ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

PROYECTO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE ANALISTA Y PROGRAMADOR DE SISTEMAS

TEMA

"*Implementación de un Sistema de Gestión de Seguridad de la Información usando la norma ISO27000 sobre un sitio de comercio electrónico para una nueva institución bancaria aplicando los dominios de control ISO27002:2005 y utilizando la metodología Magerit*"

AUTORES
Marcel Eduardo León Lafebré
Evelyn Anabell Mota Orrala
Joffre Manuel Navarrete Zambrano

DIRECTOR
Ing. Víctor Muñoz Chachapoya

AÑO
2011

AGRADECIMIENTO

Agradecemos a Dios por habernos permitido llegar a este punto en nuestra vida estudiantil, a nuestras familias que con su apoyo incondicional supieron apoyarnos en los momentos difíciles, a nuestros maestros que día a día impartieron sus conocimientos para enfrentarnos a un mejor mañana y a nuestros compañeros por permitirnos compartir gratos momentos en el transcurso nuestra carrera.

Marcel León Lafebré
Evelyn Mota Orrala
Joffre Navarrete Zambrano

DEDICATORIA

Dedicamos este logro a nuestros padres, hermanos y allegados que estuvieron incondicionalmente apoyándonos a lo largo de nuestras carreras, permitiéndonos de tal manera hacer la entrega de este proyecto.

A nuestros maestros que supieron enrumbarnos con sus metodologías por el camino correcto logrando así a ser profesionales competitivos en el campo laboral.

Finalmente a todas aquellas personas que se nos escape mencionar pero que siempre los tendremos presente.

Marcel León Lafebré

Evelyn Mota Orrala

Joffre Navarrete Zambrano

DECLARACIÓN EXPRESA

“Los autores nos responsabilizamos por el análisis, estudio y las conclusiones realizadas en este Proyecto de Graduación. Así mismo declaramos que el patrimonio intelectual del mismo pertenece a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

FIRMA EL DIRECTOR DEL PROYECTO Y MIEMBRO DEL TRIBUNAL DE GRADUACIÓN

Ing. Víctor Muñoz Chachapoya
Director del Proyecto

Mae. Enrique Salazar Meza
Delegado

FIRMA DE LOS AUTORES DEL PROYECTO

Marcel León Lafebré

Evelyn Mota Orrala

Joffre Navarrete Zambrano

RESUMEN

El presente documento contiene la información técnica de la revisión de las seguridades de un sitio web transaccional con el fin de encontrar y analizar las posibles vulnerabilidades y amenazas para poder minimizarlas y gestionar el riesgo correspondiente con la finalidad de lograr tener un sistema de seguridad de la información lo mas óptimo posible.

Considerando la importancia y sensibilidad de la información de los clientes en una institución bancaria, hemos realizado este exhaustivo estudio, mediante el cual hemos podido aplicar varios controles de los diferentes dominios existentes en la norma ISO-27000, la cual se escogió para desarrollar este proyecto

CONTROL DEL DOCUMENTO

FECHA	REVISIÓN	OBSERVACIONES
02-Mayo-2011	Versión 1.0	Elaboración de borrador inicial del documento
16-Mayo-2011	Versión 1.1	Ordenar contenido de capítulos
22-Mayo-2011	Versión 1.2	Depuración del capítulo de Análisis y Gestión de Riesgo
06-Mayo-2011	Versión 1.3	Verificación general del contenido del documento
1-Septiembre-2011	Versión 1.4	Corrección de formatos

ÍNDICE GENERAL

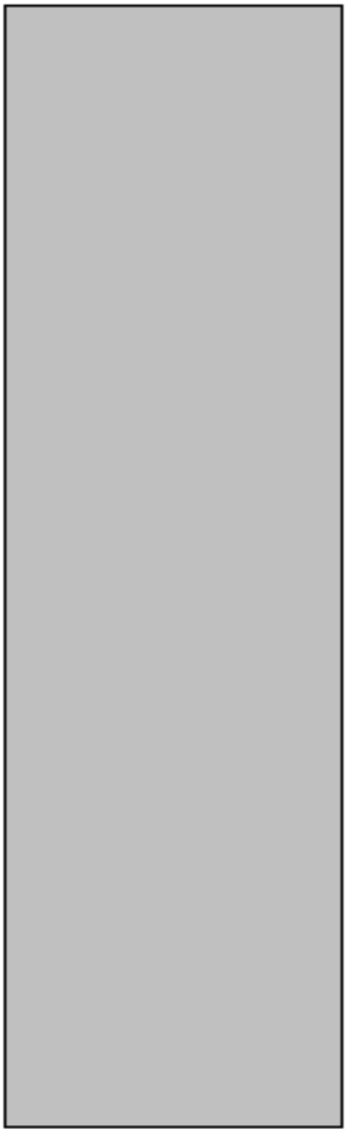
CAPÍTULO 4: POLÍTICA DE SEGURIDAD

CAPÍTULO 5: ANÁLISIS Y GESTIÓN DE RIEGOS

ÍNDICE DE ANEXOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS



CAPÍTULO 1
INTRODUCCIÓN

1. INTRODUCCIÓN

1.1. ANTECEDENTES

En la actualidad, las principales instituciones financieras del Ecuador tienen la necesidad de estar constantemente verificando las seguridades de sus sitios transaccionales, ya que así mismo existen personas y/u organizaciones bien o mal-intencionadas que buscan encontrar alguna vulnerabilidad en los sitios de estas empresas para robar información o para buscar un negocio de asesoramiento con dichas instituciones.

Vale acotar también que la banca virtual es una tecnología indispensable en la actualidad para dar un servicio de calidad a los clientes de una institución financiera.

Es claro que todo tiene su precio, por lo cual esta nueva institución financiera desea sacar su sitio transaccional pero está consciente de que necesita implementar un SGSI para minimizar el riesgo en sus operaciones.

Una directriz de la implementación de este SGSI es que va a estar aplicado en varios dominios de controles de la norma ISO.

Otro punto de mucha relevancia es determinar la metodología que se va a utilizar para la implementación del SGSI.

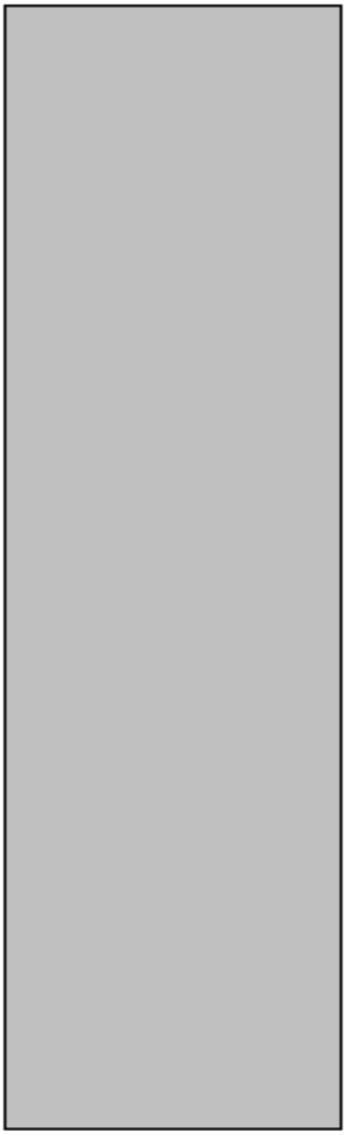
1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Implementar un SGSI para un sitio transaccional de comercio electrónico de una nueva institución financiera bajo la norma ISO27000 aplicado a varios dominios de control y utilizando la metodología MAGERIT para minimizar los riesgos y que el servicio no se vea afectado en lo mayormente posible.

1.2.2. OBJETIVOS ESPECÍFICOS

- ✓ Determinación del alcance y política de seguridad.
- ✓ Determinación del valor de los activos.
- ✓ Determinación del riesgo.
- ✓ Identificación de objetivos de control y controles.
- ✓ Definición e implementación de políticas, estándares y procedimientos para implementar los controles.
- ✓ Revisiones y auditoria de Certificación del SGSI.



CAPÍTULO 2
GENERALIDADES

2. GENERALIDADES

2.1. DEFINICIÓN DE CONCEPTOS

2.1.1. P.D.C.A.:

Es conocido como "círculo de Deming" por Edwards Deming, es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. También se denomina espiral de mejora continua. Las siglas PDCA son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

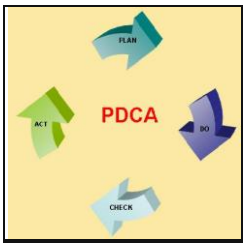


Figura 2-1: PDCA

2.1.2. LA GESTIÓN POR PROCESOS

Es la forma de gestionar toda la organización basándose en los Procesos. Entendiendo estos como una secuencia de actividades orientadas a generar un valor añadido sobre una ENTRADA para conseguir un resultado, y una SALIDA que a su vez satisfaga los requerimientos del Cliente.

2.1.3. LA ISO

Organización Internacional de Normalización. Organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

2.1.4. INFORMACIÓN

Se considera información a los diferentes conjuntos organizados de datos que utiliza Banco.

2.1.5. RECURSO O ACTIVO DE TECNOLOGÍA INFORMÁTICA Y COMUNICACIONES (TIC)

Se considera recurso TIC a todos aquellos recursos técnicos que almacenan, procesan o transmiten información de la Entidad.

2.1.6. POLÍTICA

Se considera política a la declaración, por parte de la dirección de la Entidad, de un conjunto de objetivos para regir y proteger los objetivos de la misma. Dentro de estos objetivos se encuentran prácticas generalmente aceptadas para llevar a cabo tareas de control interno, requerimientos de protección de la información, etc.

2.1.7. DIRECTIVAS

Una directiva es una declaración que provee a los miembros de la Entidad. La información acerca de los objetivos planteados en las políticas. Las directivas son diseñadas para proveer una descripción más específica de los objetivos de la Entidad, de modo que son modificadas más frecuentemente que las políticas debido a cambios en el entorno de negocios de la Entidad.

El cumplimiento de las directivas asegura el cumplimiento de los objetivos planteados en las políticas.

2.1.8. ESTÁNDAR

Un estándar es una declaración que provee una guía o lineamiento para concretar los objetivos estipulados por las directivas e indicados por las políticas.

2.1.9. PROCEDIMIENTO

Un procedimiento es una declaración que indica cómo realizar un conjunto de actividades que permitan lograr los objetivos establecidos. Un procedimiento puede tomar la forma de un manual de instalación, una guía de usuario, un manual administrativo, una lista de verificación o cualquier otro tipo de documentación operacional.

2.1.10. ACTIVO

Cualquier cosa que tenga valor para la organización.

Amenaza: una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.

2.1.11. ANÁLISIS DE RIESGO

Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

2.1.12. CONTROL

Medios para manejar el riesgo, incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida.

2.1.13. CRIPTOGRAFÍA

Es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.

2.1.14. ELECTROTÉCNICA

Es la ciencia que estudia las aplicaciones técnicas de la electricidad.

2.1.15. EVALUACIÓN DE RIESGO

Proceso de comparar la contingencia estimada con un criterio de la contingencia dada para determinar la solución del riesgo.

2.1.16. EVENTO DE SEGURIDAD DE LA INFORMACIÓN

Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red, indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

2.1.17. GESTIÓN DE RIESGO

Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

2.1.18. INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información.

2.1.19. LINEAMIENTO

Descripción que aclara ¿Qué? y ¿Cómo? se debería hacer, para lograr los objetivos establecidos en las políticas.

Medios de procesamiento de la información: cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.

2.1.20. MÉTRICA

Es una metodología de planificación, desarrollo y mantenimiento de sistemas de información.

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

2.1.21. RIESGO

Combinación de la probabilidad de un evento y su ocurrencia.

Seguridad de la información: preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-reputación y confiabilidad.

Tratamiento del riesgo es un proceso de selección e implementación de medidas para modificar el riesgo.

2.1.22. TERCERA PERSONA

Persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión.

2.1.23. VULNERABILIDAD

La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

2.2. DEFINICIÓN DE LA EMPRESA

2.2.1. PERFIL DE LA EMPRESA

Como empresa del sector financiero, la entidad tiene como objeto: la captación de fondos de entidades públicas, empresas del sector privado y los fondos de todos sus clientes para ofrecer planes de financiamiento para los sectores productivos del país con el fin de dar, mantener y mejorar la economía de la nación. Por ende necesita dar servicios de calidad a nuestros clientes, para lo cual tiene su valor añadido del sitio transaccional de banca virtual, que le permitirá al cliente hacer un sin fin de operaciones sin tener que ir a las diferentes centrales y sucursales del banco.

En la actualidad la institución está presente en las 3 más grandes ciudades del Ecuador, estando así distribuidas:

Guayaquil → Matriz
Quito → Sucursal 1
Cuenca → Sucursal 2

La empresa al adquirir la banca virtual, ofrece a sus clientes (empresas y personas) la disponibilidad del servicio 7 x 24.

La organización se mueve en un sector en el que la mejora continua es esencial para mantener el nivel de competitividad que goza actualmente.

La constante innovación tecnológica le permite a la entidad financiera una mejora continua en los procesos de negocio.

La forma de actuación de la entidad financiera sigue las pautas del P.D.C.A. (planificar, hacer, controlar y actuar), en consecuencia con una constante retroalimentación sobre la gestión de nuestros procesos.

El objetivo primordial de la política de calidad es la satisfacción y fidelidad de nuestros clientes.
La empresa considera prioritario a nivel interno:

La mejora de la competitividad de la empresa, dentro del mercado donde desarrolla su actividad.

El aumento de la rentabilidad de la empresa, mejorando los procesos.

Para alcanzar estos objetivos establecemos como primer paso la gestión de un sistema de Calidad según la Norma ISO 9000 en el servicio del ATM (cajeros automáticos) – obtenido dicho certificado en el año 2008.

Actualmente la entidad brinda a sus clientes por medio de su banca virtual los siguientes servicios de calidad:

Transferencias cuentas propias
Transferencias terceros mismo banco, otros bancos SPI, directo e internacionales
Pago de tarjetas de crédito propias
Pago de tarjetas de crédito de terceros mismo banco, otros bancos SPI, directo e internacionales.
Recarga de tarjetas de crédito
Servicios de consulta y pago de servicios públicos y privados en línea y base local
Consulta de central de crédito

2.2.2. ESQUEMA DE PROCESO

La organización ha identificado sus diferentes procesos de negocio claves para la banca virtual, como se indica en la figura 1.

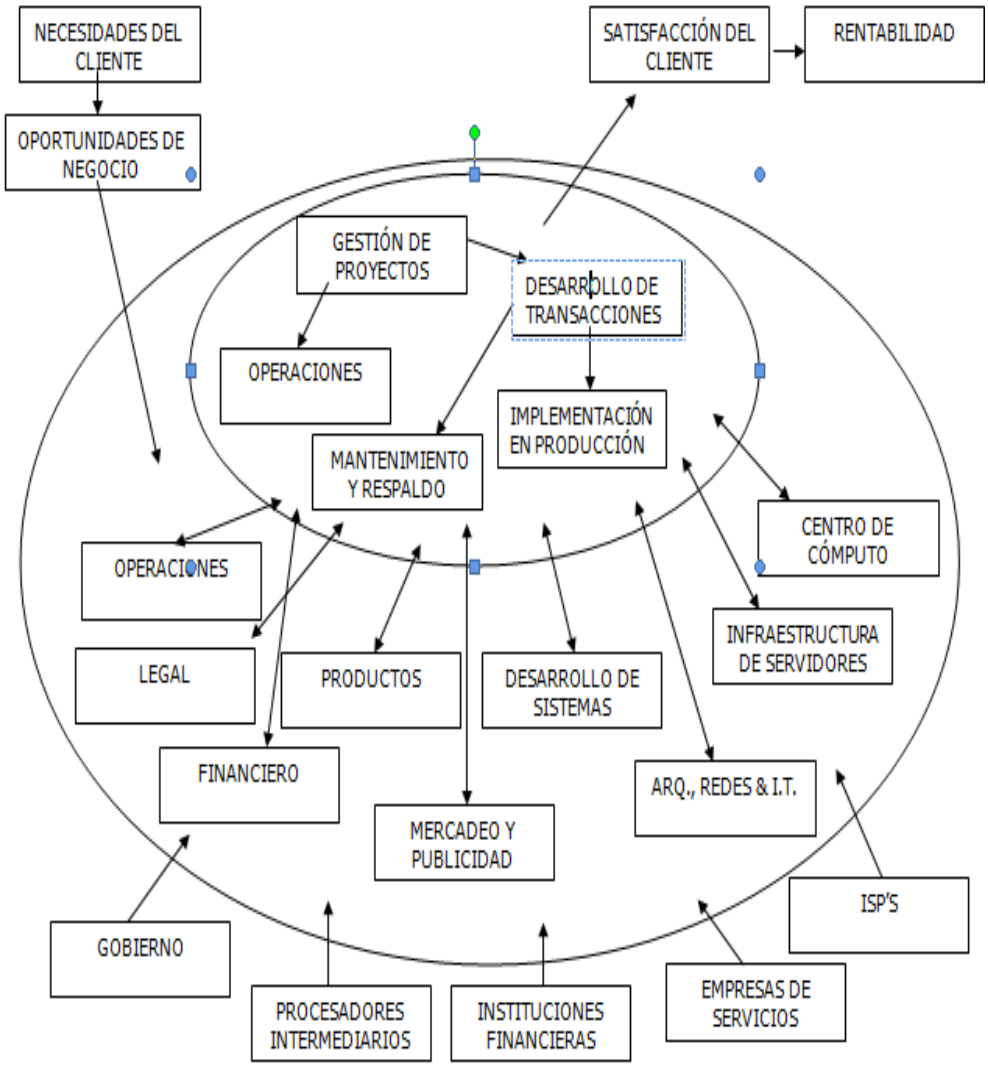


Figura 2-2: Esquema de Proceso

2.2.2.1. GESTIÓN DE PROYECTOS

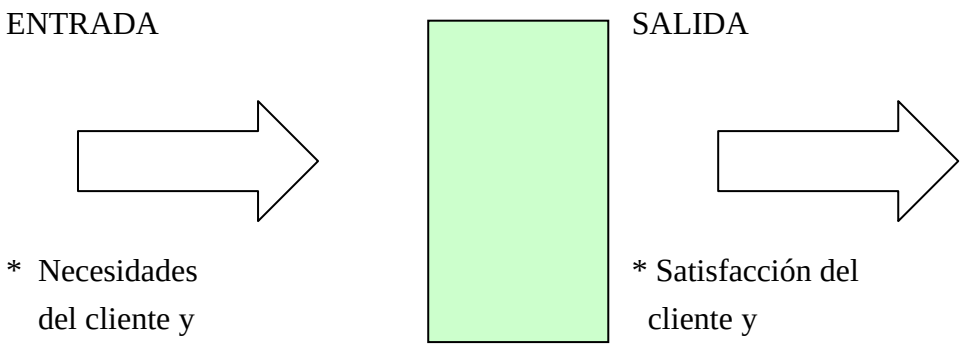


Figura 2-3: Gestión de Proyectos

2.2.2.2. DESARROLLO DE TRANSACCIONES

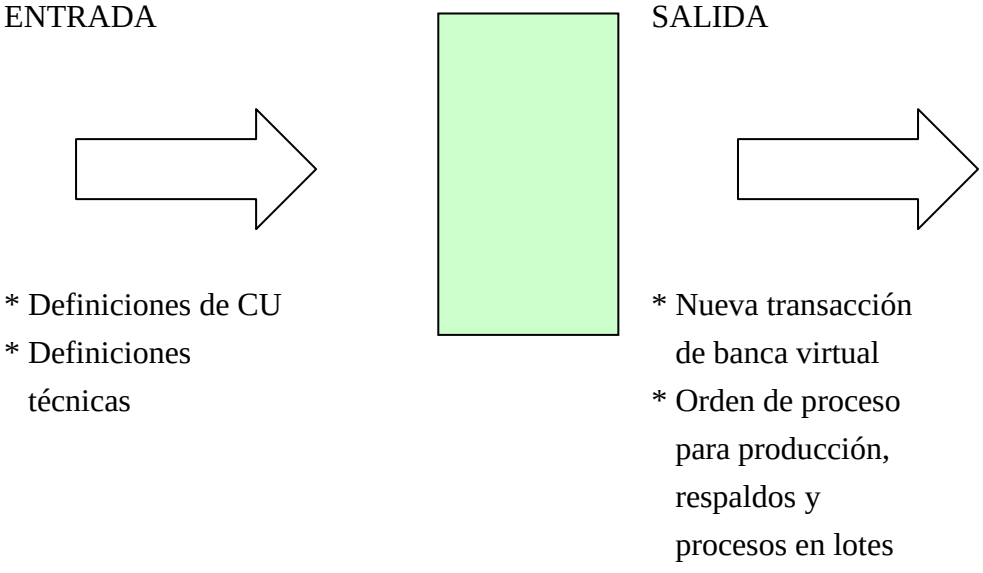


Figura 2-4: Desarrollo de Transacciones

2.2.2.3. IMPLEMENTACIÓN EN PRODUCCIÓN

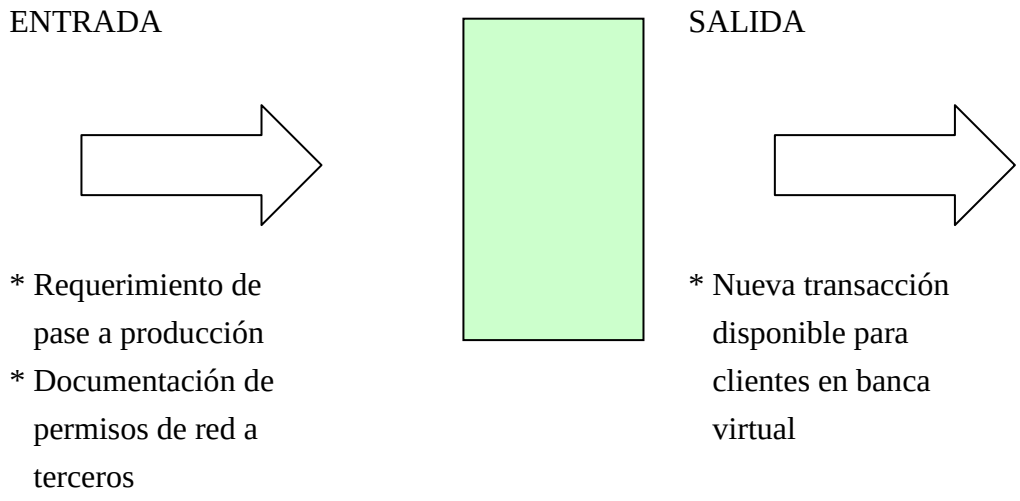


Figura 2-5: Implementación en Producción

2.2.2.4. MANTENIMIENTO Y RESPALDO

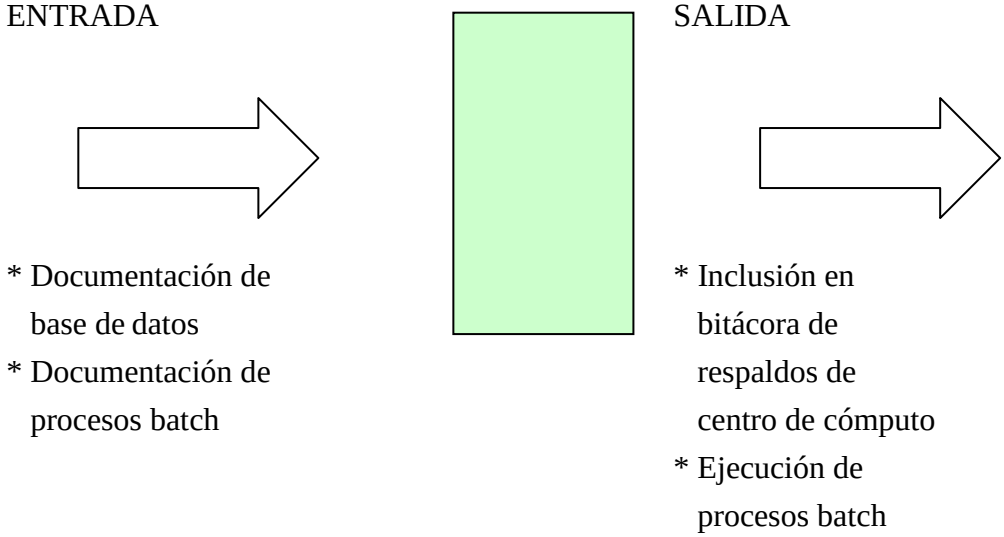


Figura 2-6: Mantenimiento y Respaldo

2.2.2.5. OPERACIONES

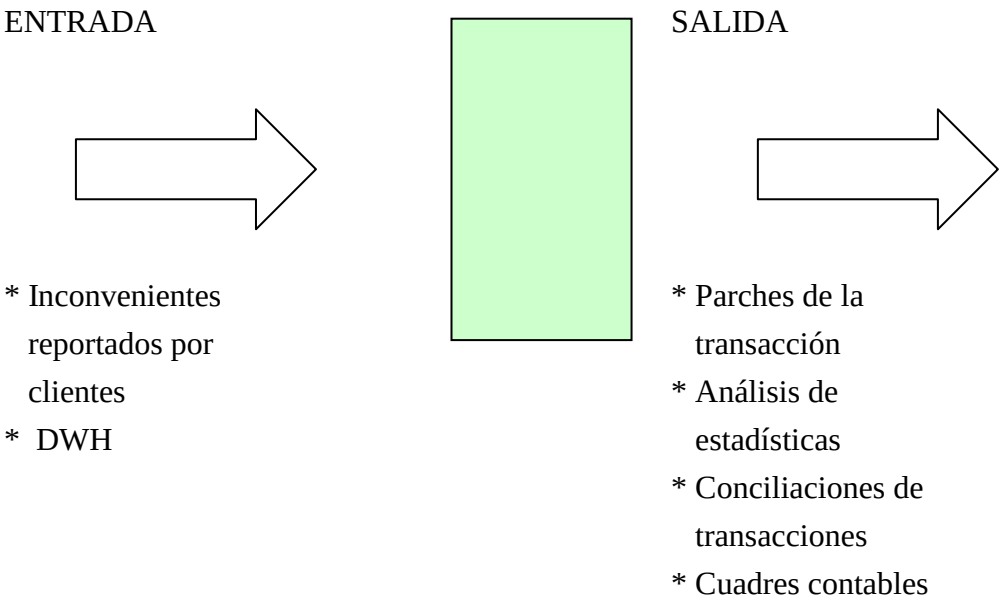


Figura 2-7: Operaciones

2.2.3. PLATAFORMA DE LA BANCA VIRTUAL

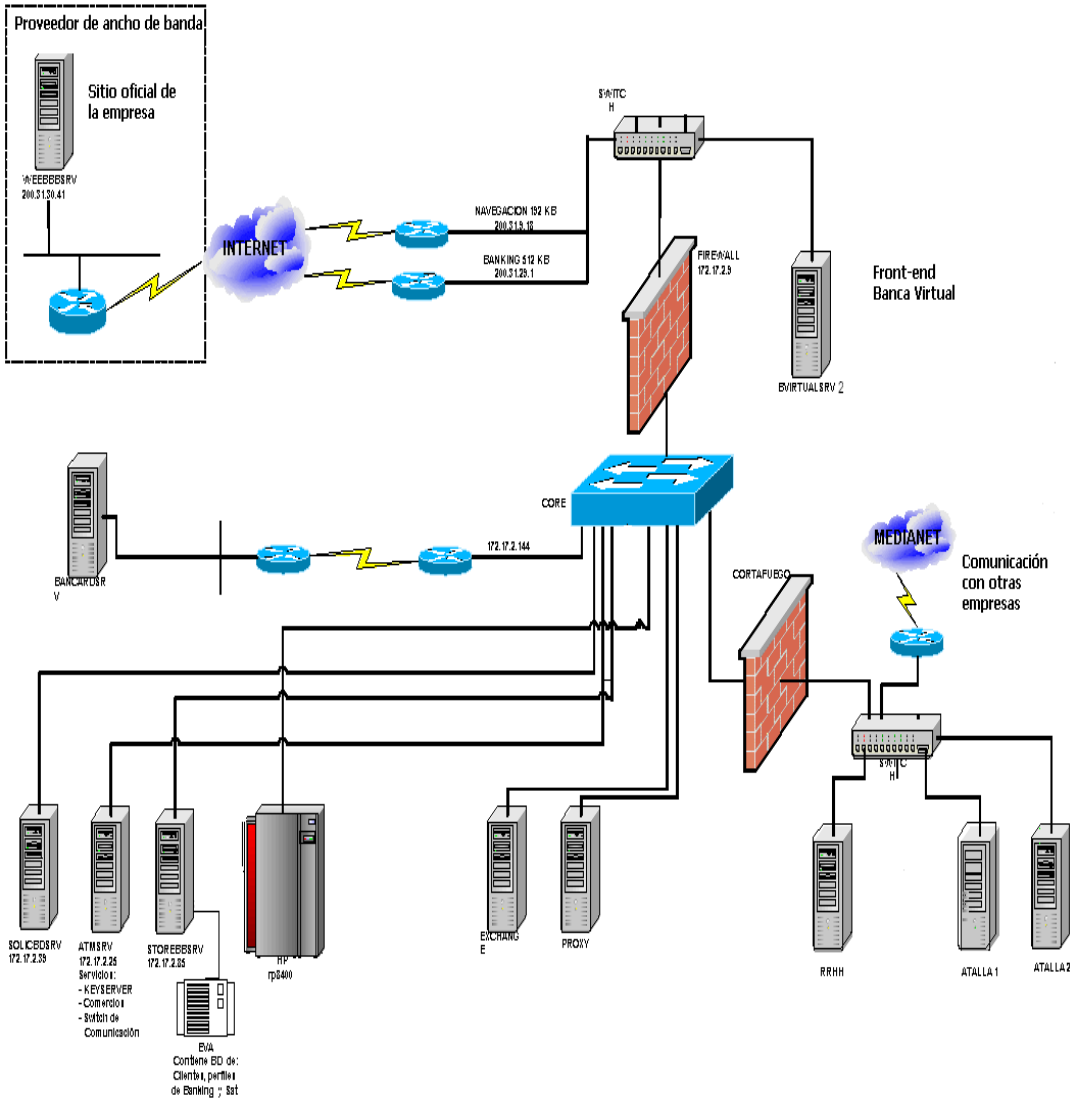


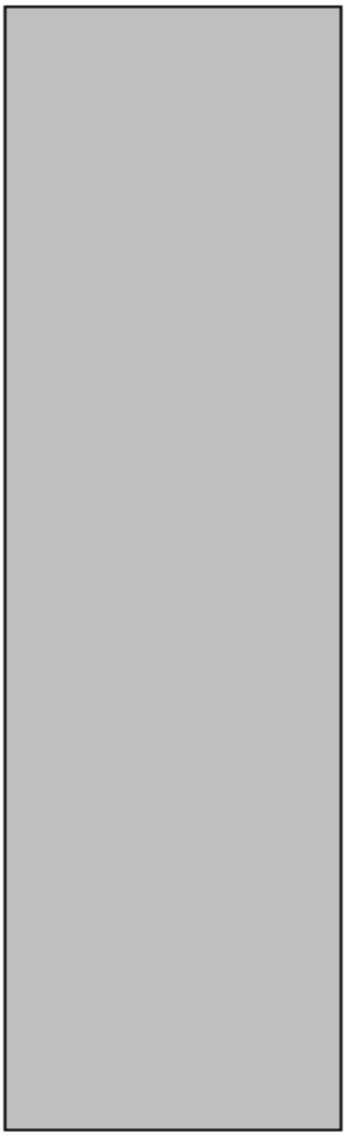
Figura 2-8: Plataforma del Servicio Virtual

NOTA: Vale indicar que existen estándares de seguridad del software utilizado en los diferentes servidores Microsoft, los cuales son los siguientes:

Sistema Operativo Windows 2003 (Ver anexo de estándares)

Motor de base de datos SQLServer 2008 (Ver anexo de estándares)

Servicios de Información de Internet 7 (IIS) (Ver anexo de estándares)



CAPÍTULO 3
ALCANCE DEL PROYECTO

3. ALCANCE DEL PROYECTO

3.1. ALCANCE A ALTO NIVEL

La gestión de la seguridad de la información en todas las actividades y desarrollo de proyectos de servicios de comercio electrónico de la entidad financiera. El mantenimiento, los servicios de valor añadido, los ingresos relacionados con dichos servicios, su consecución y el otorgarle a los clientes un servicio 7 x 24 (Las 24 horas del día y 365 días del año). Esto está de acuerdo con el documento de Declaración de Aplicabilidad (Statement Of Applicability, SOA) fechado a Abril/01/2011, v1.0.

3.2. DESCRIPCIÓN AL DETALLE DEL ALCANCE

Como empresa del sector financiero, la entidad tiene como objeto la captación de fondos de entidades públicas, empresas del sector privado privado y los fondos de todos sus clientes para ofrecer planes de financiamiento para los sectores productivos del país con el fin de dar mantener y mejorar la economía de la nación. Por ende necesita dar servicios de calidad a nuestros clientes, para lo cual tiene su valor añadido del sitio transaccional de banca virtual, que le permitirá al cliente hacer un sin fin de operaciones sin tener que ir a las instalaciones de la oficina.

En la actualidad la institución está presente en las 3 más grandes ciudades del Ecuador, estando así distribuidas:

Guayaquil → Matriz
Quito → Sucursal 1
Cuenca → Sucursal 2

La empresa al adquirir la banca virtual, ofrece a sus clientes (empresas y personas) la disponibilidad del servicio 7 x 24.

La organización se mueve en un sector en el que la mejora continua es esencial para mantener el nivel de competitividad que goza actualmente.

La constante innovación tecnológica le permite a la entidad financiera una mejora continua en los procesos de negocio.

La forma de actuación de la entidad financiera sigue las pautas del P.D.C.A. (planificar, hacer, controlar y actuar), en consecuencia con una constante retroalimentación sobre la

gestión de nuestros procesos.

El objetivo primordial de la política de calidad es la satisfacción y fidelidad de nuestros clientes.
La empresa considera prioritario a nivel interno:

- ✓ La mejora de la competitividad de la empresa, dentro del mercado donde desarrolla su actividad.
- ✓ El aumento de la rentabilidad de la empresa, mejorando los procesos.

Para alcanzar estos objetivos establecemos como primer paso la gestión de un sistema de Calidad según la Norma ISO 9000 en el servicio del ATM (cajeros automáticos) – obtenido dicho certificado en el año 2008.

3.3. JUSTIFICACIÓN

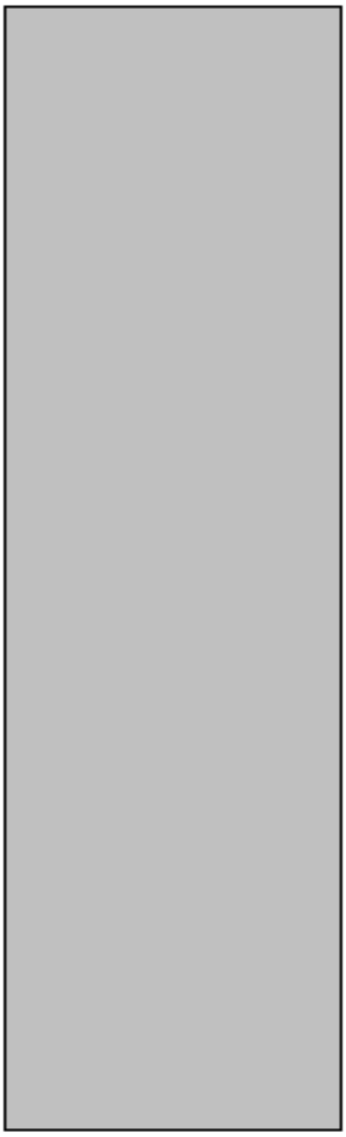
La información que se maneja en la banca virtual es un activo vital para el éxito y la continuidad en el mercado de la agencia financiera. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Este manual se basa en ISO/IEC 27000, que es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que nos permite implementar un sistema de gestión de seguridad de información de una forma metódica, documentada y basada en objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información online de la entidad financiera.

La nueva institución va a sacar su sitio transaccional de comercio electrónico, para lo cual necesita un SGSI, este es un producto en el que se mezclan dominios de control de diversas áreas, tales como:

- ✓ Aspectos organizativos
- ✓ Cumplimiento Legal
- ✓ Telecomunicaciones y operaciones
- ✓ Adquisición, mantenimiento y desarrollo de software
- ✓ Controles de Accesos
- ✓ Gestión de Incidentes

Para la implementación del SGSI se decidió implementar la metodología Magerit, la cual mencionaremos en los siguientes tópicos de esta presentación.



CAPÍTULO 4
POLÍTICA Y OBJETIVOS DE SEGURIDAD

4. POLÍTICA DE SEGURIDAD

4.1. OBJETIVO Y ALCANCE

El objetivo de la Política General de la Seguridad de la Información es establecer los lineamientos y directivas relativas a la protección de la información y activos de tecnología informática y comunicaciones de la Banca Virtual.

Las definiciones y lineamientos presentados en esta Política establecen las bases para la implementación de controles y medidas de la Seguridad de la Información que permitirán al Banco minimizar y/o controlar adecuadamente los riesgos que afectan a su información y a sus activos de tecnología informática y comunicaciones de la Entidad en las transacciones virtuales.

La responsabilidad de la seguridad de la información diaria es deber de cada funcionario y no solamente es al Área de Seguridad. La información de la Entidad debe ser administrada activamente para asegurar la seguridad, confidencialidad, integridad y disponibilidad de la misma.

4.2. ÁMBITO DE APLICACIÓN

Tanto el Banco en su conjunto, como las personas y terceros que acceden, utilizan e interactúan con sus recursos informáticos y de comunicaciones relacionados a los servicios transaccionales virtuales, se encuentran alcanzados por esta Política y las políticas derivadas, y por ende, son responsables de contribuir al logro y mantenimiento de estos objetivos en su desempeño cotidiano.

Esta Política es de aplicación para todo colaborador y/o terceros contratados por el Banco que accedan y/o utilicen información y/o recursos de tecnología informática y comunicaciones de la banca virtual.

4.3. NORMATIVA MARCO (NORMATIVAS SUPERIOR DE REFERENCIA)

Esta Política General tiene como normativa la Norma ISO 27000:2000, todo estándar y procedimiento de Banco se basan en las mejores prácticas y normas de seguridad como NIST, NSA, PCI, CIS, Resolución de la Junta Bancaria No. JB-2011-1851 entre otras.

- ✓ Normativa Derogada
  Ninguna.
- ✓ Vigencia
  Esta Política entrará en rigor a partir del 15 de Agosto del 2011.

4.4. DISPOSICIONES GENERALES Y TRANSITORIAS

Los criterios y directivas emitidos en revisiones anteriores de esta Política y los referidos en cualquier otra norma al respecto, quedan totalmente sustituidos a partir de la vigencia de la presente.

Esta política será revisada anualmente por el Área de Seguridad de la Información de Banco. Los resultados de la revisión, y los cambios que se sucedan, serán reportados a la Gerencia General y comunicados a los involucrados antes de ser implementados.
La falta de cumplimiento de las definiciones emanadas de la presente Política, y de las políticas y normas derivadas sobre seguridad y protección de la información y recursos TIC de la Entidad, estará sujeta a las sanciones disciplinarias que amerite cada caso.
Los estándares y políticas derivadas de la Política General de Seguridad seguirán la siguiente clasificación jerárquica:

Política General de Seguridad;
Políticas Específicas de Seguridad;
Normativas y Directivas de Seguridad;
Estándares de Seguridad;
Procedimientos de Seguridad.

4.5. ROLES Y RESPONSABILIDADES

La implementación satisfactoria de la Política General de la Seguridad de la Información, y de las medidas que de ella se desprendan, requiere la plena cooperación y la asistencia de todos los colaboradores de Banco que intervengan en el servicio de la banca virtual. Es imperativo, por lo tanto, que todo el personal sea consciente de, y opere de acuerdo con, los requisitos de seguridad aquí detallados.

A los efectos de definir e implementar adecuados niveles de seguridad en la información, el Banco ha designado dos órganos de trabajo, a saber:

- ✓ ***Comité de Seguridad de la Información*:** asumirá la responsabilidad de

participar en la toma de decisiones en cuestiones relativas a la Seguridad de la Información.

- ✓ ***Área de Seguridad de la Información*:** será la encargada de gestionar la protección de la información y los recursos TIC, implementando las medidas de seguridad que se desprendan de la estrategia y política definidas por el Comité de Seguridad de la Información, y controlando su eficacia para los fines buscados. Así mismo, proveerá a RRHH los recursos necesarios para asegurar que todo el personal de Banco reciba la capacitación adecuada sobre los procedimientos de seguridad relevantes, y que se brinden los medios y recursos para cumplir con dichos procedimientos.

Adicionalmente, se definen los siguientes roles relativos al cumplimiento de los requisitos de la Seguridad de la Información:

- ✓ ***Propietario*:** persona a la que, por su cargo y/o responsabilidad, Banco reconoce como responsable de un recurso TIC determinado.

Su nivel deberá ser consistente con la autoridad requerida para evaluar los riesgos a los que está expuesto el recurso TIC, respetar las medidas de protección para reducirlos, o para asumir los riesgos que no desee minimizar, dentro de los rangos de riesgos aprobados por el Comité de Seguridad de la Información.

Es responsable de establecer el nivel de criticidad y confidencialidad del recurso TIC del que es dueño.

- ✓ ***Usuario*:** persona que accede a información y/o utiliza un recurso TIC de Banco en el desarrollo de su tarea específica.

Deben firmar su conformidad con las políticas de seguridad de la Entidad, y los estándares y procedimientos que regulan sus actividades.

4.6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El principal objetivo de la Seguridad de la Información es cumplir con los siguientes principios:

- ✓ **CONFIDENCIALIDAD:** Asegurar que todos sus recursos informáticos estén protegidos contra uso no autorizado o revelaciones accidentales acorde a la clasificación otorgada por el origen y la función de la misma. Sólo las personas calificadas y autorizadas tendrán acceso a la información requerida bajo el criterio de "la necesidad de conocer" y el principio de otorgar el "mínimo privilegio" requerido para la realización de las tareas asignadas.

- ✓ **INTEGRIDAD:** Tender a la ausencia de errores y/o corrupción en toda su información y garantizar que la información sea exacta, completa y válida de acuerdo con los valores y las expectativas de Banco, y regulaciones externas.

- ✓ **DISPONIBILIDAD:** Minimizar las amenazas de interrupción del negocio y preservar la continuidad de la operatoria normal. Por lo tanto debe garantizar que:

- La información de alta criticidad sea resguardada;
- La capacidad de procesamiento sea recuperada en tiempo y forma.

4.6.1. PRINCIPALES DIRECTIVAS:

Las siguientes directivas regirán la implementación de la Seguridad de la Información en Banco:

- ✓ Política General de Seguridad de la Información

Banco define que su Política General de Seguridad de la Información, y todas las políticas derivadas, estén alineadas al estándar de seguridad ISO 27000, según las necesidades y particularidades de Banco. Esta definición también regirá para los estándares específicos y procedimientos apropiadamente detallados que constituyen el marco completo de cobertura de la seguridad de la información de Banco.

- ✓ Organización de Seguridad

Para la Administración de la Seguridad de la Información, Banco ha definido una Gerencia de Seguridad de la Información, la cual reporta directamente a la Gerencia de Riesgo.

Así mismo, la Gerencia de Seguridad de la Información cuenta con el apoyo del Comité de Seguridad de la Información.

4.6.2. CLASIFICACIÓN Y CONTROL DE ACTIVOS DE INFORMACIÓN

La información de negocio de Banco, y todos los recursos TIC relacionados, deberán encontrarse inventariados, tener asignado un Propietario, y deberán estar clasificados según su nivel de confidencialidad y criticidad para el negocio de Banco.

4.6.3. ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD

Se evaluarán los riesgos a los que están sometidos los activos TIC de Banco. El área de Seguridad de la Información en conjunto con el Propietario del recurso TIC, establecerán los riesgos que pueden afectar a dicho recurso, las implicancias de su exposición, modificación o acceso no autorizado y cuáles son las medidas de protección que se deberán implementar de acuerdo con el análisis de riesgo efectuado.

4.6.4. COMPETENCIA DEL PERSONAL EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

El personal de Banco, ya sea permanente, temporal, o perteneciente a empresas proveedoras de Banco, deberá ser informado desde el momento de su ingreso de las responsabilidades y derechos en materia de uso y protección de los recursos TIC de Banco, se revisará anualmente estas responsabilidades. Se capacitará con y para el fin de crear conciencia acerca de la importancia que adquiere este aspecto para la Entidad.

Se realizará un seguimiento del uso que se realiza de los recursos TIC para impedir daños e interferencias y evitar interrupciones de las actividades de Banco.

4.6.5. SEGURIDAD FÍSICA Y DE ENTORNO

Se protegerá adecuadamente todos los recursos TIC y las áreas donde estos residen, contra accesos no autorizados y daño intencional o no intencional, implementando medidas de protección acorde con la clasificación de criticidad, confidencialidad y riesgo otorgada a cada recurso.

4.6.6. ADMINISTRACIÓN DE EQUIPAMIENTO, OPERACIONES Y COMUNICACIONES

Se deberá asegurar la disponibilidad de los equipamientos, la integridad de los procesos operativos y la seguridad en las comunicaciones para garantizar un correcto

procesamiento de la información y resguardar la confidencialidad de la misma. Todas las comunicaciones electrónicas con el exterior deberán prever la encriptación de los datos.

4.6.7. CONTROLES DE ACCESO

El acceso a los recursos TIC deberá ser restringido de acuerdo con los requerimientos de control establecidos por sus Propietarios y el área de Seguridad de la Información, bajo el criterio de "la necesidad de conocer" y el principio de mínimo privilegio. Dicho acceso se asegurará a través de procesos de autenticación, autorización, monitoreo y posterior auditoría.

4.6.8. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Los principios de seguridad de la información deberán ser incorporados a los sistemas aplicativos en todo el ciclo de vida de los mismos, incluyendo los procesos de desarrollo, prueba, mantenimiento y puesta en producción de los sistemas aplicativos.

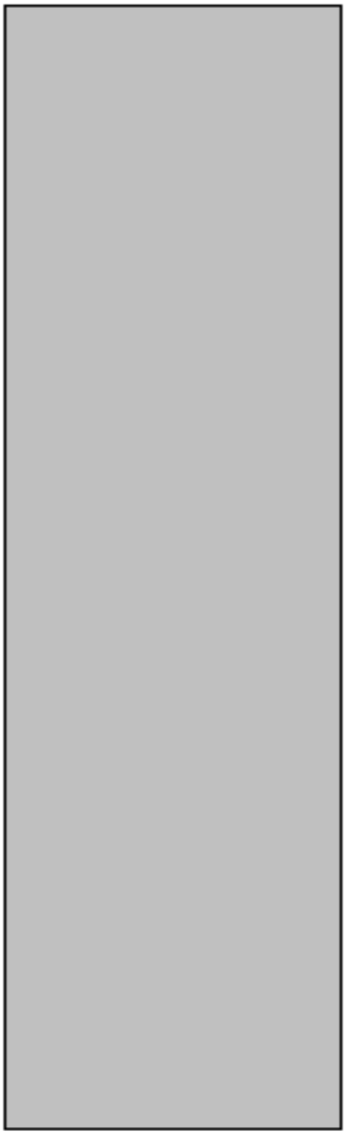
Se deberán prevenir pérdidas, modificaciones o uso inadecuado de los datos, proyectos y sistemas aplicativos de Banco.

4.6.9. ADMINISTRACIÓN DE LA CONTINUIDAD DEL NEGOCIO

Se deberá desarrollar y mantener los planes de recuperación tecnológica y continuidad de negocio requeridos por los propietarios de los recursos TIC y el área de Seguridad de la Información, de forma tal de poder responder a eventos no deseados que impacten de manera negativa sobre los procesos de negocio críticos para la Entidad.

Conformidad con Leyes, Regulaciones y Normas Internas
Se deberá garantizar que la utilización de los recursos TIC no provoque infracciones o violaciones de leyes, regulaciones, ni de las obligaciones establecidas por estatutos, normas, reglamentos o contratos vigentes en cada ámbito de actuación.

Asimismo, se deberá evaluar y asegurar el cumplimiento de las normas internas (políticas, reglas, estándares, procedimientos) relativos a la Seguridad de la Información.



CAPÍTULO 5
ANÁLISIS Y GESTIÓN DE RIESGO

5. ANÁLISIS Y GESTIÓN DE RIESGOS

5.1. METODOLOGÍA

Debido al gran nivel de importancia que tiene la información de la banca virtual, se optó por utilizar la metodología Magerit, ya que permite no solo valorizar los riesgos, sino también permitirá saber cuánto de este valor está en juego y según ese nivel ayudará a proteger la información.
Con la metodología Magerit podemos:

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

5.2. ANÁLISIS DE GESTIÓN DE RIESGO

Esta etapa procederá a puntuar los activos que posee el banco (Banca Virtual) y en base aquello a puntuar las amenazas, salvaguardas, estimar los riesgos y el impacto que dichas amenazas producen sobre cada uno de los activos.

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- ✓ Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
- ✓ Determinar a qué amenazas están expuestos aquellos activos
- ✓ Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- ✓ Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- ✓ Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

5.3. IDENTIFICACIÓN DE ACTIVOS

A continuación se enlistan los activos incluidos en el servicio de estudio del entorno de seguridad de la entidad:

ACTIVOS	DESCRIPCIÓN	CARACTERÍSTICAS	CANTIDAD
Transacciones de banca virtual	Servicios que pueden utilizar los clientes del banco	Disponible las 24 horas del día	7
Transferencias cuentas propias	Transacción a través de la cual los clientes pueden transferir dinero entre sus propias cuentas de la institución	Disponible las 24 horas del día	1
Transferencias terceros mismo banco, otros bancos SPI, directo e internacionales	Transacciones a través de la cuales los clientes pueden transferir dinero a cuentas no propias del mismo banco, a otros bancos en batch o en línea e incluso a bancos del extranjero.	Disponible las 24 horas del día	4
Pago de tarjetas de crédito propias	Transacción a través de la cual los clientes pueden realizar pagos a sus propias tarjetas de crédito de la institución	Disponible las 24 horas del día	1
Pago de tarjetas de crédito de terceros mismo banco, otros bancos SPI, directo e internacionales.	Transacciones a través de la cuales los clientes pueden realizar pagos a tarjetas de crédito no propias del mismo banco, a otros bancos en batch o en línea e incluso a bancos	Disponible las 24 horas del día	4

	del extranjero.		
Recarga de tarjetas de crédito	Transacción a través de la cual los clientes pueden realizar recargas de saldos a tarjetas de crédito	Disponible las 24 horas del día	1
Servicios de consulta y pago de servicios públicos en línea y base local	Transacción a través de las cuales los clientes pueden consultar y cancelar los valores de servicios públicos (luz, agua, teléfono)	Disponible las 24 horas del día	3
Consulta de central de crédito	Transacción a través de la cual los clientes pueden consultar el total de sus deudas registrados en la central de crédito del Ecuador.	Disponible las 24 horas del día	1
Mensajería electrónica	Servicio para el envío de notificaciones a los clientes vía correo electrónico	Microsoft Exchange Server	1
Servicios de Información de Internet	Servicios que sirven para publicar el sitio transaccional en la internet	Internet Information Service 7	1
Sistema Operativo Servidor	Componente que administra el hardware y software de un equipo	Windows 2003 Server Edición Estándar	
Motor de Base de Datos	Software que permite la creación y el funcionamiento	SqlServer 2008 Edición Profesional	

	de la base de datos		
Antivirus y anti espías	Software para evitar programas que alteren el correcto funcionamiento de las pc's y servidores, y que prohíban el ingreso de códigos que puedan espiar las actividades de un equipo de la organización	Mc-Afee Profesional versión 4.0 con 200 licencias	2
Servidores Windows BD	Servidores que contienen las bases de datos SQLServer	Servidores virtualizados con procesadores Pentium I7, Memoria de 8 Gb y 1 Tb de disco duro con SO Windows 2003 Server.	4
Servidores Windows FE	Servidores que contienen las páginas y el servicio de información de internet y otras aplicaciones para el correcto funcionamiento de la banca virtual	Servidores virtualizados con procesadores Pentium I7, Memoria de 8 Gb y 1 Tb de disco duro con SO Windows 2003 Server.	6
Servidores Unix BD	Servidor que contiene la bases de datos principales en ambiente Sybase	Servidor HP físico PN:583967001 DL-380 G7 E5640	1
Estaciones de trabajo (Operadores de centro de cómputo, Ingenieros Administradores de redes e Infraestructura,	Pc's de los funcionarios del banco	Equipos Dell Optiplex GX620 Pentium 4 de 3 Ghz en adelante De 1 a 2 Gb dependiendo de las	20

Desarrolladores)		actividades 80 Gb en disco duro	
Cortafuegos	Hardware y software que permite la administración de permisos de usuarios a través de las redes de la organización	Uno para administrar la comunicación entre la DMZ y la Red de Producción Uno para administrar la comunicación entre la Red del Banco y proveedores de servicios Uno para administrar la comunicación entre las otras redes internas del Banco	2
Base de datos de clientes de banca virtual	Repositorio de información de los clientes de la banca virtual	Base SqlServer de datos de clientes de la banca virtual alojada en el STOREBBSRV.	1
Base de datos transaccional de banca virtual	Repositorio de información de las transacciones realizadas por los clientes en banca virtual	Base SqlServer de transaccionalidad de clientes en banca virtual alojada en el STOREBBSRV.	1
Base de datos de los maestros de cuentas y tarjetas de crédito y débito	Repositorio de cuentas corrientes y ahorros, tarjetas de crédito y tarjetas de débito.	Base Sybase de maestros de cuentas de ahorros, corrientes, tarjetas de crédito y	4

		débito, alojadas en el servidor central HP.	
Base transaccional de movimientos de cuentas	Repositorio de información de las transacciones monetarias realizadas por los clientes	Base Sybase de transacciones de clientes alojada en el servidor central HP.	1
Bases históricas	Repositorios de información histórica de las bases de datos	Base Sybase de histórico de movimientos de clientes alojada en el servidor central HP. Base SqlServer de histórico de transaccionalidad de clientes en banca virtual alojada en el STOREBBSRV.	2
Respaldos en cinta	Respaldos de información de las bases de datos	Cintas HP que guardan los datos de las bases con una fidelidad alta	9
Red Local	Sistema de comunicaciones que permite la comunicación entre los diferentes equipos de cómputo de la institución	Dividida en subredes de: Desarrollo de sistemas Pre-producción Producción interna y DMZ Empleados que no	1

		pertenecen a tecnología administrados por 20 switch de comunicación	
Edificio Matriz	Espacio físico donde funcionan las instalaciones de la institución y en el que se encuentra el Centro de cómputo principal	Ubicado en el centro de la ciudad, en un edificio de 5 pisos con sistema central de climatización y acceso restringido controlado con seguridad física (guardias de seguridad y empleados de áreas restringidas) y seguridad electrónica (controles biométricos: torniquetes, lectores de huellas dactilares y tarjetas de acceso)	1
Centro alterno	Espacio físico donde que se encuentra el Centro de cómputo de contingencia de la institución	Ubicado en las afueras de la ciudad, con un espacio físico de 20 m2 y sistema de climatización y acceso restringido.	1
Operadores de centro de cómputo, Ingenieros Administradores de redes e Infraestructura, Desarrolladores	Personal humano que labora en la institución y desempeñan funciones que están implicadas dentro del entorno de la banca virtual	Ingenieros y Analistas de Sistemas encargados del correcto funcionamiento, desarrollo de nuevas transacciones y el	20

		mantenimiento de los componentes de la banca virtual	

Tabla 5-1: Identificación de Activos

5.4. VALORACIÓN DE ACTIVOS

Las valoraciones para escala cualitativa de Activos serán las siguientes de acuerdo a la utilidad y servicio de cada una.

- Muy Alta - MA
- Alta - A
- Media - M
- Baja - B
- Muy Baja - MB

Activo	Disponibilidad	Confidencialidad e Integridad	Valoración promedio
Transacciones de banca virtual	MA	MA	MA
Mensajería electrónica	A	MA	MA
Servicios de Información de Internet	MA	A	MA
Sistema Operativo Servidor	MA	A	MA
Motor de Base de Datos	MA	A	MA
Antivirus y antiespías	MA	A	MA
Servidores Windows BD	MA	A	MA
Servidores Windows FE	MA	A	MA
Servidores Unix BD	MA	A	MA
Estaciones de trabajo	M	M	M
Cortafuegos	MA	A	MA
Base de datos de clientes de banca virtual	MA	MA	MA
Base de datos transaccional de banca virtual	MA	MA	MA
Base de datos de los maestros de cuentas y tarjetas de crédito	MA	MA	MA

y débito			
Base transaccional de movimientos de cuentas	MA	MA	MA
Bases históricas	MA	A	MA
Respaldos en cinta	A	MA	MA
Red Local	M	A	A
Edificio Matriz	A	MA	MA
Centro alterno	A	MA	MA
Empleados	MA	MA	MA

Tabla 5-2: Valoración de Activos

5.5. INTERRELACIÓN DE LOS ACTIVOS

Para el cuadro de las relaciones y dependencias entre los activos se utilizará una nueva columna con el fin de identificar por abreviaturas los activos.

Activo	Abreviatura
Transacciones de banca virtual	TRX_BV
Mensajería electrónica	MSG
Servicios de Información de Internet	IIS
Sistema Operativo Servidor	SO
Motor de Base de Datos	M_BD
Antivirus y antiespías	ANT
Servidores Windows BD	SW_BD
Servidores Windows FE	SW_FE
Servidores Unix BD	SU_BD
Estaciones de trabajo	PCS
Cortafuegos	FRW
Base de datos de clientes de banca virtual	BD_CBV
Base de datos transaccional de banca virtual	BD_TBV
Base de datos de los maestros de cuentas y tarjetas de crédito y débito	BD_MAE
Base transaccional de movimientos de cuentas	BD_MOV
Bases históricas	BD_HIS

Respaldos en cinta	BACKUP
Red Local	LAN
Edificio Matriz	EDIF.
Centro alterno	ALT
Empleados	RRHH

Tabla 5-3: Abreviatura de Activos

Teniendo en cuenta las dependencias para operar (disponibilidad) y de almacenamiento de datos (integridad y confidencialidad) se ha determinado la siguiente matriz de dependencia entre activos:

	TRX_BV	MSG	IIS	SO	M_BD	ANT	SW_BD	SW_FE	SU_BD	PCS	FRW	BD_CBV	BD_TBV	BD_MAE	BD_MOV	BD_HIS	BACKUP	LAN	EDIF.	ALT	RRHH
TRX_BV		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
MSG	X		X	X	X	X	X	X	X	X	X	X						X	X	X	X
IIS	X	X		X				X											X		
SO	X	X	X		X	X	X	X	X	X								X	X	X	X
M_BD	X	X		X			X		X			X	X	X	X	X	X	X	X		
ANT	X	X		X						X									X		
SW_BD	X	X		X	X	X		X	X	X	X	X	X	X		X		X	X	X	X
SW_FE	X	X	X	X															X		
SU_BD	X	X		X	X	X													X		
PCS	X	X		X		X													X		
FRW	X	X															X		X		
BD_CBV	X	X			X	X	X										X		X		
BD_TBV	X				X	X	X										X		X		
BD_MAE	X				X	X											X		X		
BD_MOV	X				X	X											X		X		
BD_HIS	X				X	X	X										X		X		
BACKUP	X				X	X	X					X	X	X	X	X			X		
LAN	X	X		X	X	X	X												X		
EDIF.	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X
ALT	X	X		X															X		
RRHH	X	X		X															X		

Tabla 5-4: Interrelación de Activos

5.6. AMENAZAS

Las amenazas identificadas en términos de seguridad y disponibilidad del servicio de banca virtual para los activos son las siguientes:

ACTIVOS	AMENAZAS
Servicio de banca virtual	Inconvenientes en producción Acuerdos legales
Mensajería electrónica	Código malicioso Paso de virus
Servicios de Información de Internet	Caída del servicio
Sistema Operativo Servidor	Falla de software Falla de hardware Virus
Motor de Base de Datos	Falla del servicio Espacio en disco
Antivirus	Caducidad de las actualizaciones
Servidores Windows BD	Fallas de hardware apagones de luz intrusos
Servidores Windows FE	Fallas de hardware apagones de luz intrusos
Servidores Unix BD	Fallas de hardware apagones de luz intrusos
Estaciones de trabajo (Operadores de centro de cómputo, Ingenieros Administradores de redes e Infraestructura, Desarrolladores)	Virus Falsificación de identidades acceso a información no debida
Cortafuegos	Virus falla de software falla de hardware
Base de datos de clientes de banca virtual	Robo de información acceso a información no debida
Base de datos transaccional de banca virtual	Robo de información acceso a información no debida

Base de datos de los maestros de cuentas y tarjetas de crédito y débito	Robo de información acceso a información no debida
Base transaccional de movimientos de cuentas	Robo de información acceso a información no debida
Bases históricas	Robo de información acceso a información no debida
Respaldos en cinta	Extravíos Deterioros de las cintas físicas
Red Local	Acceso no autorizado Caída de la red por hardware
Edificio Matriz	Incendio o terremoto
Centro alterno	Incendio o terremoto
Operadores de centro de cómputo, Ingenieros Administradores de redes e Infraestructura, Desarrolladores	Extorsiones por información de clientes

Tabla 5-5: Amenazas

5.7. VALORACIÓN DEL IMPACTO

Las valoraciones de los impactos que causaren las amenazas identificadas para cada uno de los activos serán las siguientes de acuerdo a la degradación y violación de seguridad del servicio de cada una.

- Muy Bajo - 1
- Bajo - 2
- Media - 3
- Alto - 4
- Muy Alto - 5

Se valorará bajo los siguientes parámetros:

- ✓ **Costos de reposición:** adquisición e instalación del activo más el costo de mano de obra (especializada) invertida en recuperar el valor del activo.
- ✓ **Capacidad de operar:** confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas.
- ✓ Sanciones por incumplimiento de la ley u obligaciones contractuales.

ACTIVOS	AMENAZAS	Costo de Reposición	Capacidad de Operar	Valoración promedio del impacto
TRX_BV	Inconvenientes en producción	5	5	5
	Acuerdos legales	1	5	3
MSG	Código malicioso	4	4	4
	Paso de virus	3	5	4
IIS	Caída del servicio	5	5	5
SO	Falla de software	5	5	5
	Falla de hardware	5	4	5
	Virus	4	4	4
M_BD	Falla del servicio	5	5	5
	Espacio en disco	3	5	4
ANT	Caducidad de las actualizaciones	3	3	3
SW_BD	Fallas de hardware	5	4	5
	apagones de luz	4	4	4
	Intrusos	5	5	5
SW_FE	Fallas de hardware	5	4	5
	apagones de luz	4	4	4
	Intrusos	5	5	5
SU_BD	Fallas de hardware	5	4	5
	apagones de luz	4	4	4
	Intrusos	5	5	5
PCS	Virus	4	3	4
	Falsificación de identidades	3	5	4
	acceso a información no debida	5	5	5
FRW	Virus	5	5	5
	falla de software	5	5	5
	falla de hardware	5	5	5
BD_CBV	Robo de información	5	5	5
	acceso a información no debida	5	5	5
BD_TBV	Robo de información	5	5	5

	acceso a información no debida	5	5	5
BD_MAE	Robo de información	5	5	5
	acceso a información no debida	5	5	5
BD_MOV	Robo de información	5	5	5
	acceso a información no debida	5	5	5
BD_HIS	Robo de información	5	5	5
	acceso a información no debida	5	5	5
BACKUP	Extravíos	5	5	5
	Deterioros de las cintas físicas	3	5	4
LAN	Acceso no autorizado	5	5	5
	Caída de la red por hardware	5	5	5
EDIF.	Incendio o terremoto	5	5	5
ALT	Incendio o terremoto	5	5	5
RRHH	Extorsiones por información de clientes	4	4	4

Tabla 5-6: Valoración del Impacto

5.8. CONTROLES

Ya que la base del funcionamiento del negocio de la entidad financiera radica en uso de tecnologías y su principal proceso 7 x 24 son las transacciones disponibles para los clientes en la banca virtual, nos fijaremos como meta trazada la de mantener en línea y funcionamiento los sistemas que permiten se realice este proceso. Las salvaguardadas existentes son las siguientes:

ACTIVOS	AMENAZAS	CONTROL
TRX_BV	Inconvenientes en producción	Pruebas técnicas y funcionales en ambiente de desarrollo. Política de pases a producción. Usuarios de dominio o servidores para pases a servidores. Protección de inyección de código.
	Acuerdos legales	Análisis de departamento comercial y legal
MSG	Código malicioso	Eliminar servicio SMTP de servidores con IIS Permisos hacia el servidor Exchange debidamente documentados y autorizados por el área de Seguridad Informática
	Paso de virus	Antivirus actualizados en pc's de usuarios y servidores Administración de correo interno y externo Depuración de cuentas de clientes y usuarios internos
IIS	Caída del servicio	Scripts y tareas automáticas para restauración, Implementación de recicladores de pools aplicativos de los sitios publicados
SO	Falla de software	Determinación de que actualizaciones del SO tener al día y cuales no dependiendo de aplicativos
	Falla de hardware	Mantenimientos de hardware y tunning de hardware en horarios exclusivos
	Virus	Antivirus actualizados
M_BD	Falla del servicio	Planes de mantenimientos
	Espacio en disco	Alertas de avisos de espacio en disco
ANT	Caducidad de las actualizaciones	Sistema de registro de compras de licencias, fechas y caducidad de antivirus
SW_BD	Fallas de hardware	Servidores de contingencia
	apagones de luz	UPS
	Intrusos	Detección de comportamientos anormales

SW_FE	Fallas de hardware	Servidores de contingencia
	apagones de luz	UPS
	Intrusos	Detección de comportamientos anormales
SU_BD	Fallas de hardware	Servidores de contingencia
	apagones de luz	UPS
	Intrusos	Detección de comportamientos anormales
PCS	Virus	Servidores de contingencia
	Falsificación de identidades	UPS
	acceso a información no debida	Detección de comportamientos anormales
FRW	Virus	Antivirus actualizados
	falla de software	Procedimiento de configuración
	falla de hardware	Firewall de contingencia
BD_CBV	Robo de información	Sensores de usuarios de db conectados
	acceso a información no debida	Asignación de permisos por usuario
BD_TBV	Robo de información	Sensores de usuarios de db conectados
	acceso a información no debida	Asignación de permisos por usuario
BD_MAE	Robo de información	Sensores de usuarios de db conectados

	acceso a información no debida	Asignación de permisos por usuario
BD_MOV	Robo de información	Sensores de usuarios de db conectados
	acceso a información no debida	Asignación de permisos por usuario
BD_HIS	Robo de información	Sensores de usuarios de db conectados
	acceso a información no debida	Asignación de permisos por usuario
BACKUP	Extravíos	Respaldo en bitácora
	Deterioros de las cintas físicas	Temperatura adecuada
LAN	Acceso no autorizado	Monitoreo de tráfico de red
	Caída de la red por hardware	Switches de contingencia
EDIF.	Incendio o terremoto	Política de desastres
ALT	Incendio o terremoto	Política de desastres
RRHH	Extorsiones por información de clientes	Ingeniería Social

Tabla 5-7: Controles

5.9. DETERMINACIÓN DEL RIESGO

5.9.1. FRECUENCIA DE OCURRENCIA DE LAS AMENAZAS

Para determinar las probabilidades con la que ocurra un evento que amenace la integridad de los activos, vamos a utilizar la siguiente escala:

100 = muy frecuente a diario

10 = frecuente mensualmente

1 = normal una vez al año

1/10 = poco frecuente cada varios años

Cabe indicar que la tabla de frecuencias está basada en un análisis estadístico.

ACTIVOS	AMENAZAS	FRECUENCIA
TRX_BV	Inconvenientes en producción	10
	Acuerdos legales	1
MSG	Código malicioso	100
	Paso de virus	100
IIS	Caída del servicio	1
SO	Falla de software	1
	Falla de hardware	1/10
	Virus	10
M_BD	Falla del servicio	1
	Espacio en disco	1
ANT	Caducidad de las actualizaciones	10
SW_BD	Fallas de hardware	1
	apagones de luz	1
	Intrusos	100
SW_FE	Fallas de hardware	1
	apagones de luz	1
	Intrusos	100
SU_BD	Fallas de hardware	1
	apagones de luz	1
	Intrusos	100
PCS	Virus	10
	Falsificación de identidades	1/10
	acceso a información no debida	10
FRW	Virus	10
	falla de software	1
	falla de hardware	1
BD_CBV	Robo de información	100

	Acceso a información no debida	10
BD_TBV	Robo de información	100
	Acceso a información no debida	10
BD_MAE	Robo de información	100
	Acceso a información no debida	10
BD_MOV	Robo de información	100
	Acceso a información no debida	10
BD_HIS	Robo de información	100
	Acceso a información no debida	10
BACKUP	Extravíos	10
	Deterioros de las cintas físicas	1
LAN	Acceso no autorizado	100
	Caída de la red por hardware	10
EDIF.	Incendio o terremoto	1/10
ALT	Incendio o terremoto	1/10
RRHH	Extorsiones por información de clientes	1

Tabla 5-8: Análisis estadístico

5.10. DOCUMENTO DE DECLARACIÓN DE APLICABILIDAD (SOA)

Declaración de Aplicabilidad

Fecha de actualización:

Leyenda (para los controles seleccionados y las razones para la selección de los controles)

2011 Junio 01

RL: Requerimientos legales, **OC**: obligaciones contractuales, **RN/MP**: requerimientos de negocio/mejores prácticas adoptadas, **RER**: resultados de evaluación de riesgos, **TSE**: hasta cierto punto

ISO 27001:2005 Controles			Controles Actuales	Observaciones (Justificación de exclusión)	Controles Seleccionados y Razones para Selección				Observaciones (Vista general de los objetivos de implementación)
					RL	OC	RN/MP	RER	
Cláusula	**Sec.**	**Objetivo de Control/Control**							
Política de Seguridad	5,1	Política de Seguridad de la Información							
	5.1.1	Documento de Política de Seguridad de la Información	□	Controles existentes			□		
	5.1.2	Revisión de Política de Seguridad de la Información	□	Controles existentes			□		
Organización de	6,1	Organización Interna							

Seguridad de la Información	6.1.1	Gestión de Compromiso de Seguridad de la Información	□	Controles existentes	□	□	□		
	6.1.2	Coordinación de Seguridad de la Información	□				□		
	6.1.3	Asignación de responsabilidades de Seguridad de la Información	□				□		
	6.1.4	Proceso de autorización para Instalaciones de Procesamiento de Información	□				□		
	6.1.5	Acuerdos de Confidencialidad	□	Controles existentes		□	□		
	6.1.6	Contacto con las Autoridades	□				□		
	6.1.7	Contacto con Grupos de Intereses Especiales					□		
	6.1.8	Revisión Independiente de Seguridad de la Información	□				□		
	6,2	Partes Externas							
	6.2.1	Identificación de riesgos relacionados con Agentes Externos	□	Controles existentes			□	□	
	6.2.2	Manejo de Seguridad con Clientes	□	Controles existentes			□	□	
	6.2.3	Manejo de Seguridad en Acuerdos con Terceros	□	Controles existentes	□	□	□	□	
Gestión de Activos	7,1	Responsabilidad de Activos							
	7.1.1	Inventario de Activos	□	Controles existentes			□		
	7.1.2	Propiedad de los Activos	□					□	
	7.1.3	Uso Aceptable de los Activos	□				□		
	7,2	Clasificación de la Información							

	7.2.1	Clasificación de Directrices					□	□	
	7.2.2	Etiquetado y Manipulación de la Información					□	□	
Seguridad de Recursos Humanos	8,1	Antes del Empleo							
	8.1.1	Funciones y Responsabilidades	□						
	8.1.2	Selección	□						
	8.1.3	Términos y Condiciones de Empleo	□					□	
	8,2	Durante el Empleo							
	8.2.1	Gestión de Responsabilidad	□						
	8.2.2	Concientización, educación y entrenamiento de la Seguridad de la Información	□	Controles existentes	□	□	□	□	
	8.2.3	Proceso disciplinario	□						
	8,3	Finalización o Cambio de Empleo							
	8.3.1	Culminación de responsabilidades	□				□		
	8.3.2	Devolución de Activos	□						
	8.3.3	Quitar Derechos de Acceso	□			□	□		
Seguridad Física y Ambiental	9,1	Seguridad en Áreas							
	9.1.1	Perímetro de seguridad física	□	Controles existentes		□			
	9.1.2	Controles de entrada de personal	□	Controles existentes		□	□	□	Control con tarjeta de acceso a los centros de cómputo y establecer registro de control de visitas
	9.1.3	Seguridad de oficinas e instalaciones.	□	Controles existentes			□	□	

	9.1.4	Protección contra amenazas externas y ambientales	□	Controles existentes			□	□	
	9.1.5	Trabajo en áreas seguras	□				□		
	9.1.6	Acceso público, repartición y áreas de carga	□						
	9,2	Seguridad de Equipos							
	9.2.1	Permanencia y Protección de Equipos	□	Controles existentes		□		□	
	9.2.2	Utilidades de Apoyo	□			□		□	
	9.2.3	Seguridad de Cableado	□	Controles existentes		□			
	9.2.4	Mantenimiento de Equipos	□	Controles existentes		□	□	□	
	9.2.5	Seguridad de Equipos fuera de las Instalaciones	□						
	9.2.6	Seguridad en reuso o eliminación de equipos	□	Controles existentes			□		Procedimiento a implementar para cuando se migran equipos físicos a virtualizados
	9.2.7	Eliminación de Propiedad	□						
Comunicaciones y Gestión de Operaciones	10,1	Procedimientos de Operaciones y Responsabilidades							
	10.1.1	Procedimientos de Operaciones Documentados	□				□	□	
	10.1.2	Gestión del Cambio	□				□		
	10.1.3	Separación de Ambientes	□	Controles existentes			□	□	
	10.1.4	Separación de desarrollo y operaciones de instalaciones	□						

	10,2	Gestión de servicios de proveedores							
	10.2.1	Prestación de servicios	□	Controles existentes	□	□	□	□	
	10.2.2	Monitoreo y revisión de proveedores	□	Controles existentes				□	Política a implementar para calificación de proveedores
	10.2.3	Gestión de cambios en proveedores	□					□	
	10,3	Sistema de Planificación y Aceptación							
	10.3.1	Capacidad de Gestión					□		
	10.3.2	Sistema de Aceptación					□		
	10,4	Protección contra código malicioso y dispositivos móviles							
	10.4.1	Controles contra código malicioso	□	Controles existentes			□	□	Existió un taller de prácticas y luego se creó un procedimiento.
	10.4.2	Controles contra código en dispositivos móviles	□						
	10,5	Respaldo							
	10.5.1	Respaldo de Información	□	Controles existentes		□	□	□	Implementar encriptación a data sensible
	10,6	Gestión de Seguridad en Redes							
	10.6.1	Controles de Redes	□	Controles existentes		□	□		
	10.6.2	Seguridad de los Servicios de Red	□	Controles existentes		□	□		**Política de Monitoreo de redes**
	10,7	Manejo de Medios							
	10.7.1	Gestión de Medios Extraíbles	□	Controles existentes			□	□	Control evadido por cambios en regedit
	10.7.2	Disposición de Medios					□		

	10.7.3	Procedimientos de Manipulación de Información					□		
	10.7.4	Seguridad del Sistema de Documentación	□				□		
	10,8	Intercambio de Información							
	10.8.1	Políticas y procedimientos de intercambio de información	□	□					
	10.8.2	Acuerdos de Intercambio	□	□					
	10.8.3	Medios físicos en tránsito	□				□		
	10.8.4	Mensajería Electrónica	□	Controles existentes	□	□	□	□	**Política de Correo electrónico e Internet.** Control para correos por salida de exchange desde máquinas de Desarrollo o Preproducción que solicitan Permiso
	10.8.5	Sistemas de Información de Negocio	□	Controles existentes			□		
	10,9	Servicios de Comercio Electrónico							
	10.9.1	Comercio Electrónico	□	Controles existentes	□	□	□		
	10.9.2	Transacciones en Línea	□	Controles existentes	□	□	□		**Política de atención de incidentes en producción - Política de manejo de ambiente de pre-producción.**
	10.9.3	Información pública disponible	□	Controles existentes	□	□	□		
	10,10	Monitoreo							
	10.10.1	Registro de Auditoría	□	Controles existentes			□	□	Grabar todos los campos necesarios para ciertas

									transacciones
	10.10.2	Uso del Sistema de Monitoreo	□				□		**Política de Monitoreo de redes - Política de Monitoreo de Servidores**
	10.10.3	Protección del registro de Información	□				□		
	10.10.4	Administrador y Operador de Log	□				□		
	10.10.5	Registro de Fallas	□				□		
	10.10.6	Sincronización					□		
Control de Acceso	11,1	Requerimientos de Negocio para Control de Acceso							
	11.1.1	Política de Control de Acceso	□	Controles existentes			□	□	**Política de accesos a las bases de datos**
	11,2	Gestión de Acceso de Usuarios							
	11.2.1	Registro de Usuarios	□	Controles existentes		□	□		
	11.2.2	Medición de Privilegios	□	Controles existentes			□		
	11.2.3	Administración de contraseñas de Usuarios	□	Controles existentes			□		
	11.2.4	Revisión de derechos de acceso de Usuarios	□				□		
	11,3	Responsabilidad de Usuarios							
	11.3.1	Uso de contraseñas	□	Controles existentes	□		□	□	Se debe migran algunas contraseñas de aplicaciones antiguas que se encuentra en

									Regedit y en archivos planos a Framework de Seguridad.
	11.3.2	Equipo de Usuarios sin Vigilancia	□				□		
	11.3.3	Política de información transparente	□				□		
	11,4	Control de Acceso a la Red							
	11.4.1	Política de Usos de Servicios de Red	□	Controles existentes	□		□		
	11.4.2	Autenticación de Usuarios para Conexiones Externas	□	Controles existentes	□		□	□	
	11.4.3	Identificación de Equipos en Redes	□	Controles existentes			□		
	11.4.4	Diagnóstico Remoto y Configuración de Protección de Puertos	□	Controles existentes	□		□		
	11.4.5	Segregación de Redes	□	Controles existentes			□	□	Revisar el cumplimiento del tiempo de ciertos permisos
	11.4.6	Control de Conexión de Red	□	Controles existentes			□		
	11.4.7	Control de Enrutamiento de Red	□	Controles existentes			□		
	11,5	Funcionamiento del Sistema de Control de Acceso							
	11.5.1	Procedimientos de Inicio de Sesión Seguros	□	Controles existentes	□		□	□	**Se debe implementar o mejorar los mecanismos de acceso a la banca virtual por nueva ley de fraudes electrónicos vigente a partir del 23 de Marzo/2011**
	11.5.2	Identificación y Autenticación de	□	Controles			□	□	

		Usuarios		existentes					
	11.5.3	Sistema de Gestión de Contraseñas	□	Controles existentes			□		Mejora de la política para que los oficiales del área de Seguridad Informática tengan el acceso desde su área física de trabajo, ya que es un riesgo cuando deben ir al área de infraestructura a colocar las contraseñas en los equipos
	11.5.4	Uso de Utilidades del Sistema	□				□		
	11.5.5	Tiempo de sesión	□	Controles existentes			□	□	Navegadores actuales dejan la sesión del usuario abierta cuando abandonan por el botón de la ventana
	11.5.6	Tiempo Límite de Conexión	□	Controles existentes			□	□	Ajustar el tiempo para ciertas transacciones o ciertos usuarios en base a identificación de IP o segmento de cliente
	11,6	Aplicación de Control de Acceso							
	11.6.1	Restricción de Acceso de Información	□	Controles existentes	□		□	□	Procedimiento aplicado a medias, ya que existen usuarios de desarrollo que en sus aplicativos podrían solicitar acceso a producción y divulgar la información
	11.6.2	Aislamiento de Sistemas Sensibles							
	11,7	Computación móvil and Teleworking							
	11.7.1	Computación móvil y comunicación					□		
	11.7.2	Teleworking					□		

Adquisición, desarrollo y mantenimiento de sistemas informáticos	12,1	Requisitos de Seguridad de Sistemas de Información							
	12.1.1	Análisis y Especificaciones de Requerimientos de Seguridad	□	Controles existentes			□		Procedimiento netamente técnico, ya que el Ingeniero de Procesos que prueba la transacción previo a salir a producción no hace todas las validaciones necesarias.
	12,2	Procesamiento Correcto en Aplicaciones							
	12.2.1	Validación de datos de entrada	□	Controles existentes					
	12.2.2	Control de Procesamiento Interno	□	Controles existentes	□		□		
	12.2.3	Integridad de los Mensajes	□	Controles existentes			□		Procedimiento netamente técnico, ya que el Ingeniero de Procesos que prueba la transacción previo a salir a producción no hace todas las validaciones necesarias.
	12.2.4	Validación de datos de salida	□	Controles existentes			□		Procedimiento netamente técnico, ya que el Ingeniero de Procesos que prueba la transacción previo a salir a producción no hace todas las validaciones necesarias.
	12,3	Controles Criptográficos							

	12.3.1	Política del uso de Controles Criptográficos	□	Controles existentes			□	□	Aplicado a información sensible. Actualmente la organización se encuentra en el proceso de PCI para enmascaramiento y aislamientos de tarjetas de débito y crédito
	12.3.2	Administración de Claves					□		
	12,4	Seguridad de Sistema de Archivo							
	12.4.1	Control de Software Funcional						□	
	12.4.2	Protección de datos de prueba del Sistema					□		
	12.4.3	Control de acceso a librería de fuentes de programas					□		
	12,5	Seguridad en Desarrollo y Procesos de Apoyo							
	12.5.1	Control de Cambio de Procedimientos	□				□		
	12.5.2	Revisión técnica de solicitudes después de cambios en el sistema	□						
	12.5.3	Restricciones en cambios a Paquetes de Software					□		
	12.5.4	Fuga de Información	□	Debe implementarse política			□		**Política de usos de pen-drives y Política de información compartida**
	12.5.5	Desarrollo Externo de Software	□	Controles existentes			□		Validación con área de Seguridad Informática para el desarrollo de software Proveedores
	12,6	Gestión de vulnerabilidades técnicas							

	12.6.1	Control de vulnerabilidades técnicas	□	Controles existentes			□		El área aplicativa revisa y realiza parches para superar las vulnerabilidades
Gestión de Incidente de Seguridad de l Información	13,1	Reportes de Evento y Debilidades de Seguridad de la Información							
	13.1.1	Reportes de Eventos de Seguridad de la Información	□	Controles existentes			□		El área de Monitoreo de Seguridad Informática se encarga de esta tarea
	13.1.2	Reportes de Debilidades de Seguridad de la Información	□				□		
	13,2	Gestión y Mejora de Incidentes de Seguridad de la Información					□		
	13.2.1	Responsabilidades y Procedimientos					□		
	13.2.2	Aprendizaje de Incidentes de Seguridad de la Información					□		
	13.2.3	Recolección de evidencias	□	Controles existentes	□	□	□		
Gestión de Continuidad del Negocio	14,1	Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio							
	14.1.1	Inclusión de Seguridad de la Información en Gestión de procesos de continuidad del negocio					□	□	
	14.1.2	Continuidad del Negocio y Evaluación de Riesgos	□	Controles existentes	□	□	□	□	

	14.1.3	Desarrollo e Implementación de planes de continuidad incluyendo seguridad de la información					□	□	
	14.1.4	Marco de planificación de la continuidad del negocio					□	□	
	14.1.5	Pruebas, mantenimiento and re-evaluación de planes de continuidad de negocio					□	□	
Cumplimiento	15,1	Complimiento de Requisitos Legales							
	15.1.1	Identificación de legislaciones aplicables	□	Controles existentes	□	□	□		
	15.1.2	Derechos de Propiedad Intelectual (DPI)	□	Controles existentes	□	□	□		
	15.1.3	Protección de registros de la organización	□		□		□	□	
	15.1.4	Protección de datos y privacidad de información personal	□	Controles existentes	□	□	□		
	15.1.5	Prevención del uso indebido de las instalaciones de proceso de información	□				□		
	15.1.6	Regulación de controles criptográficos							
	15,2	Estándares y técnicas de cumplimiento de Políticas de Seguridad							
	15.2.1	Cumplimiento de políticas de seguridad	□				□		
	15.2.2	Verificación de cumplimientos técnicos					□		

	15,3	Consideraciones del Sistema de Información de Auditoría							
	15.3.1	Controles del sistema de información de auditoría	□				□		
	15.3.2	Protección de herramientas del sistema de información de auditoría					□		

Tabla 5-9: SOA

5.11. CONTROLES A IMPLEMENTAR

Como resultado del análisis de riesgos creemos que se deben implementar los siguientes procedimientos y los cuales se describen al detalle en el siguiente capítulo:

- ✓ Política de manejo de ambiente de Preproducción
- ✓ Política del uso de Pendrives
- ✓ Política de información compartida
- ✓ Política de correo electrónico e internet
- ✓ Política de Control de accesos
- ✓ Política de Atención de incidentes
- ✓ Política de Monitoreo de Base de datos
- ✓ Política de Monitoreo de Redes
- ✓ Política de Monitoreo de Servidores

Control	Dominios de control de la norma ISO27001	Objetivo
Ambiente de pre-producción	Desarrollo y mantenimiento de sistemas	Probar las transacciones desarrolladas de la banca virtual en un ambiente casi como producción para minimizar los errores y dar un servicio de calidad.
Uso de pendrives	Aspectos organizativos para la seguridad	Evitar la fuga de información de propiedad de la institución
Información compartida	Aspectos organizativos para la seguridad	Restringir y controlar los accesos a ciertos documentos
Correo electrónico e Internet	Gestión de comunicaciones y operaciones	Evitar el mal uso del correo electrónico y de la navegación en internet
Accesos a las bases de datos	Control de accesos	Regularizar los privilegios de usuarios de las bases de datos
Atención a incidentes	Desarrollo y mantenimiento de sistemas	Procedimiento con el fin de atender alguna anormalidad en producción
Monitoreo de Base de Datos	Desarrollo y mantenimiento de sistemas	Revisión y alertas del desempeño y accesos no

		autorizados a las bases de datos.
Monitoreo de Redes	Desarrollo y mantenimiento de sistemas	Revisión y alertas del desempeño y accesos no autorizados a las redes del Banco.
Monitoreo de Servidores	Desarrollo y mantenimiento de sistemas	Revisión y alertas del desempeño y accesos no autorizados a los servidores de la institución.

Tabla 5-10: Controles a Implementar

5.12. PROCEDIMIENTOS DOCUMENTADOS.

5.12.1. ATENCIÓN DE INCIDENTES

5.12.1.1. OBJETIVO:

Asegurar la correcta y oportuna atención y mitigación de incidentes, de manera que no se vea afectada la operación normal de la banca virtual.

Notificación y atención inmediata de incidentes dentro de los plazos de tiempo.
Alertas: Monitoreo y verificación de servicios, ejecución de procesos, desempeño de la plataforma.

LO NUEVO: Alertas del BAC

Todo servicio debe contar con su contingencia, desde que entra a PRODUCCIÓN.
Niveles de alertas:

ALERTA AMARILLA: Riesgo medio de que algún recurso pueda quedar fuera de servicio.
ALERTA NARANJA: Riesgo alto de que algún recurso pueda quedar fuera de servicio.
ALERTA ROJA: Paralización total de un recurso o alta degradación del mismo.
ESTADO DE EMERGENCIA: Afectación grave de recursos / servicios del banco o tiempo máximo de resolución de problemas excedido.

Registro de incidentes en SISTEMA DE MANEJO DE NOVEDADES DEL OPERADOR.

5.12.1.2. RESPONSABILIDADES:

Dar voz de alerta: todo el personal que intervenga en el servicio online.

- ✓ Registro de incidente en Sistema de Novedades, llevar control de tiempo transcurrido en solución, escalar / mantener informado del estado de la atención del problema a la Gerencia y Jefatura: Operador.
- ✓ Atención inmediata de incidentes, activación de contingencias, planificación de acciones correctivas, actualización de PDC: Grupos de solución.
- ✓ Seguimiento de Novedades, cierre: AYC.
- ✓ Revisión de documentación técnica actualizada: Control de Calidad.
- ✓ Operador únicamente puede dar atención a incidentes sencillos y

documentados.

- ✓ Personal involucrado en atención de incidente debe permanecer en sitio hasta mitigar problema.
- ✓ Atención y escalamiento en horario fuera de oficina:
- ✓ Operador: 5 minutos
- ✓ Jefe de Centro de Cómputo: 5 minutos
- ✓ Grupo de solución: 20 minutos.
- ✓ Cambios entre nivel de alerta: 20 minutos.

5.12.1.3. CLASIFICACIÓN DE ALERTAS

- ✓ AMARILLA:
  - Recurso degradado en 50%,
  - Lentitud en tiempo de respuesta,
  - ATM fuera de servicio,
  - Irregularidad de HW/SW en equipos,
  - Virus
  - Otros
- ✓ NARANJA:
  - Recurso degradado en 75%,
  - Tiempo de ALERTA AMARILLA excedido.
  - Según impacto del incidente.

- ✓ ROJA:
  - Recurso degradado en 99% o paralizado,
  - Tiempo de ALERTA NARANJA excedido.
  - Según impacto del incidente.

5.12.1.4. ESTADO DE EMERGENCIA

- ✓ Tiempo de ALERTA ROJA excedido.
  - Según impacto del incidente.

5.12.1.5. NOTIFICACIONES:

- ALERTA AMARILLA: Jefe de Centro de Computo, responsable principal o alterno del servicio o recurso afectado, Stand-by de turno.

5.12.2. MONITOREO DE BASE DE DATOS

OBJETIVO: Definir las gestiones necesarias para garantizar el adecuado funcionamiento de las bases de datos de los productos y/o servicios puestas en el sistema central.

Monitoreo: únicamente con herramientas aprobadas por el banco. Herramientas deben brindar información detallada (alertas, logs, espacio utilizado, calendarización de Jobs, rendimiento, conexiones entre bases, procesos activos, transacciones demoradas, bloqueos, otros).

LO NUEVO: Alertas del BAC

- Bases a monitorear deben ser definidas entre Líderes Aplicativos y personal de Base de Datos.
- Monitoreo según esquema definido en la política de monitoreo:
- Rendimiento BD Sybase
- Rendimiento BD SQL
- Espacio BD Sybase
- Espacio BD SQL

A través de la revisión de las bases de datos se debe identificar: rendimiento del estado de la memoria en el servidor, disco, consumo del CPU, procesos ejecutándose, tiempo de espera, procesos Bach, entre otros.

- En caso de error o fallo a nivel de base de datos, el operador envía mail de notificación a Grupo de Base de Datos y registra novedad de Sistema de Manejo de Novedades.
- Al recibir la alerta, el personal de Base de Datos debe confirmar si persiste la alerta. En caso de mantenerse, se debe notificar del incidente al Líder de Grupo y Subgerente de IDS, e iniciar atención.

Informar al Líder Aplicativo relacionado sobre los fallos presentados y las acciones que se van a tomar para resolver el incidente.

- Una vez solucionado el incidente, confirmar OK de bases de datos y procesos afectados. Notificar del estado OK al Líder de Base de Datos y Subgerente de IDS. Informe de gestión: mensual.

5.12.2.1. RESPONSABILIDADES:

- ✓ Líder de Grupo BD: Armar calendario de turnos y difundirlo (una vez aprobado). Instrucción del personal a su cargo.
- ✓ Subgerente de IDS: aprobar calendario de turnos. Revisión de informe y definir acciones correctivas / mejoras.
- ✓ Personal de BD: elaboración y entrega de informe.

5.12.3. MONITOREO DE REDES

5.12.3.1. OBJETIVO

Verificar de manera constante la disponibilidad y funcionalidad de los dispositivos de red; para detección, corrección y seguimiento oportuno de las fallas o incidentes que se presenten.

Todo servicio del banco debe ser monitoreado y revisado constantemente para garantizar su correcto funcionamiento.

LO NUEVO: Alertas del BAC

ELABORACIÓN DE INFORME DE DISEÑO APROBADO POR SUBGERENTE de IDS. Con acceso restringido. Entrega de informes: los 5 días hábiles del periodo siguiente. Monitoreo de las Redes del BB debe ser efectuado a través de aplicaciones de uso autorizado en el banco y que generen información detallada sobre fallas o errores. Tipos de monitoreo:

- ✓ Seguridad Perimetral del IPS Tipping Point (mensual)
- ✓ Uso de Ancho de Banda - Internet (cada 15 ds)
- ✓ Disponibilidad Recursos Routers (mensual)

5.12.3.2. RESPONSABILIDADES:

- ✓ Monitoreo regular de la red y control de incidentes.
- ✓ Entrega de informes: Personal de Redes.
- ✓ Presentar propuesta de mejora según resultados de informe: Jefe Redes.
- ✓ Revisión y aprobación de informes: Subgerente de IDS.
- ✓ Publicación de informe APROBADO: Personal de Redes.

5.12.3.3. PROCEDIMIENTO:

- Etapas:

1. Priorización de monitoreos a realizar.
2. Monitoreo y elaboración de informe (incluye recomendaciones).
3. Aprobación y publicación de informe.

5.12.4. MONITOREO DE SERVIDORES

5.12.4.1. OBJETIVO

Mantener óptimo rendimiento SERVIDORES a través de monitoreo frecuente para detectar riesgos o fallos y aplicar el seguimiento preventivo o correctivo.

Monitoreo: solo a través de aplicaciones autorizadas por el banco, y que brinden información detallada de eventos.

Tareas a ser monitoreadas: Son definidas por Líderes Aplicativos y especificadas en la documentación técnica asociada. Una vez aprobado, monitoreo debe ser implementado. Cambios en servicio / servidor deben ser notificados por Líder Aplicativo a IDS y AYC (actualización de documentación).

Complementar tareas de monitoreo con revisión periódica de servidores. A la detección de fallos, la novedad se registra en el Sistema de Manejo de Novedades (operador). El escalamiento al personal de IDS solo cuando se requiera una revisión especializada.

LO HUEVO: Alertas BAC

Atención de fallos por parte de Grupo de Servidores incluye confirmar si persiste el problema, analizar estatus de servicio / dispositivo afectado. Registrar en el Sistema de Novedades el detalle de acciones a tomar y clasificar como CRITICO/NO CRITICO:

- NO CRÍTICO: solución directa.
- CRITICO: requiere ayuda de grupo de otros grupos de solución. Persona que atiende el fallo debe cerrar novedad en Sistema de Manejo de Novedades e informar del estado del incidente a Líder de Grupo y Subgerente de IDS. Envío de informe con actividades atendidas al final de día / turno. Cambios de configuración de servidores únicamente con OK del Líder de Grupo, Subgerente de IDS y Líder Aplicativo.

5.12.4.2. RESPONSABILIDADES:

- ✓ Personal de Servidores: Atención de incidentes, envío de informe con tareas atendidas, elaboración y envío de informe de monitoreo diario.
- ✓ • Líder Grupo Servidores: Elaborar informe de disponibilidad de servicio (compendio de informes de atención diaria) y proponer mejoras.
- ✓ Subgerente de IDS: revisar informe y aprobar acciones correctivas (en conjunto con Gerencias / subgerencias del área).
- ✓ Uso de claves de servidores a discreción.

5.12.4.3. PROCEDIMIENTO:

1. Recibe notificación de incidente.
2. Busca información del problema en logs de herramienta de monitoreo.
3. Realiza pruebas, verificando si persiste el problema.
4. Catalogan incidente (normal o crítico) y determinan acciones a tomar.
5. Solucionan problema(s) y comprueba en la herramienta de monitoreo.
6. Informe de solución a involucrados, reportes diarios, Sistema de Manejo de Novedades.
7. Elaboración de informe a fin de mes y aprobación del Subgerente de IDS.

5.12.5. POLÍTICA DE MONITOREO

5.12.5.1. OBJETIVO

Monitoreo del funcionamiento, rendimiento, mantenimiento y comportamiento de elementos de la infraestructura tecnológica.

Todo servicio que se brinda debe ser monitoreado y revisado para garantizar su funcionalidad.

Informes compartidos en file server, con acceso restringido. Definir responsable y periodicidad de entrega.

Informes mensuales: Plazo de entrega hasta 5 días hábiles del mes siguiente.

5.12.5.2. Monitoreo por elemento

- ✓ INFRAESTRUCTURA (IOS):
- Recursos disponibles asignados y cambios de máquinas virtuales (IDS)
- Disponibilidad de servicios (IDS)
- Revisión de estado de antivirus (IDS)

- ✓ REDES:
- Seguridad perimetral del IPS
- Uso de ancho de banda
- Uso de switch
- ✓ BASE DE DATOS:
- Rendimiento de Sybase / SQL
- Espacio disponible de datos, Sybase / SQL.
- ✓ SOPORTE:
- Seguridad de correo
- Navegación y contenido (Internet).

5.12.5.3. ARQUITECTURA:

Monitoreo de plataforma de integración

5.12.5.4. RESPONSABILIDADES:

- ✓ Líder de Grupo de Solución: Asegurar que se cumplan las actividades de monitoreo y entrega de informes.
- ✓ Subgerente responsable: Revisión de informes y determinar acciones a tomar.
- ✓ AYC: Revisar disponibilidad de informes.

- ✓ Políticas de manejo de ambiente de Preproducción

General:

- ✓ El ambiente Preproducción no será utilizado para desarrollar aplicaciones, este ambiente está destinado para realizar pruebas de usuarios final..
- ✓ Todas las aplicaciones existentes y nuevas con sus mejoras o cambios deben ser probadas en este ambiente Pre-producción, antes de instalarlas en el ambiente de Producción.
- ✓ La administración de este ambiente estará bajo la responsabilidad de Bases de Datos por el lado de Ingeniería, el jefe de desarrollo y el jefe de Banca Virtual.
- ✓ Sólo el administrador de desarrollo manejará el cambio de fecha del kernel, el mismo que debe coordinar con el grupo de desarrollo y el área de productos el momento apropiado para hacer dicho cambio.
- ✓ En este ambiente no se ejecutará procesos de producción
- ✓ Se tendrá que delegar un backup del Jefe de Desarrollo, el administrador backup tomará acción solo si el administrador principal no se encontrare disponible.
- ✓ Se definirán un grupo de usuarios de consulta en este ambiente Pre-producción, los mismos que serán utilizados por los desarrolladores en la verificación de data resultado de las pruebas efectuadas por los usuarios finales.
- ✓ El ambiente Desarrollo y Pre-Producción físicamente son los mismos por lo tanto los mismos directorios se van a visualizar en los dos ambientes. La diferencia entre los ambientes es que cada uno tiene su propio ambiente SYBASE.
- ✓ El grupo de banca virtual tendrá un usuario como dbo de sus bases para sus propias compilaciones.

Será responsabilidad de Ingeniería – Base de Datos

- ✓ Subir la información de respaldo (dump), el administrador de desarrollo debe coordinar con los implicados y definir el set de datos a cargar, se debe notificar la orden de carga a Base de datos con 24 horas de anticipación.
- ✓ Crear un usuario operador con los accesos necesarios para realizar los pases. El buen uso del usuario operador es responsabilidad del administrador de desarrollo.
- ✓ Crear los usuarios aplicativos de lectura a la base.
- ✓ Actualizar los password de los usuarios de cobis, cada vez que se realice un dump de la base cobis.
- ✓ Replicación al ambiente branch Windows
- ✓ Se harán copias actualizando el filesystem /fuentes del ambiente Pre-producción

con la información almacenada en el filesystem /fuentes de Producción. La copia debe ser solicitada por el administrador de desarrollo y avalada por Administración y control

- ✓ En caso de tener problemas con el ambiente (conectividad, performance, etc.) será comunicado a Base de Datos para su solución. Base de datos informará al administrador de desarrollo del problema y el tiempo necesario para su solución.
- ✓ Crear el usuario dbo para las bases de Banca Virtual

Será responsabilidad de Desarrollo

- ✓ Ejecutar los pases de desarrollo en dicho ambiente..
- ✓ Luego de haber compilado se enviará la confirmación vía mail.
- ✓ Mantener la confidencialidad de la clave del usuario operador.
- ✓ Facilitar a los desarrolladores la creación de menús para ejecución de batch.

Será responsabilidad de Banca Virtual

- ✓ Ejecutar los pases de banca virtual en dicho ambiente.
- ✓ Luego de haber compilado se enviará la confirmación vía mail.
- ✓ Mantener la confidencialidad de la clave del usuario de banca virtual.

Será responsabilidad de Desarrollo – Banca virtual – Líderes aplicativos.

- ✓ Cada aplicativo deberá generar un archivo con la lista de los programas a compilar y enviar la solicitud de compilación vía mail con la ruta del archivo generado. Esta lista deberá contener la ruta completa del programa a compilar en orden de ejecución (script's, spsql y sqr), en caso de que el pase incluya bcp de archivos, o alguna otra consideración especial se deberá enviar obligatoriamente el archivo cmd.
- ✓ Revisar que los cambios que se están pasando no afecten a los productos que se encuentren haciendo pruebas
- ✓ Informar a todo desarrollo los cambios generales que afectan la interoperabilidad con los otros módulos.
- ✓ Plantear un esquema de reverso de los cambios realizados (datos y objetos DDL) en el ambiente Pre-producción, de tal manera que el borrado de datos o cambios no deseados puedan reversarse oportunamente.
- ✓ Actualizar en el módulo de batch de nuevos programas o cambios en los menús para generación de mismo en las pruebas.

Ejecutar sus procesos batch por menús.

Será responsabilidad de Productos

- ✓ Enviar copia del requerimiento a Control de Calidad.
- ✓ Entregar Plan de pruebas a Control de Calidad con 15 días de anticipación al inicio de las mismas.
- ✓ Solicitar al(los) Administrador(es) de desarrollo del ambiente asignación de fechas de pruebas y horarios con tiempo de anticipación.
- ✓ Comunicar a Desarrollo y Productos el horario de pruebas para evitar conflictos entre grupos de trabajo.
- ✓ Solicitar a Contraloría la creación de transacciones autorizadas.

Será responsabilidad de Control de Calidad

- ✓ Revisar / Aprobar plan de pruebas del proyecto.
- ✓ Será responsabilidad de Contraloría
- ✓ Creación de procedimientos, transacciones, catálogos, roles, etc.
- ✓ Asignación de transacciones a roles
- ✓ Ambiente de Información

Dada a la gran cantidad de requerimiento de información que solicitan constantemente los organismos de control se estableció:

- ✓ Crear un device, y denominarlo cob_base.(en desarrollo), la cantidad de espacio asignado dependerá de la disponibilidad de almacenamiento. Esto será notificado por Base de Datos a los involucrados en el proceso.
- ✓ La disponibilidad del ambiente estará bajo la responsabilidad de Jefe de desarrollo.
- ✓ Toda solicitud de información debe ser aprobada por Contraloría.
- ✓ La subida de información estará bajo la responsabilidad de Base de Datos, la subida de información debe ser coordinada con 24 horas de anticipación.

5.12.6. POLÍTICA DE CONTROL DE ACCESO

5.12.6.1. OBJETIVO

Crear procedimientos para la asignación de permisos y control de accesos a bases de datos.

5.12.6.2. ALCANCE

Permisos y control de acceso asignados a personal de Computación a los sistemas informáticos computacionales del Banco.

5.12.6.3. PERFILES DE USUARIOS

Los usuarios se crearán bajo los siguientes perfiles:

- ✓ Administrador de la Base de datos: login adminbd
- ✓ Oficial de Seguridad: login of_seg
- ✓ Operador: Login de Usuarios Operadores de Centro de Cómputo
- ✓ Lectura: Login de Desarrolladores de Banca Virtual y Desarrollo
- ✓ Actualizadores: Usuarios aplicativos de sistemas.

5.12.6.4. POLÍTICA:

Seguridad Informática administrará el control de acceso a la base de datos Sybase de producción. Seguridad Informática autorizará la asignación de permisos de usuarios a bases de datos SQLsrv y sistemas operativos de los servidores NT.
Seguridad Informática en los casos que estime necesario solicitará autorización a Contraloría para otorgar permisos.

Otorgará permisos a requerimientos del líder aplicativo, y Jefe de Desarrollo a través de los formularios de seguridad. Los permisos serán solicitados por medio de los formularios elaborados. Todo usuario será personal y deberá llenarse el Acta de compromiso.

IDS administrará el control de acceso a las bases de datos SQLsrv de los servidores NT de Producción. Administrará el control de acceso a los sistemas operativos de los servidores NT y HP del Banco.

Todo permiso a los diferentes sistemas de bases de datos, sistemas operativos y acceso físico al centro de cómputo del Banco será aprobado por Seguridad Informática. Seguridad Informática autorizará permisos solamente a logines personalizados.
Los permisos serán asignados a través de los formularios:
Bases de datos sybase
Bases de datos SQL

5.12.7. PERMISO DE RED O SISTEMAS OPERATIVOS

Los requerimientos de permisos llegarán a Seguridad Informática, los analizará, evaluará, consultará con los responsables aplicativos y aprobará o rechazará solicitud. Si un líder aplicativo no recomienda algún permiso Seguridad Informática, rechazará la solicitud.

Los permisos de accesos a la base de datos sybase de Producción serán ejecutados por Seguridad Informática. Los permisos a usuarios aplicativos solo se asignarán de lectura y de acceso a tablas, no se concede permiso a ejecutables. Los cambios de password deben ser inmediatamente recibidos el nuevo login.

El password de operadores y administradores debe cambiarse en producción y replicador.

El password de desarrolladores debe cambiarse solo en producción.

Los permisos a la base de datos Seguridad Informática concederá solamente a los aplicativos asignados. Los accesos a datos de cuentas corrientes y ahorros Seguridad Informática asignarán solamente a personal autorizado del grupo de cuentas. Las siguientes tablas de las correspondientes bases de datos solo serán concedidas a personal de Cuentas:

ase	Tablas
Cuentas	cc_ctacte, cc_ctacte_fin, cc_ctacte_agd
Cuentas_his	cc_his_movimiento, cc_his_disponible ***cc_his_movimiento_ant,cc_his_disponible_ant***
Cuentas_acum	cc_his_movimiento_acum
Ahorros	ah_cuenta, ah_cuenta_fin, ah_cuenta_agd
Ahorros_his	ah_his_movimiento, ah_saldo_diario
Ahorros_acum	ah_his_movimiento_acum

Tabla 5-11: Tablas

Las tablas correspondientes de diferido para Banca Virtual solo serán autorizadas al responsable del departamento, en el caso de ATMs se concederá sólo al líder aplicativo.

Seguridad Informática restringirá el acceso en línea a las bases acum y his por el volumen o tamaño de estas bases.

Los permisos de accesos a servidores NT y bases de datos SQL aprobados los canalizará a través de IDS para su ejecución. Los permisos a usuarios aplicativos a bases de datos solo se asignarán de lectura y de acceso a tablas, no se concede permiso a ejecutables.

Se entregarán usuarios de login con el standard: GGonzaleR, de donde se escribe la inicial del primer nombre, seis caracteres por el apellido y la inicial del segundo apellido. El uso y custodia de la clave de acceso es de exclusiva responsabilidad del usuario y no deberá permitir que terceros accedan a ella.

Los accesos en producción a usuarios aplicativos queda restringido al siguiente horario: lunes a viernes estarán bloqueados de 10am a 5pm, los usuarios del grupo de mantenimiento de 10am a 2pm. Los fines de semanas estarán bloqueados totalmente. Estos bloqueos se harán automáticamente. El levantamiento del bloqueo de fin de semana se realizará los lunes 7H00.

Seguridad Informática podrá suspender o revocar las claves de acceso, sea por motivos de mal uso de las aplicaciones bancarias, por sospecha de indebida utilización, no compromiso de la seguridad tecnológica o por otras circunstancias.

Los empleados que sean sorprendidos haciendo uso de claves no permitidas a su nivel serán sancionados de acuerdo con las circunstancias. Esta conducta es causal de visto

bueno y podrá determinar el despido.

5.12.8. POLITÍCA DE CUENTA

Se tiene grupos diferenciados con acceso a producción y los cuales detallamos a continuación:

5.12.8.1. USUARIO SA

- ✓ Se cambiará este password cada mes.
- ✓ Los usuarios con características del SA pueden ser: El Administrador de la Base de datos, Seguridad Informática como Administrador de control de accesos a la base de datos y el Administrador del sistema central.

5.12.8.2. USARIO DE CONSULTA / LECTURA

- ✓ El acceso de desarrollo será solamente de lectura.
- ✓ El usuario de consulta es para revisión de problemas.
- ✓ Deberán regirse al horario de uso asignado.
- ✓ Deben conectarse solo por el tiempo necesario, no deberán mantener conexiones abiertas por largo tiempo, peor de un día al otro.
- ✓ Los permisos serán otorgados de acuerdo al grupo aplicativo que manejen.

5.12.8.3. APLICATICATIVOS/ACTUALIZACIONES

- ✓ Usuarios creados para manejo interno en las aplicaciones
- ✓ Estos usuarios no deben ser conectados en equipos no autorizados (área de desarrollo)
- ✓ Los password de estos usuarios deben cumplir con la política de seguridad (encriptamiento)

5.12.8.4. OPERADORES

- ✓ Por política sólo los operadores podrán sacar respaldos y restaurar.
- ✓ El usuario Operador para los procesos batch tendrá acceso con rol SA.
- ✓ El usuario operador es el único autorizado para compilación de programas

5.12.8.5. ADMINISTRADORES DE BASE DE DATOS

- ✓ Por política realizará monitoreo de la base de datos
- ✓ No puede realizar consultas a información de la base
- ✓ Alertará sobre mal uso de los recursos de la base

5.12.8.6. OFICIAL DE SEGURIDAD

- ✓ Realizará la creación y eliminación de usuarios.
- ✓ Asignación de permisos y seguimiento de usuarios.

5.12.9. POLÍTICA DE PASSWORD

- ✓ Longitud del password: superior o igual a 8 caracteres.
- ✓ Expiración de la clave: 90 días.
- ✓ Para administradores cambiará cada 30 días.
- ✓ El número de sesiones concurrentes de un mismo usuario es limitado.
- ✓ El usuario debe ser usado en el equipo personal a él asignado.
- ✓ El password es personal e intransferible.

5.12.10. ACTA DE COMPROMISO

Para revisión de problemas en ambiente de Producción en el Centro de Cómputo del Banco, se han establecido claves de acceso a bases de datos, con el objeto de que se pueda leer únicamente la información o datos a los que se está autorizado.
En tal virtud me comprometo a cumplir las políticas de seguridad de datos que tiene implementadas el Banco

5.12.10.1. POLÍTICAS:

1. De acuerdo con la Ley General de Instituciones del Sistema Financiero, la información que guarda la institución está sujeta al Sigilo Bancario.

2. Cualquier mal uso de este permiso para revisar las bases de datos o incumplimiento del procedimiento de seguridad de datos, será objeto de sanciones según las circunstancias. Esta conducta puede motivar el término de la relación laboral.

3. La clave de acceso es personal e intransferible y debe ser cambiada cada 2 semanas por el responsable de la misma.

4. Está terminantemente prohibido que empleados o externos no autorizados accesen directamente a los datos, archivos o librerías para su lectura o modificación. Teniendo la responsabilidad absoluta la persona que suministre la clave de acceso para que se incumpla esta disposición.

5.12.10.2. DECLARACIÓN:

Declaro libre y voluntariamente que conozco las políticas de seguridad de claves de acceso a la base de datos en ambiente de producción del Centro de Cómputo del Banco y declaro que haré buen uso de la clave que me ha sido asignada y acepto el establecimiento de las sanciones que el banco estimare pertinente por el mal uso de

la misma.

Fecha: _____

Nombre: _____

Cargo: _____

Firma: _____

Login: _____

5.12.11. POLÍTICA DE USO DE PENDRIVES

5.12.11.1. OBJETIVO

Regular el uso de pen-drive o flash drive en los equipos de computación de la institución.

Evitar el flujo de información a través de estos dispositivos no autorizados.

5.12.11.2. GENERALIDADES

Los dispositivos removibles siempre van a existir, actualmente se están sacando de circulación las disqueteras pero igualmente se crean otros como los dispositivos en discusión el USB pen-drive o también llamados USB flash disk y tantos otros. En este caso son dispositivos de lectura y grabación como cualquier disquete o disco duro (disco extraíble), con altas capacidades como 4GB y 8GB, totalmente portables, en la mayoría de los casos plug and play.

5.12.11.3. MOTIVO DE LA REGULACIÓN

Realmente es bastante difícil controlar estos dispositivos por cuanto no tienen una identificación como número de serie, lo cual impide controlar su duplicación o identificar los dispositivos autorizados. Tampoco es posible mantener control de red con unicenter sobre los puertos para el uso de estos dispositivos.

5.12.11.4. POLÍTICAS

5.12.11.4.1. DRIVER USB DESHABILITADO

Al solicitar las computadoras los usuarios deben solicitar a través de su Gerente de Area el driver USB habilitado de lo contrario el equipo será entregado con este puerto deshabilitado. Es decir el driver USB estará habilitado solamente por pedido del Gerente de Área. Helpdesk notificará a través de la Hoja de Instalación de Software el estado en que queda el driver. Una copia deberá reposar en los archivos de AyC.

5.12.11.4.2. MONITOREO DE DRIVERS HABILITADOS

Por Unicenter IDS/Helpdesk monitoreará los drivers habilitados y deshabilitados, los casos de drivers habilitados los verificará contra las instalaciones de software, de encontrar casos incongruentes los reportará al usuario y a AyC. Procederá a desahabilitar el puerto de ser necesario.

5.12.11.4.3. PASSWORD, ENCRIPTACIÓN Y RESPALDO DE ARCHIVOS

El usuario deberá asegurarse de grabar sus archivos o data sensitiva con password. El manejo y cuidado del password correrá bajo responsabilidad del usuario final –ver Política de Identificación de Usuarios y contraseñas-.

Dependiendo del alto nivel de sensibilidad debe encriptar sus archivos.

En todos los casos deberá sacar respaldos a medios externos.

5.12.11.4.4. CARPETAS COMPARTIDAS DE RED

El usuario deberá colocar sus archivos o data sensitiva fuera de carpetas compartidas con varios usuarios y deberá analizar y restringir los casos innecesarios a compartir, ver política de Información compartida.

5.12.11.4.5. PEN-DRIVE AUTORIZADO

Están autorizados a usar Pen-drive los Gerentes de Area y División y quienes estas personas autoricen. Las personas autorizadas deben estar comunicadas a la Gerencia de Computación.

5.12.11.5. ADVERTIR A USUARIOS

- ✓ Comunicar o advertir de manera general la existencia de estos dispositivos para mejor cumplimiento de estas disposiciones.
- ✓ El usuario deberá bloquear o apagar su equipo cada vez que se movilice de su puesto.
- ✓ No dar password de desbloqueo o de inicio del equipo a nadie.
- ✓ Cambiar su password periódicamente, recomendado cada dos meses dependiendo de la sensibilidad de sus datos el período debe ser más corto.

5.12.11.6. Política de información compartida

Objetivos :

- Difundir los riesgos de compartir directorios y/o archivos;
- Definir la política y establecer el procedimiento para excepción de la misma.

5.12.11.6.1. RIESGOS DE COMPARTIR DIRECTORIOS Y/O ARCHIVOS

El compartir información a través de la red, se ha convertido en una utilidad riesgosa para la seguridad de nuestra información, equipo y red institucional. Está comprobado que el compartir archivos y/o directorios, es un camino seguro al contagio de virus informáticos que puedan ingresar desde un equipo y desplazarse por la red; además que la información en los computadores es de carácter confidencial y no puede estar libre para cualquier usuario por el riesgo de fuga de información de manera interna o externa a través del correo electrónico o dispositivos de almacenamiento.

Cada persona que labora en el Banco, tiene la responsabilidad de salvaguardar el equipo que se le asigna así como la información que contiene y genere como producto de su trabajo.

5.12.11.6.2. SISTEMA DE DOCUMENTACIÓN

Recomendamos el uso del servicio del sistema de documentación para compartir archivos. Ver Política del Sistema de Documentación y el Manual del Usuario del Sistema de Documentación.

Este servicio tiene como finalidad, atender la necesidad de compartir archivos, dentro de la red del Banco; lo cual no es posible realizar por limitaciones técnicas en la herramienta de correo electrónico ni por procedimiento a través de carpetas compartidas en la red.

EXCEPCIONES

Las excepciones serán dirigidas al Oficial de Seguridad Informática para su evaluación, definición y atención.

Objetivo :

- Establecer políticas y procedimientos claros y ágiles para solicitar cuentas de mail tanto internos como externos, así como acceso la navegación a Internet.
- Definir ciertas recomendaciones para asegurar el buen uso de las herramientas de correo e Internet.

5.12.11.6.3. POLÍTICA DE CORREO ELECTRÓNICO E INTERNET

1. Todos los empleados que por sus responsabilidades y funciones necesiten contactarse vía mail con otras áreas, departamentos u oficinas, podrán solicitar correo interno de acuerdo a los procedimientos que se establecen en este documento.

2. Todos los colaboradores y funcionarios que por sus responsabilidades y funciones necesiten contactarse vía e-mail con compañías y/o organismos externos, podrán solicitar correo externo de acuerdo a los procedimientos que se establecen en este documento.

3. Ciertos cargos ya establecidos tendrán asignado cuentas de correo (interna y/o externa) como parte de las aplicaciones necesarias para el cumplimiento de sus funciones. Esto no los exime de cumplir con los procedimientos que se establecen en este documento.

4. La navegación en Internet sólo se permitirá en casos estrictamente necesarios, y con permisos restringidos a las páginas donde se amerite su uso, a aquellos funcionarios que por sus funciones y responsabilidades, debidamente justificadas, lo soliciten conforme a los procedimientos que se establecen en este documento.

En cualquiera de los casos antes mencionados, se requerirá el pedido formal del servicio a través del formulario establecido para este fin.

5.12.11.6.3.1. PROCEDIMIENTO

Para solicitar cuentas de correos y navegación a internet, los formularios de las solicitudes deberán ser enviados exclusivamente por la Gerencia de Departamento/Oficina al Oficial de Seguridad Informática y/o Gerencia de Productos.

Los formularios deberán venir con la respectiva justificación de este requerimiento llenando todos los campos solicitados en este.

La Gerencia de Productos podrá realizar evaluación de dichas funciones en caso de que lo considere necesario, y procederá a contestar dicha petición, en un lapso no mayor a una semana.

El oficial de Seguridad Informática realizará una evaluación técnica de la petición, esto incluye disponibilidad de licencias, posibilidades de congestión del enlace, etc; y procederá a contestar dicha petición, en un lapso no mayor a una semana.

En caso de ser aprobado, se entregará la aprobación al Administrador de Correos, quien habilitará el servicio en el lapso no mayor a una semana y le comunicará a la Gerencia de Área/Banca que solicitó dicha cuenta de mail.

En caso de no ser aprobado, la Gerencia de Productos y/o el Oficial de Seguridad Informática, comunicará a la Gerencia de Area/Oficina las razones por las cuales fue negada su petición.

5.12.11.7. RECOMENDACIONES

5.12.11.7.1. CORREO ELECTRÓNICO

El correo electrónico o mail (Exchange, Outlook o Webmail) es una herramienta que permite enviar mensajes a través de la red a otros usuarios conectados a la misma. Su uso es similar al correo que conocemos; existe el concepto de oficina de correo (que es un servidor) a donde llegan temporalmente los mensajes para que luego estos viajen al usuario destino. El tiempo en que un mensaje llega de un remitente a uno o más destinatarios en particular es probabilística, es decir que no es inmediato y depende de variables como carga en el servidor de correo y tráfico en la red.

Otra notable característica del mail es que se pueden adjuntar al mensaje enviado, documentos de Word, hojas electrónicas Excel, presentaciones Power Point, etc. **Es importante que NO se envíen documentos extensos y de gran tamaño, ya que esto degrada todo el sistema.**

Dada la gran cantidad de correos entrantes y salientes hacia personas externas al Banco a través de este servicio, se establecerá el **tamaño límite de 250 Kb** en cada mensaje enviado hacia Internet. Si se envía un correo de tamaño superior al especificado, el Administrador de correo enviará un error "No entregable" informándole de que no es posible enviar el mensaje.

A continuación algunos puntos que debe considerar para realizar un buen uso de las herramientas del correo:

- ✓ El correo electrónico es una herramienta confidencial. Por lo tanto será atendido de preferencia solo por el usuario designado. No es adecuado ni ético abrir correos de otras personas, a menos que estemos expresamente autorizados para hacerlo.

- ✓ Una medida de seguridad que existe en el mail es aplicar passwords a sus carpetas personales (archivos .pst). **Estos passwords son responsabilidad del usuario**. **En caso de olvidarlos, perderá su información.** El Administrador del Sistema no tiene incidencia en el uso de sus carpetas personales, por ello se recomienda NO utilizar este tipo de seguridad, salvo criterio personal.

- ✓ Otra medida de seguridad es bloquear el equipo cuando se retira de este por más de cinco minutos. En equipos Windows 2000 puede realizar el bloqueo con las teclas Ctrl + Alt + Supr. Para los equipos con Windows 95 y 98 utilice protectores de pantallas con clave de acuerdo a los estándares establecidos.
- ✓ Las comunicaciones organizacionales, que generalmente se envían a nivel general serán canalizadas a través de Recursos Humanos. Se incluyen por ejemplo mensajes acerca de la excelencia, del comportamiento en general, del trabajo, de las funciones, etc.
- ✓ Es recomendable que realice las siguientes acciones para evitar daño de los archivos de mail:
    - Depurar su información. Mantener pocos mensajes en las carpetas Bandeja de Entrada, Elementos Eliminados, Elementos Enviados y Calendario.
    - Una vez que leyó un mensaje y considera que no necesita guardarlo, deberá borrarlo inmediatamente.
    - Organice sus mensajes creando carpetas.
    - En caso de notar problemas con sus archivos de mensajes, contactarse con Computación para que realicen una revisión.
    - Solicite a Computación (Help Desk, 1911) que le indiquen la frecuencia con la que se debe crear un nuevo archivo para mensajes (*.pst) de acuerdo al volumen de mails que ud. maneja y pídalos de acuerdo a lo recomendado.
    - No envíe ni guarde nada que no quiera hacer público
- ✓ Dude de los mensajes que llegan en inglés o de remitentes que usted no conoce. Es preferible que los borre.
- ✓ Solo abra mensajes concernientes a su trabajo. Elimine aquellos mensajes que incluyen imágenes, juegos, etc. Recuerde que muchos virus vienen a través de este tipo de mensajes y pueden borrar información valiosa de su equipo.
- ✓ Si Ud. es funcionario, no solicite cuentas de usuarios que realmente no necesita.
- ✓ En el caso de hacer un reenvío, no incluir información sin consentimiento de su propietario.
- ✓ Sea precavido en el uso de lenguaje no apropiado en mensajes privados o públicos.
- ✓ Evite el envío de mensajes a todos los usuarios del sistema o grupos de correo, ya que esto ocasiona tráfico en la red y congestionamiento del sistema. Seleccione a las personas interesadas y que REALMENTE están involucradas en el tema.
- ✓ Enfoque un solo tema por mensaje.
- ✓ Sea cauteloso de lo que se dice de los demás. Un mensaje de correo electrónico puede ser reenviado fácilmente.
- ✓ Respete las cadenas de autoridad cuando establezca correspondencia con sus superiores.

- ✓ Determine los usuarios para quiénes su mensaje debe ser leído; no envíe copias de mensajes a otros usuarios innecesariamente.
- ✓ Debe tener en cuenta el verdadero uso del correo, el mail no constituye una herramienta para establecer temas de discusión.
- ✓ Es importante recalcar que todos los mensajes que se envían son privados; para el administrador de correos u otro usuario al que no está dirigido el mensaje es imposible ver el contenido del mismo. Por lo tanto el mensaje perdido se considera irrecuperable.

Todos los correos enviados / recibidos son controlados y supervisados a través de herramientas para este fin. En caso de mal uso de las herramientas de correo, se procederá a establecer las sanciones respectivas.

5.12.11.7.2. Navegación en Internet

La conexión a Internet que posee el Grupo Financiero Banco sirve para muchos propósitos:

- ✓ Permitir la conexión con otras entidades
- ✓ Intercambiar información con otras entidades
- ✓ Investigar sobre múltiples temas de interés

Esta conexión está dada por un canal dedicado de 256 K que proporciona nuestro ISP (Internet Service Provider) que es la empresa Impsat. A través de este canal fluye la información resultante de conectarnos a sitios, que recibimos al hacer consultas, bajar información o transferencia de archivos, la conexión de los clientes al servidor transaccional, etc.

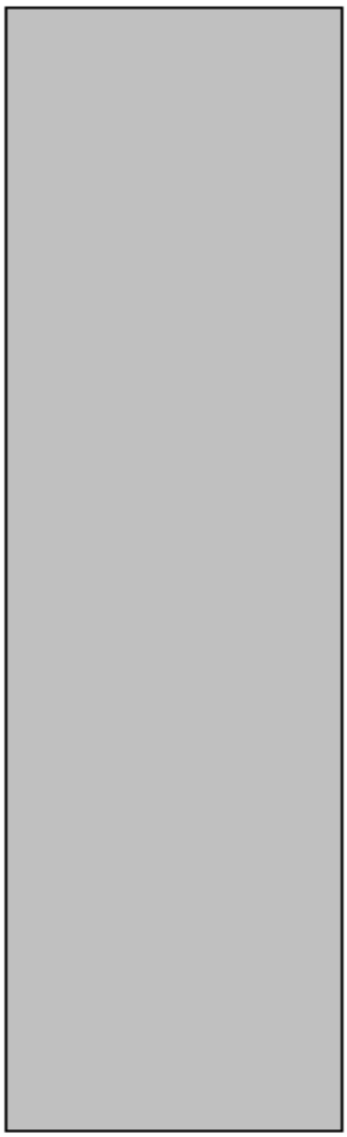
Considere que este canal o acceso a Internet como una herramienta de trabajo que el banco proporciona, por lo tanto no haga un mal uso de ella.

Siendo prioritario para el Grupo Financiero Banco dar un excelente servicio a los clientes del Internet Banking, es necesario que se haga un uso moderado de este canal, tomando las siguientes consideraciones:

- ✓ En horas laborables, accese a Internet solo cuando sea estrictamente necesario y por necesidades de información para sus funciones en el banco. Es decir si necesita información de entidades como el Banco Central, la Superintendencia de Bancos, otros entidades financieras, etc.

- ✓ Si usted necesita realizar una investigación o bajar información de interés particular, puede hacerlo siempre y cuando no sea en horas laborables, es decir a partir de las 18h00 y solo si se encuentra autorizado.
- ✓ El Administrador de la red puede interrumpir su conexión si considera que está haciendo un uso indebido del canal e interfiere con el resto de usuarios que utilizan este recurso.
- ✓ Considere que todo acceso a Internet que usted realiza queda registrado, por lo tanto, en cualquier momento puede generarse un reporte en donde se indique fecha, hora, el computador, usuario de red y sitio al que accesó. Evite conectarse a sitios indebidos.
- ✓ La gerencia de División usará este reporte para llamar la atención a los usuarios que se conecten a sitios que se consideren indebidos y para crear una lista de estos sitios con la finalidad de prohibir su acceso.
- ✓ Mucho software gratuito se encuentra en Internet, siendo uno de los puntos de mayor vulnerabilidad, el proceso de download puede tener algunos riesgos, especialmente si no se conoce bien el servidor desde donde se realice el download. Toda información que necesite ser bajada deberá ser coordinada con el Departamento de Computación. Evite bajar juegos, bitmaps, archivos gif, jpg, sharewares, etc., o cualquier tipo de archivos que no correspondan a sus necesidades de información de trabajo.
- ✓ Tenga en cuenta que un programa instalado en cualquier computador que esté conectado a la red, tiene la capacidad de hacer uso de ella. Al conectarse a Internet, su equipo y por consiguiente la red pueden exponerse a algún ataque poco probable e inesperado de los denominados hackers o de los virus que pueden guardarse en los archivos o programas que usted baja de Internet. Aún cuando se han implementado herramientas de alta seguridad y reconocidas en el mercado que minimizan estos riesgos, evite ser un punto vulnerable para la red del Grupo.

Los sitios a los que ud. accesa por internet son monitoreados y resumidos en informe a su inmediato superior. En caso de mal uso de esta herramienta, se procederá a establecer las sanciones respectivas.



CAPÍTULO 6
CONCLUSIONES
Y RECOMENDACIONES

6. CONCLUSIONES Y RECOMENDACIONES

Esta sección presentará las conclusiones y recomendaciones surgidas durante la elaboración de este proyecto. Se presentará las conclusiones generales y posteriormente se presentarán todas las recomendaciones aplicables al proyecto.

6.1. CONCLUSIONES

Este proyecto es un esfuerzo para lograr el objetivo de obtener la calidad total en el servicio de transaccionalidad vía web para una institución bancaria luego de haber realizado un exhaustivo análisis del entorno de la Seguridad de la Información.

Una de las principales metas de este trabajo es llegar al alcance establecido dentro del tiempo programado; al finiquitar la investigación de este proyecto, tenemos la enorme complacencia de presentar resultados altamente favorables para la implementación y mantenimiento del sitio de comercio electrónico de la institución bancaria de estudio. El principal indicio se verá manifestado en las estadísticas de seguridad obtenidas luego de la puesta en producción del aplicativo.

Creemos viable que se ponga en marcha nuestra propuesta, por lo que es un proyecto de inversión; es por esto que la rentabilidad se adquiere cuando el sitio empiece a ser utilizado por los clientes de la entidad financiera y en el mercado las expectativas como organización serán grandes, ya que el sitio será más utilizado a medida que aumentan el número de usuarios de la banca virtual.

Finalmente tenemos la seguridad que este proyecto tendrá la continuidad y apoyo necesario de la administración de la organización para un futuro llegar a ser certificado bajo la norma ISO-27000 y así la institución tendrá un reconocimiento internacional que es importante en el mundo globalizado actual.

6.2. RECOMENDACIONES

Como recomendaciones se sugiere lo siguiente.

En primer orden recomendamos seguir al pie de la letrea los procedimientos de las políticas creadas a partir de e análisis y gestión de riesgos.

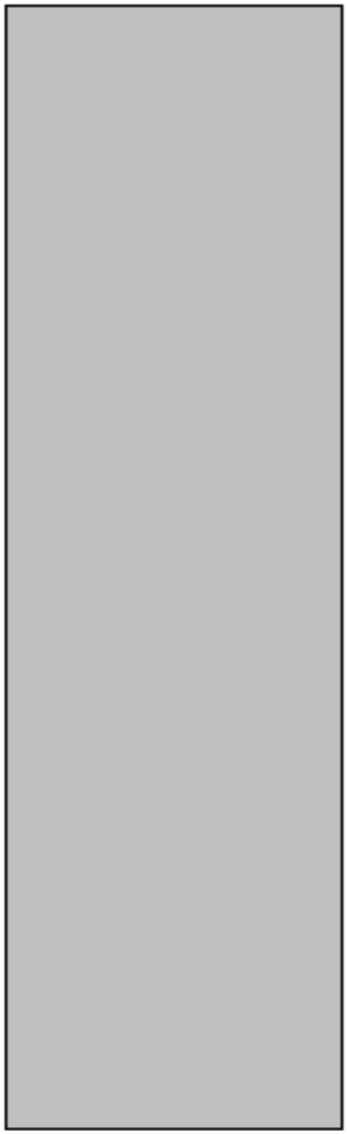
Y como acto seguido se recomienda planificar las revisiones constantes de los controles para la seguridad de la información implementados a través de este proyecto.

Es primordial que nuestro sitio transaccional se afiance a corto, o máximo a mediano plazo en lo que a calidad transaccional se refiere, lo cual se obtiene con la correcta gestión de las áreas implicadas para el correcto funcionamiento de este servicio; recordemos que la calidad va asociada a la seguridad-

Mantener reuniones periódicas para la evaluación de las políticas y actuales procedimientos de seguridad de la información con el objetivo de verificar y actualizar dichos procedimientos para ir cada vez afinando cada vez mas los detalles de seguridad tecnológica; recordemos que la gestión de seguridad de la información es un ciclo.

Una vez posicionado nuestro sitio web transaccional de banca virtual las áreas comerciales en conjunto con las áreas tecnológicas de la institución financiera podrán implementar más transacciones al servicio para el uso de los clientes, con lo cual la imagen de la organización tendrá alto relieve en el mercado ecuatoriano.

Por último, con el mecanismo que está en auge, de supuestos grupos ideólogos revolucionarios, tales como Anonymus, que en realidad no son más que piratas informáticos, recomendamos para la institución contratar un software y hardware de balanceadores de carga `para evitar la denegación del servicio.



ANEXOS

ESTANDAR DE SEGURIDAD PARA WINDOWS 2003 SERVER

VALIDACIONES DE ESTANDAR

Evelyn Mota – Joffre Navarrete	20 – abril– 2011	Marcel León Lafebré	25 – abril– 2011
Aprobación Preliminar (Validación)	**Fecha**	**Aprobación Definitiva**	**Fecha**

ASPECTOS GENERALES

OBJETIVOS

Definir las medidas necesarias para implementar el esquema de seguridad en el ambiente Windows 2003 Server según las políticas de Seguridad de la Información de Banco.

ÁMBITO DE APLICACIÓN

Todos los servidores del entorno de producción de Banco que utilicen Windows 2003 Server como sistema operativo, ya sea en el caso de Controladores de Dominio, servidores Miembros del dominio o servidores Stand-Alone.

NORMATIVA MARCO (NORMATIVAS SUPERIOR DE REFERENCIA)

PC.POL.1- Política General de Seguridad de la Información

NORMATIVA DEROGADA

Ninguna.

OTRAS NORMATIVAS ASOCIADAS

Ninguna.

VIGENCIA

Este estándar de configuración entrará en rigor a partir del 1 de Noviembre de 2007.

DISPOSICIONES GENERALES Y TRANSITORIAS

Este estándar de configuración deberá ser revisado anualmente por el Área de Seguridad de la Información de Banco. Los resultados de la revisión, y los cambios que se sucedan, serán reportados al Comité de Seguridad de la Información y comunicados a los involucrados antes de ser implementados.

La falta de cumplimiento de las definiciones descriptas en el presente procedimiento, estará sujeta a las sanciones disciplinarias que amerite cada caso.

ROLES Y RESPONSABILIDADES

ÁREA DE SEGURIDAD DE INFORMACIÓN

Responsable de Seguridad de la Información: Tendrá a su cargo el mantenimiento del presente estándar, junto con las tareas de verificación del cumplimiento del mismo.

GERENCIA DE SISTEMAS

Gerente de Sistemas: Deberá garantizar que los funcionarios del área de sistemas, encargados de realizar la administración de la plataforma Windows, implementen los estándares de configuración definidos en forma efectiva y oportuna.

Administradores y Operadores de plataforma Windows 2003: Serán encargados de implementar el presente estándar, siguiendo los lineamientos y tareas mencionadas en el mismo. Asimismo, deberán informar al Gerente de Sistemas sobre las configuraciones de seguridad que no puedan ser implementadas por restricciones técnicas y/o de negocio, las cuales deberán quedar adecuadamente documentadas.

CONFIGURACIÓN DE SEGURIDAD PARA EL HARDWARE DE SERVIDORES

OBJETIVO

Definir la configuración de seguridad de los componentes de hardware de los servidores de Banco que operarán con Windows 2003 como sistema operativo de base.

ACCESO FÍSICO A SERVIDORES SENSITIVOS

El acceso físico a servidores sensitivos como ser los controladores de dominio o los servidores que soportan la información crítica de negocio, deberá estar adecuadamente restringido al responsable de seguridad, al administrador del entorno Windows y a los operadores de los servidores de Banco.

UBICACIÓN DE CONTRASEÑAS PARA CONFIGURACIÓN

El acceso a la configuración de hardware de cada servidor deberá estar restringido al responsable de seguridad y al administrador del entorno Windows, mediante una contraseña específica y común para todos los equipos, conocida exclusivamente por dicho personal y resguardada en sobre cerrado de acuerdo al Procedimiento de Administración de Usuarios de Máximos Privilegios.

UTILIZACIÓN DE CONTRASEÑAS DE ARRANQUE

Los servidores no deberán tener asignada una contraseña de encendido.

En caso de ser necesaria la utilización de una contraseña de encendido, deberá consultarse al responsable de seguridad, quien deberá formalizar su conformidad justificando la necesidad de utilizar este mecanismo de protección.

ARRANQUE DE SISTEMAS

En la configuración de hardware de los servidores deberá especificarse como única unidad de arranque, el disco rígido donde se encuentre instalado el sistema operativo, impidiendo de esta manera la inicialización del mismo desde un disquete o CD.

CONEXIONES A DISPOSITIVOS DE HARDWARE Y PERIFÉRICOS

Se deberá deshabilitar toda conexión a dispositivos que no posean una función específica definida por el área de Sistemas, tales como puertos serie, paralelo, USB, etc.

CONEXIONES A DISPOSITIVOS DE HARDWARE Y PERÍFERICOS

Se deberá establecer una función principal por servidor, se deshabilitaran los servicios y protocolos innecesarios e inseguros que no sean necesarios para la función del mismo

CONFIGURACIÓN GENERAL DE DOMINIOS

OBJETIVO

Presentar la configuración del esquema lógico y físico adoptado por Banco para brindar, proteger y administrar el servicio de directorios "Active Directory - Directory Services" y todos los recursos asociados al mismo.

ESTRUCTURA LÓGICA DE ACTIVE DIRECTORY

ESTRUCTURA DE FOREST Y ESPACIO DE NOMBRES

El servicio de directorios Windows de Banco está estructurado en un único Forest conformado por un único Dominio, con el fin de facilitar la administración y disminuir los costos asociados de hardware.

El único dominio existente (Forest Root Domain) deberá responder al nombre .fin.ec según se indica en el esquema siguiente:

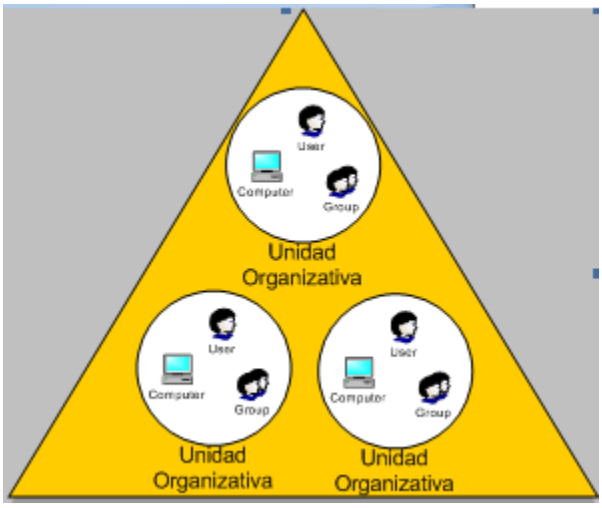


Figura 1: Estructura Forest

INTEGRACIÓN DE NUEVOS DOMINIOS Y RELACIONES DE CONFIANZA

Ante la necesidad de incorporación de nuevas empresas al esquema de dominios de Banco, para las cuales se defina que adoptarán el carácter de controladas desde el punto de vista de la administración de sistemas, y que además posean dominios propios preexistentes, se evaluará la posibilidad de migrar los servidores al dominio .fin.ec como uno o mas sitios nuevos.

En caso de no ser posible la migración mencionada y de ser necesario mantener el dominio de dicha empresa, el mismo se integrará al Forest mediante el establecimiento de una relación de confianza "external" unidireccional con el dominio .fin.ec siempre que sea posible.

Tanto el establecimiento de nuevas relaciones de confianza con dominios de otras empresas y/o sitios, como las modificaciones al esquema de Active Directory (Schema), deberán ser debidamente analizadas y autorizadas por el Responsable de Seguridad.
Todas las tareas de análisis y aprobación deberán ser formalizadas e impulsarán la actualización del presente estándar de configuración siempre que sea necesario.

ESTRUCTURA DE UNIDADES ORGANIZATIVAS "OUs"

El esquema de unidades organizativas de Banco para el dominio .fin.ec, responde a la estructura real de unidades de negocio ya que dicho modelo se adecua mejor a las necesidades administrativas y de aplicación de políticas de grupos de Banco.

Dicho esquema se encuentra dividido en cuatro niveles bien definidos, el primero de los cuales contendrá cuatro "Unidades Organizativas (OUs)" básicas a saber:

- ✓ Una OU general denominada " " creada a los efectos de contener los objetos lógicos que representan a las áreas de negocio p.e: usuarios, estaciones de trabajo, impresoras, etc. Esto se realiza fundamentalmente por una cuestión organizativa, a los efectos de obtener una consola administrativa con una estructura raíz que no sea demasiado extensa;

- ✓ Una OU para alojar a los controladores de dominio llamada "Domain Controllers";

- ✓ Una OU denominada "Member Servers", la cual será utilizada para agrupar a todos los servidores Windows 2000 miembros del dominio, la cual a su vez contendrá OUs de menor jerarquía que responderán a los distintos roles que cumplen los servidores.

- ✓ Una OU denominada "Member Servers 2003", la cual será utilizada para agrupar a todos los servidores Windows 2003 miembros del dominio, la cual a su vez contendrá OUs de menor jerarquía que responderán a los distintos roles que cumplen los servidores.

Asimismo, en el segundo nivel de la OU se encontrarán las unidades organizativas que representan a cada área de negocio, las cuales en su tercer nivel podrán contener subdivisiones representando a cada sector del área o finalmente los objetos que representan a las mismas según se indica en el diagrama siguiente:

Diseño de Unidades Organizativas de Banco Bolivariano

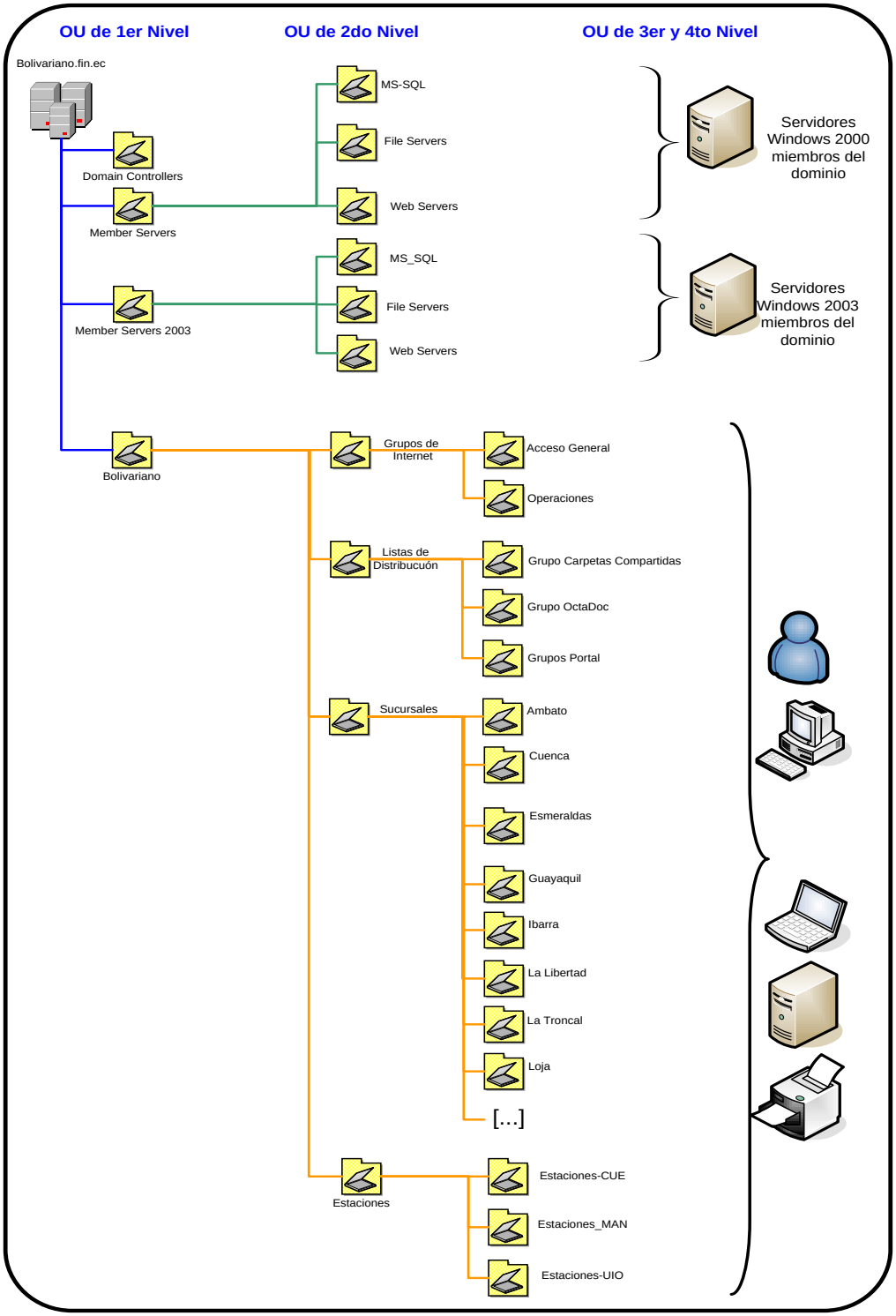


Figura 2: **Estructura de unidades organizativas**

DEFINICIÓN DE OBJETOS DEL SERVICIO DE DIRECTORIOS Y ASIGNACIÓN DE PERMISOS

Las cuentas de usuarios, grupos, equipos e impresoras serán definidas en el dominio .fin.ec e incluidas en la unidad organizativa del sitio al que correspondan.

La asignación de permisos de acceso a usuarios finales en producción, se hará a través de la inclusión de dichos usuarios a grupos globales y de la asignación de grupos globales a grupos locales sobre los cuales se aplicarán los permisos efectivos. El esquema operativo asociado se presenta en el diagrama siguiente:

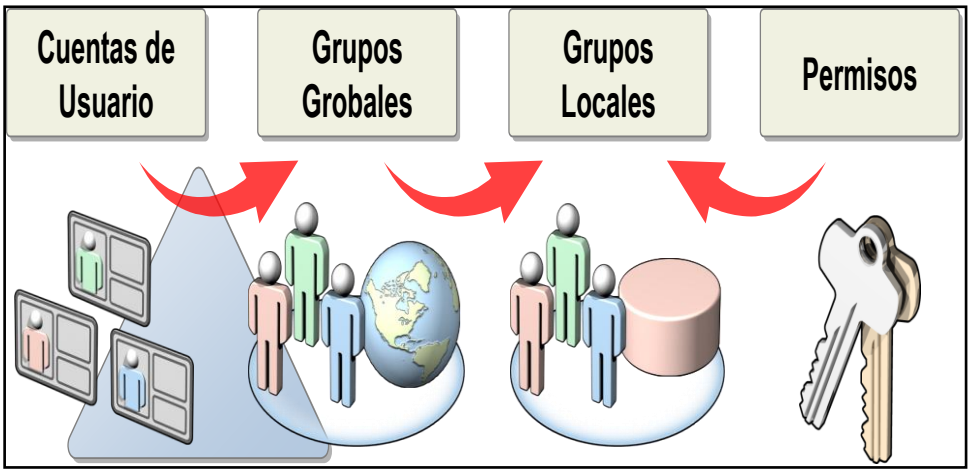


Figura 3: Objetos del servicio de directorios y asignación de permisos

ESTRUCTURA FÍSICA DE ACTIVE DIRECTORY

La topología de sitios de Active Directory es la representación lógica de la red física y es diseñada primariamente para controlar los siguientes aspectos:
Tráfico de replicación: Cuando un cambio ocurre en Active Directory, los sitios son usados para controlar cómo y cuando el cambio es replicado a un controlador de dominio en otro sitio.

Autenticación del usuario: Cuando un usuario se autentica, Windows 2003 busca en primera instancia un controlador de dominio que este en el mismo sitio en donde esta la estación de trabajo del usuario.

File Replication Service (FRS): FRS es un servicio usado para replicar el contenido del directorio SYSVOL, el cual incluye scripts de logon y logoff, Group Policy settings y políticas del sistema para clientes W9x y WNT. FRS usa la topología de sitios para determinar la topología de replicación.

Distributed File System (DFS): Cuando una carpeta compartida tiene múltiples localizaciones, un usuario será direccionado a un servidor en su propio sitio, si existe, reduciendo el tráfico a través de los vínculos.

OTRAS APLICACIONES ACTIVE DIRECTORY AWARE

ESTRUCTURA DE SITIOS Y LINKS

Sitios (Sites): Se entiende por "Site" a todo conjunto de subredes conectadas a alta velocidad (10Mbps o más) que cuentan al menos con un Controlador de Dominio. De acuerdo con ello, la estructura de "Sites" de Banco se definirá teniendo en cuenta la distribución geográfica del equipamiento y la cantidad de clientes que hacen uso de los servicios desde dichas locaciones.

Vínculos entre sitios (Site Links): Los "Site Links" se utilizan para unir dos "Sites", y de este modo, configurar la replicación óptima entre los mismos. La definición y creación de "Site Links" responderá al esquema de "Sites" existentes.

A continuación se presenta un diagrama que esquematiza la situación actual:

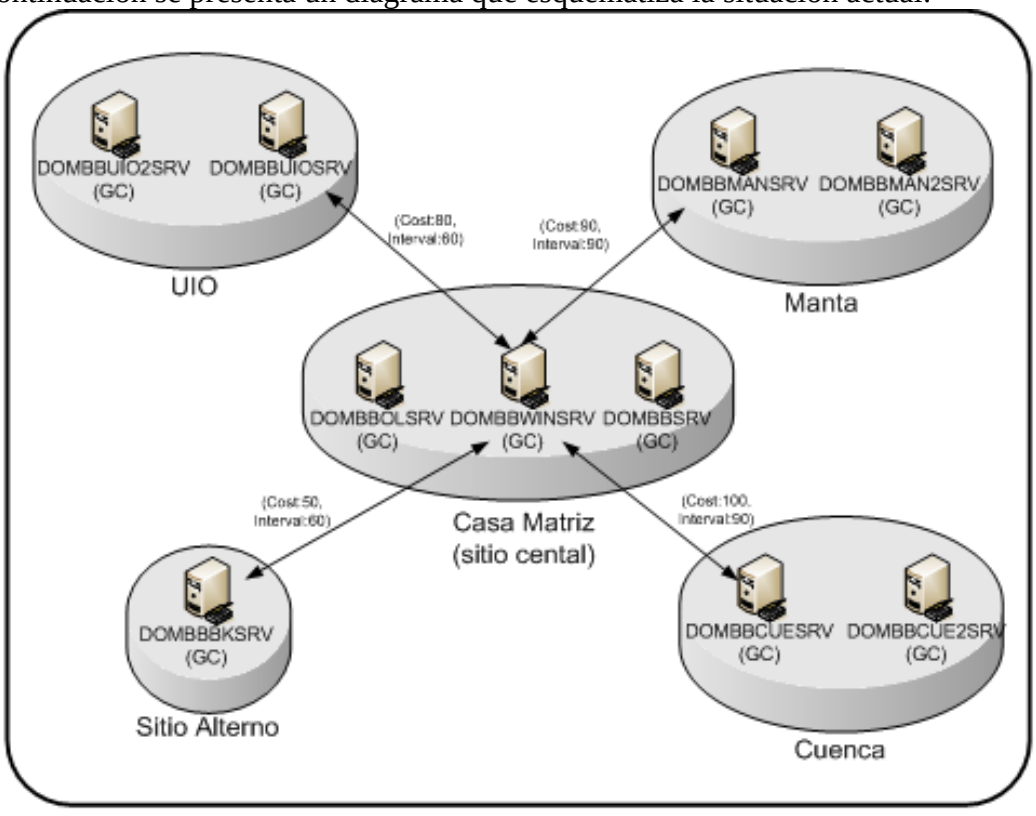


Figura 4: Esquema de Sitios de Active Directory

PRINCIPALES SERVICIOS DE INFRAESTRUCTURA (CORE SERVICE)

Se define como "Core Services" a los servicios de infraestructura principales que hacen a la arquitectura de Windows 2003 y Active Directory. Entre estos servicios se encuentran: WINS y DNS, como así también servicios intrínsecos a Active Directory como los Flexible Single Master Roles, en adelante FSMO Roles, y como se localizan y se distribuyen los Controladores de Dominio.

UBICACIÓN DE CONTROLES DE DOMINIO Y CATÁLOGOS GLOBALES

Para la determinación de la ubicación y cantidad de Controladores de Dominio requeridos para asegurar la operatividad del servicio de autenticación y autorización, se deberán seguir las siguientes directivas:

Un controlador para el dominio .fin.ec en el sitio central, para centralizar los servicios de autenticación y autorización de usuarios. Dicho controlador de dominio deberá cumplir los siguientes roles:

- ✓ Schema Master
- ✓ Domain Naming Master
- ✓ PDC Emulator
- ✓ RID Master
- ✓ Infraestructure Master
- ✓ Global Catalog

Un controlador para el dominio .fin.ec en el sitio central, para redundancia, el cual deberá cumplir el rol de "Global Catalog"

Un controlador de dominio por cada locación física con más de 50 usuarios, a fin de agilizar el inicio de sesión de los usuarios. Dichos controladores de dominio deberían a su vez cumplir el rol de "Global Catalog" en aquellos sitios que cuenten con más de 100 usuarios activos.

Adicionalmente siempre deberá tenerse en consideración el ancho de banda del vínculo de comunicaciones y la cantidad de usuarios, para asegurar que la replicación del esquema Active Directory genera menos tráfico en la red de datos que los pedidos de autenticación de los usuarios remotos.

DNS (DOMAIN NAME SYSTEM)

En el ámbito operativo de la Entidad se pueden diferenciar dos entornos diferentes de DNS:

- ✓ DNS en ambiente cerrado: Son aquellos servidores de DNS que soportan a los dominios internos de Windows 2003 de Banco y que prestan servicio a clientes del dominio para la localización de los controladores de dominio, resolver nombres y registrar dinámicamente su nombre de estación de trabajo en la red.

- ✓ DNS con presencia en Internet: No se utilizarán servidores DNS con presencia en Internet para la resolución de nombres externos. En su reemplazo, se utilizarán zonas de Forward Lookup, a través de las cuales se referenciará a los DNS del proveedor para resolver los nombres de dominios externos.

DNS (DOMAIN NAME SYSTEM) EN AMBIENTE CERRADO

El servicio de DNS interno de Windows 2003 Server para el dominio .fin.ec, será configurado como zona Active Directory integrated y para que acepte registraciones vía Secure Updates. De esta forma las "zonas de información" serán guardadas, replicadas y aseguradas en el esquema Active Directory y permitirá que el servicio de DNS esté disponible a pesar de que exista algún problema en los vínculos de comunicaciones.

ACTUALIZACIONES DINÁMICAS

Las actualizaciones dinámicas de registros habilitan a los clientes de DNS a registrar su nombre y dirección IP en forma automática, al iniciar el equipo o cuando la dirección IP cambia. Las actualizaciones dinámicas estarán habilitadas únicamente (de forma segura), en aquellos servidores en los que las zonas sean Active Directory integrated.

TRANSFERENCIA DE ZONAS

Dado que la transferencia de zonas permite "mover" todos los registros de una zona DNS particular entre servidores, las zonas de Forward Lookup y Reverse Lookup de los dominios deben configurarse para que estas transferencias se efectúen solamente a servidores autorizados, entre los cuales se deberán encontrar solamente los controladores de dominio de Banco .En caso de ser necesaria la transferencia de zona en servidores de DNS instalados como Stand-Alone, se deberá analizar cada caso en particular previo a especificar las direcciones IP de dichos servidores en la lista de servidores habilitados.

CONFIGURACIÓN DE CLIENTES

Los clientes serán configurados manualmente, de manera que registren y utilicen los servicios de los DNS designados.

SERVIDORES DNS INTERNOS

Los servidores de DNS serán configurados para que su DNS Primario sean ellos mismos y como regla general se ubicará un DNS en cada controlador de dominio, de manera de contar con resolución de nombres en el caso de corte de comunicaciones entre los sitios secundarios y el sitio central.

Los servidores con servicio DNS son los siguientes:

- ✓ *DOMBBSRV:* Dirección IP: 172.17.2.55 (Controlador de Dominio primario de Casa Matriz)

- ✓ *DOMBBWINSRV:* Dirección IP: 172.17.2.10 (Controlador de Dominio secundario de Casa Matriz)

Asimismo, las zonas de DNS existentes para Active Directory son:

- ✓ bce.fin.ec
- ✓ bkuxprod
- ✓ .com
- ✓ .corp
- ✓ .fin.ec
- ✓ creditreport.ec
- ✓ des. .corp
- ✓ ecuagiros.com
- ✓ faxmaker.com

WINS – WINDOWS INTERNET NAMING SERVICE

Actualmente existe un modelo de resolución de nombres basado principalmente en DNS y apoyado sobre WINS como método secundario, el cual se deberá conservar hasta tanto no existan clientes pre-Windows 2000 los cuales requieran resolución NETBIOS.

La estructura de WINS se encontrará centralizada en Casa Matriz y de ser necesario se deberá evaluar la instalación de un servicio WINS por sitio, a fin de proporcionar resolución de nombres NetBIOS en el caso de corte de comunicaciones.
Al igual que en el caso del servicio DNS, los clientes serán configurados manualmente.

ESQUEMA DE SEGURIDAD EN ACTIVE DIRECTORY

OBJETIVO

Presentar el esquema de seguridad asociado al servicio de directorios "Active Directory – Directory Services" y los mecanismos utilizados para implementar el mismo.

POLITÍCAS DE GRUPO (GPO)

A fin de agilizar las tareas de administración de la seguridad y para garantizar que todos los objetos que forman parte del servicio de directorios Windows de Banco cumplan con los lineamientos de seguridad definidos, Banco utiliza políticas de grupo o GPOs. Así mismo, la utilización de GPOs extiende el concepto de las antiguas "System Policies" de NT y brinda las siguientes funcionalidades:

- ✓ Implementación de configuraciones de seguridad, derechos de usuarios y políticas de auditoría.
- ✓ Administración del ambiente de servidores y estaciones de trabajo.
- ✓ Distribución y configuración de aplicaciones.
- ✓ Procesamiento de scripts de autenticación como ser "Logon / Logoff / Start-up / Shutdown".
- ✓ Redireccionamiento de carpetas y utilización de carpetas fuera de línea, entre otros.

Los parámetros de configuración que se definen en las políticas de grupo de Windows 2003 son utilizados para controlar los elementos de los entornos de clientes y servidores Windows 2000/2003/XP y pueden ser creados para utilizarse en los distintos niveles del diseño de unidades organizativas, brindando de esta manera flexibilidad y granularidad para implementar configuraciones y políticas de seguridad de acuerdo al esquema jerárquico que se describe en el gráfico siguiente:

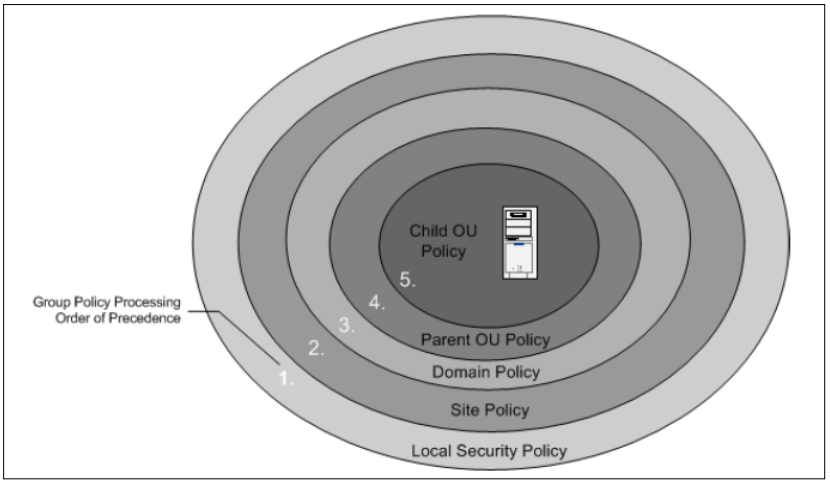


Figura 5: GPO

Actualmente el esquema de las principales políticas de grupo de Banco, las cuales establecen los lineamientos básicos de seguridad, está compuesto por las siguientes políticas de seguridad, estas son:

- ✓ Política general para el dominio.
- ✓ Política para controladores de dominio.
- ✓ Política para servidores miembro y stand alone Windows 2003.
- ✓ Política para servidores miembro y stand alone Windows 2000.
- ✓ Política de usuarios del dominio.
- ✓ Política de estaciones de trabajo windows 2000/XP.
- ✓ Políticas de replicación del servicio WSUS (aplicadas a nivel de Site).

Nota: Cabe destacar que en la práctica también se podrán aplicar políticas para casos particulares (tales como bloqueo de puertos USB, políticas de distribución de software, etc) a nivel de las unidades organizativas de tercer o cuarto nivel, siempre que las mismas sean más restrictivas que las políticas de los niveles superiores.

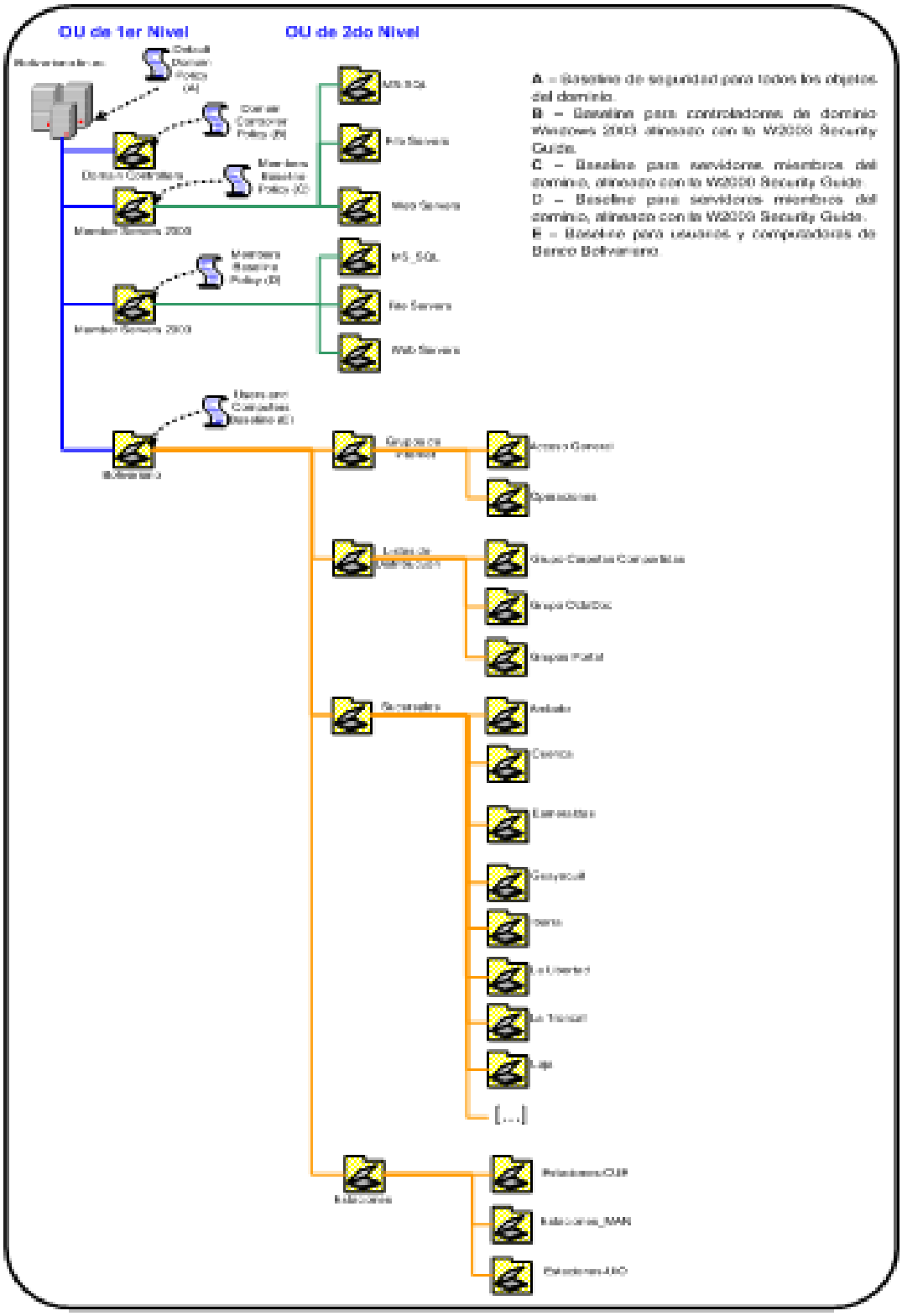


Figura 6: Diseño de Políticas de Grupo

Complementariamente, cabe señalar que cada grupo de servidores miembro que compartan un rol (Por ejemplo servidores web IIS, servidores de bases de datos SQL,

etc), tendrán a su vez sus características específicas de configuración y en consecuencia sus políticas de grupo asociadas. Dichas políticas deberán ser aplicadas a nivel de la OU correspondiente y los valores de configuración específicos deberán respetar los estándares de configuración de las plataformas involucradas.

Finalmente, para los casos en los que los servidores sean Stand-Alone, la aplicación de las políticas de configuración deberá ser efectuada en forma local, según los lineamientos establecidos en el presente estándar de seguridad y/o en los estándares asociados al rol específico del servidor.

POLÍTICAS DE CUENTAS

A través de la correcta configuración y aplicación de las políticas de cuentas se podrán implementar las directivas de seguridad definidas por Banco para las contraseñas utilizadas por los usuarios.

DIRECTIVAS DE CUENTAS- POLÍTICAS DE CONTRASEÑAS

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
Enforce password history	Not Defined	3 passwords	3 passwords
Maximum password age	Not Defined	90 days	90 days
Minimum password age	Not Defined	1 days	1 days
Minimum password length	Not Defined	8 characters	8 characters
Passwords must meet complexity requirements	Not Defined	Enabled	Enabled
Store password using reversible encryption for all users in the domain	Not Defined	Disabled	Disabled

Tabla 1: Políticas de Contraseñas

DIRECTIVAS DE CUENTAS – POLÍTICAS DE BLOQUEO DE CUENTAS

Directiva	**Política de Dominio**	**Política de DC**	**Servidores Miembro y Stand-Alone**
Account lockout duration	Not Defined	0 minutes	0 minutes Para Stand-Alone: Not Applicable
Account lockout threshold	Not Defined	3 invalid login attempts	3 invalid login attempts Para Stand-Alone: 0 invalid login attempts
Reset account lockout counter after	Not Defined	30 minutes	30 minutes Para Stand-Alone: 0 minutes

Tabla 2: Políticas de Bloqueo de Cuentas

DIRECTIVAS DE CUENTAS – POLÍTICAS DE KERBEROS

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
Enforce user logon restrictions	Not Defined	Not Defined	Not Defined
Maximum lifetime for service ticket	Not Defined	Not Defined	Not Defined
Maximum lifetime for user ticket	Not Defined	Not Defined	Not Defined
Maximum lifetime for user ticket renewal	Not Defined	Not Defined	Not Defined
Maximum tolerance for computer clock synchronization	Not Defined	Not Defined	Not Defined

Tabla 3: Políticas de Kerberos

AUDITORIA DE EVENTOS Y OBJETOS

Se deberán configurar los parámetros de auditoría a nivel de sistema operativo, de acuerdo a lo establecido en el Estándar de configuración de clientes para el registro de LOGs de Banco.

DERECHOS DE USUARIOS

La posibilidad de definir los derechos de los usuarios en el sistema es un gran aporte a la seguridad del esquema Active Directory. Los valores definidos por Banco para implementar en servidores se detallan a continuación:

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
Access this computer from the network	Not Defined	- Administrators - Administradores - IDS - Enterprise Domain Controllers - Enterprise Admins	Se debe analizar y documentar en un anexo la configuración en función de cada rol. Administrators Authenticated Users Backup Operators Power Users Cuando se trate de un servidor con IIS 6.0. ASPNET Iusr_Máquina Iwam_Máquina Cuando se trate de un servidor con IIS 5.0 y 6.0. Users
Act as part of the operating system	Not Defined	- No one	- No one
1Add workstations to domain **(P)**	Not Defined	- Administrators - Administradores - IDS - Server operators	- No one

Adjust memory quotas for a process	Not Defined	- Administrators - LOCAL SERVICE - NETWORK SERVICE	- Administrators - LOCAL SERVICE - NETWORK SERVICE Cuando se trate de un servidor con IIS 6.0. - Iwam_máquina
Allow logon on locally	Not Defined	- Administrators - Administradores - IDS - operador	- Administrators - Power Users - Backup Opertors Cuando se trate de un servidor con IIS 6.0. - IUSR_Máquina
2Allow logon Through Terminal Services **(P)**	Not Defined	- Administrators	- Administrators
3Back up files and directories **(P)**	Not Defined	-Administrators - Backup Operators	- Administrators - Backup Operators
Bypass traverse checking	Not Defined	- Administrators - Authenticated Users	- Administrators - Backup Operators - Power Users - Authenticated Users Cuando se trate de un servidor con IIS 6.0. - IIS_WPG
4Change the system time**(P)**	Not Defined	- Administrators - Local Service	- Administrators - Local Service
5Create a pagefile **(P)**	Not Defined	- Administrators	- Administrators
6Create a token object **(P)**	Not Defined	- No one	- No one
7Create global objects **(P)**	Not Defined	- Administrators - SERVICE	- Administrators - SERVICE
8Create permanent	Not Defined	- No one	- No one

shared objects **(P)**			
9Debug programs **(P)**	Not Defined	- Administrators	- Administrators
10Deny access to this computer from the network **(P)**	Not Defined	- SUPPORT_388945a0	- SUPPORT_388945a0
11Deny logon as a batch job **(P)** ***** En la plantilla: AseguramientoBase Plus sin Disco w2k3-v10-IIS solamente se incluya a Support_388945a0	Not Defined	- Guests - Support_388945a0	- Guests - Support_388945a0
12Deny logon as a service **(P)**	Not Defined	- No one	- No one
13Deny logon locally**(P)**	- user_service	- SUPPORT_388945a0	- SUPPORT_388945a0 - Se pueden adicionar más usuarios que puedan definirse. Cuando se trate de un servidor con IIS 6.0. - ASPNET
14Deny log on Through Terminal Services**(P)**	Not Defined	- Guests	- Guests - Se pueden adicionar más usuarios que puedan definirse.
15Enable computer and user accounts to be trusted for delegation**(P)**	Not Defined	- Administrators	- nadie
16Force shutdown from a remote system**(P)**	Not Defined	- Administrators	- Administrators

17Generate security audits**(P)**	Not Defined	- Local Service - Network Service	- Local Service - Network Service
Impersonate a client after authentication	Not Defined	- Administrators - SERVICE	- Administrators - SERVICE Cuando se trate de un servidor con IIS 6.0. - ASPNET - IIS_WPG
18Increase scheduling priority**(P)**	Not Defined	- Administrators	- Administrators
19Load and unload device drivers**(P)**	Not Defined	- Administrators	- Administrators
20Lock pages in memory**(P)** ***** En la plantilla AseguramientoBase Plus sin Disco w2k3-v10-SQL2000 se encuentra con Not Defined debe ser revisado por Servidor.	Not Defined	- No one	- No one
Log on as a batch job	Not Defined	Se debe analizar y documentar en un anexo la configuración en función de cada rol.	Se debe analizar y documentar en un anexo la configuración en función de cada rol. Local Service Cuando se trate de un servidor con IIS 6.0. ASPNET IIS_WPG Iusr_maquina Iwam_maquina

Log on as a service	Not Defined	Se debe analizar y documentar en un anexo la configuración en función de cada rol.	Se debe analizar y documentar en un anexo la configuración en función de cada rol. Network Service Cuando se trate de un servidor con IIS 6.0. - ASPNET
21Manage auditing and security log **(P)**	Not Defined	- Administrators - Administradores - IDS	- Administrators - Administradores - IDS
22Modify firmware environment values **(P)**	Not Defined	- Administrators	- Administrators
23Perform Volume Maintenance Tasks **(P)**	Not Defined	- Administrators	- Administrators
24Profile single process **(P)**	Not Defined	- Administrators	- Administrators
25Profile system performance **(P)**	Not Defined	- Administrators	- Administrators
26Remove computer from docking station **(P)**	Not Defined	- Administrators	- No one
Replace a process level token	Not Defined	- Local Service - Network Service	- Local Service - Network Service Cuando se trate de un servidor con IIS 6.0: -Iwam_maquina
27Restore files and directories **(P)**	Not Defined	- Administrators	- Administrators
28Shut down the system **(P)**	Not Defined	- Administrators	- Administrators
29Synchronize directory service data **(P)**	Not Defined	- No one	- No one

30Take ownership of files or other objects **(P)**	Not Defined	- Administrators	- Administrators

Tabla 4: Derechos de Usuarios

DERECHOS DE USUARIOS ESPECIALES ASIGNADOS A CUENTAS DE SERVICIO

En aquellos servidores que presenten aplicaciones que requieran el uso de cuentas de servicio, se deberá además otorgar derechos adicionales a dichas cuentas en función del servicio instalado.

Los casos más relevantes se detallan en la siguiente tabla:

Servicio/Aplicación	Grupo de cuentas	Derechos especiales
SQL Server	ADMIN_SQL	log on as a service act as a part of the operating system replace process level token Adjust memory quotas for a process logon as a batch job
Exchange Server	ADMIN_EXC	log on as a service Back up files and directories
Servicios de Backup	ADMIN_BKP	Act as part of the operating system Back up files and directories Restore files and directories
Internet Information Services	ADMIN_IIS	Access this computer from network Logon localy

Tabla 5: Políticas de Bloqueo de Cuentas

Nota: El otorgamiento de derechos a nuevas aplicaciones o servicios deberá ser analizado y aprobado por el Responsable de Seguridad de Banco.

OPCIONES DE SEGURIDAD

Las opciones de seguridad que deberán aplicarse a los servidores principales de la entidad se detallan a continuación:

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
1Accounts: Administrator account status**(P)**	Not Defined	Enabled	Enabled Para stand-alone: Not Applicable
2Accounts: Guest account status**(P)**	Not Defined	Disabled	Disabled Para stand-alone: Not Applicable
3Accounts: Limit local account use of blank passwords to console logon only **(P)**	Not Defined	Enabled	Enabled
Accounts: Rename administrator account	Not Defined	XXXXXX	Not Defined
4Accounts: Rename guest account**(P)**	Not defined	xxxxxx	Not Defined
5Audit: Audit the access of global system objects**(P)**	Not Defined	Disabled	Disabled
6Audit: Audit the use of Backup and Restore privilege**(P)**	Not Defined	Disabled	Disabled
7Audit: Shut down system immediately if unable to log security audits**(P)**	Disabled	Disabled	Disabled
8DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax**(P)**	Not Defined	Not Defined	Not Defined

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
9DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax**(P)**	Not Defined	Not Defined	Not Defined
10Devices: Allow undock without having to log on **(P)**	Not Defined	Enabled	Enabled
11Devices: Allowed to format and eject removable media **(P)**	Not Defined	Administrators Power Users	Administrators
12Devices: Prevent users from installing printer drivers **(P)**	Disabled	Enabled	Enabled
13Devices: Restrict CD-ROM access to locally logged-on user only **(P)**	Not Defined	Enabled	Enabled
14Devices: Restrict floppy access to locally logged-on user only **(P)**	Not Defined	Enabled	Enabled
15Devices: Unsigned driver installation behavior **(P)**	Warn but allow installation	Warn but allow installation	Warn but allow installation
16DC: Allow server operators to schedule tasks **(P)**	Not Defined	Disabled	Not Defined
17DC: LDAP server signing requirements **(P)**	Not Defined	Not Defined	Not Defined
18DC: Refuse machine account password changes **(P)**	Not Defined	Disabled	Disabled
20Domain member: Digitally encrypt or sign secure channel data (always)	Not Defined	Disabled	Enabled
21Domain member: Digitally encrypt secure channel data	Not Defined	Enabled	Enabled

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
(when possible) **(P)**			
22Domain member: Digitally sign secure channel data (when possible) **(P)**	Not Defined	Enabled	Enabled
19Domain member: Disable machine account password changes **(P)**	Not Defined	Disabled	Disabled
23Domain member: Maximum machine account password age **(P)**	Not Defined	Not Defined	Not Defined Para stand alone: 0
24Domain member: Require strong (Windows 2000 or later) session key **(P)**	Not Defined	Not Defined	Not Defined
25Interactive logon: Display user information when the session is locked **(P)**	Not Defined	Not Defined	Not Defined
26Interactive logon: Do not display last user name **(P)**	Enabled	Enabled	Enabled
27Interactive logon: Do not require CTRL+ALT+DEL **(P)**	Disabled	Disabled	Disabled
29Interactive logon: Message text for users attempting to log on **(P)**	El uso de este sistema está restringido solamente a personal autorizado. Todo otro uso del mismo será penado de acuerdo a las políticas vigentes de la Entidad. Ante cualquier	El uso de este sistema está restringido solamente a personal autorizado. Todo otro uso del mismo será penado de acuerdo a las políticas vigentes de la Entidad. Ante cualquier	El uso de este sistema está restringido solamente a personal autorizado. Todo otro uso del mismo será penado de acuerdo a las políticas vigentes de la Entidad. Ante

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
	inconveniente comunicarse con Seguridad Informática. Muchas gracias	inconveniente comunicarse con Seguridad Informática. Muchas gracias	cualquier inconveniente comunicarse con Seguridad Informática. Muchas gracias
30Interactive logon: Message title for users attempting to log on **(P)**	ADVERTENCIA	ADVERTENCIA	ADVERTENCIA
31 Interactive logon: Number of previous logons to cache(in case domain controller is not available **(P)**	3 logons	Not Defined	2 logons Para Stand Alone:0
28Interactive logon: Prompt user to change password before expiration **(P)**	7 días	7 días	7 días
32Interactive logon: Require Domain Controller authentication to unlock workstation **(P)**	Not Defined	Enabled	Enabled
33Interactive logon: Require smart card **(P)**	Not Defined	Not Defined	Not Defined
34Interactive logon: Smart card removal behavior **(P)**	Not Defined	Not Defined	Not Defined
36Microsoft network client: Digitally sign communications (always) **(P)**	Not Defined	Disabled	Disabled
37Microsoft network client: Digitally sign communications (if server agrees) **(P)**	Not Defined	Enabled	Enabled
35Microsoft network client: Send unencrypted password	Not Defined	Disabled	Disabled

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
to third-party SMB servers **(P)**			
38Microsoft network server: Amount of idle time required before suspending session **(P)**	Not Defined	15 minutos	15 minutos
40Microsoft network server: Digitally sign communications (always) **(P)**	Not Defined	Disabled	Disabled
41Microsoft network server: Digitally sign communications (if client agrees) **(P)**	Not Defined	Enabled	Enabled
39Microsoft network server: Disconnect clients when logon hours expire **(P)**	Not Defined	Disabled	Enabled
42Network access: Allow anonymous SID/Name translation **(P)**	Disabled	Enabled	Disabled
43Network access: Do not allow anonymous enumeration of SAM accounts **(P)**	Not Defined	Enabled	Enabled
44Network access: Do not allow anonymous enumeration of SAM accounts and shares **(P)**	Not Defined	Enabled	Enabled
45Network access: Do not allow storage of credentials or .NET Passports for network authentication **(P)**	Not Defined	Enabled	Enabled
46Network access: Let	Not Defined	Disabled	Disabled

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
Everyone permissions apply to anonymous users			
47Network access: Named Pipes that can be accessed anonymously **(P)**	Not Defined	Not Defined	vacio
48Network access: Remotely accessible registry paths **(P)**	Not Defined	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion
49Network access: Remotely accessible registry paths and subpaths **(P)**	Not Defined	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersi	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentV

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
		on\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog	ersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\Curre

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
			ntControlSet\ Services\Sys monLog
50Network access: Restrict anonymous access to Named Pipes and Shares **(P)**	Not Defined	Enabled	Enabled
51Network access: Shares that can be accessed anonymously **(P)**	Not Defined	Not Defined	Not Defined Ninguno.
52Network access: Sharing and security model for local accounts **(P)**	Not Defined	Classic - Local users authenticate as themselves	Classic - Local users authenticate as themselves
53Network security: Do not store LAN Manager hash value on next password change **(P)**	Not Defined	Disabled	Disabled[1]
54Network security: Force logoff when logon hours expire **(P)**	Not Defined	Not Defined	Enabled
55Network security: LAN Manager authentication level **(P)**	Not Defined	Send NTLM Response only	Send NTLM Response only
56Network security: LDAP client signing requirements **(P)**	Not Defined	Negotiate Signing	Negotiate Signing
57Network security: Minimum session security for NTLM SSP based (including secure RPC) clients **(P)**	Not Defined	Not Defined	No Requirements

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
58Network security: Minimum session security for NTLM SSP based (including secure RPC) servers **(P)**	Not Defined	Not Defined	No Requirements
59Recovery console: Allow automatic administrative logon **(P)**	Not Defined	Disabled	Disabled
60Recovery console: Allow floppy copy and access to all drives and all folders **(P)**	Not Defined	Disabled	.....
61Shutdown: Allow system to be shut down without having to log on **(P)**	Not Defined	Disabled	Disabled
62Shutdown: Clear virtual memory pagefile **(P)**	Not Defined	Disabled	Disabled
63System cryptography: Force strong key protection for user keys stored on the computer **(P)**	Not Defined	User is prompted when the key is first used	User is prompted when the key is first used
64System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing **(P)**	Not Defined	Not Defined	Disabled
65System objects: Default owner for objects created by members of the Administrators group **(P)**	Not Defined	Object Creator	Object Creator
66System objects: Require case insensitivity for non-Windows subsystems **(P)**	Not Defined	Enabled	Enabled
67System objects: Strengthen default permissions of internal system objects (e.g.	Not Defined	Enabled	Enabled

Directiva	Política de Dominio	Política de DC	Servidores Miembro y Stand-Alone
Symbolic Links) **(P)**			
68System settings: Optional subsystems **(P)**	Not Defined	No one	No one
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies **(P)**	Not Defined	Not Defined	Disabled

Tabla 6: Opciones de Seguridad

Existen Derechos de Usuarios y Opciones de Seguridad que se encuentran implementados en Plantillas de Políticas creadas en el GPO del Active Directory.

Las Plantillas de Políticas se encuentran aplicadas sobre OU's creadas deacuerdo al rol que tienen los servidores y sitio al que pertenezcan, por lo tanto cuando se incluya un nuevo equipo es necesario identificar el nivel de la OU al que pertenece para que pueda tener una correcta aplicación de la plantilla de política de aseguramiento.

Las plantillas de políticas existentes para Controladores de Dominio y Servidores Miembro con su respectiva Ruta son las siguientes:

Controladores de Dominio	Ruta	Servidores Miembros	Ruta
Aseguramiento Domain Controllers	.fin.ec/Domain Controllers	Aseguramiento Base Plus sin Disco w2k3-v10	.fin.ec/Servidores/Servidores Producción/Servidores Windows 2003/Servidores de Aplicaciones/Aplicativos
			.fin.ec/Servidores/Servidores Producción/Servidores Windows 2003/Servidores de Aplicaciones/Aplicativos/Qu

			ito
			.fin.ec/Servidores/Servidores Producción/Servidores Windows 2003/Servidores de Aplicaciones/File Server
			.fin.ec/Servidores/Servidores Producción/Servidores Windows 2003/Servidores de Aplicaciones/File Server/Quito
			.fin.ec/Servidores/Servidores Producción/Servidores Windows 2003/Servidores de Base de Datos/SQL 2005
			.fin.ec/Servidores/Servidores Producción/Servidores Windows 2003/Servidores de Base de Datos/SQL 2005
			.fin.ec/Servidores/Servidores Producción/Servidores Windows 2003/Servidores Especiales
		Aseguramiento Base Plus sin Disco w2k3-v10-exchange	.fin.ec/Servidores/Servidores Producción/Servidores Windows 2003/Servidores de Páginas/Exchange 2003 Server
		Aseguramiento Base Plus sin Disco w2k3-v10-IIS	.fin.ec/Servidores/Servidores Producción/Servidores Windows 2003/Servidores

			de Páginas/Servicios Web
		Aseguramiento Base Plus sin Disco w2k3-v10-MSQ	.fin.ec/Servidores/Servidores Producción/Servidores Windows 2003/Servidores de Aplicaciones/Message Queuing
		Aseguramiento Base Plus sin Disco w2k3-v10-SQL2000	.fin.ec/Servidores/Servidores Producción/Servidores Windows 2003/Servidores de Base de Datos/SQL 2000

Tabla 7: Controladores de Dominio

Nota: En el cuadro de Derechos de usuarios y Opciones de seguridad existe una (P) que indica las opciones que están implementadas en las plantillas de políticas para Servidores Miembros de Windows 2003. Con respecto a la plantilla de política de Controladores de Dominio todas las opciones se encuentran en está excepto dos que pertenecen a Opciones de Seguridad y que son: Accounts: Rename administrator account y Accounts: Rename guest account.

ADMINISTRACIÓN DE RECURSOS COMPARTIDOS

En la presente sección se definen los parámetros generales de seguridad para la administración de recursos compartidos de red.

Impresoras

La creación, configuración, mantenimiento y borrado de impresoras en el esquema de Active Directory será responsabilidad del personal de soporte técnico.

Las impresoras serán definidas en los servidores de Banco mediante el programa Wizard "Add Printer", teniendo en consideración que al momento de la creación se deberán completar los siguientes campos:

Campo	Contenido
Printer name	Nombre de la Impresora
Share as	Nombre con que se comparte
Location	Ubicación física de la impresora Piso-Sector
Comment	Incluir dirección IP, Características (B/N, color, formularios, etc.)

Tabla 1: Administración de Recursos Compartidos

Asimismo, al momento de compartir un recurso de este tipo se deberá especificar la opción de publicación en el servicio de directorio y una vez creado se le deberán aplicar los permisos definidos a continuación:

Grupo	Permiso
Administrators	Full Control
Print Operators	Full Control
Creator Owner	Manage Documents
Users	Print

Tabla 2: Permisos por Grupo

Finalmente, se deberá mover la impresora a la OU del área de negocio correspondiente.

Archivos, directorios y unidades de disco compartidos (Shares)

Administración de carpetas compartidas en servidores:

La responsabilidad de la creación de accesos asociados a directorios o discos compartidos (Shares) en los servidores, será responsabilidad del administrador

designado por el propietario del recurso.

Todas las carpetas compartidas deberán ser analizadas y autorizadas por el responsable de seguridad con anterioridad a la publicación de las mismas.

Carpetas compartidas en servidores – Generalidades:
Dado que el acceso efectivo de un usuario a un directorio compartido se determina en base a los permisos que tiene sobre el "Share" y los permisos que tiene sobre el sistema de archivos, se deberá implementar sobre ambos la misma restricción a nivel de permisos (tanto sobre el sistema de archivos como a nivel de carpeta compartida). Cada carpeta compartida personalizada, a excepción de aquellas creadas por defecto por el sistema operativo, deberá tener el siguiente esquema de permisos:

Grupo	Permiso
Administrators	Full Control
Usuarios autorizados por el Propietario de la información	Change

Tabla 3: Permisos por Grupo

ESQUEMA DE CARPETAS COMPARTIDAS

A continuación se detalla el esquema de directorios compartidos básicos, definidos en un servidor de Banco al instalar el sistema operativo:

Lectora de CD / DVD	No debe estar compartida
Disquetera	No debe estar compartida
Impresoras	No deben existir impresoras instaladas en los DC
Unidad$	Creados por defecto en la instalación
ADMIN$	Creados por defecto en la instalación
PRINT$	Creados por defecto en la instalación
NETLOGON	Creados por defecto en la instalación
IPC$	Creados por defecto en la instalación

Tabla 4: Esquema de Carpetas Compartidas

Nota: Esta lista de recursos compartidos sólo detalla la cantidad mínima de shares que deben existir, pudiendo existir otros que hayan sido creados de acuerdo a los lineamientos de Seguridad Informática.

ESTRUCTURA DE DIRECTORIOS Y PERMISOS ASIGNADOS

Con el objeto de asegurar la integridad de los datos almacenados en los servidores, se deberá respetar la estructura y los permisos sobre los directorios más relevantes, de acuerdo al esquema siguiente.

ASIGNACIÓN DE PERMISOS SOBRE LA ESTRUCTURA ELEMENTAL DE DIRECTORIOS

La asignación de permisos deberá efectuarse a través de los grupos locales y globales previamente definidos y no en forma directa a los usuarios finales, a fin de evitar la pérdida de permisos ante el borrado y nueva copia de los mismos.

Solamente deberán asignarse permisos a usuarios particulares en sus correspondientes directorios personales. Para ello, todos los discos utilizados por Windows 2003 Server deberán formatearse con el sistema de archivos NTFS.

Los permisos deberán ser aplicados en el orden en que se presentan, a través del uso de una plantilla de seguridad que mantenga las definiciones desarrolladas a continuación.

CONTROLADORES DE DOMINIO

Directorio o Archivos	Grupo	Permiso	Aplica sobre	Modo de aplicarlos
%systemdrive%\	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Creator Owner	Full Control	Subfolders & Files only	Replace

Directorio o Archivos	Grupo	Permiso	Aplica sobre	Modo de aplicarlos
	Server Operators	Modify	This folder, subfolders & Files	Replace
	Authenticated users	Read & Execute	This folder only	Replace
%systemdrive%\boot.ini	Administrators	Full Control	This folder only	Replace
	System	Full Control	This folder only	Replace
	Server Operators	Modify	This folder only	Replace
%systemdrive%\ntbootdd.sys	Administrators	Full Control	This folder only	Replace
	System	Full Control	This folder only	Replace
	Server Operators	Modify	This folder only	Replace
%systemdrive%\ntdetect.com	Administrators	Full Control	This folder only	Replace
	System	Full Control	This folder only	Replace
	Server Operators	Modify	This folder only	Replace

Directorio o Archivos	Grupo	Permiso	Aplica sobre	Modo de aplicarlos
%systemdrive%\ntldr	Administrators	Full Control	This folder only	Replace
	System	Full Control	This folder only	Replace
	Server Operators	Modify	This folder only	Replace
%systemdrive%\Program Files	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Server Operators	Modify	This folder, subfolders & Files	Replace
	Creator Owner	Full Control	This folder, subfolders & Files	Replace
	Authenticated users	Read & Execute	This folder, subfolders & Files	Replace
%windir%	Administrators	Full Control	This folder, subfolders & Files	Replace

Directorio o Archivos	Grupo	Permiso	Aplica sobre	Modo de aplicarlos
	System	Full Control	This folder, subfolders & Files	Replace
	Creator Owner	Full Control	This folder, subfolders & Files	Replace
	Server Operators	Modify	This folder, subfolders & Files	Replace
	Authenticated users	Read & Execute	This folder, subfolders & Files	Replace
%windir%\Ntds	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
%windir%\Repair	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace

Directorio o Archivos	Grupo	Permiso	Aplica sobre	Modo de aplicarlos
%windir%\Security	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Server Operators	Read & Execute	This folder, subfolders & Files	Replace
	Authenticated users	Read & Execute	This folder, subfolders & Files	Replace
%windir\System32\ Config	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Creator Owner	Full Control	This folder, subfolders & Files	Replace
	Server Operators	List Folder Contents	This folder, subfolders & Files	Replace

Directorio o Archivos	Grupo	Permiso	Aplica sobre	Modo de aplicarlos
%windir%\System32\dllcache	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
%windir%\System32\spool	Printer Operators	Modify	This folder, subfolders & Files	Propagate
%windir%\Sysvol[1]	Administrators	Full Control	This folder, subfolders & Files	Replace
	Creator Owner	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Server Operators	Read & Execute	This folder, subfolders & Files	Replace
	Authenticated users	Read & Execute	This folder, subfolders & Files	Replace

Solo para Domain Controllers. Sobre estos directorios también se generarán automáticamente permisos de read & execute para todos los grupos sobre los que aplique una GPO.

Directorio o Archivos	Grupo	Permiso	Aplica sobre	Modo de aplicarlos
%windir%\Sysvol\<Domain>\Policies	Administrators	Full Control	This folder, subfolders & Files	Replace
	Creator Owner	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Group Policy Creator Owner	Modify	This folder, subfolders & Files	Replace
	Authenticated users	Read & Execute	This folder, subfolders & Files	Replace
	Server Operators	Modify	This folder, subfolders & Files	Replace
	Users	Read	This folder, subfolders & Files	Replace

Tabla 1: Controladores de Dominio

SERVIDORES MIEMBRO STAND ALONE

Directorio o Archivos	Grupo	Permiso	Aplica sobre	Modo de aplicarlos
%systemdrive%\	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Creator Owner	Full Control	Subfolders & Files only	Replace
	Power Users	Modify	This folder, subfolders & Files	Replace
	Authenticated users	Read & Execute	This folder only	Replace
%systemdrive%\boot.ini	Administrators	Full Control	This folder only	Replace
	System	Full Control	This folder only	Replace
	Power Users	Modify	This folder only	Replace
%systemdrive%\ntdetect.com	Administrators	Full Control	This folder only	Replace
	System	Full Control	This folder only	Replace
	Power Users	Modify	This folder only	Replace
%systemdrive%\ntldr	Administrators	Full Control	This folder only	Replace
	System	Full Control	This folder only	Replace
	Power Users	Modify	This folder only	Replace
%systemdrive%\Program Files	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Power Users	Modify	This folder, subfolders & Files	Replace
	Creator Owner	Full Control	Subfolders & Files Only	Replace

Directorio o Archivos	Grupo	Permiso	Aplica sobre	Modo de aplicarlos
	Authenticated users	Read & Execute	This folder, subfolders & Files	Replace
%windir%	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Creator Owner	Full Control	Subfolders & Files Only	Replace
	Power Users	Modify	This folder, subfolders & Files	Replace
	Authenticated users	Read & Execute	This folder, subfolders & Files	Replace
%windir%\Repair	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
%windir%\Security	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Power Users	Read & Execute	This folder, subfolders & Files	Replace
	Authenticated users	Read & Execute	This folder, subfolders & Files	Replace

Directorio o Archivos	Grupo	Permiso	Aplica sobre	Modo de aplicarlos
%windir%\System32\Config	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Creator Owner	Full Control	Subfolders & Files Only	Replace
	Power Users	List Folder Contents	This folder and subfolders	Replace
%windir%\System32\dllcache	Administrators	Full Control	This folder, subfolders & Files	Replace
	System	Full Control	This folder, subfolders & Files	Replace
%windir%\System32\spool	Administrators	Full Control	This folder, subfolders & Files	Replace
	Creator Owner	Full Control	Subfolders & Files Only	Replace
	System	Full Control	This folder, subfolders & Files	Replace
	Power Users	Modify	This folder, subfolders & Files	Replace
	Authenticated users	Read & Execute	This folder, subfolders & Files	Replace

Tabla 2: Servidores Miembro Stand Alone

ADMINISTRACIÓN DE RECURSOS

ALTA DE CUENTAS DE USUARIOS

El administrador del entorno Windows deberá asignar a cada usuario de la red un único "identificador de usuario" en el dominio .fin.ec el cual será de carácter personal. Dicho identificador de usuario deberá ser incluido en él o los grupos globales correspondientes de acuerdo al rol de la persona que hará uso del mismo. Adicionalmente la cuenta deberá ubicarse en la unidad organizativa de "Usuarios" correspondiente al área de negocios en la cual el usuario realizará sus tareas habituales.

Cada vez que se cree una cuenta de usuario se deberá incluir la siguiente información:

ACCOUNT

Deberá completarse de la siguiente manera:

Propiedad	**Valor / Descripción**
User logon name	La cuenta de usuario personal deberá responder a la nomenclatura estándar utilizada por Banco, tal como se detalla en la Política de control de acceso de la Entidad (PC.POL.1.4). El dominio de inicio de sesión del usuario deberá ser @ *.fin.ec*
User logon name (Pre-Windows 2000)	Será identico al "*User logon name"*. El dominio de inicio de sesión del usuario será "Matriz\"
Logon Hours	En general no deberán restringirse los accesos a los usuarios a determinados períodos de tiempo.
Log On To	En general no deberán restringirse los accesos a los usuarios a determinados equipos.
User must change password at next logon	***Se seleccionará esta característica*** para obligar al usuario a que modifique la contraseña la próxima vez que ingrese a la red.
User cannot change password	***No se seleccionará esta opción***, permitiendo que el responsable de la cuenta modifique la contraseña cuando lo considere necesario.
Password never expires	***No se seleccionará esta opción*** para implementar el vencimiento de contraseña según los valores generales.
Store password	Determina si las contraseñas de usuario pueden ser almacenadas

Propiedad	Valor / Descripción
using reversible encription	usando un hash de dos direcciones. Almacenar contraseñas en este formato es similar a almacenarlas en texto plano por lo que ***esta opción debe estar desactivada.***
Account is disabled	Se seleccionará esta opción para que permanezca bloqueada hasta que el usuario se comunique con el responsable de seguridad para su ingreso.
Smart Card is required for interactive logon	Solicita el uso de una Smart Card para permitir el inicio de sesión del usuario. ***Esta opción debe estar deshabilitada.***
Account is trusted for delegation	Brinda a los servicios corriendo bajo una cuenta de usuario la habilidad de reenviar tickets de Kerberos. Existen muchos servicios en los que este parámetro es necesario y solo debe ser activado en cuentas que corren estos servicios. Un ejemplo de servicio que requiere delegación es cuando un usuario se conecta a un servidor Web y recupera su mail desde un servidor de Exchange. No aplica para cuentas de usuario. Esta opción debe estar deshabilitada.
Account is sensitive and cannot be delegated	Habilitar esta opción significa que un usuario no puede redireccionar sus credenciales. Deberá estar seleccionada para cuentas administrativas o sensibles.
Use DES encryption types for this account	Permite el uso de encripción DES de 56 bits en lugar de la encripción RC4 de 128 bits utilizada en la implementación de Kerberos de Microsoft. Esta opción está incluida para interoperar con implementaciones de Kerberos en Unix mas viejas. ***Esta opción debe estar deshabilitada.***
Do not require Kerberos preauthenticatio n	Requerir pre-autenticación hace significativamente más difícil que un atacante pueda reunir información en caso de producirse un ataque de adivinación de contraseñas. ***Esta opción debe estar deshabilitada.***
Account expires	En general las cuentas de usuario no deberán tener fecha de expiración, salvo en los casos de personal que efectúe trabajos temporarios y se conozca con certeza la fecha en que dejarán de prestar servicio.

Tabla 1: Account

PASSWORD

Como contraseña inicial deberá ingresarse una palabra combinada de ocho (8) caracteres como mínimo, que estará formada por letras y números.

GENERAL

Deberá completarse con los datos descriptivos del usuario a saber: Nombre, Apellido, Iniciales, Descripción (cargo que ocupa, para aquellas cuentas pertenecientes a terceros contratados, se agregará el indicativo "(Externo)"), Oficina Número de teléfono, y Dirección de e-mail.

ADDRESS

Deberá completarse con los datos del lugar de trabajo donde el usuario efectúa sus tareas habituales, a saber: Calle, Número, Ciudad, Estado o Provincia, Código postal y país.

PROFILE

Deberá completarse de la siguiente manera:

Profile path	En los casos en los que se habilite al usuario a tener un roaming profile el mismo deberá permanecer en el directorio de usuario, esto es : \\SERVER\Usr*Usuario*
Logon script	En caso de que el usuario cuente con scripts de inicio de sesión los mismos deberán ser mencionados en este cuadro y ubicarse en \\DOMBBSRV\WINDOWS\scripts\run_block.vbs
Connect	

Tabla 2: Profile

TELEPHONES

Completar con teléfonos móviles, Fax, Pager, otras oficinas, etc.....

ORGANIZATION

Deberá completarse de la siguiente manera:

Title	Completar con el cargo que desempeña el usuario.
Department	Departamento en el cual desempeña sus tareas.
Company	Compañía

EXCHANGE

Por Default debe tener deshabilitado en propiedades, características del Exchange:

Outlook Mobile Access	En los casos en los que se habilite el buzón con un teléfono móvil u otros dispositivos inalámbricos.
Sincronización iniciada por el usuario	Permite que el usuario sincronice el buzón con dispositivos inalámbricos.
Notificaciones de Actualización	Mantiene siempre actualizados los datos de dispositivos inalámbricos.
Outlook Web Access	Permite que el usuario tenga acceso al buzón con un explorador web.
POP3	Permite que el usuario tenga acceso al buzón con un cliente de correo electrónico POP3.
IMAP4	Permite que el usuario tenga acceso al buzón con un cliente de correo electrónico IMAP4.

Tabla 3: Exchange

TERMINAL SERVICE PROFILE, ENVIROMENT Y SESSION

En general ningún usuario poseerá un perfil de de "Terminal Services" habilitado, salvo que alguna instalación de servidor de aplicaciones lo requiera, en cuyo caso se analizará cada situación en particular.

REMOTE CONTROL

Deberá configurarse de manera que ningún usuario esté habilitado para controlar u observar remotamente ninguna sesión de usuario.

PROFILE

En general todos los usuarios deben crearse con el logon script run_block.vbs.

EXCHANGE

Deberá configurarse de manera que ningún usuario esté habilitado para tener acceso al buzón de correo electrónico con un explorador Web, excepto los usuarios que tengan blackberry autorizados por el Banco.

ALTA DE CUENTA DE SERVICIOS

Para aquellos servicios que requieran ejecutarse con una cuenta diferente a Localsystem, el administrador de seguridad deberá asignar un único "identificador de usuario de servicio" a nivel local o en el dominio de Banco , que deberá ser incluido en él o los grupos globales necesarios para la asignación de derechos de usuarios y permisos. Además la cuenta deberá ubicarse en la unidad organizacional de "Usuarios" correspondiente al sitio en el cual se ejecuta el servicio al que la cuenta pertenece. Para las cuentas de los sistemas que no puedan ser modificadas se conservará la configuración original. Por ej.: Builtin Accounts o cuentas de sistemas pre-configurados y cerrados.

Cada vez que se cree una cuenta de servicio se deberá incluir la siguiente información:

ACCOUNT

Deberá completarse de la siguiente manera:

Propiedades	Valores / Descripción
User logon name	La nomenclatura utilizada para los identificadores de usuarios de servicio deberá responder de acuerdo a las siguientes consideraciones: El nombre de la cuenta comenzará con las siglas "Admin_" indicando que se trata de una cuenta de servicio. Los tres caracteres siguientes con el código correspondiente al tipo de servicio. Los últimos tres caracteres con un número secuencial definido por el responsable de seguridad. En el caso en que el servicio no requiera una cuenta especial podrá utilizar la cuenta "System Local Account". (Ver en este mismo capítulo "Consideraciones adicionales"). El dominio de inicio de sesión de las cuentas deberá ser @ *.fin.ec*

Propiedades	Valores / Descripción
User logon name (Pre-Windows 2000)	Idem a User logon name. El dominio de inicio de sesión de la cuenta será "Matriz\"
Logon Hours	En general no deberá restringirse el acceso de las cuentas de servicio a determinados períodos de tiempo.
Log On To	Las cuentas de servicio deberán estar restringidas exclusivamente a aquellos servidores en los que el servicio que es soportado necesita loguearse.
User must change password at next logon	Salvo que la funcionalidad de la cuenta especial lo permita, ***esta opción no deberá activarse.***
User cannot change password	***Se seleccionará esta opción***, permitiendo que solo el administrador del entorno Windows modifique la contraseña de la cuenta cuando lo considere necesario.
Password never expires	***Se seleccionará esta opción*** para inhabilitar el vencimiento de contraseña según los valores generales.
Store password using reversible encription	Determina si las passwords de usuario pueden ser almacedas usando un hash de dos direcciones. Almacenar passwords en este formato es similar a almacenarlas en texto plano por lo que ***esta opción debe estar desactivada.***
Account is disabled	Se seleccionará esta opción para que permanezca bloqueada hasta que el responsable del servicio que la cuenta soporta se comunique con el responsable de seguridad requiriendo su habilitación.
Smart Card is required for interactive logon	Solicita el uso de una Smart Card para permitir el inicio de sesión del usuario. ***Esta opción debe estar deshabilitada.***
Account is trusted for delegation	Brinda a los servicios corriendo bajo una cuenta de usuario la habilidad de reenviar tickets de Kerberos. Existen muchos servicios en los que este parámetro es necesario y solo debe ser activado en cuentas que corren estos servicios. Un ejemplo de servicio que requiere delegación es cuando un usuario se conecta a un servidor Web y recupera su mail desde un servidor de Exchange. ***Esta opción deberá estar deshabilitada***, salvo en los casos

Propiedades	Valores / Descripción
	especiales en los que el servicio lo requiera lo cual deberá ser analizado por el responsable de seguridad.
Account is sensitive and cannot be delegated	Habilitar esta opción significa que un usuario no puede redireccionar sus credenciales. Esta opción debe estar habilitada.
Use DES encryption types for this account	Permite el uso de encripción DES de 56 bits en lugar de la encripción RC4 de 128 bits utilizada en la implementación de Kerberos de Microsoft. Esta opción está incluída para interoperar con implementaciones de Kerberos sobre Unix antiguas. ***Esta opción debe estar deshabilitada.***
Do not require Kerberos preauthentication	Requerir pre-autenticación hace significativamente mas difícil que un atacante pueda reunir información en caso de producirse un ataque de adivinación de passwords. Esta opción debe estar deshabilitada.
Account expires	En general las cuentas de servicios o aplicaciones no deberán tener fecha de expiración. Esta opción debe estar deshabilitada.

Tabla 4: Alta de Cuentas de Servicio

PASSWORD

Como contraseña de las cuentas de servicio deberá ingresarse una palabra combinada de catorce (14) caracteres como mínimo, que estará formada por letras, números y caracteres especiales.

GENERAL

Deberán completarse los siguientes campos:

Display Name	Idem User Logon name en Account
Description	Se indicará la función para la cual fue creada la cuenta, o bien el servicio que la estará utilizando y el servidor en el que corre.

Tabla 5: Alta de Cuenta de Servicio Password

ADDRESS, PROFILE, TELEPHONES Y ORGANIZATION

No deberá completarse con ningún dato adicional.

TERMINAL SERVICES, PROFILE, ENVIROMENT Y SESSION

Ninguna cuenta de servicio poseerá un Profile de Terminal Services habilitado.

REMOTE CONTROL

Ninguna cuenta de servicio estará habilitada para controlar u observar remotamente ninguna sesión de usuario.

CONSIDERACIONES ADICIONALES

La cuenta "Administrator" deberá ser renombrada y resguardada en sobre cerrado junto con su contraseña.

Las cuentas "Guest"," TSInternetUser" y "Krbtgt" deberán inhabilitarse.
En los casos en que los servicios de Internet Information Services (IIS) no requieran el uso del inicio de sesión anónimo o en los Domain Controllers, las cuentas "IWAM_Server" e "IUSR_Server" deberán inhabilitarse.

ALTAS A CUENTAS DOMAIN ADMIN

Las solicitudes de cuentas Domain Admins deben ser aprobadas por el Gerente de Sistemas y el Gerente de Seguridad Informática

Establecer el sistema propietario de la cuenta, la contraseña debe estar encriptada y justificar documentadamente el requerimiento

La nueva cuenta Domain Admins debe estar ensobrada
Establecerse los derechos de usuarios de la cuenta (limitar sus autorizaciones de acceso a lo necesario)

DEFINIR EN QUE EQUIPOS ÚNICAMENTE PUEDE DAR LOGON

Las cuentas Domain Admins para usuarios personales, además de cumplir con los requerimientos establecidos por Seguridad Informática deben estar aprobados por el Área de Seguridad de acuerdo con sus procedimientos.

ADMINISTRACIÓN DE GRUPOS

Grupos sensitivos creados en la instalación (En proceso de depuración por parte de seguridad informática y sistemasEn los controladores de dominio de Banco, los grupos creados por defecto en la instalación del sistema operativo deberán estar asociados a los siguientes usuarios:

Nombre del Grupo	Alcance	Descripción	Miembros del Grupo
Domain admin.	Global	Sus miembros tienen privilegios máximos sobre el dominio.	El documento que contiene los nombres del grupo es: Sig_Domain_Admins.xls
Domain Users	Global	Usuarios del Dominio	Usuarios del dominio
Domain Guests	Global	Usuarios Invitados.	Sin usuarios
Administrators	Local	Sus miembros tienen privilegios máximos sobre el sistema.	Domain Admin. Enterprise Admin.
Server Operators	Local	Sus miembros administran los servidores.	El documento que contiene los nombres del grupo es: Sig_server_operators.xls
Account Operators	Local	Sus miembros administran las cuentas de los usuarios y los grupos.	Sin Usuarios
Print Operators	Local	Sus miembros administran las impresoras.	Sin usuarios
Back Up Operators	Local	Sus miembros efectúan tareas de generación/restauración de copias de respaldo.	Cuentas de usuario utilizadas por el software de backup
Everyone	Local	Todas las cuentas de usuarios que han establecido una conexión con el servidor.	Todos los usuarios conectados
Users	Local	Sus miembros tienen los permisos necesarios para ejecutar aplicaciones y administrar ciertos archivos.	Usuarios del dominio sin privilegios especiales.
Guests	Local	Permite que cualquier persona sin una cuenta definida acceda a	TSInternetUser

Nombre del Grupo	Alcance	Descripción	Miembros del Grupo
		la red.	
Power Users (Servidores Miembro)	Local	Grupo con derechos especiales de operación.	En función del rol del servidor, se deben identificar los usuarios con privilegios especiales sobre el mismo.

CREACIÓN DE GRUPOS Y ASIGNACIÓN DE GRUPOS A USUARIOS

Se deberá seguir con la siguiente premisa a la hora de crear grupos en el dominio, siempre y cuando ninguna especificación técnica lo impida:

Se crearán Grupos locales de dominio (Domain local groups) a los cuales se les asignará permisos sobre los recursos.

Se crearán Grupos Globales basados en la funciones o roles de trabajo del personal.

Se agregarán las cuentas de usuarios a estos grupos globales y estos últimos dentro de los grupos locales a los cuales se les asigno los permisos apropiados.

Siempre se deberá evitar asignar permisos directamente a las cuentas de usuario.

CONSIDERACIONES MÍNIMAS SOBRE PERMISOS PERMITIDOS/NO PERMITIDOS

A continuación se detallan los servicios que podrán estar ejecutándose o no, en los servidores de Banco. Cualquier otro servicio que no esté en este listado, o que no cumpla una función específica en el servidor, deberá ser analizado, para verificar si puede ser inhabilitado o es necesario para el normal funcionamiento del servidor en cuestión.

CONTROLADORES DE DOMINIO

Servicio	Modo de activación
Automatic Updates**(P)**	Automático
DHCP Server	Deshabilitado
Distributed File System**(P)**	Automático
DNS Server**(P)**	Automático
Event Log**(P)**	Automático
File Replication**(P)**	Automático
Intersite Messaging**(P)**	Automático
Kerberos Key Distribution Center**(P)**	Automático
Net Logon**(P)**	Automático
NT LM Security Support Provider**(P)**	Automático
Remote Procedure Call (RPC)**(P)**	Automático
Windows Time**(P)**	Automático
Distributed Link Tracking Server**(P)**	Deshabilitado
Fax	Deshabilitado
FTP Publishing Service	Deshabilitado
IIS Admin Service	Deshabilitado
Simple Mail Transport Protocol (SMTP)	Deshabilitado
Telnet**(P)**	Deshabilitado

Tabla 6: Controladores de Dominio

MEMBER SERVERS Y STAND ALONE

Servicio	Modo de activación
1Automatic Updates**(P)**	Automático
2Distributed File System**(P)**	Automático
3Event Log**(P)**	Automático
4Remote Procedure Call (RPC)**(P)**	Automático
5Windows Time**(P)**	Automático
DHCP Server	Deshabilitado
6Distributed Link Tracking Server**(P)**	Deshabilitado
7DNS Server**(P)**	Deshabilitado
Fax	Deshabilitado
FTP Publishing Service	Deshabilitado[1]
IIS Admin Service	Deshabilitado[2]
8Intersite Messaging**(P)** * En la plantilla de AseguramientoBase Plus sin Disco w2k3-v10-exchange está como Not Defined.	Deshabilitado[3]
9Kerberos Key Distribution Center**(P)**	Deshabilitado
10NT LM Security Support Provider**(P)** * En las plantillas de AseguramientoBase Plus sin Disco w2k3-v10-MSQ. AseguramientoBase Plus sin Disco w2k3-v10-exchange está con automático.	Deshabilitado[4]
Simple Mail Transport Protocol (SMTP)	Deshabilitado[3]
Telnet**(P)**	Deshabilitado
File Replication**(P)**	Manual
Net Logon**(P)** En las plantillas la opción queda con Automático.	Manual

Tabla 7: Member Servers y Stand Alone

1 Habilitar en servidores FTP

2 Habilitar en servidores IIS

3 Habilitar en servidores Exchange o SMTP

4 Habilitar en servidores Exchange

Para los servicios específicos deben tenerse en cuenta los diferentes estándares de configuración, según las funcionalidades brindadas por los servidores.
Los servicios se encuentran también implementados en las plantillas de políticas implementadas en el GPO de Active Directory y que se encuentran detalladas anteriormente.

Nota: En el cuadro de servicios para Controladores de Dominio y Servidores Miembro/Stand Alone existe una (P) que indica las opciones que están implementadas en la plantillas de política.

SUBSISTEMAS OS/2 y POSIX

Deberán estar deshabilitados los subsistemas OS/2 y POSIX ya que la seguridad de los mismos no se encuentra completamente probada.

Para quitar el soporte para OS/2 y POSIX deberán realizarse las siguientes acciones:
Eliminar de "%windir%\system32\dllcache" los siguientes archivos: os2.exe, os2ss.exe, os2srv.exe, doscall.dll, netapi.os2 y netapi.dll

Eliminar de "%windir%\system32" los siguientes archivos: os2.exe, os2ss.exe, os2srv.exe, psxss.exe, posix.exe y psxdll.dll

Eliminar de "%windir%\system32\os2\dll" los archivos: doscall.dll y netapi.dll.

Nota de implementación: Cabe destacar que las librerías DLL son utilizadas por programas de tecnología system16, por lo cual en caso de ser necesaria la utilización de aplicaciones de dichas características se recomienda reinstalar las mismas.
Nota de implementación: Los archivos deben eliminarse en el orden indicado.

ESTÁNDAR DE SEGURIDAD PARA MS SQL SERVER 2008

Validaciones del estándar

Evelyn Mota – Joffre Navarrete	20-Abril-2011	Marcel León Lafebré	26-Abril-2011
Aprobación Preliminar (Validación)	**Fecha**	**Aprobación Definitiva**	**Fecha**

ASPECTOS GENERALES

OBJETIVO

Definir las medidas necesarias para implementar un ambiente seguro en los servidores de base de datos Microsoft SQL Server 2008 de Banco.

ÁMBITO DE APLICACIÓN

Todos los servidores de base de datos MS SQL Server 2008 de Banco.

Normativa Marco (Normativas Superior de Referencia)

PC.POL.1- Política General de Seguridad de la Información

Normativa Derogada

Ninguna.

Otras Normativas Asociadas

Ninguna.

Vigencia

Este Estándar de Configuración entrará en vigencia a partir del mes de Agosto de 2011.

Disposiciones Generales y Transitorias

Este estándar de configuración deberá ser revisado anualmente por el Área de Seguridad de la Información de Banco. Los resultados de la revisión, y los cambios que se sucedan, serán reportados al Comité de Seguridad de la Información y comunicados a los involucrados antes de ser implementados.

La falta de cumplimiento de las definiciones descriptas en el presente procedimiento, estará sujeta a las sanciones disciplinarias que amerite cada caso.

ROLES Y RESPONSABILIDADES

Área de Seguridad de la Información:

- ✓ **Responsable de Seguridad de la Información:** Tendrá a su cargo el mantenimiento del presente estándar, junto con las tareas de verificación del cumplimiento del mismo.

- ✓ **Gerente de Sistemas:** Deberá garantizar que los funcionarios del área de sistemas, encargados de realizar la administración de los servidores de base de datos MS SQL Server 2008, implementen los estándares de configuración definidos en forma efectiva y oportuna.

- ✓ **Administradores de plataforma MS SQL Server 2008:** Serán encargados de implementar el presente estándar, siguiendo los lineamientos y tareas mencionadas en el mismo. Asimismo, deberán informar al Gerente de Sistemas sobre las configuraciones de seguridad que no puedan ser implementadas por restricciones técnicas y/o de negocio, las cuales deberán quedar adecuadamente documentadas.

CONFIGURACIÓN GENERAL DE LA SEGURIDAD

OBJETIVO

Considerar las medidas básicas de seguridad a tener en cuenta al configurar el servidor Microsoft SQL 2008.

CUENTA DE SERVICIO

- ✓ Para los equipos Stand-Alone:

  En caso que el servicio de MSSQL Server no requiera la conectividad o utilización de otros recursos de la red (como ser link de bases de datos) deberá utilizar la cuenta local de sistema "Local Service" para inicializar los servicios de la instancia. En caso contrario, se deberá utilizar la cuenta "Network Service".

- ✓ Para los equipos Miembros del Dominio:

  Se deberá asignar una cuenta de dominio con la nomenclatura Admin_SQL_nnn, donde nnn es un número interno adecuado asignado por el Responsable de Seguridad de la Información de la Entidad.

  La misma deberá ser incluida en los grupos de servicio de MSSQL (los cuales se detallan en las siguientes secciones del presente documento) y ser configurada como cuenta inicializadora de los servicios de SQL Server de la instancia (a excepción del servicio SQL Server VSS Writer, para el cual deberán mantenerse los permisos por defecto sobre la cuenta SYSTEM), según se muestra a continuación:

La contraseña asignada a la cuenta de servicios utilizada deberá poseer asignada una contraseña compleja, con una contraseña de al menos 8 caracteres de longitud, y ser almacenada en sobre cerrado, de acuerdo a lo establecido en el procedimiento de administración de usuarios de máximos privilegios de la Entidad.

Como complementos adicionales de seguridad, durante la instalación de la instancia de bases de datos, serán generados seis grupos especiales a nivel de sistema operativo. Cada uno de los grupos mencionados se encuentra asociado a un servicio particular de la instancia y poseen asociados los privilegios mínimos requeridos sobre el sistema operativo para que estos funcionen de manera consistente. A continuación se detallan dichos grupos, con sus correspondientes privilegios asignados:

Servicio de SQL Server	Grupo	Permisos asignados por defecto durante la instalación
SQL Server	Instancia por defecto: SQLServerMSSQLUser$ComputerName$MSSQLSERVER Instancia renombrada (el nombre no es por defecto): SQLServerMSSQLUser$ComputerName$InstanceName	Log on as a service Log on as a batch job Replace a process-level token Bypass traverse checking Adjust memory quotas for a process Permisos para iniciar el servicio SQL Server Active Directory Helper Permisos para iniciar el servicio *SQL Writer* Permisos para leer el servicio de *Event Log* Permisos para leer el servicio de *Remote Procedure Call*
SQL Server Agent	Instancia por defecto: SQLServerSQLAgentUser$ComputerName$MSSQLSERVER Instancia renombrada (el nombre no es por defecto): SQLServerSQLAgentUser$ComputerName$InstanceName	Log on as a service Log on as a batch job Replace a process-level token Bypass traverse checking Adjust memory quotas for a process
Analysis Services	Instancia por defecto: SQLServerMSOLAPUser$ComputerName$MSSQLSERVER Instancia renombrada (el nombre no es por defecto): SQLServerMSOLAPUser$ComputerName$InstanceName	Log on as a service
SSRS	***Instancia por defecto:***	Log on as a service

Servicio de SQL Server	Grupo	Permisos asignados por defecto durante la instalación
	SQLServerReportServerUser$ComputerName$MSRS10.MSSQLSERVER Instancia renombrada (el nombre no es por defecto): SQLServerReportServerUser$ComputerName$MSRS10.InstanceName	
Integration Services	Instancia por defecto o renombrada: SQLServerDTSUser$ComputerName	Log on as a service Permisos para escribir en el *application event log.* Bypass traverse checking Impersonate a client after authentication
Full-text Search	Instancia por defecto: SQLServerFDHostUser$ComputerName$MSSQL10.MSSQLSERVER Instancia renombrada (el nombre no es por defecto): SQLServerFDHostUser$ComputerName$MSSQL10.InstanceName	Log on as a service
SQL Server Browser	Instancia por defecto o renombrada: SQLServerSQLBrowserUser$ComputerName	Log on as a service
SQL Server Active Directory Helper	Instancia por defecto o renombrada: SQLServerMSSQLServerADHelperUser$ComputerName	Ninguno(2)
SQL Writer	N/A	Ninguno(2)

Tabla 1: Cuentas de Servicio

La instalación de SQL Server no controla o asigna Permisos para este servicio.

DIRECTORIOS DE INSTALACIÓN Y PERMISOS EN WINDOWS 2003/2008

El producto y sus archivos ejecutables se instalarán en el directorio C:\MSSQL, mientras que los archivos correspondientes a datos, auditoría, copias de respaldo, etc. serán almacenados en otras particiones del equipo, respetando el como raíz el directorio <drive>\MSSQL.

Usuario/Grupo	Directorio
Auditoria	<drive>\MSSQL\AUDITORIA
Copias de respaldo	<drive>\MSSQL\BACKUP
Datos	<drive>\MSSQL\DATA

Tabla 1: Directorios de Instalación

Deberán asignarse los siguientes permisos sobre los directorios C:\MSSQL y <drive>\MSSQL, replicándolos sobre los subdirectorios dependientes:

Usuario/Grupo	Permisos
Administradores	Full Control
System	Full Control
SQLServerMSSQLUser$ComputerName$Instance Name	Read & Execute

Tabla 2: Permisos en Windows

Deberán asignarse los siguientes permisos sobre los directorios C:\MSSQL\DATA y <drive>\MSSQL\DATA, <drive>\MSSQL\AUDITORIA y <drive>\MSSQL\BACKUP replicándolos sobre los subdirectorios dependientes:

Usuario/Grupo	Permisos
Administradores	Full Control
System	Full Control
SQLServerMSSQLUser$ComputerName$Instance Name	Full Control

Tabla 3: Permisos

Todos los archivos del sistema operativo que contienen bases de datos deben ubicarse en el directorio <drive>\MSSQL\DATA, tanto para los archivos primarios (extensión .mdf), secundarios (extensión .ndf), y de log (extensión .ldf).

Los usuarios no deberán poseer permisos sobre estos archivos, ya que SQL Server se encarga de gestionar los accesos a través de su propia seguridad. Por lo tanto, regirán para este subdirectorio los mismos permisos mencionados para el directorio principal de la base de datos.
Política de Contraseñas

CUENTA DE ADMINISTRADOR

La contraseña de la cuenta del usuario administrador "SA" ("System Administrator") será cambiada, deberá poseer una longitud mínima de 8 caracteres y será administrada de acuerdo al Procedimiento de Administración de Usuarios de Máximos Privilegios de la Entidad.

Si bien la cuenta SA deberá contar con las políticas de contraseñas y cuentas de usuario definidas en el estándar de la plataforma Windows 2000/2003, dicha cuenta deberá contar con la excepción a la política de expiración de contraseñas, tal como se muestra a continuación:

CUENTA DE USUARIOS FINALES

Todas las cuentas locales de la instancia deberán contar con la política de contraseñas y expiración de cuentas activa. Además, para todo cambio de contraseña que efectúe el administrador (sea por creación o cambio de la misma) deberá seleccionar la opción que la contraseña cambie en el próximo inicio de sesión del usuario. A continuación se muestra dicha configuración:
Cabe destacar, que podrán ser utilizados los mecanismos de autenticación por certificado o clave asimétrica provistos por SQL Server 2008.

MODO DE SEGURIDAD

El modo de autenticación a utilizar para el acceso al servidor de base de datos es el basado en SQL Server y Windows, tal como se muestra a continuación:

CONEXIONES CON OTROS USUARIOS REMOTE SERVER

Se deberá desactivar la funcionalidad incluída en el servicio para la ejecución de stored procedures desde servidores remotos. La misma deberá ser reemplazada por la utilización de linked servers.

Para desactivar la funcionalidad mencionada deberá establecerse la siguiente configuración:

LINKED SERVERS

Esta facilidad debe habilitarse sólo en caso de ser requerida para asegurar la funcionalidad de alguna aplicación. En particular, no debe utilizarse para fines administrativos.

Las opciones deben configurarse de la siguiente manera:

- ✓ Data access: Habilitarse sólo en caso de precisarse la ejecución de consultas contra el servidor remoto.
- ✓ RPC: Debe estar inhabilitado.
- ✓ RPC out: Habilitarse sólo en caso de precisarse la ejecución de stored procedures en el servidor remoto.
- ✓ Lazy Schema Validation: siempre debe estar en False
- ✓ Distributor/Publisher: habilitarse solo en caso de querer publicar información que sea accesible desde otros db-links.
- ✓ Las opciones de seguridad deben configurarse de la siguiente manera:

Seguridad para usuarios no definidos específicamente: Debe seleccionarse la primera opción, a fin de denegar el acceso a usuarios no especificados.

Lista de usuarios: De acuerdo al esquema de permisos utilizado por la aplicación, se presentan las siguientes alternativas:

VÍNCULO USUARIO-USUARIO

El administrador de Base de Datos deberá vincular, en una relación de uno a uno, los usuarios del servidor local, que necesiten acceso, con los usuarios del servidor remoto.

VÍNCULO USUARIO – USUARIO GENÉRICO

El administrador de Base de Datos deberá vincular los usuarios del servidor local, que necesiten acceso, con un usuario genérico del servidor remoto.

VÍNCULO USUARIO – USUARIO CON OPCION IMPERSONATE

El administrador de Base de Datos deberá incorporar a la lista a los usuarios que necesiten acceder al servidor remoto, activando la opción de impersonate, lo que obliga a que los usuarios en ambas bases posean el mismo login id y contraseña. Se recomienda utilizar esta alternativa.

CONFIGURACIÓN DE SQL SERVER AGENT

CONEXIÓN DEL SQL AGENT CON SQL

Por defecto, SQL Server 2008 utiliza el modo de autenticación nativa de Windows. En caso que se haya podido habilitar la opción de seleccionar el mecanismo de autenticación local, deberá utilizarse el modo de autenticación de Windows.

CASILLA DE CORREO ASOCIADA A SERVICIOS

Se permitirá la asignación de una casilla de correo a los servicios de SQL y SQL Server Agent, posibilitando el envío de mensajes y alertas a los operadores. A continuación se muestra como debería configurarse:

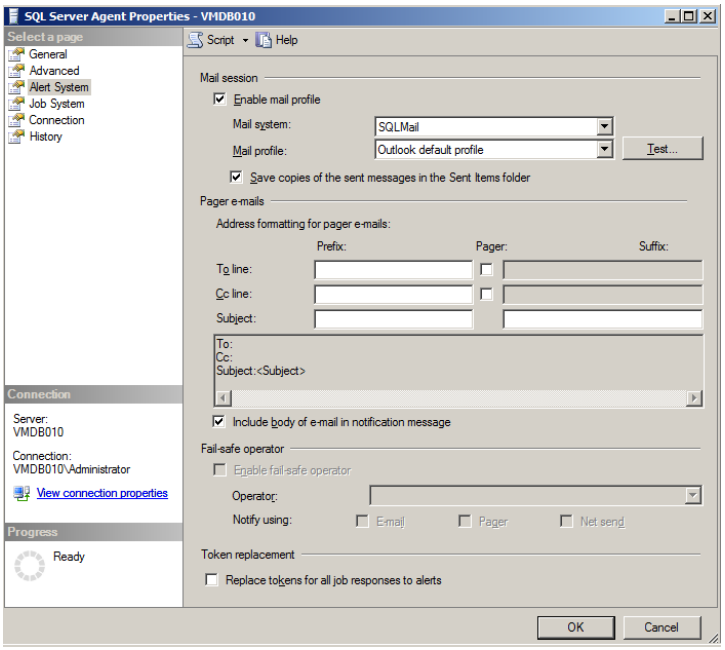


Figura 7: Configuración de SQL

Asimismo, dichas casillas deberán parametrizarse teniendo en cuenta los siguientes lineamientos:

- ✓ Se deberá seleccionar el sistema de correo SQLMail, para poder asignar una cuenta de correos Exchange.

- ✓ El perfil de correos (Mail profile) deberá ser un perfil válido en Exchange (una cuenta de correos válida).
- ✓ Se deberá configurar al menos la línea de destinatario principal.
- ✓ Las demás propiedades de la casilla deben completarse según las consideraciones sobre casillas genéricas descriptas en el Estándar de Seguridad

de Microsoft Exchange.

- ✓ Se deberá crear una lista de distribución denominada "Alertas SQL", en la cual se incorporará al personal involucrado de los sectores de Administración de Bases de Datos, Seguridad de la Información, o los funcionarios que se considere necesario.
- ✓ Las tareas programadas en los equipos deberán enviar un mensaje, a la lista de distribución mencionada previamente, una vez finalizada en forma exitosa o fallida.
- ✓ Consideraciones adicionales
- ✓ Usuario Guest: No debe crearse el usuario guest en ninguna base de datos. Cualquier login id que no tenga un usuario propio es asociado a guest, lo cual permitiría a un usuario no autorizado acceder a una base de datos, y obtener los derechos del grupo Public.
- ✓ En el caso de las bases de datos master, tempdb, el usuario guest es creado por el servidor SQL automáticamente y no debe eliminarse.
- ✓ En el caso de la base msdb, si bien el usuario también es creado por defecto, debe ser eliminado.
- ✓ Asimismo, este usuario deberá eliminarse de la base de datos model, para que las futuras bases que sean generadas no lo incluyan.

ROLES DE ADMINISTRACIÓN DEL SERVIDOR

OBJETIVO

Describir las pautas a tener en cuenta al configurar el acceso de usuarios con derechos de administración al servidor SQL.

ESQUEMA DE ROLES

La responsabilidad de administración de servidores SQL descansa exclusivamente sobre las áreas de Sistemas (sector de Ingeniería) y Seguridad de la Información de Banco

Se identifican las siguientes funciones o roles de administración a tener en cuenta:

- ✓ Administrador de Base de Datos
- ✓ Tiene a su cargo las siguientes tareas:
- ✓ Creación y mantenimiento de bases de datos
- ✓ Generación de copias de respaldo adicionales a las programadas
- ✓ Restauración de bases de datos
- ✓ Administración de alertas, tareas y operadores
- ✓ Monitoreo y revisión de los servidores
- ✓ Resolución de problemas técnicos y de mantenimiento del producto
- ✓ Instalación de actualizaciones.

Para cumplir esta función se requieren los privilegios de acceso del rol predefinido System Administrator.

Debido al nivel de acceso que este perfil posee, deberá ser auditada toda su actividad (ref. Sección Auditoria de Eventos del presente documento).

ADMINISTRADOR DE SEGURIDAD

Tiene a su cargo las tareas relacionadas con la administración de logins, contraseñas, usuarios, y sus autorizaciones en las bases de datos. Para esto, precisará las autorizaciones pertinentes por parte del Propietario de los Datos.

Para cumplir esta función se requieren los privilegios de acceso de los siguientes roles predefinidos:

- ✓ Security administrator (rol de servidor securityadmin)
- ✓ db_accessadmin (rol de base de datos)
- ✓ db_securityadmin (rol de base de datos)

  Debido al nivel de acceso que este perfil posee, debe ser auditada toda su actividad (ref. Sección Auditoría de Eventos del presente documento).

ADMINISTRACIÓN DE CONTRASEÑAS

A fin de posibilitar al Administrador de Seguridad la reasignación de contraseñas en caso de solicitud por parte del responsable de la cuenta, debe modificarse el stored procedure sp_password.

El procedimiento por defecto restringe el cambio de contraseñas al titular de una cuenta, y a los integrantes del rol sysadmin. La modificación a incorporar consiste en extender esta capacidad a miembros del rol securityadmin.

ADMINISTRADOR DEL SERVICIO PARA EMERGENCIAS

En caso de precisarse el acceso con privilegios de administrador sobre la base de datos ("System Administrator") y no hallarse presente el Administrador designado de Base de Datos, debe utilizarse la cuenta "sa", tal como se define en el Procedimiento de administración de usuarios de máximos privilegios de la Entidad.

Asociación entre la cuenta de usuario Administrator y el rol System Administrators
Teniendo en cuenta el esquema de accesos establecido precedentemente, debe eliminarse la asociación que por defecto realiza SQL Server con la cuenta de usuario administrator, con el rol System Administrators.

Los únicos usuarios habilitados con el rol mencionado deben ser aquellos que lo necesiten, como por ejemplo el Administrador de Base de datos.

BASES DE DATOS

OBJETIVO

Definir pautas de seguridad para las bases de datos.

CONFIGURACIÓN DE BASE DE DATOS

Bases de datos de ejemplo

Las bases de datos de ejemplo Pubs y Northwind deben ser eliminadas de los servidores de producción dado que representan objetivos conocidos por los atacantes y con mínimas restricciones.

CRECIMIENTO DE ARCHIVOS

En caso de especificarse que el o los archivos que contienen la base de datos puedan crecer automáticamente, debe restringirse su tamaño a un valor máximo a través de la opción "Restrict filegrowth", tanto para los datos, como para el log de transacciones.

Debe seleccionarse un valor adecuado para cada base de datos, en función al tamaño inicial del archivo y al espacio disponible en disco.

OPCIONES DE BASE DE DATOS

Las opciones de cada base de datos deben configurarse como se indica a continuación:

PAGE VERIFY

Esta opción debe configurarse en "CHECKSUM", a fin de permitir la detección temprana de fallas durante operaciones de lectura/escritura.

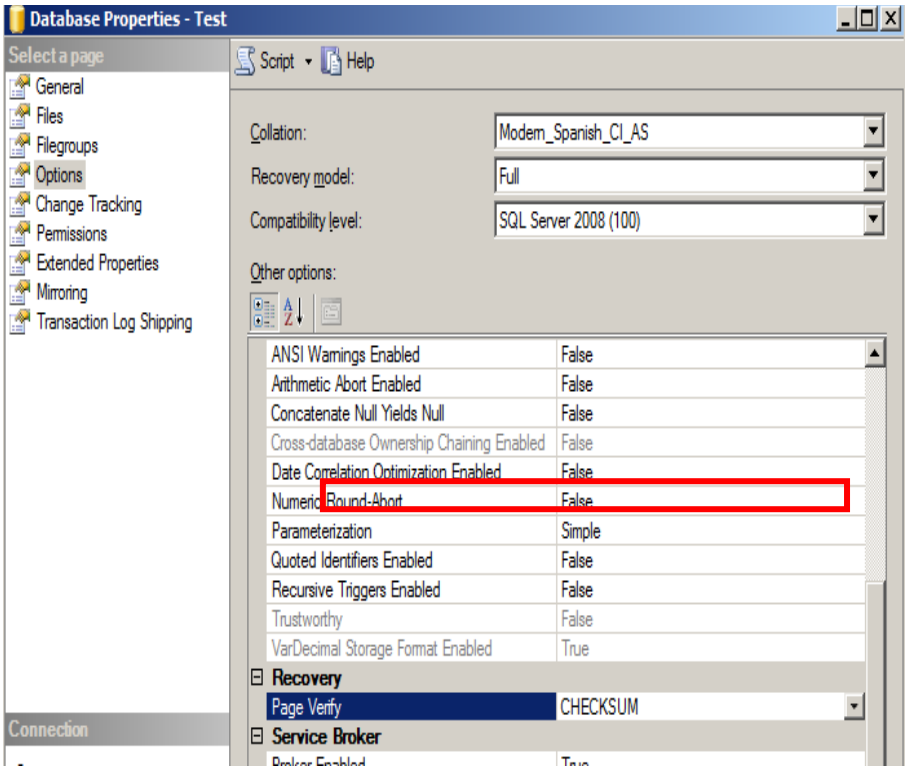


Figura 8: Detección de fallas de lectura/escritura

ENCRYPTION ENABLED

En caso de el contenido de la base de datos deba ser encriptado (por ej. debido a requerimientos regulatorios), se deberán seguir los pasos detallados en la sección "Encripción de Datos" del presente documento para su configuración.

ENCRIPTACIÓN DE DATOS

OBJETIVO

Definir las consideraciones necesarias para la encripción transparente de los datos en la instancia (TDE de sus siglas en inglés "Transparent Data Encryption").

Descripción del funcionamiento de la encripción transparente

El siguiente diagrama presenta la funcionalidad de TDE:

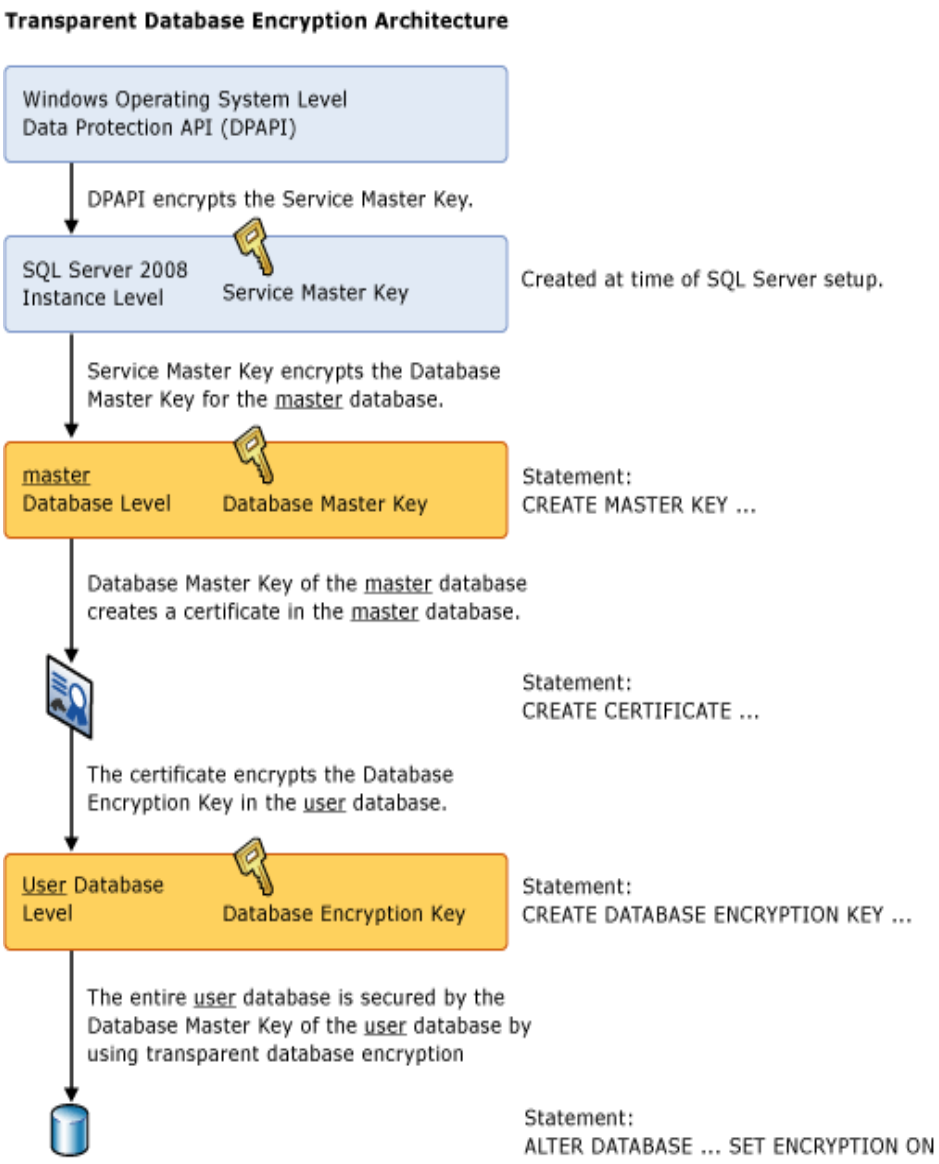


Figura 9: Encriptación de datos

PASOS A SEGUIR PARA GENERAR LA CLAVE DE ENCRIPTACIÓN

Generar la clave maestra de encripción. Para ello, ejecutar los siguientes comandos SQL en el gestor de consultas, reemplazando las variables que contienen signos <>:

```
USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<PasswordCompleja>';
GO
```

Generar el certificado del servidor. Para ello ejecutar los siguientes comandos SQL en el gestor de consultas, reemplazando las variables que contienen signos <>:

```
CREATE CERTIFICATE <MiCertificadoDeServidor> WITH SUBJECT = '<Mi Certificado>'
go
```

Seleccionar la base de datos (esquema) que se desea encriptar y generar la clave de encripción. Para ello ejecutar los siguientes comandos SQL en el gestor de consultas, reemplazando las variables que contienen signos <>:

```
USE <BaseAplicacion>
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE <MiCertificadoDeServidor>
GO
```

Activar la encripción en la base de datos. Para ello ejecutar los siguientes comandos SQL en el gestor de consultas, reemplazando las variables que contienen signos <>:

```
ALTER DATABASE <BaseAplicacion>
SET ENCRYPTION ON
GO
```

AUDITORÍA DE EVEN TOS

OBJETIVO

Definir las consideraciones necesarias para la generación de los registros de auditoría.

AUDITOR DE EVENTOS

Se deberán configurar los parámetros de auditoría de la base de datos, de acuerdo a lo establecido en el Estándar de configuración de clientes para el registro de LOGs de Banco.

CONSIDERACIONES ADICIONALES DE SEGURIDAD

OBJETIVO

Definir pautas adicionales de seguridad.

CONEXIÓN PARA SERVIDORES EXTERNOS

En caso de requerirse vínculos con servidores SQL ubicados fuera de la red interna (por ejemplo servidores de la DMZ), el sentido de la comunicación deberá realizarse desde el servidor interno hacia el externo (conexión saliente).

No deberán utilizarse conexiones entrantes desde bases de datos externas hacia bases de datos internas. Dichas conexiones deben impedirse en el dispositivo de control de acceso (firewall), a fin de evitar riesgos originados en la exposición del servidor y la red interna del banco.

ESTÁNDAR DE SEGURIDAD PARA INTERNET INFORMATION SERVICES 7

OBJETIVO

Definir las medidas necesarias para implementar el esquema de seguridad en el ambiente de servidores Web Microsoft Internet Information Services (IIS) versión 7, según la normativa de Seguridad de la Información.

Ámbito de Aplicación

Todos los servidores Web de Banco que brinden servicio Web basado en Internet Information Services 7 (IIS), los cuales pertenezcan al entorno de producción de la Entidad.

Normativa Marco (Normativas Superior de Referencia)

PC.POL.1 - Política General de Seguridad de la Información

Normativa Derogada

Ninguna.

Otras Normativas Asociadas

Ninguna.

Vigencia

Este estándar de configuración entrará en vigencia a partir de Marzo de 2011.

Disposiciones Generales y Transitorias

Este estándar de configuración deberá ser revisado anualmente por el Área de Seguridad Informática de Banco. Los resultados de la revisión, y los cambios que se sucedan, serán reportados al Comité de Seguridad de la Información y comunicados a los involucrados antes de ser implementados.

La falta de cumplimiento de las definiciones descriptas en el presente estándar, estará sujeta a las sanciones disciplinarias que amerite cada caso.

Roles y Responsabilidades

Seguridad Informática:

Responsable de Seguridad Informática: Tendrá a su cargo el mantenimiento del presente estándar, junto con las tareas de verificación del cumplimiento del mismo.

Gerencia de Sistemas:

Gerente de Sistemas: Deberá garantizar que los funcionarios del área de sistemas, encargados de realizar la administración de los servidores Web, implementen los estándares de configuración definidos en forma efectiva y oportuna.

Administradores y Operadores de la plataforma: Serán encargados de implementar el presente estándar, siguiendo los lineamientos y tareas mencionadas en el mismo. Asimismo, deberán informar al Gerente de Sistemas sobre las configuraciones de seguridad que no puedan ser implementadas por restricciones técnicas y/o de negocio, las cuales deberán quedar adecuadamente documentadas.

CONSIDERACIONES GENERALES DEL SISTEMA OPERATIVO

OBJETIVO

Definir las consideraciones de seguridad necesarias para el correcto funcionamiento de la plataforma Microsoft Windows 2008 sobre la cual se encuentra instalado el servicio Internet Information Services.

Seguridad a nivel de sistema operativo Windows 2008
Se deberá configurar la plataforma Microsoft Windows 2008 de acuerdo a los parámetros definidos en el Estándar de Seguridad para Microsoft Windows 2008 de Banco.

Cuentas de usuario creadas por defecto en la instalación
Durante la instalación de IIS se crea por defecto una cuenta integrada, garantizada por el sistema operativo para tener siempre un SID único. El nombre real que es utilizado para la nueva cuenta nunca será localizado. Por ejemplo, independientemente del idioma de Windows que se instala, el nombre de cuenta de IIS siempre será IUSR. Esto le indica a IIS utilizar la nueva cuenta integrada para todas las solicitudes de autenticación anónima.

La cuenta IUSR sustituye a la cuenta IUSR_MachineName de IIS 6 (donde "MachineName" es el nombre del equipo donde reside IIS). La cuenta IUSR_MachineName seguirá siendo creada y utilizada si se instala el servidor FTP 6 compatibles que se incluye en Windows Server 2008. Si no instala el servidor FTP que se incluye con Windows Server 2008, esta cuenta no se creará.

Asimismo, esta versión de IIS utiliza varias cuentas de usuarios propias del sistema operativo, estas son:

- ✓ Local System: Esta cuenta tiene por defecto permisos de "Full access". Es parte del grupo de administradores locales con alto nivel de permisos de acceso. Si un proceso de trabajo se ejecuta con la cuenta de usuario "Local System", entonces este proceso tendrá acceso full al sistema.
- ✓ Network Service: Esta cuenta de usuario negocia con otro sistema teniendo credenciales de la cuenta de la computadora. Tiene menos permisos que "Local System" sobre el sistema.

- ✓ Local Service: Esta cuenta de usuario tiene menos privilegios que "Network Service" y limita los permisos de usuario solo a la computadora local. La misma es utilizada por procesos que no requieren acceso a servidores externos.

A fin de reforzar la seguridad del servicio Web, y según corresponda, deberán implementarse las siguientes consideraciones de seguridad:
En caso de ser requerido el acceso anónimo, dichas cuentas deberán estar definidas a nivel local en el equipo (No deberán utilizarse cuentas de dominio), "No" deberá permitirse el cambio de las contraseñas de las mismas y la contraseña "No" deberá expirar, según se muestra en la siguiente figura:

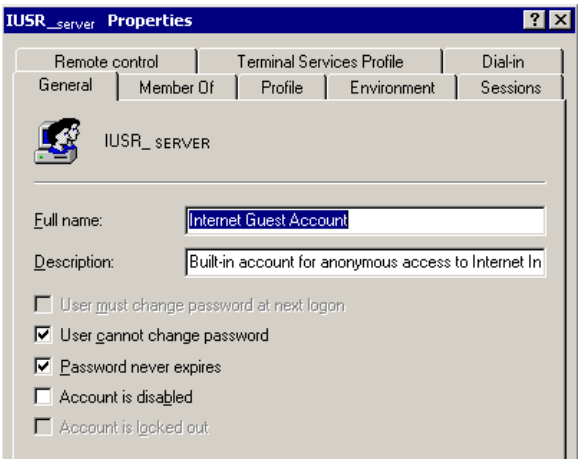


Figura 10: Creación de cuentas de usuario

La cuenta de usuario IUSR_MachineName que se crea si se instala ser servidor de FTP 6, debe ser renombrada con el objetivo de eliminar todo tipo de configuraciones propias de la instalación. La nomenclatura a utilizar en la misma es la siguiente:

IUSR_NombreAplicacion_NombreServidor

Para cambiar el nombre de la cuenta de usuario mencionada, se deberán ejecutar las siguientes tareas:
Hacer clic con el botón secundario del mouse en "My Computer" y, a continuación, hacer clic en "Manage".
Hacer doble clic en "Configuration", luego en "Local Users and groups" y, a continuación, hacer clic en la carpeta "Users".
Hacer clic con el botón secundario del mouse en la cuenta IUSR_<NombreEquipo> y, a continuación, seleccionar "Rename".
Escribir el nuevo nombre y presionar "Enter".

SEPARACIÓN DE APLICACIONES EN GRUPOS

Las aplicaciones se pueden separar en grupos. Un grupo de aplicaciones es un grupo de una o varias direcciones URL que ofrece un proceso de trabajo o un conjunto de ellos. Estos pueden ayudar a mejorar la confiabilidad del servidor Web, ya que cada aplicación funciona de forma independiente con respecto a las demás.

En IIS 7, los grupos de aplicaciones se ejecutan en uno de los siguientes modos: el modo integrado y el modo clásico. El modo del grupo de aplicaciones afecta a cómo el servidor procesa las solicitudes de código administrado. Si una aplicación administrada se ejecuta en un grupo de aplicaciones con el modo integrado, el servidor utilizará la arquitectura integrada de procesamiento de solicitudes de IIS y ASP.NET para procesar la solicitud. Sin embargo, si una aplicación administrada se ejecuta en un grupo de aplicaciones con el modo clásico, el servidor seguirá a las solicitudes de las rutas de código administrado a través de Aspnet_isapi.dll, es decir procesa las solicitudes de la misma forma que si la aplicación se ejecutara en IIS 6.0.

La mayoría de las aplicaciones administradas se debe ejecutar con éxito en grupos de aplicaciones con el modo integrado, pero puede que tenga que ejecutarse en el modo clásico por razones de compatibilidad.

Todos los procesos en ejecución en un sistema operativo Windows disponen de una identidad, que determina el modo en que el proceso tiene acceso a los recursos del equipo. Cada grupo de aplicaciones cuenta además con una identidad de proceso, que es una cuenta ejecutada con los permisos mínimos que requiere la aplicación. Esta identidad de proceso se puede utilizar para permitir el acceso anónimo al sitio o a las aplicaciones Web.

En caso de utilizar “Pools” de Aplicaciones, deberán configurarse para utilizar la cuenta predefinida “NetworkService”, si no se requieren privilegios superiores.
Para configurar la identidad para un pool de aplicaciones:

- ✓ Hacer Clic derecho sobre un pool de aplicaciones;
- ✓ Seleccionar “Advanced Settings” en el menú contextual;
- ✓ En la ventana “Advanced Settings”, seleccionar la sección “ProcessModel”;
- ✓ Seleccionar la opción “Identity” y luego hacer clic en el botón que aparece al lado derecho.
- ✓ En la ventana que aparece “Aplication Pool Identity” en la sección de “Built-in account” seleccionar Network Service.

DEFINICIÓN DE GRUPOS

Con el objetivo de organizar y administrar los usuarios relacionados al IIS y asignarle privilegios a los mismos, se deberán crear los siguientes grupos locales y se deberá relacionar a los mismos los usuarios indicados:

Grupo	Miembros
WebAdmins	Usuarios administradores de los sitios.
IIS_IUSRS (Se crea por defecto)	Network Service Local Service LocalSystem

Tabla 0-1: Definición de Grupos

Por otra parte, la cuenta "IUSR_NombreEquipo" o IUSR deberá quitarse del grupo "Guests".

DERECHOS DE USUARIOS

Finalmente, al grupo creado para las cuentas de servicio de IIS ("IIS_IUSRS") y a las cuentas de usuario de servicio, deberán asignársele los derechos de usuario que se detallan a continuación:

Derechos de Usuario	Permisos
Access this computer from the network	Administrators Users Backup Operators
Adjust memory quotas for a process	LOCAL SERVICE NETWORK SERVICE Administrators
Allow log on locally	Administrators Users Backup Operators
Bypass traverse checking	LOCAL SERVICE NETWORK SERVICE Administrators

	Users Backup Operators
Impersonate a client after authentication	LOCAL SERVICE NETWORK SERVICE Administrators IIS_IUSRS SERVICE
Log on as a batch job	Administrators Backup Operators Performance Log Users IIS_IUSRS
Replace a process level token	LOCAL SERVICE NETWORK SERVICE

Tabla 2: Derechos de Usuarios

Dicha configuración deberá ser aplicada a través de la utilización de políticas de grupo aplicadas a nivel de la OU "Member Servers 2008\Web Servers", en caso de tratarse de un servidor miembro del dominio, o aplicadas a nivel local en caso de tratarse de un servidor Stand-Alone.

SERVICIOS – REDUCCIÓN DE LOS COMPONENTES DE INSTALACIÓN POR DEFECTO

Junto con el servicio de World Wide Web en IIS están incluidos otros servicios como por ejemplo los servicios FTP y SMTP. Es esencial habilitar solamente aquellos servicios que son requeridos para el normal funcionamiento de la aplicación y/o sitio Web que se procesa en el servidor. Teniendo en cuenta que los mismos pueden o no estar en el listado de servicios del servidor, las configuraciones recomendadas de los componentes de IIS 7 son las siguientes:

Subcomponentes de Internet Information Services (IIS)		
Subcomponente	**Configuración por defecto**	**Observaciones**
Background Intelligent Transfer Service (BITS)	Deshabilitado	Habilitar este componente si un software depende de, por ejemplo Windows Update para aplicación automática de services packs, o instalación de otro software en el servidor Web.
Common HTTP Features	Habilitado	En servidores Web dedicados, estos archivos son requeridos por IIS.
File Transfer Protocol (FTP)	Deshabilitado	Este componente no es utilizado en servidores Web dedicados. Si no es requerido este servicio, debe quedar deshabilitado.
IIS Management Console	Habilitado	Interfaz de administración para IIS. Deshabilitar si el servidor Web no es administrado localmente.
Internet Printing	Deshabilitado	Permite que las impresoras sean compartidas usando HTTP. Si no se requiere esta característica, debe permanecer deshabilitado.
IIS 6 Management Console	Deshabilitado	Provee compatibilidad con la administración de componentes de IIS 6, necesario para la administración de SMTP y FTP.
SMTP Service	Deshabilitado	Soporta la transferencia de correo electrónico. Este componente debe quedar habilitado en caso de que se requiera.
World Wide Web Service	Habilitado	Provee servicios de Internet, como contenido estático y dinámico, a clientes. Si este componente no esta habilitado, sus subcomponentes tampoco lo están.

Tabla 3: Servicios

CONSIDERACIONES BÁSICAS DE SEGURIDAD DEL SERVICIO WEB

OBJETIVO

Detallar las configuraciones básicas de seguridad comunes a todos los directorios virtuales y páginas del sitio web.

REDUCCIÓN DE LOS COMPONENTES DE WORLD WIDE WEB POR DEFECTO

El servicio de World Wide Web en IIS está compuesto por diversos sub componentes. Es esencial habilitar solamente aquellos requeridos indefectiblemente por la aplicación y/o sitio Web que se procesa en el servidor. A continuación se detallan las configuraciones recomendadas de los sub componentes del servicio de World Wide Web:

Subcomponentes de World Wide Web		
Subcomponente	**Configuración por defecto**	**Observaciones**
Active Server Pages	Deshabilitado	Provee soporte para ASP. Debe deshabilitarse este componente cuando no se necesite su uso. El mismo deberá ser evaluado y en caso de ser requerido, habilitado.
Management Service	Deshabilitado	Provee conexión para clientes remotos al servidor para su administración. Permite la restricción por IP de dichos clientes.
Server - Side Includes	Deshabilitado	Provee soporte para archivos .shtm, .shtml y .stm. Sino se requiere este componente, debe permanecer deshabilitado.

Tabla 1: Reducción de los Componentes www

Los sub componentes nombrados pueden ser habilitados o deshabilitados desde la consola de administración del servidor en la parte de roles, ya sean dentro o fuera de la funcionalidad de IIS.

SITIO WEB POR DEFECTO

Si bien IIS 7.0 se instala en modo seguro (conocido como "locked-down"), contiene un sitio web por defecto y archivos de ejemplo. Se sugiere eliminar todos los archivos y carpetas por defecto que se hereden de la instalación.

El sitio web por defecto es "Default Web Site" y su directorio raíz es "%systemdrive%\inetpub\wwwroot".

COMPONENTE FILESYSTEMOBJECT(FSO)

Este componente proporciona métodos y propiedades para trabajar con unidades, carpetas y ficheros. Si no se requiere utilizar estas características, se deberá deshabilitar este componente.

Para deshabilitar este componente:

- ✓ Abrir la ventana del "Command Prompt";
- ✓ Localizar el directorio "%windir%\system32";
- ✓ Escribir "regsvr32 scrrun.dll /u" y presionar "Enter". Aparecerá el siguiente mensaje "DllUnregisterServer un scrrun.dll suceded";
- ✓ Clic "OK";
- ✓ Renombrar el archivo "scrrun.dll" con el nombre "scrrun_dll.bak".
- ✓ **Permisos sobre los archives de configuración**
- ✓ IIS 7.0 incluye un nuevo sistema de configuración. La metabase XML ya no se utiliza. La raíz del archivo de configuración de IIS 7.0 es "applicationHost.config"

Dado que dicho archivo es sensitivo, se deberá velar por la seguridad del mismo a partir del cumplimiento de los siguientes lineamientos:

- ✓ Se deberán realizar copias de seguridad del mismo;
- ✓ Solo los miembros del grupo "Administradores" y "LocalSystem" deben tener permisos de acceso "Full" sobre este archivo.

Nota: El archivo se almacena en la siguiente ruta "%SystemDrive%\ Windows\System32\inetsrv\config."

IIS 7.0 también incluye la característica de compatibilidad de metabase (un servicio de función opcional) que permite a los usuarios modificar las configuraciones de IIS 7.0 con la estructura clásica de la metabase en IIS 6.0 o 5.x (por ejemplo: a través de WMI o ADSI).

Para obtener información detallada acerca de IIS 7.0 nuevo sistema de configuración, puede referirse a:
http://learn.iis.net/page.aspx/122/getting-started-with-iis-7-configuration/

PERMISOS DE ACCESO A DIRECTORIOS

UBICACIÓN Y DEFINICIÓN DE PERMISOS PARA ARCHIVOS DE de IIS

Con el fin de aumentar la seguridad de los archivos de IIS, se deberán implementar los siguientes lineamientos mínimos de configuración:

Todas las particiones de disco del servidor deberán estar en formato NTFS, a fin de permitir la adecuada aplicación de permisos de acceso.

Los archivos de sistema y los archivos propios del sitio Web deberán alojarse en particiones separadas.

CONFIGURACIÓN DE LISTAS DE CONTROL DE ACCESO (ACL)

Asimismo, a fin de reforzar los permisos de acceso a los archivos de configuración del servicio WEB y/o a los archivos de las páginas publicadas, se deberán implementar permisos de acceso sobre estos servicios y/o archivos.
Con la instalación del IIS se asignan los siguientes permisos al grupo "IIS_IUSRS", sobre los siguientes directorios involucrados:

Ubicación	Configuración	Descripción
%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files	Full Control	Acceso al directorio de compresión
Directorio de publicación	Read & Execute	Acceso al directorio raíz para el contenido Web.
%windir%\System32\Inetsrv\MetaBase.xml	NT AUTHORITY\SYSTE	Almacena los datos de la configuración de los servicios

Ubicación	Configuración	Descripción
	M: Full control BUILTIN\Administrators: Full control WebAdmins: Modify	del IIS.
%windir%\System32\Inetsrv\MBSchema.xml	NT AUTHORITY\SYSTEM : Full control BUILTIN\Administrators : Full control WebAdmins: Modify	Almacena el esquema para los archivos de configuración. El esquema define que propiedades del IIS son configuradas a ciertas claves de la metabase.
%windir%\System32\Inetsrv\History	NT AUTHORITY\SYSTEM : Full control BUILTIN\Administrators : Full control WebAdmins: Modify	Almacena los archivos del historial de la metabase que son creadas automáticamente por el IIS.
%windir%\System32\Inetsrv\MetaBack	NT AUTHORITY\SYSTEM : Full control BUILTIN\Administrators : Full control WebAdmins: Modify	Almacena los archivos de backup de la metabase, que son creados bajo demanda por la configuración de Backup/Restore.

Tabla 1: Permiso de Acceso a Directorios

Asimismo, se deberán definir los permisos mínimos requeridos en el filesystem para restringir el acceso a los archivos utilizados a través de IIS. El esquema básico que deberá ser evaluado se presenta a continuación:

Tipos de archivos	Permisos NTFS
Archivos CGI (.exe, .dll, .cmd, .pl)	IIS_IUSRS (execute) Administrators (full control) System (full control) WebAdmins (Modify)

Tipos de archivos	Permisos NTFS
Archivos de Script (.asp)	IIS_IUSRS (execute) Administrators (full control) System (full control) WebAdmins (Modify)
Archivos de Include (.inc, .shtm, .shtml)	IIS_IUSRS (execute) Administrators (full control) System (full control) WebAdmins (Modify)
Archivos de contenido estático (.txt, .gif, .jpg, .htm, .html)	IIS_IUSRS (read-only) Administrators (full control) System (full control) WebAdmins (Modify)

Tabla 2: Permiso de Acceso a Directorios

CONFIGURACIÓN DE CONTENIDO DINÁMICO

Luego de instalar IIS 7, por defecto solo se permitirá resolver peticiones de contenido estático. En caso de que la aplicación y/o Sitio Web requiera resolver pedidos de contenido dinámico, se deberán tener en cuenta que se debe activar dicho contenido desde "Add Role Services" de IIS 7.

CONFIGURACIÓN DEL REGISTRO DE WINDOWS

En el registro de Windows (Registry) se pueden configurar ciertas opciones extras que aumentan la seguridad del IIS 7. Estas opciones, en general, se encuentran correctamente configuradas en las instalaciones por defecto pudiendo aparecer explícitamente o no en el registro de sistema de windows. No obstante deben verificarse las siguientes opciones:

EnableTraceMethod
Registry Path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters
Data Type: REG_DWORD
Default Value: 0 (disabled)
Range: 0 – 1
Determina si IIS reconoce el método HTTP TRACE

AlwaysLogEvents
Registry Path: HKLM\System\CurrentControlSet\Services\WAS\Parameters
Data Type: REG_DWORD
Default Value: 0 (disabled)
Range: 0 – 1
Determina la grabación de actividades erróneas en el archivo log
EnableLogging
Registry Path: HKLM\SOFTWARE\Microsoft\WebManagement\Server
Data Type: REG_DWORD
Default Value: 1 (enabled)
Range: 0 – 1
Determina la grabación de actividades exitosas en el archivo log

Tabla 3: Configuración del Registro de Windows

COMPATIBILIDAD CON VERSIONES ANTERIORES DE IID

Si en IIS 7 es necesario trabajar con características de IIS 6 se debe habilitar dicha compatibilidad en los Servicios del Rol de IIS.

CONFIGURACIÓN DE URLSCAN 3.1

URLScan es un filtro ISAPI que bloquea solicitudes HTTP basadas en un conjunto de reglas susceptible de ser configurado. Por ejemplo, puede configurar URLScan para que bloquee todas las solicitudes efectuadas en relación con una determinada extensión de nombre de archivo, para que bloquee ciertos verbos HTTP (como GET o POST), o para que bloquee solicitudes que contengan caracteres frecuentemente incluidos en ataques a servidores Web.

Si se determina que por cuestiones de simplicidad en la administración se debe utilizar URLScan, se deberá considerar que:

- ✓ UrlScan 3.1 no está incluido dentro del producto IIS 7. Al momento de requerir la instalación del mismo, se deberá obtener desde la página oficial del proveedor antes de proceder a la instalación y configuración del mismo.
- ✓ Aplicaciones como Exchange, FPSE y Microsoft Visual Studio .NET dependen de IIS para la funcionalidad correcta. Si URLScan no se configura correctamente, estas aplicaciones pueden dejar de funcionar correctamente.
- ✓ UrlScan versión 3.1 mantiene características y funcionalidad de su predecesor (UrlScan versión 2.5). El formato de configuración es el mismo, pero incluye algunas secciones adicionales que se pueden utilizar para las nuevas características. Si actualmente está usando UrlScan versión 2.5, puede utilizar el

mismo archivo de configuración con Urlscan.ini UrlScan versión 3.1.

CONFIGURACIÓN DE LAS PROPIEDADES "GENERALES" DE LOS SITIOS WEB

A continuación se detallan las "Propiedades" de configuración que deben ser aplicadas por defecto a todos los sitios Web.

OPCIÓN "AUTENTICACIÓN"

No se deberá aplicar un esquema de autenticación. A este nivel se deberá utilizar el esquema basado en accesos anónimos únicamente.

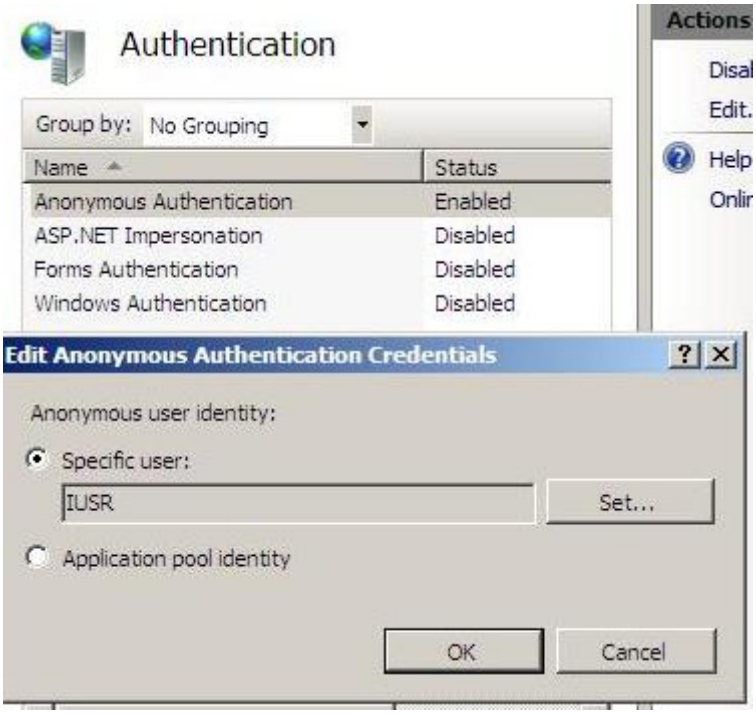


Figura 11: Autenticación de usuarios

OPCIÓN "DEFAULT DOCUMENT"

Se recomienda que el administrador proporcione siempre un documento por defecto, el que todos los usuarios verán al tener acceso a los sitios. Esto ayuda a evitar la exhibición de la estructura del directorio del sitio a un usuario.

Por lo tanto dicha opción debe estar habilitada.

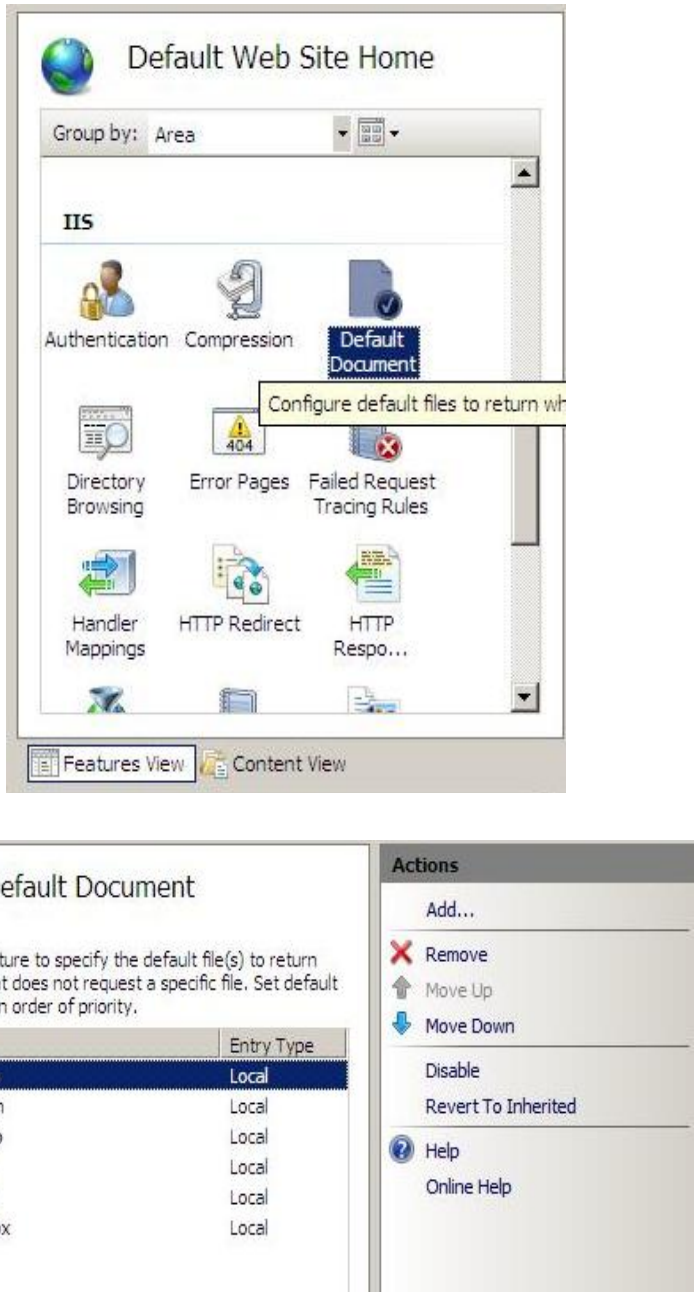


Figura 12: Sitio Web predeterminado

OPCIÓN "DIRECTORY BROWSING"

Esta opción muestra información cuando se lista un directorio. Dicha opción debe estar deshabilitada.

Figura 13: Buscador de directorio

OPCIÓN "ERROR PAGE"

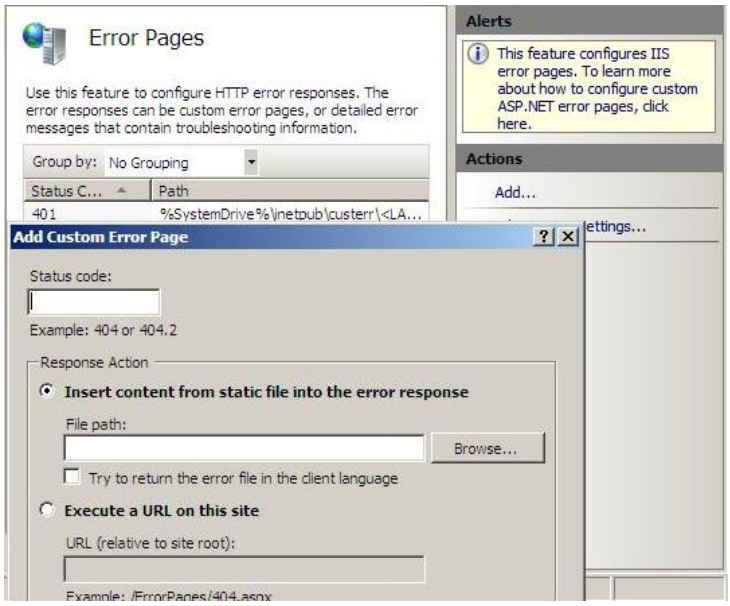


Figura 14: Errores de Páginas

Una de las principales fuentes de información utilizadas por los atacantes para vulnerar la seguridad de los sitios Web, son los mensajes de error presentados por los componentes de infraestructura y aplicaciones. Dichos mensajes son comúnmente utilizados para comprender la naturaleza de la infraestructura utilizada por la víctima y de aquí planificar nuevos ataque de mayor impacto. Debido a ello, las mejores prácticas

de seguridad para sitios web establecen que los mensajes de error presentados a los usuarios finales no deben ser descriptivos y/o contener información de las plataformas y versiones de software utilizadas.

Seleccionando la opción de "Error Pages" podremos cambiar la configuración de las páginas "por defecto" que se presentan al usuario cada vez que ocurre un error en el servicio Web. Las mismas deberán ser establecidas de acuerdo a los criterios mencionados anteriormente, evitando divulgar información alguna de la plataforma o tipo de error. Por ejemplo se podrá presentar la siguiente leyenda:

"Se ha detectado un error en la aplicación, por favor sepa disculpar las molestias"
Los mensajes de error personalizados deberán ser almacenados dentro de la nueva ubicación (diferente a la de sistema operativo) del sitio web por defecto y deberán ser comunes para todos los directorios virtuales del sitio web.

OPCIÓN "LOGGING"

En todos los servidores Web será mandatario que la auditoría se encuentre habilitada. Para activar las pistas de auditoría (LOGs) se debe tener habilitada esta opción.
Se deberá configurar un log por servidor en formato W3C. Así mismo, en la lista desplegable que se activa al hacer click en el botón "Select Fields se deberán seleccionar los siguientes componentes.

- ✓ Client IP Address
- ✓ User Name
- ✓ Service Name
- ✓ Method
- ✓ URI Stem
- ✓ URI Query
- ✓ Win32 Status
- ✓ User Agent
- ✓ Server IP Address
- ✓ Server Port

Las opciones restantes deberán quedar configuradas con los valores otorgados al momento de la instalación, como se muestra en la siguiente figura:

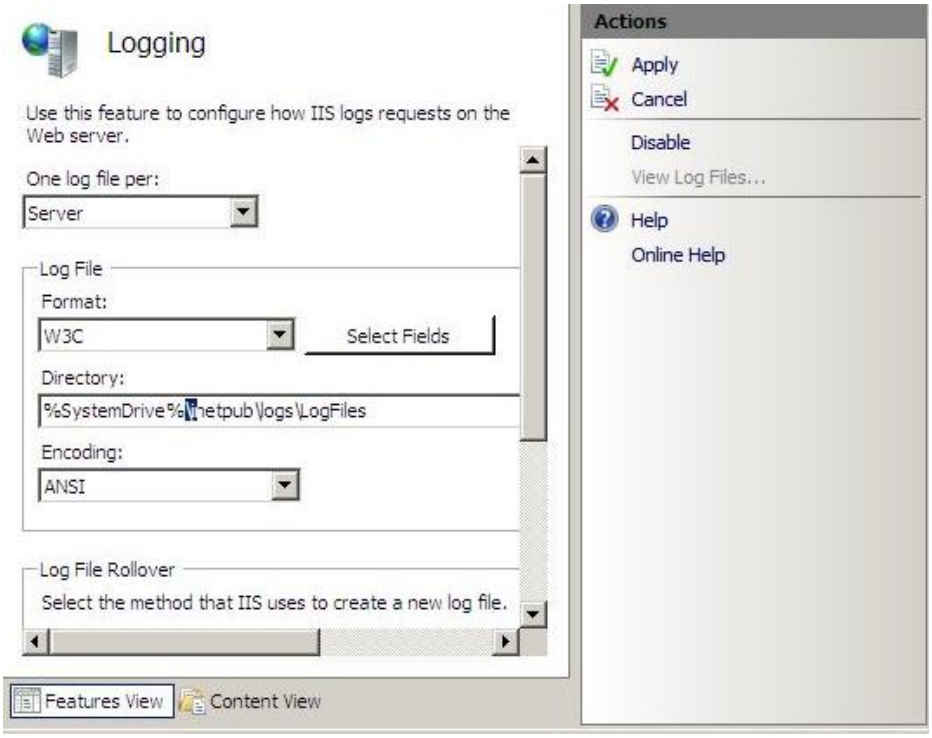


Figura 15: Configuración del web server

CONSIDERACIONES AVANZADAS DE SEGURIDAD DEL SERVICIO WEB

Luego de implementar las consideraciones mínimas de seguridad detalladas en las secciones anteriores, las cuales aplican a todos los sitios Web publicados en el servidor, se deberán aplicar las configuraciones avanzadas detalladas en esta sección.

Deberá considerarse que dichas configuraciones aplican a cada uno de los sitios virtuales definidos, dependiendo de los requerimientos específicos de seguridad del servicio brindado.

Las configuraciones detalladas a continuación deberán aplicarse utilizando la consola de administración de IIS, modificando las propiedades de los sitios Web y directorios virtuales definidos en la sección "Sites" de dicha consola.

CONFIGURACIÓN DE LAS PROPIEDADES "ESPECÍFICAS" DE LOS SITIOS WEB

A continuación se detallan las "Propiedades" de configuración adicionales, que deberán ser configuradas a nivel de cada sitio virtual (Virtual Host), dependiendo de las características del servicio brindado. Estas configuraciones complementan el esquema básico presentado en la sección anterior.

Para editar estas configuraciones se debe situar en el sitio virtual y escoger las opciones del panel de la derecha bajo el titulo de IIS:
Opción "Default Document":

En cada caso deberá especificarse el documento por defecto que se presentará al usuario al acceder al sitio Web. Por ejemplo index.asp.

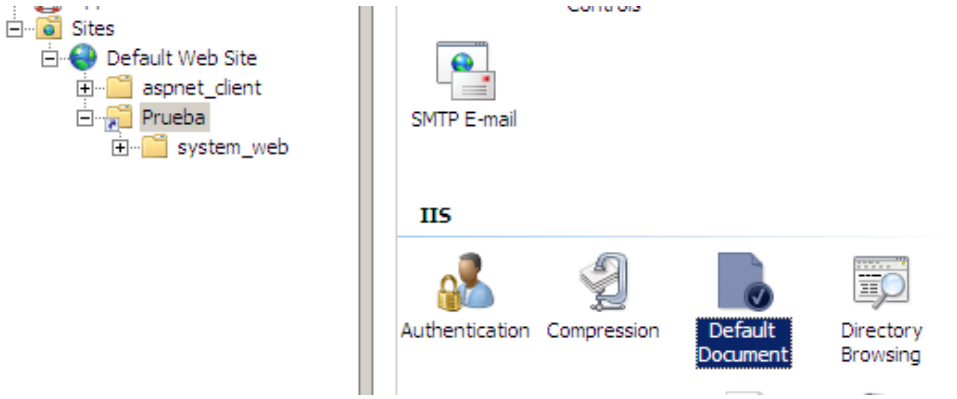


Figura 16: Configuración de las propiedades de los sitios web

OPCIÓN "ADVANCED SETTINGS – VIRTUAL DIRECTORY"

Complementando la configuración establecida a nivel general, para cada "Virtual Host" se deberán considerar las siguientes opciones de configuración:

El "path" local indica la ubicación donde residirán todas las páginas albergadas por el directorio virtual, el mismo deberá ser local y diferir respecto del "path" de instalación del sistema operativo. Su configuración será la +siguiente:
<UNIDAD>:\inetpub\wwwroot\<virtual host>

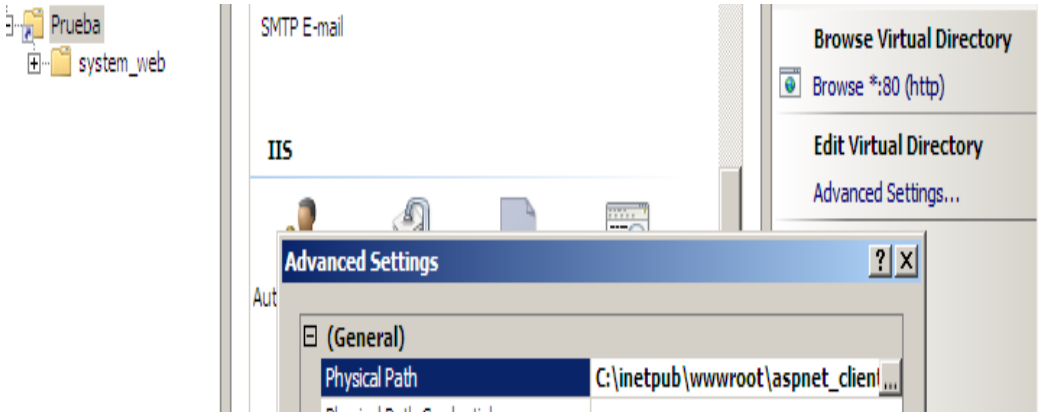


Figura 17: Definición del sitio a albergarse las páginas

OPCIÓN "HANDLER MAPPINGS"

En esta opción establecer las extensiones de páginas dinámicas que aceptará el directorio virtual, eliminando todas aquellas no requeridas. Como se muestra en la siguiente figura:

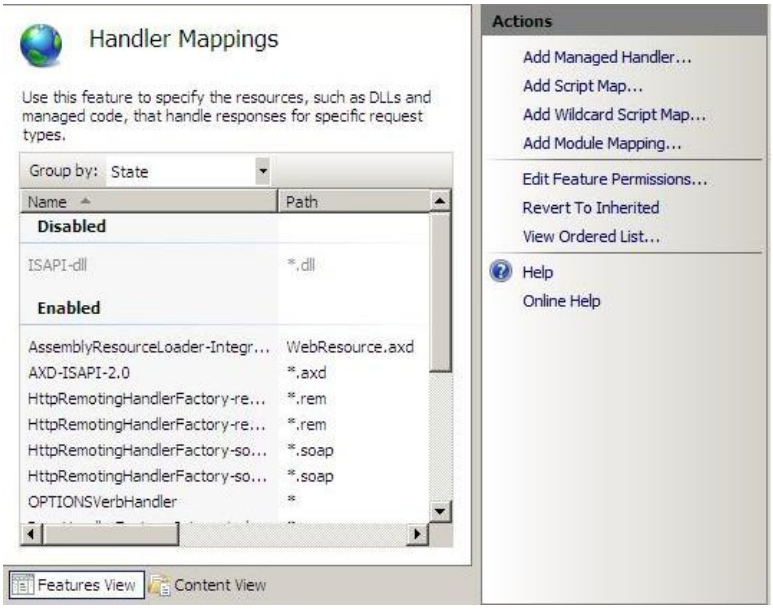


Figura 18: Establecer las extenciones de páginas dinámicas

OPCIÓN "AUTHENTICATION"

Con el objetivo de realizar un acceso seguro a los recursos del servidor Web, se deberá definir cuál es el tipo de autenticación que el mismo requerirá soportar. En este aspecto deberá aplicarse alguna de las configuraciones que se presentan a continuación dependiendo del servicio que se esté brindando:

ACCESO ANÓNIMO

A ser utilizado en casos donde no se requiera autenticación para acceder a las páginas publicadas, como en el caso de servidores públicos o internos que utilicen controles de acceso a nivel de formularios aplicativos.
Esta opción podrá ser seleccionada para servidores Web públicos.

Acceso Restringido:

Autenticación integrada con Windows: A ser utilizado en el caso de servidores Web que soportan servicios internos, los cuales utilizan controles de acceso a archivos a partir de listas de control de accesos NTFS.

En servidores públicos deberá evitarse la utilización de autenticación integrada de Windows, dado que la misma podría ser utilizada por un potencial atacante para realizar ataques del tipo "Fuerza Bruta".

Siempre que se trate de un servidor público y se requiera autenticación, se deberá priorizar la autenticación basada en formularios de aplicación y no métodos propios del servicio Web.

OPCIÓN "IPv4 ADDRESS AND DOMAIN RESTRICTIONS"

Deberán aplicarse las reglas de filtrado requeridas por el servicio prestado. Este tipo de reglas no pueden ser numeradas ya que dependen de características dinámicas de cada servicio y deberán ser evaluadas en cada caso.

En IIS 7, todas las direcciones IP (Protocolo de Internet), equipos y dominios pueden obtener acceso a su sitio de forma predeterminada. Para mejorar la seguridad, puede limitar el acceso a su sitio creando una regla de permiso que conceda acceso a todas las direcciones IP (valor predeterminado), a una dirección IP específica, a un intervalo de direcciones IP o a un dominio concreto. Por ejemplo, si tiene un sitio en un servidor de intranet que está conectado a Internet, puede impedir que los usuarios de Internet obtengan acceso al sitio de la intranet permitiendo sólo el acceso a los miembros de su Intranet.

Los procedimientos para configurar el acceso a contenido basándose en las reglas de direcciones IP y nombres de dominio se pueden realizar en los siguientes niveles de IIS:

- ✓ Servidor web
- ✓ Sitio
- ✓ Aplicación
- ✓ Directorios físicos y virtuales
- ✓ Archivo (dirección URL)

Se requiere que el siguiente módulo este habilitado:
IpRestrictionModule

El mismo que es habilitado cuando en los Servicios del Rol de IIS en la parte de seguridad se habilita la opción "Ip and Domain Restrictions".

Los pasos para habilitar esta opción son:

- ✓ Abra el Administrador de IIS y navegue hasta el nivel que desee administrar.
- ✓ En Features View, haga doble clic en IPv4 Address and Domain Restrictions.

- ✓ En el panel Actions, haga clic en Add Allow Entry.
- ✓ En el cuadro de diálogo Add Allow Restriction Rule, seleccione Specific Ipv4 address, Ipv4 address range o Domain Name, agregue la dirección IPv4, intervalo, máscara o nombre de dominio y, a continuación, haga clic en Aceptar.
- ✓ Para agregar nombres de dominio, debe habilitar primero las restricciones de nombre de dominio haciendo clic en Edit Feature Settings en el panel Actions y, a continuación, seleccionando Enable domain name restrictions en el cuadro de diálogo Edit IP and Domain Restrictions Settings.

OPCIÓN "AUTHORIZATION RULES"

Se puede conceder o denegar el acceso de dominios, grupos de equipos o equipos concretos a sitios, aplicaciones, directorios o archivos de su servidor. Por ejemplo, su servidor de intranet hospeda contenido que está disponible para todos los empleados, además del contenido que deberían ver sólo los miembros de grupos concretos, como Finanzas o Recursos humanos. Al configurar las reglas de autorización de direcciones URL, puede evitar que empleados que no sean miembros de esos grupos especificados obtengan acceso al contenido restringido.

Los procedimientos para configurar las reglas de la autorización de direcciones URL se pueden realizar en los siguientes niveles de IIS:

- ✓ Servidor web
- ✓ Sitio
- ✓ Aplicación
- ✓ Archivo (dirección URL)

Se requiere que el siguiente módulo este habilitado:
UrlAuthorizationModule

El mismo que es habilitado cuando en los Servicios del Rol de IIS en la parte de seguridad se habilita la opción "URL Authorizations".

OPCIONES "ERROR PAGES" Y "DIRECTORY BROWSING"

Estas secciones podrán quedar configuradas por defecto a menos que por temas operativos se deban aplicar configuraciones específicas.

CONSIDERACIONES DE SEGURIDAD SOBRE EL SERVICIO FTP

Como parte de los servicios incluidos en el producto IIS 7 se incluye un servidor FTP (File Transfer Protocolo) básico, el cual presenta limitadas características de seguridad, principalmente en relación a la ausencia de mecanismos de encripción del canal de comunicaciones cliente servidor, y al pobre esquema de autenticación brindado. Debido a ello, se deberán tomar en cuenta las siguientes consideraciones generales:

- ✓ Siempre que sea posible se deberá deshabilitar el servicio;
- ✓ En caso de requerir el servicio FTP en servidores públicos, se deberá estudiar la posibilidad de utilizar algún producto software alternativo que permita implementar SFTP (FTP con encripción SSL);
- ✓ Será recomendable configurar el servidor FTP de forma tal que se prohíba la escritura de archivos en el mismo;
- ✓ En caso que sea necesario escribir archivos en el servidor, se deberá crear un directorio independiente en el cual se alojarán los nuevos documentos.
- ✓ Sin embargo, en caso de ser requerido el servicio FTP provisto por el producto IIS 7, el mismo deberá ser configurado siguiendo los lineamientos presentados a continuación.

Cabe recalcar que para poder administrar este servicio se debe tener instalada la compatibilidad con la consola administrativa de IIS 6.

SOLAPA "FTP SITE" (SITIOS FTP)

En primer lugar se deberá configurar la información de identificación del sitio FTP, el número de conexiones y el tiempo de expiración de las sesiones inactivas, entre otros parámetros generales.
En esta sección deberán implementarse los siguientes lineamientos de configuración:

Puerto TCP: Siempre que sea posible se deberá modificar el puerto por defecto asignado a este servicio (puerto 21), utilizando el puerto 2121 para la prestación del mismo.
Auditoria: Se deberá habilitar la auditoría tildando la opción "Enable Logging" y seleccionando el formato de "LOGs" con formato "W3C Extended Log File Format".
Límite de conexiones concurrentes: El número máximo de sesiones concurrentes permitidas deberá estar limitado para acotar el impacto de posibles ataques de denegación de servicio. Si bien este valor dependerá de la función y el dimensionamiento del servicio, el mismo no deberá ser mayor a 500 conexiones

concurrentes.

Tiempo de expiración de las sesiones: Se deberá establecer un tiempo menor a 30 minutos para la expiración de sesiones inactivas. Preferentemente, y en caso de ser factible, dicho valor deberá estar definido en 10 minutos (600 segundos).

La siguiente figura muestra la configuración discutida previamente:

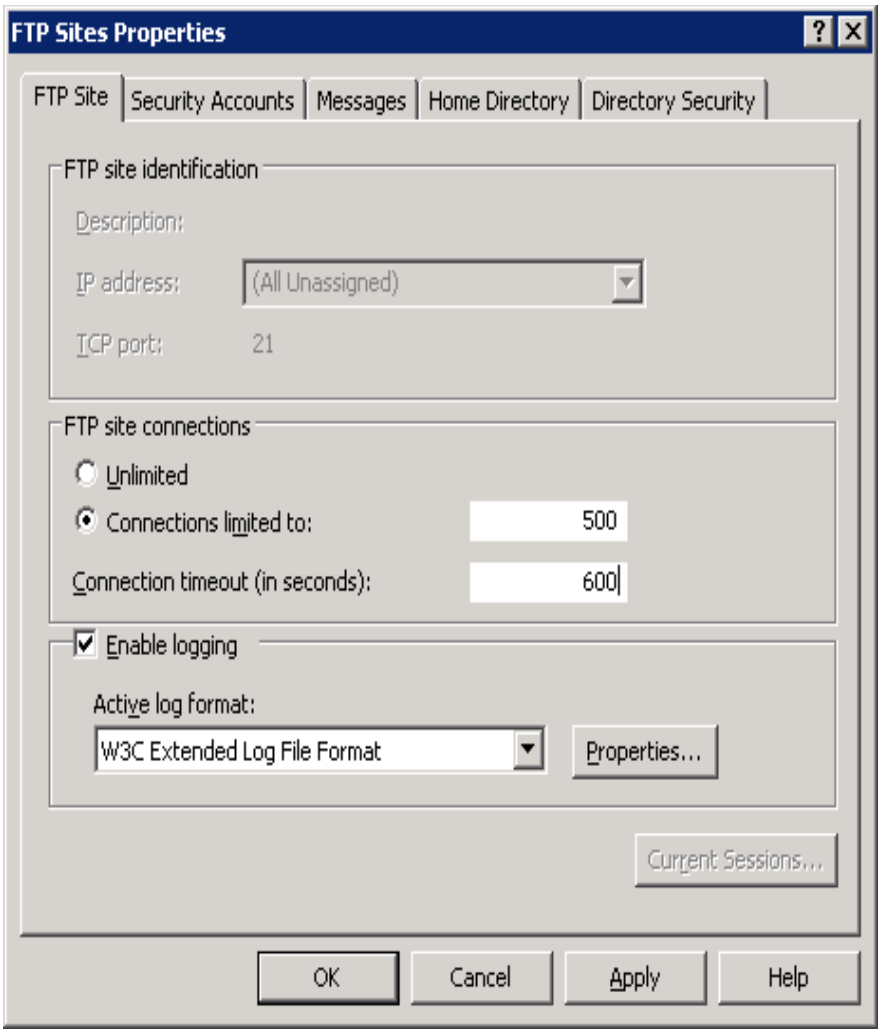


Figura 19: Configuración del servicio FTP

Aquellos valores que no han sido especificados podrán adoptar el valor más conveniente de acuerdo al criterio del administrador de la plataforma y/o a la naturaleza del servicio.

SOLAPA "SECURITY ACCOUNTS" (CUENTAS DE SEGURIDAD)

Esta solapa permite configurar si el servicio FTP podrá o no aceptar conexiones anónimas, en la misma se deberá, siempre que sea posible, deshabilitar la opción "Allow Anonymous Connections", ya que la misma permite ingresar al servicio y consultar información sin tener un usuario ni contraseña válidos.

SOLAPA "MESSAGES" (MENSAJES)

Existen 3 tipos de mensajes que se pueden mostrar al usuario, estos son: "Mensaje de inicio de sesión", "Mensaje de salida" y "Mensaje de cantidad máxima de conexiones".

Dado que este tipo de mensajes podría brindar información del producto utilizado a un potencial atacante, en todos los casos se recomienda presentar mensajes donde no se indiquen datos sensibles del servicio como ser: versión del sistema operativo, datos del responsable del sitio, etc.

Siempre que sea posible se deberán implementar los siguientes mensajes:

- ✓ Banner: "Welcome / Bienvenido".
- ✓ Welcome: "ADVERTENCIA: El uso de este sistema está restringido solamente a personal autorizado. Todo otro uso del mismo será penado de acuerdo a las políticas vigentes de la Compañía o a la legislación vigente en el país. Ante cualquier inconveniente comunicarse con Seguridad Informática. Muchas gracias.".
- ✓ Exit: "La sesión ha finalizado. Muchas gracias por utilizar el servicio".
- ✓ Maximum Connections: "Ha ocurrido un error. Por favor contacte al departamento de Seguridad Informática".

SOLAPA "HOME DIRECTORY" (DIRECTORIO RAIZ)

En esta solapa se configurarán los permisos de acceso al directorio FTP, así como la ubicación del mismo.

Este directorio deberá, siempre que se pueda, contemplar los siguientes criterios:

- ✓ La carpeta en la cual se alojarán los archivos y carpetas utilizadas por el servicio FTP, deberá estar definida a nivel local.
- ✓ No debe localizarse en la misma unidad que el sistema operativo del servidor.
- ✓ Solo debe tener acceso de lectura.
- ✓ Si se requiere que los usuarios realicen "Uploads" de archivos, se deberán crear dos directorios en el directorio del ftproot. Uno, solamente con acceso de lectura a los archivos que están disponibles para una transferencia directa, y uno con permisos de escritura solamente para el "Upload" de archivos.

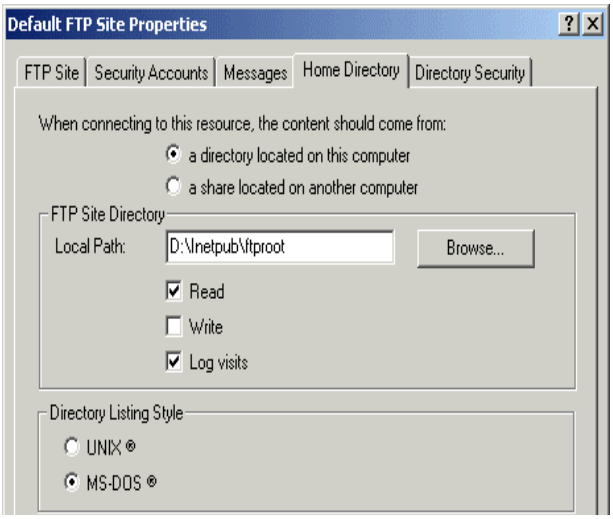


Figura 20: Configuración de permisos de acceso del directorio FTP

SOLAPA "DIRECTORY SECURITY" (SEGURIDAD DE SIRECTORIOS)

Esta solapa permitirá establecer filtros de acceso basados en la utilización de direcciones IP de origen. Dichos filtros deberán ser establecidos contemplando que siempre que se pueda se deberá permitir el acceso "únicamente" a aquellos usuarios que requieran acceder al servicio (Por ejemplo IPs de los administradores).

CONSIDERACIONES DE SEGURIDAD SOBRE EL SERVICIO SMTP

El servidor SMTP no está instalado de forma predeterminada. SMTP se puede agregar a través del área Resumen Características de la herramienta Administrador de servidores en Windows Server® 2008.

Al igual que en el caso del servicio FTP, en caso de no ser necesaria la utilización de este servicio, no se debe instalar. Caso contrario, el mismo deberá ser configurado siguiendo las correspondientes instrucciones.

A continuación se detallan las configuraciones que deben realizarse en las propiedades del servicio SMTP (Default SMTP Virtual Server Properties), para mitigar ciertos riesgos asociados con el mismo.

Cabe recalcar que para poder administrar este servicio se debe tener instalada la compatibilidad con la consola administrativa de IIS 6.

SOLAPA "GENERAL"

En esta solapa se muestran las opciones generales del servidor SMTP, como ser la interfaz de red a través de la cual atenderá las peticiones de los usuarios y las opciones de auditoría.

En esta sección se deberán configurar los siguientes aspectos:

- ✓ Habilitar la auditoria. Para eso debe estar seleccionada la opción de "Enable Logging";
- ✓ Definir el tipo de LOG a generar, seleccionando el formato de "LOGs" con formato "W3C Extended Log File Format";
- ✓ Establecer el tiempo máximo para desconexión de sesiones inactivas en 10 minutos;
- ✓ Limitar el número de sesiones concurrentes de ser posible a 50 conexiones, aunque dicho valor podrá ser adaptado de acuerdo a los requerimientos del servicio.

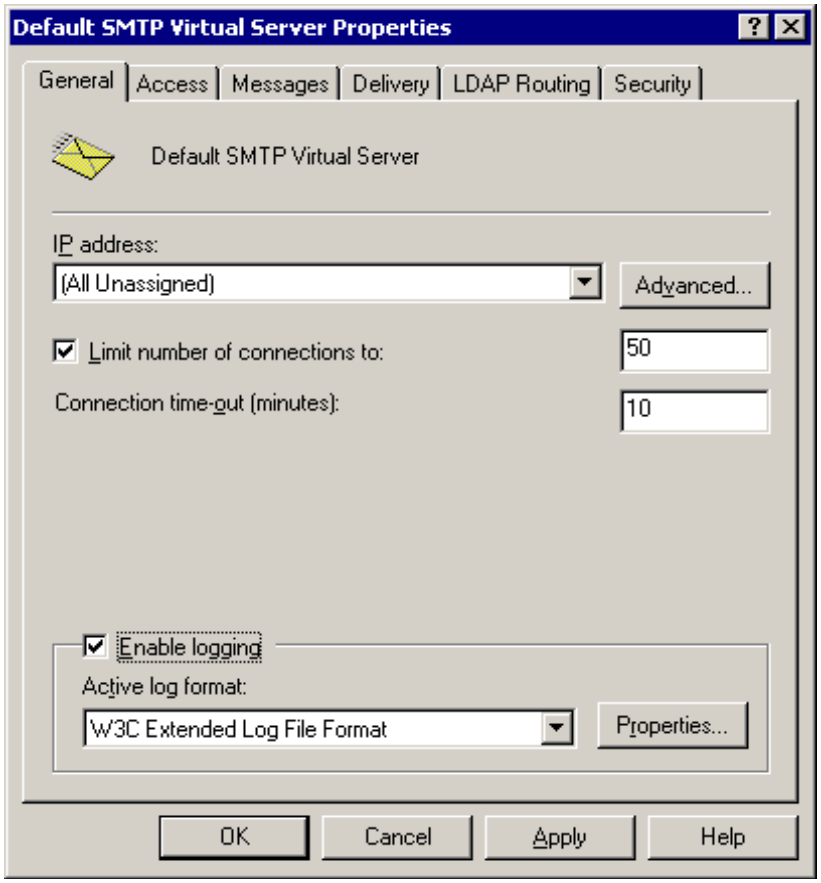


Figura 21: Configuración del servicio SMTP

SOLAPA "ACCESS" (ACCESO)

En esta sección se establecen aspectos de configuración relativos al control de accesos como ser:

- ✓ Control de acceso
- ✓ Seguridad del canal de comunicaciones
- ✓ Control de conexiones
- ✓ Restricciones de Relay

A continuación se profundizan los valores recomendados para cada uno de los aspectos mencionados.

CONTROLES DE ACCESO

Las opciones de autenticación de SMTP son similares a las presentadas para el servicio HTTP.

Siempre que sea posible se deberá evitar el acceso anónimo debiendo seleccionarse autenticación "Básica con TLS" o autenticación integrada a Windows "Windows Security Package"

SEGURIDAD EN LAS COMUNICACIONES

IIS cuenta con TLS (Transfer Layer Security) como medio para establecer conexiones encriptadas. Siempre que sea posible se deberá seleccionar "Require secure channel" y "Require 128-bit encryption", de acuerdo a la siguiente figura:

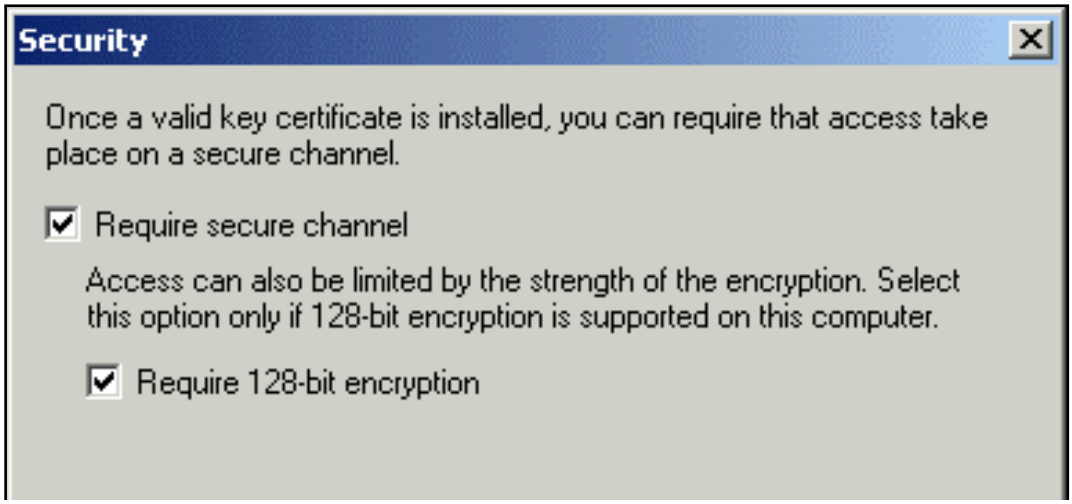


Figura 22: Configuración de acceso

CONTROL DE CONEXIONES

Se deben definir, en el caso que existan, restricciones de IP o Nombres de Dominio al servidor SMTP, para mitigar el riesgo de acceso y utilización del servicio por parte de personal no autorizado.

RESTRICCIONES DE RELAY

Se deberá permitir el "Relay" únicamente a servidores preestablecidos, los cuales deberán ser listados en la sección "Relay Restrictions" por dirección IP.

Así mismo, la opción "Allow all computers which successfully authenticate to relay, regardless of the list above", deberá quedar deshabilitada.

SOLAPA "MESSAGES" (MENSAJES)

Esta solapa nos brinda la posibilidad de configurar el tamaño de los mensajes, la cantidad máxima de peticiones admitidas por el servidor. Los valores deben ser establecidos de acuerdo a los requerimientos del servicio.

SOLAPA "DELIVERY" (ENTREGA)

En caso que se requiera activar la autenticación para mensajes salientes, se deberá acceder a esta solapa para seleccionar uno de los métodos de autenticación disponibles.
Siempre que sea posible se deberá evitar el acceso anónimo debiendo seleccionarse autenticación "Básica con TLS" o autenticación integrada a Windows "Windows Security Package"

SOLAPA "SECURITY" (SEGURIDAD)

Esta sección permite definir los grupos de usuarios responsables de administrar el servicio. A tal fin se deberá crear un grupo local llamado "SMTPAdmins" al cual se deberán asociar los usuarios habilitados para realizar tareas administrativas.

Dicho grupo deberá ser incluido en la sección "Security" para delegar los privilegios de administración sobre el servicio junto con el grupo local "Administrators" o "Administradores.
Se debe definir correctamente el grupo de operadores que tienen permisos full sobre el servidor SMTP. Adicionalmente se debe incluir el grupo "Administrators", "LOCAL SERVICE" y "NETWORK SERVICE".

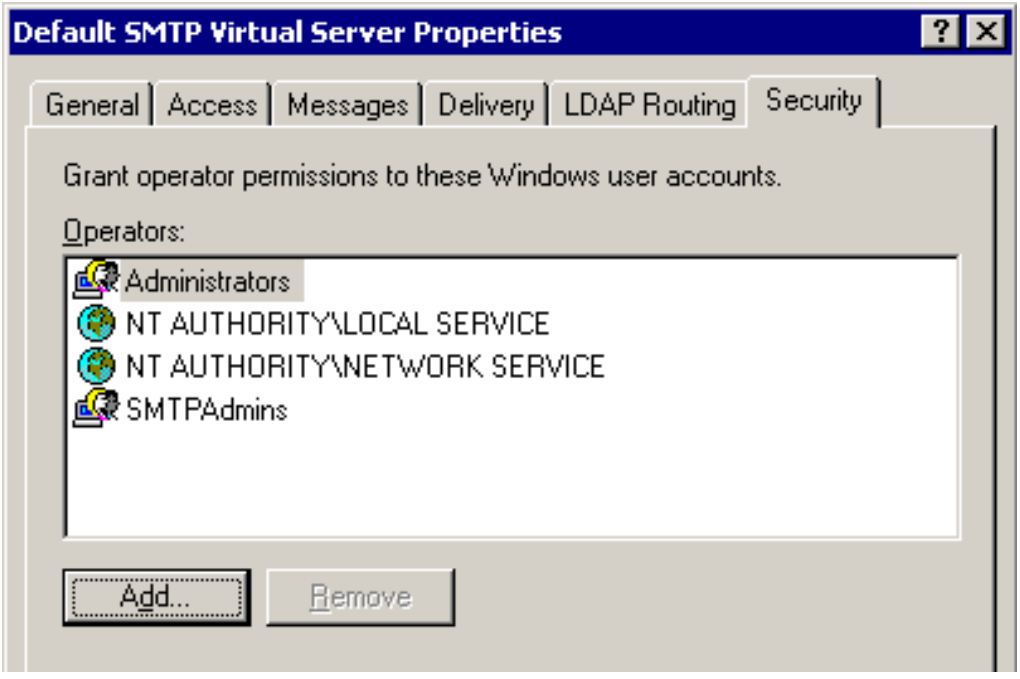


Figura 23: Configuración del servicio SMTP

DOCUMENTACIÓN DE REFERENCIA

Especificación de servicios, grupos especiales y derechos de usuarios asignados
http://technet.microsoft.com/en-us/library/ms143504.aspx

Encripción transparente de datos (TDE)
http://technet.microsoft.com/en-us/library/bb934049.aspx#Mtps_DropDownFilterText

Auditoría de datos
http://technet.microsoft.com/en-us/library/cc280663.aspx