreo y auditoría solamente o también seguridad?	Ambas, monitoreo/auditoría y seguridad.

Requerimientos	Respuesta
¿Instancias de base de datos?	2 instancias en 1 servidor y ambas se monitorearán. Para cada uno de los otros 3 servidores, sólo una instancia se monitoreará.
Tipo de Soporte (9x5 ó 24x7x365):	24x7

Fuente: Elaboración propia

- Levantamiento de información

  Se definió un diagrama de la topología de la red en la cual se instalará la solución:

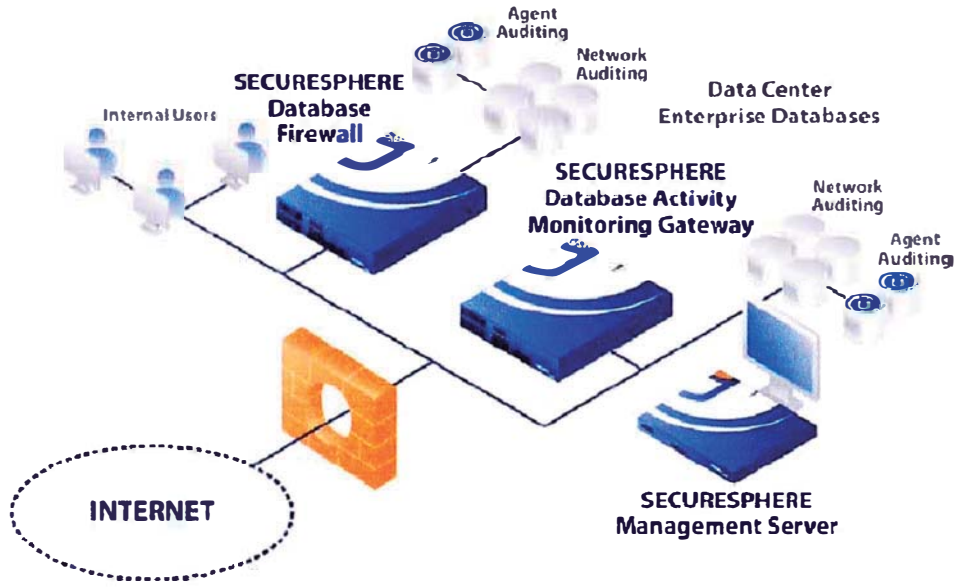


Gráfico 15: Topología de red propuesta

Fuente: IMPERVA

3.5.4. Fase 2. Instalación básica de componentes

- Instalación física de componentes

  En esta etapa se realizó la instalación física de los siguientes equipos:

Gráfico 16: Componentes físicos

Fuente: IMPERVA

- Instalación de Firmware

  En esta etapa se cargaron las últimas imágenes de firmware a los Appliance instalados.

- Configuración de parámetros de red

  En esta etapa se configuraron los parámetros de red de los Appliances instalados de acuerdo a los requerimientos del equipo de redes. Esto incluye la definición del modo de operación y asignación de direcciones IP de gestión.

3.5.5. Fase 3. Configuración de funcionalidad de monitoreo

- Definición de grupo de servers

  En esta etapa se configuró la dirección IP y los puertos TCP de los servidores de bases de datos a ser monitoreados y protegidos. De la misma forma se importarán las llaves privadas SSL y los certificados así como los passwords de Kerberos requeridos para decriptar las sesiones de bases de datos encriptados.

- Definición de reglas de auditoría

  En esta tarea se crearon y configuraron las reglas de auditoría de base de datos para tener trazabilidad de cualquier actividad sujeta a inspección.

- Creación de reportes

  En esta tarea se crearon y configuraron los reportes de acuerdo con el relevamiento realizado inicialmente.

- Definición de acciones

  En esta tarea se configuró todo el conjunto de acciones dentro de las soluciones orientadas a enviar reportes u otro tipo de notificaciones significativas vía e-mail.

3.5.6. Fase 4. Configuración de políticas de protección

- Gestión de perfiles

  Se realizaron las actividades asociadas a mantener una eficiencia de los perfiles configurados, considerando las siguientes validaciones:

  - Gestión de cuentas de usuarios de DB
  - Gestión de cuentas de usuarios de aplicación
  - Gestión de cuentas de usuarios de DB no clasificados

- Revisión y monitoreo de alertas

  En esta tarea se verificaron los parámetros de alertas establecidos y se compararon con los datos obtenidos, con el fin de realizar los ajustes necesarios.

- Revisión de logs de eventos del sistema

  En esta tarea se verificó que la plataforma no exceda límites establecidos de performance o que se estén generando mensajes de severidad alta.

- Definición de políticas de protección

  En esta tarea se definieron las políticas de seguridad y el conjunto de acciones de acuerdo a la información que se recolecte de la aplicación de las reglas de auditoría de las bases de datos bajo el alcance del proyecto.

3.5.7. Fase 5. Transferencia de conocimiento y documentación

En esta parte se brindó la instrucción acerca del proceso técnico seguido durante el proceso de instalación y se documentaron los cambios de configuración realizados en las diferentes fases de despliegue. Se creó un documento el cual incluye todos los cambios de configuración y pasos seguidos durante el proceso.

CAPÍTULO IV: RESULTADOS

4.1. BENEFICIOS CUALITATIVOS

Con la implementación de la solución de auditoría y seguridad en base de datos, la EMPRESA obtuvo los siguientes beneficios cualitativos:

- La autorización de la Superintendencia de Banca, Seguros y AFP para la utilización del método estándar alternativo en el cálculo de los requerimientos de patrimonio efectivo por riesgo operacional, evidenciando un nivel razonable en la gestión de sus riesgos operacionales y de seguridad de la información.

- Una mayor visibilidad de las actividades realizadas en las bases de datos por usuarios privilegiados y usuarios de negocio, así como alertas en tiempo real de las actividades no autorizadas y bloqueo de ataques por inyección SQL. Obteniendo registros completos de todas las actividades realizadas por estas cuentas, reduciendo la posibilidad de fraude interno.

- Cumplimiento de los criterios de aseguramiento de integridad y confidencialidad según las regulaciones SOX y PCI, evidenciándose a través de reportes completos.

4.2. ANÁLISIS BENEFICIO COSTO

4.2.1. Evaluación

Las variables utilizadas para el análisis beneficio costo son las siguientes:

- Costos de implementación: Son los costos por la adquisición de los equipos, el licenciamiento y soporte por el primer año, los servicios de consultoría y capacitación por parte del proveedor, y los gastos del personal de la EMPRESA que participará en el proyecto; según se detalla en la sección *4.2.2 Costos de la implementación*.

- Costos de mantenimiento: Son los costos anuales por la renovación del licenciamiento y el soporte del proveedor. Asimismo, se consideran los gastos del personal que administrará la solución; según se detalla en la sección *4.2.3 Costos del mantenimiento*.

- Beneficios esperados: Estos se determinan en base a la reducción de los requerimientos de patrimonio efectivo por riesgo operacional y el indicador de rentabilidad financiera (ROE: Return Over Equity), que muestra el retorno para los accionistas en base a su inversión.

    - La reducción de los requerimientos patrimoniales se calculan en el cuadro siguiente:

Tabla 11: Requerimientos patrimoniales

Concepto	Monto
Requerimientos de capital antes de la implementación [a]	S/.35,950,000
Requerimientos de capital después de la implementación [b]	S/.11,000,000
Disminución de requerimientos de capital (en soles) [a]-[b]	S/.24,950,000
Disminución de requerimientos de capital (en dólares)[1]	$9,788,152

Fuente: Elaboración propia

[1] Tipo de cambio al 31-Dic-12: 2.549

- La rentabilidad sobre el patrimonio (ROE) se define como la proporción calculada entre el beneficio neto después de impuestos y el patrimonio:

$$ROE = \frac{Utilidades\ después\ de\ impuestos}{Patrimonio}$$

El ROE de la EMPRESA se ha incrementado sostenidamente en los últimos 3 años, siendo este valor al cierre del año 2012 37.3% [2]. Para la estimación de los beneficios tangibles se considerará el ROE a Diciembre de 2012.

Tabla 12: ROE de la EMPRESA

Concepto	Dic-12	Dic-11	Dic-10
ROE (prom.)	37.3%	34.7%	34.6%

Fuente: Apoyo y asociados

4.2.2. Costo de la implementación

- Adquisición de equipos: Se considera la adquisición de los equipos Database Activity Monitoring y Management Server:

  - Database Activity Monitoring: Este equipo permite gestionar la auditoría continua de los accesos a datos confidenciales de los usuarios. Asimismo, permite alertar sobre solicitudes de acceso anormales y ataques bases de datos en tiempo real.

  - Management Server: Este equipo permite gestionar y controlar de forma centralizada los equipos de monitoreo de actividades. Asimismo, permite visualizar el estado de seguridad y los incidentes de tiempo real a través de panel de control de seguridad.

- Licenciamiento de IMPERVA SecureSphere: La adquisición del licenciamiento de IMPERVA SecureSphere nos permitirá utilizar la funcionalidad completa de los equipos. Asimismo, el licenciamiento permite la posibilidad de elevar los incidentes o problemas hacia el soporte de segundo nivel a cargo del propio fabricante.

- Soporte y mantenimiento de IMPERVA SecureSphere: El soporte y mantenimiento de IMPERVA SecureSphere nos brindará un soporte 24x7 (24 horas al día, los 7 días de la semana) a cargo de un partner local especializado. Esta empresa resolverá las consultas, asesorará la configuración y será el soporte de primer nivel.

- Consultoría y capacitación: La configuración inicial y el apoyo en la instalación estará a cargo del proveedor, que también brindará una capacitación de las principales funcionalidades administrativas de la herramienta.

- Gastos de personal: Para la implementación de la solución IMPERVA SecureSphere, se considerará el apoyo del personal del área de Seguridad de la Información y del área de Infraestructura Tecnológica de la EMPRESA; por tanto, es necesario considerar las horas que serán dedicadas para la implementación de la solución:

    - Supervisión: Se consideran las labores de supervisión a cargo del Jefe de Seguridad de la Información. Para la realización de estas tareas, se deberán destinar 10 horas a una tasa de US$20 por hora (sin IGV).

    - Operación y Monitoreo: Se consideran las labores operación y monitoreo de eventos a cargo del Analista de Seguridad

Informática. Para la realización de estas tareas, se deberán destinar 40 horas a una tasa de US$10 por hora (sin IGV).

- Implementación física: Se consideran las labores de instalación física de los equipos en el centro de cómputo a cargo del Analista de Infraestructura. Para la realización de estas tareas, se deberán destinar 20 horas a una tasa de US$10 por hora (sin IGV).

A continuación se presenta un cuadro con el detalle de los conceptos descritos anteriormente:

Tabla 13: Costos de implementación

Concepto	Precio unitario (en US$)	Cantidad	Subtotal (sin IGV)	IGV (18%)	Total (incluido IGV)
IMPERVA SecureSphere					
Adquisición de equipos (hardware)	$25,000	1	$25,000	$4,500	$29,500
Licenciamiento (anual)	$15,000	1	$15,000	$2,700	$17,700
Soporte y mantenimiento (anual)	$8,000	1	$8,000	$1,440	$9,440
Consultoría y capacitación	$10,000	1	$10,000	$1,800	$11,800
Gastos de personal					
Supervisión (Jefe de Seguridad de la Información)	$20 por hora	10 horas	$200	$36	$236
Operación y monitoreo (Analista de Seguridad Informática)	$10 por hora	40 horas	$400	$72	$472
Implementación física (Analista de Infraestructura)	$10 por hora	20 horas	$200	$36	$236
TOTAL (con impuestos)					**$69,384**

Fuente: Elaboración propia

4.2.3. Costo del mantenimiento

Para calcular el costo total del mantenimiento anual se consideran los siguientes conceptos:

- Licenciamiento de IMPERVA SecureSphere: La renovación del licenciamiento anual de IMPERVA SecureSphere nos permitirá obtener las últimas actualizaciones que permitirán resolver posibles problemas de seguridad y mejorar la funcionalidad de los equipos. Asimismo, el licenciamiento permite la posibilidad de elevar los incidentes o problemas hacia el soporte de segundo nivel a cargo del propio fabricante.

- Soporte y mantenimiento de IMPERVA SecureSphere: El soporte y mantenimiento de IMPERVA SecureSphere nos brindará un soporte 24x7 (24 horas al día, los 7 días de la semana) a cargo de un partner local especializado. Esta empresa resolverá las consultas, asesorará la configuración y será el soporte de primer nivel.

- Gastos de personal: La administración de los equipos IMPERVA SecureSphere estará a cargo del personal del área de Seguridad de la Información de la EMPRESA; por tanto, es necesario considerar las horas que serán dedicadas para la administración de la solución:

    - Supervisión: Se consideran las labores de supervisión a cargo del Jefe de Seguridad de la Información. Para la realización de estas tareas, se deberán destinar 5 horas mensuales (60 horas anuales) a una tasa de US$20 por hora (sin IGV).

    - Operación y Monitoreo: Se consideran las labores operación y monitoreo de eventos a cargo del Analista de Seguridad

Informática. Para la realización de estas tareas, se deberán destinar 40 horas mensuales (480 horas anuales) a una tasa de US$10 por hora (sin IGV).

A continuación se presenta un cuadro con el detalle de los conceptos descritos anteriormente:

Tabla 14: Costos de mantenimiento

Conceptos	Precio unitario (en US$)	Cantidad	Subtotal (sin IGV)	IGV (18%)	Total (incluido IGV)
IMPERVA SecureSphere					
Licenciamiento (anual)	$15,000	1	$15,000	$2,700	$17,700
Soporte y mantenimiento (anual)	$8,000	1	$8,000	$1,440	$9,440
Gastos de personal					
Supervisión (Jefe de Seguridad de la Información)	$20 por hora	60 horas	$1,200	$216	$1,416
Operación y monitoreo (Analista de Seguridad Informática)	$10 por hora	480 horas	$4,800	$864	$5,664
TOTAL (con impuestos)					**$34,220**

Fuente: Elaboración propia

4.2.4. Estimación de los beneficios tangibles

La estimación de los beneficios tangibles se realizará considerando los conceptos descritos en la tabla siguiente:

Tabla 15: Estimación de beneficios tangibles

	Año 0	Año 1	Año 2	Año 3
Costos				
Costo de implementación	-$69,384			
Costo de mantenimiento		-$34,220	-$34,220	-$34,220
Beneficios				
Disminución en requerimientos de capital (1)	$9,788,152			
ROE (2)	37.3%			
Retorno (3)		$3,650,981	$3,650,981	$3,650,981
TOTAL	**-$69,384**	**$3,616,761**	**$3,616,761**	**$3,616,761**

Fuente: Elaboración propia basado en PCI DSS

(1) Reducción de requerimientos de capital por riesgo operacional

(2) ROE al 31/12/12

(3) Retorno anual estimado calculado en base a la disminución de requerimientos de capital y el ROE.

Por tanto, según los supuestos considerados, los beneficios estimados serían aproximadamente $3,616,761 anuales.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- La implementación de una solución para la auditoría y seguridad en bases de datos permitió obtener la autorización de la Superintendencia de Banca, Seguros y AFP para la utilización del método estándar alternativo, lo que permitió tener una reducción importante en los requerimientos de patrimonio efectivo.

- Las alertas en tiempo real y los registros de todas las actividades en las base de datos de la EMPRESA permiten implementar controles de monitoreo preventivo y detectivo, respectivamente, y así prevenir la ocurrencia de escenarios de fraude.

- El cumplimiento proactivo de los criterios y controles considerados en las regulaciones SOX y PCI, respecto al aseguramiento de la integridad y confidencialidad de la información en las bases de datos de la EMPRESA, previene la generación de no conformidades u observaciones en futuras auditorías.

RECOMENDACIONES

- Los montos resultantes de la reducción en requerimientos de capital deberían ser invertidos en las operaciones de negocio para obtener un retorno sobre la inversión para la EMPRESA, según como se ha detallado en la estimación de los beneficios tangibles.

- Para aprovechar la funcionalidad de la herramienta IMPERVA SecureSphere, la EMPRESA debe implementar un proceso periódico de revisión de los registros para la identificación de actividades sospechosas y prevenir la ocurrencia de fraude.

- Asimismo, la EMPRESA debe implementar un proceso formal para la administración, mantenimiento y actualización continua de la herramienta IMPERVA SecureSphere, para así garantizar la correcta y óptima funcionalidad.

BIBLIOGRAFÍA

[1] Superintendencia de Banca, Seguros y AFP, «Resolución SBS N° 11356-2008,» Lima, 2008.

[2] APOYO & ASOCIADOS, «Clasificación de Riesgo - Financiera EDYFICAR,» FitchRatings, Lima, 2013.

[3] Financiera EDYFICAR, «Memoria Anual,» Financiera EDYFICAR, Lima, 2011.

[4] Superintendencia de Banca, Seguros y AFP, «Resolución SBS N° 2115-2009,» Lima, 2009.

[5] Superintendencia de Banca, Seguros y AFP, «Resolución SBS N° 2116-2009,» Lima, 2009.

[6] Superintendencia de Banca, Seguros y AFP, «Circular SBS N° G-140-2009,» Superintendencia de Banca, Seguros y AFP, Lima, 2009.

[7] PCI Council, «Payment Card Industry Data Security Standard (PCI DSS),» 2010.

[8] Imperva, «The Business Case for Database Security,» California, 2011.

[9] Imperva, «Imperva Data Security and Compliance Lifecycle,» Imperva White Paper, California, 2008.

[10] IBM InfoSphere Guardium family, «http://www-03.ibm.com/software/products/es/es/infoguarfami,» 2012.

[11] 107th Congress of the United States, «Sarbanes-Oxley Act Pub. L. 107-204,» United States of America, 2002.

[12] L. Ponemon, «What Senior Executives Think about Data Protection,» Ponemon Institute, 2012.

GLOSARIO

Appliance: Hardware de propósito específico con sistemas específicos embebidos que proveen funcionalidad limitada y que operan de forma autónoma.

Solución: Conjunto de servicios y herramientas de software que realizan las funciones requeridas por las entidades.

DataBase Monitoring Gateway: Realiza monitoreo de bases de datos y aplicaciones proporcionando total visibilidad en como los datos son usados en la organización sin importar si estos son accesados de manera directa o indirecta por la aplicación.

DataBase Monitor Agent: El agente instalado sobre el servidor de bases de datos monitorea la actividad local en la base de datos ya sea que se use una consola o una sesión SSH sobre la red. Los agentes registran tráfico de la base de datos y envían este al Gateway para almacenamiento y análisis. Los agentes pueden también ser usados para monitorear sitios remotos en los cuales un Gateway no pueda ser implementado.

DataBase Security Gateway: Realiza tareas de monitoreo y bloqueo de tráfico malicioso.

Management Server: Provee una gestión centralizada hasta para 15 Gateways permitiendo la implementación de extensos ambientes distribuidos.

Instancia: Se llama instancia al estado que presenta una base de datos en un tiempo dado. Véase como una fotografía que se toma de la base de datos en un tiempo t; después de que transcurre el tiempo t, la base de datos ya no es la misma.

Esquema: Es la descripción lógica de la base de datos, proporciona los nombres de las entidades y sus atributos especificando las relaciones que existen entre ellos. Es un banco en el que se inscriben los valores que irán formando cada uno de los atributos. El esquema no cambia los que varían son los datos y con esto tenemos una nueva instancia.

Motor de base de datos: Es el aplicativo de base de datos como tal. Por ejemplo: Oracle, SQL Server, DB2, etc.

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

ANEXO 1. CIRCULAR SBS G-140-2009 ARTÍCULO 5°

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

5.1 Seguridad lógica

a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.

b) Revisiones periódicas sobre los derechos concedidos a los usuarios.

c) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.

d) Controles especiales sobre utilidades del sistema y herramientas de auditoría.

e) Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.

f) Controles especiales sobre usuarios remotos y computación móvil.

5.2 Seguridad de personal

a) Definición de roles y responsabilidades establecidos sobre la seguridad de información.

b) Verificación de antecedentes, de conformidad con la legislación laboral vigente.

c) Concientización y entrenamiento.

d) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.

e) Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos.

5.3 Seguridad física y ambiental

a) Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.

b) Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales.

5.4 Inventario de activos y clasificación de la información

a) Realizar y mantener un inventario de activos asociados a la tecnología de información y asignar responsabilidades respecto a la protección de estos activos.

b) Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

5.5. Administración de las operaciones y comunicaciones

a) Procedimientos documentados para la operación de los sistemas.

b) Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.

c) Separación de funciones para reducir el riesgo de error o fraude.

d) Separación de los ambientes de desarrollo, pruebas y producción.

e) Monitoreo del servicio dado por terceras partes.

f) Administración de la capacidad de procesamiento.

g) Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.

h) Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.

i) Seguridad sobre el intercambio de la información, incluido el correo electrónico.

j) Seguridad sobre canales electrónicos.

k) Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.

5.6. Adquisición, desarrollo y mantenimiento de sistemas informáticos

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

a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.

b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.

c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.

d) Controlar el acceso a las librerías de programas fuente.

e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.

f) Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.

5.7. Procedimientos de respaldo

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

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

5.8. Gestión de incidentes de seguridad de información

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

a) Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.

b) Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

5.9. Cumplimiento normativo

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

5.10. Privacidad de la información

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

ANEXO 2. ESTADOS FINANCIEROS DE LA EMPRESA

Estado de Ganancias y Pérdidas

	2010		2011	
Ingresos Financieros	**284,944**	**100%**	**376,051**	**100%**
Intereses por Disponible	1,642	1%	4,543	1%
Intereses y Comisiones por Fondos Interbancarios	-	0%	42	0%
Ingresos por Inversiones	1,484	1%	1,370	0%
Intereses y Comisiones por Créditos	272,802	96%	367,081	98%
Ganancia por productos financieros derivados	8,898	3%	-	0%
Diferencia de Cambio	-	0%	2,378	1%
Otros	118	0%	637	0%
Gastos Financieros	**48,104**	**17%**	**63,022**	**17%**
Intereses y Comisiones por Oblig. Con el Publico	5,748	2%	14,660	4%
Intereses por Depósitos del Sistema y Org. Int	5	0%	589	0%
Intereses por Comisiones por Adeudos y Obi. Fin.	28,400	10%	35,548	9%
Intereses por Obligaciones en Circ.no Sub.	1,450	1%	4,058	1%
Intereses por Obligaciones en Circ. Sub.	-	0%	846	0%
Perdida por productos financieros derivados	-	0%	5,256	1%
Diferencia de Cambio	8,234	3%	-	0%
Otros	4,267	1%	2,065	1%
MARGEN FINANCIERO BRUTO	236,840	83%	313,029	83%
Provisiones por Malas Deudas y Desv. De Inv	32,770	12%	50,800	14%
MARGEN FINANCIERO NETO	204,070	72%	262,229	70%
Ingresos Netos por Servicios Financieros	1,695	1%	1,336	0%
Gastos Operativos	**132,847**	**47%**	**167,490**	**45%**
Personal y Directorio	93,686	33%	122,893	33%
Generales	39,161	14%	44,597	12%
MARGEN OPERACIONAL NETO	72,918	26%	96,075	26%
Ingresos / Gastos No Operacionales	774	0%	464	0%
Otras Provisiones y Depreciaciones	-6,011	-2%	-6,976	-2%
UTILIDAD / PERDIDA ANTES DE IMP. Y REI	67,681	24%	89,563	24%
Participación de los Trabajadores	-	0%	-	0%
Impuesto a la Renta	20,356	7%	26,125	7%
UTILIDAD NETA	47,326	17%	63,438	17%

ANEXO 3. EVALUACIÓN CUALITATIVA

Categoría	Ponderación	Peso	Criterio	IMPERVA SecureSphere		IBM InfoSphere Guardium	
				% Alcanzado	% Ponderado	% Alcanzado	% Ponderado
Funcionalidades	**60%**	**9**		**89%**	**53%**	**89%**	**53%**
¿Refuerza la segregación de funciones?		0	No es soportado por la aplicación	3		3	
		1	Sí; pero con un producto de otro fabricante				
		2	Sí; con un licenciamiento adicional del mismo fabricante				
		3	Sí; ya se encuentra con el licenciamiento solicitado				
¿Brinda bloqueo de ataques y alertas en tiempo real?		0	No brinda bloqueo de ataques ni alertas en tiempo real	3		3	
		1	Sólo brinda alertas				
		2	Brinda alertas en tiempo real				
		3	Brinda alertas en tiempo real y bloqueo de ataques				
¿El despliegue se podrá realizar de manera transparente?		0	Se requieren grandes cambios en las aplicaciones y las bases de datos	2		2	
		1	Se requieren algunos cambios en las aplicaciones				
		2	Se requieren pequeñas configuraciones de red				
		3	No se requiere ningún cambio en la plataforma actual				

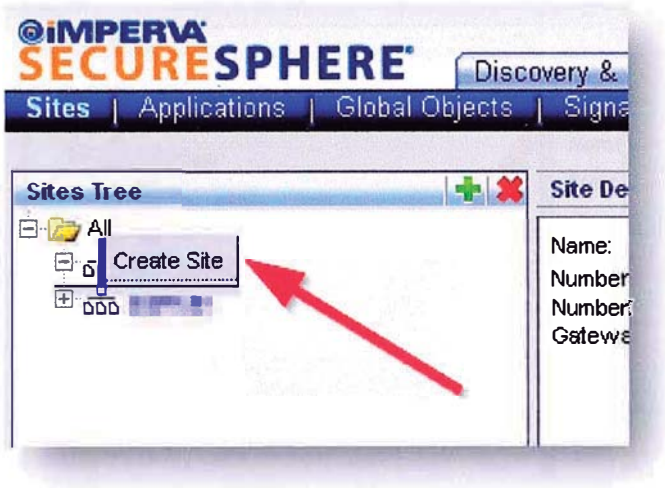
Categoria	Ponderación	Peso	Criterio	IMPERVA SecureSphere		IBM InfoSphere Guardium	
				% Alcanzado	% Ponderado	% Alcanzado	% Ponderado
Estándares	**10%**	**9**		**100%**	**10%**	**100%**	**10%**
PCI DSS		0	No soporta	3		3	
		1	Sí; pero con un licenciamiento adicional y no son parametrizables				
		2	Sí; incluidos pero no son parametrizables				
		3	Sí; incluidos por defecto, parametrizables y actualizables				
SOX		0	No soporta	3		3	
		1	Sí; pero con un licenciamiento adicional y no son parametrizables				
		2	Sí; incluidos pero no son parametrizables				
		3	Sí; incluidos por defecto, parametrizables y actualizables				
Personalizados		0	No soporta	3		3	
		1	Sí; pero con un licenciamiento adicional y se configuran durante la instalación				
		2	Sí; incluidos con el licenciamiento y se configuran durante la instalación (no parametrizables)				
		3	Sí son soportados y son parametrizables				

Categoría	Ponderación	Peso	Criterio	IMPERVA SecureSphere % Alcanzado	IMPERVA SecureSphere % Ponderado	IBM InfoSphere Guardium % Alcanzado	IBM InfoSphere Guardium % Ponderado
Arquitectura	**15%**	**9**		**89%**	**13%**	**89%**	**13%**
Impacto en la disponibilidad de aplicaciones y bases de datos		0	Impacto alto en la disponibilidad (más de 4 horas)	2		2	
		1	Impacto moderado en la disponibilidad (más de 10 minutos y menos de 4 horas)				
		2	Impacto bajo en la disponibilidad (menos de 10 minutos)				
		3	Ningún impacto en la disponibilidad				
Tipo de impacto en el desempeño de las bases de datos		0	Impacto alto en la disponibilidad (retrasos notorios por los usuarios y administradores)	3		3	
		1	Impacto moderado en el desempeño (retrasos notorios sólo por los administradores)				
		2	Impacto bajo en el desempeño (retrasos imperceptibles por los usuarios y los administradores)				
		3	Ningún impacto en el desempeño				

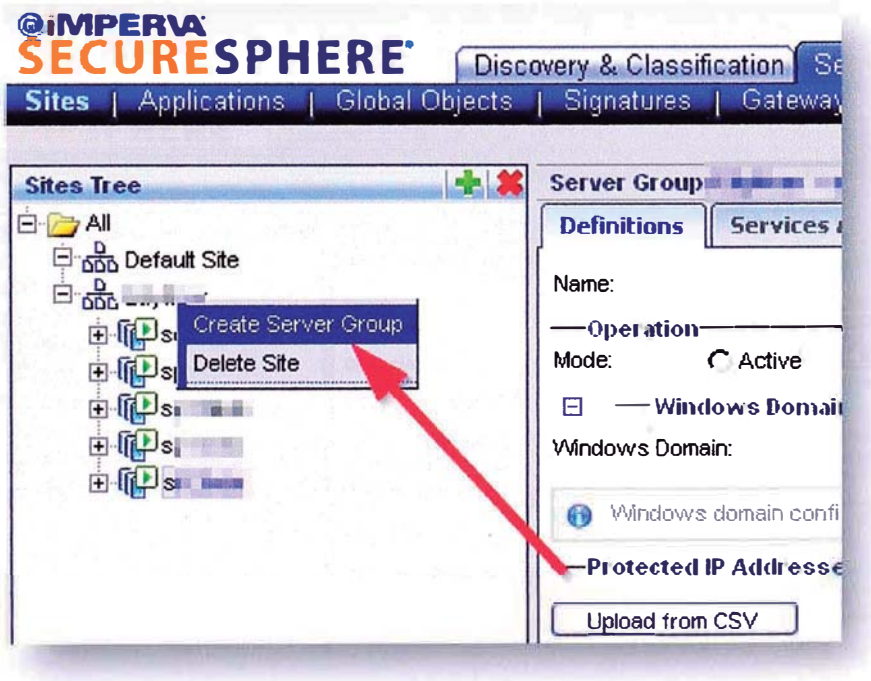
Categoría	Ponderación	Peso	Criterio	IMPERVA SecureSphere		IBM InfoSphere Guardium	
				% Alcanzado	% Ponderado	% Alcanzado	% Ponderado
Arquitectura	**15%**	**9**		**89%**	**13%**	**89%**	**13%**
Utiliza agentes para su funcionamiento		0	Sí utiliza agentes intrusivos en las bases de datos para todo tráfico	3		3	
		1	La instalación de los agentes se realiza en el sistema operativo y es requerida para el tráfico local y de red				
		2	La instalación de los agentes se realiza en el sistema operativo y sólo para el tráfico local. Pero no es posible parametrizar el uso de recursos.				
		3	La instalación de los agentes se realiza en el sistema operativo y sólo para el tráfico local. Es posible parametrizar el uso de recursos.				
Seguridad	**15%**	**3**		**67%**	**10%**	**100%**	**15%**
Autorización de accesos a la herramienta		0	No requiere autenticación	2		3	
		1	Requiere autenticación y no es configurable				
		2	Requiere autenticación y es configurable				
		3	Requiere autenticación, es configurable y se puede integrar con Active Directory				
			TOTAL	**87%**		**92%**	

ANEXO 4. INSTRUCTIVO DE CREACIÓN DE POLÍTICAS

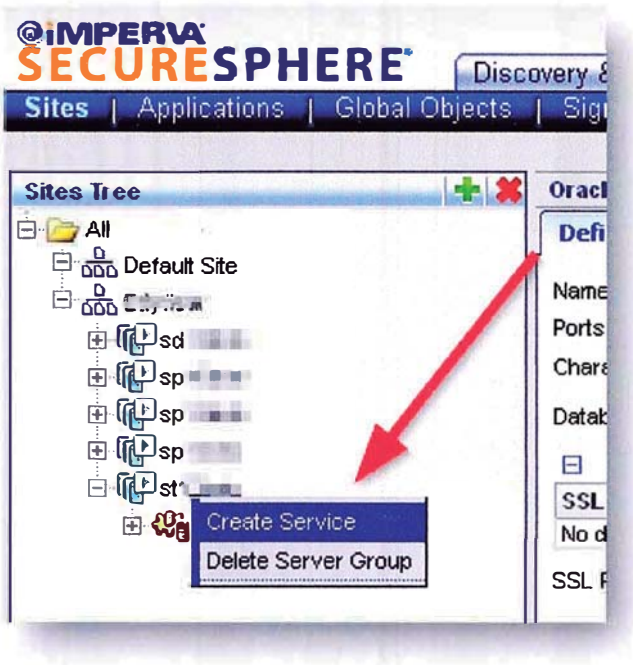
Paso 1: Crear Sitio



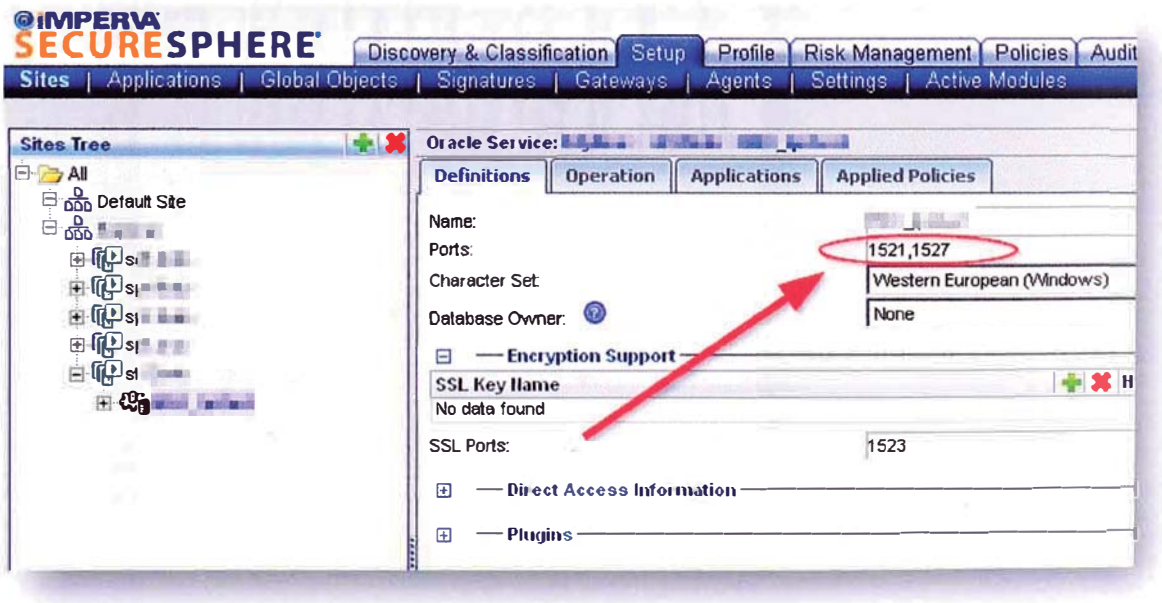
Paso 2: Crear el grupo de servidores que serán monitoreados



Paso 3: Crear los servicios que serán monitoreados en los servidores



Paso 4: Configurar los puertos del servicio (el puerto por defecto para Oracle es el 1521)



Paso 5: Configurar políticas de seguridad aplicables