
*Banco de la República*
*Bogotá D. C., Colombia*

**Departamento de Seguridad Informática**
SUBGERENCIA DE INFORMÁTICA

# MECANISMOS DE SEGURIDAD DE LOS SERVICIOS INFORMÁTICOS

**USI-ASI-1**

Junio de 2007

Versión 3

# CONTENIDO

# 1 INTRODUCCIÓN

## 1.1 OBJETIVO

Dar a conocer y oficializar entre los clientes de sistemas informáticos del Banco de la República, las tecnologías de seguridad informática que aplican a los servicios basados en plataformas informáticas.

Este documento sirve igualmente para determinar las responsabilidades de los clientes frente a los mecanismos de seguridad.

## 1.2 ALCANCE

Este documento aplica para los servicios en producción basados en plataformas informáticas que soportan operaciones del negocio.

## 1.3 AUDIENCIA

Está dirigido a todos los clientes externos e internos que sean usuarios de los Servicios Electrónicos del Banco de la República.

# 2 CONTENIDO

A continuación se describirán las tecnologías de seguridad informática que buscan garantizar la seguridad informática de los sistemas informáticos del Banco.

## 2.1 DESCRIPCIÓN DEL MODELO DE SEGURIDAD INFORMÁTICA DEL BANCO DE LA REPUBLICA

El modelo de seguridad informática para el Banco de la República está conformado por políticas, estándares, procedimientos y mecanismos de seguridad, basados en siete fundamentos que son la plataforma para la conformación del modelo.

Son fundamentos de la seguridad informática: confidencialidad, integridad, disponibilidad, autenticación, autorización, no repudiación y observancia de la información.

a) *Confidencialidad*: Cuando la información es solo accesible por aquellos a los cuales se ha autorizado a tener acceso. Un ejemplo de control para garantizar la confidencialidad son los mecanismos de encripción.

b) *Integridad*: Cuando la información es exacta y completa. Un ejemplo de control para garantizar la integridad son los algoritmos de cifras de control.

) *Disponibilidad*: Cuando la información es accesible a los usuarios autorizados en el momento de requerirla. Un ejemplo de control para garantizar la disponibilidad son los planes de contingencia.

d) *Autenticación*: Cuando se puede garantizar la identidad de quien solicita acceso a la información. Ejemplo: Firmas digitales.

e) *Autorización:* Cuando la información es accedida solo por los usuarios que tienen los privilegios necesarios y suficientes para hacerlo. Ejemplo: perfiles de usuario en las aplicaciones.

f) *No repudiación*: Cuando la información involucrada en un evento corresponde a quien participa, quien no podrá evadir su intervención en éste. Ejemplo: Un emisor de un mensaje no puede negar que lo generó y viceversa, un receptor de un mensaje no puede negar que lo recibió.

g) *Observancia*: Cuando la información relacionada con las acciones y actividades de los usuarios (personas o procesos) se encuentra debidamente registrada y monitoreada. Adicionalmente, la administración de la seguridad y accesos privilegiados también son monitoreados. La observancia promueve el adecuado funcionamiento de todo el modelo de seguridad informática. Ejemplo: Logs de las transacciones que un usuario ha realizado en un sistema determinado.

## 2.2 DESCRIPCIÓN DE LOS MECANÍSMOS DE SEGURIDAD INFORMÁTICA

En la siguiente tabla se presentan los mecanismos de seguridad informática en relación con el fundamento que permite garantizar, de tal manera que en el momento de utilizar alguno de estos mecanismos es importante tener claro cual de los fundamentos se está soportando.

Es recomendable utilizar estos mecanismos en combinación con el fin de proveer de manera integral la seguridad.

En las siguientes secciones del capítulo 2.2 se aclararán un poco más las tecnologías/mecanismos que se presentan a continuación.


| No. | *Tecnologías/Fundamentos* | Autenticación | Integridad | Confidencialidad | No Repudiación | Autorización | Disponibilidad | Observancia | Descripción |
|---|---|---|---|---|---|---|---|---|---|
| 1 | ACL | X | | | | X | | | Lista de Control de Acceso sobre el servidor de WEB |
| 2 | Alta disponibilidad (soluciones Hardware - Software) | | | | | | X | | Sistemas Cluster para máquinas y/o discos espejados y/o sincronizados cada T tiempo |
| 3 | Análisis de Riesgos e Impactos | X | X | X | X | X | X | X | Metodologías, herramientas y estándares en gestión del riesgo |
| 4 | Antivirus | | X | | | | X | | Herramientas antivirus |
| 5 | Atención de Incidentes | X | X | X | X | X | X | X | Grupo de atención de incidentes de seguridad de la información |
| 6 | Auditorias Bases de Datos, Sistemas Operativos, Webs, equipos de comunicación | | | | X | | | X | Herramientas propias o de terceros que permite administrar y hacer seguimiento a las auditorias |
| 7 | Biométricos | X | | | | | | | Esquemas de autenticación vía la característica "algo que se es" |
| 8 | Certificados | X | X | | X | | | | Sobres digitales para garantizar la procedencia de una llave pública. |
| 9 | Cifras de Control (Hash) | | X | | | | | | Control de integridad. |
| 10 | Códigos de Autenticación | X | | | | | | | Mecanismos de autenticación para contingencia. |
| 11 | Continuidad del Negocio | | | | | | X | | Planes de contingencia. Coordinación y administración de la crisis. Propender porque los servicios corporativos estén disponibles los servicios informáticos del Banco. |
| 12 | Doble Autenticación | | | | | X | | | Control de segregación (solicita una segunda autenticación). |
| 13 | Doble Intervención | | | | | X | | | Control de segregación (solicita la redigitación de datos). |
| 14 | Encripción Asimétrica | X | X | X | X | | | | Ciframiento a través de llaves complementarias. No hay problema en la distribución de las llaves. |
| 15 | Encripción Simétrica | | X | X | | | | | Ciframiento a través una sola llave. Puede haber problemas en la distribución de las llaves. Es más o menos 1.000 veces más rápido que los algoritmos asimétricos. |
| 16 | Firewalls | X | | | | X | | X | Barrera de contención del medio de Internet y/o redes privadas hacia y/o desde la red interna del Banco. |
| 17 | Firmas Digitales | X | X | | X | | | | Producto del uso de tecnologías de hashing y llaves públicas y privadas. Garantizan autenticidad, integridad y no repudio. |
| 18 | Horarios y Holguras | | | | | X | | | Restricciones de horario en las transacciones. |
| 19 | IDS, IPS, Scans | | X | | | X | X | X | Tecnologías de detección de intrusos. |
| 20 | Monitoreo 7x24 | X | X | X | X | X | X | X | Servicio de monitoreo en línea (todos los días del año durante las 24 horas) de los segmentos y objetos más sensibles dentro de la organización. |
| 21 | Passwords | X | | | | | | | Mecanismo de autenticación basado en la característica "algo que se sabe" |
| 22 | Políticas de Acceso | | | | | X | | X | Módulos independientes de control de acceso. Cada servicio corporativo requiere de políticas de autorización |
| 23 | PKI | X | X | X | X | X | | | Infraestructura de Llaves Públicas y Privadas. |
| 24 | Políticas de Seguridad | X | X | X | X | X | X | X | Políticas, normas y estándares de seguridad que rigen los servicios informáticos del Banco. |
| 25 | Pruebas de Vulnerabilidad | X | X | X | X | X | X | X | Mecanismos especializados en probar modelos y tecnologías para descubrir vulnerabilidades. |
| 26 | SET | X | X | X | X | | | | Estándar seguro en el pago de transacciones vía Internet. |
| 27 | Smart Cards (token cards - RSA) | X | | | | | | | Tarjetas de autenticación vía tecnología RSA. Generan un único token que puede ser utilizado una sola vez y es válido durante un minuto. Se basa en dos características "algo que se tiene y algo que se sabe". |
| 28 | SSL | X | X | X | | | | | Secure Socket Layer. Protocolo de seguridad. |
| 29 | Transferencia segura de archivos | X | X | X | X | X | | X | Sistema seguro de transferencia de archivos |
| 30 | VPN | X | X | X | X | | X | | Tecnología de redes virtuales privadas. Túneles de acceso seguro al Banco (Triple-DES, AES). |

### 2.2.1 POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS

Para que la infraestructura de seguridad opere debidamente deben diseñarse, implantarse y divulgarse políticas, estándares y procedimientos claros que den las pautas a seguir frente al modelo de seguridad.

Es importante tener en cuenta que algunos controles tendrán que ser de tipo procedimental en los casos donde no aplique tener un control automatizado, para lo cual deben seguirse las políticas y estándares particulares para el manejo de la información.

Igualmente cada mecanismo de seguridad cuenta con los respectivos procedimientos e instructivos de utilización que servirán para que los usuarios de los mecanismos de seguridad sigan los estándares de seguridad informática.

A continuación se definen los términos política, estándar y procedimiento.

Política: Una política de seguridad informática es una directriz de alto nivel en la cual se expresan valores y objetivos de la organización para proporcionar dirección y soporte a la alta gerencia en los temas relacionados con seguridad informática.

Estándar: Conjunto de requisitos de obligatorio cumplimiento, que especifican tecnologías y métodos, para implementar las políticas de seguridad informática expuestas por la alta gerencia, establecen un marco de acción coordinado que busca alinear los esfuerzos de la organización para procurar los fundamentos de la seguridad informática.

Procedimiento: Define un conjunto de pasos operacionales específicos sugeridos para efectuar una labor particular, que se puede modificar en respuesta a los cambios en la dinámica del negocio y la tecnología. P.e Procedimiento para toma de respaldos.
En términos generales, este mecanismo apoya todos los fundamentos de seguridad informática.

### 2.2.2 PLAN DE CONTINUIDAD DEL NEGOCIO

Un plan de continuidad del negocio pretende garantizar la continuidad de las operaciones de la organización, a pesar de eventos fortuitos o desastres que puedan presentarse. En esto planes se definen las responsabilidades, las notificaciones, las acciones, la recuperación, la vuelta a la normalidad, entre otros elementos, que permiten que se logre la disponibilidad de los servicios en los tiempos y momentos requeridos.

### 2.2.3 PROCEDIMIENTOS DE CONTINGENCIA Y BACKUPS

Un plan de contingencia permite actuar y recuperarse adecuada y oportunamente frente a la ocurrencia de un evento adverso que atente contra la buena marcha del negocio. En este punto es vital la participación de los clientes en las acciones que los procedimientos de contingencia estipulen.

Con el fin de garantizar disponibilidad de la plataforma que soporta los servicios, es importante contar con un plan de contingencia adecuado. Así mismo tener monitoreo de la utilización de los recursos de las máquinas que se están consumiendo con el fin de no tener sobrecarga en las mismas.

El manejo de backups es altamente sensible, por cuanto las políticas y estándares en este sentido deben ser bastante sólidas.

### 2.2.4 ALTA DISPONIBILIDAD Y TOLERANCIA A FALLAS

Debido a la necesidad de mantener los servicios y aplicaciones críticas operativas de manera continua, tanto a nivel de procesamiento como en comunicaciones, se cuenta con equipos de hardware para tolerancia a fallas y alta disponibilidad que permite brindar el nivel de disponibilidad que se requiere para que estos servicios sean ofrecidos adecuadamente, de tal manera que el impacto sobre la operación es mínimo utilizando estos sistemas.

### 2.2.5 CONTRASEÑAS (PASSWORDS)

Las contraseñas o passwords son palabras de conocimiento exclusivo de un individuo particular, y de la buena utilización de éstas y las política que sobre ellas aplique depende la garantía de autenticación en un sistema.

### 2.2.6 SISTEMAS DE AUTENTICACIÓN (TARJETAS O BIOMÉTRICOS )

Los sistemas de autenticación que exigen al individuo presentar un elemento que tiene en su poder o que lo caracteriza en su cuerpo, permite autenticar de manera más certera su identidad, minimizando así la posibilidad de una suplantación frente a un sistema.

### 2.2.7 CÓDIGOS DE AUTENTICACIÓN

Los códigos de autenticación son números aleatorios que identifican de manera única a un individuo.

Los códigos de autenticación se encuentran en un sobreflex que son entregados a cada entidad que quiera autenticarse con el Banco de la República.

La forma de utilizarlos es que la entidad selecciona secuencialmente del sobrefex que le pertenece uno de estos códigos y lo escribe en un papel, para luego enviarlo bien sea por fax o mediante mensajero hacia el Banco de la República, donde mediante el software GAC es validado a que entidad pertenece.

### 2.2.8 POLÍTICAS DE ACCESO

Una vez un individuo a sido autenticado y se encuentra dentro del sistema, el siguiente paso es determinar a que tiene derecho de acceder y que procesos puede ejecutar, de tal manera que mediante los perfiles de acceso se determina el comportamiento que cada individuo puede tener en un sistema.

### 2.2.9 ACL O LISTAS DE CONTROL DE ACCESO

Una lista de control de acceso es una tabla que informa qué usuarios pueden entrar a un sistema y qué derechos de acceso tiene cada uno. En nuestro caso, las ACL son un servicio provisto por el servidor Web del Banco para restringir la entrada a un sitio Web.

En una ACL cada carga tiene asociada una clave (que se encripta por seguridad). La estructura de una ACL es:

```
CARGA: CLAVE ENCRIPTADA

CARGA: CLAVE ENCRIPTADA

CARGA: CLAVE ENCRIPTADA
```

Para entrar a un sistema protegido con una ACL aquél preguntará por una carga (o nombre de usuario) y por una clave. Si la carga introducida está especificada dentro de la ACL y la clave colocada es la respectiva para esa carga (proceso que se conoce como validación con ACL), el usuario puede entrar al sistema.

Cada ACL está asociada a una página, de manera que los usuarios en ella registrados son los que están autorizados a acceder a esta página.

### 2.2.10 CIFRAS DE CONTROL

Las cifras de control son números que se calculan mediante algoritmos denominados HASH, utilizando la información que se pretende proteger, asociando el número obtenido de manera única con esta información, de tal manera que si se modifica la información, la cifra de control deja de ser válida.

## 2.2.11 ENCRIPCIÓN SIMÉTRICA Y ASIMÉTRICA

La encripción en general permite brindar confidencialidad a la información mediante algoritmos matemáticos especiales y datos privados que solo quien los conozca podrá obtener acceso a la información.

Uno de estos datos privados es una palabra clave secreta, sin embargo en los algoritmos simétricos esta clave secreta debe ser conocida tanto por el individuo que encriptó la información como por el individuo que la pretende desencriptar, de tal manera que debe idearse una manera "confiable" de hacer conocer esta clave al segundo individuo, teniendo una vulnerabilidad en el sentido de que ya la clave es conocida por mas de dos personas dejando de ser secreta.

Por otro lado los algoritmos asimétricos manejan dos palabras claves, una de ellas es "secreta" y la otra es "pública", de tal forma que para encriptar alguna información, se encriptaría con la primera de ellas y se desencriptaría con la segunda que es de conocimiento público, permitiendo así mantener la clave "secreta" en conocimiento de una sola persona, quien es su dueño.

## 2.2.12 LLAVES PÚBLICAS Y PRIVADAS

En este esquema, cada uno de los participantes tiene dos llaves: una que dará a conocer, llamada llave pública, y una que no compartirá, llamada llave privada. Estas llaves sirven para dos eventos de seguridad:

Para encriptar la información de tal manera que un mensaje encriptado con cierta llave pública sólo podrá ser descifrado con la llave privada correspondiente.

Para firmar la información: Mediante algoritmos especiales cualquier individuo puede emplear su llave privada, que solo es conocida por él, para firmar la información y el receptor utiliza la llave pública correspondiente para verificar quien firmó la información.

Cuando se manejan llaves públicas y privadas, se requiere de una etapa previa que se denomina intercambio de llaves, la cual consiste en que las dos partes que van a comunicarse se entregan la una a la otra, la llave pública.

Si se emplea la llave privada del emisor, para firmar digitalmente la información y adicionalmente la llave pública del receptor para encriptar la información, se podrá garantizar los siguientes fundamentos con este mecanismo:

- Autenticación
- Confidencialidad.
- Integridad
- No repudiación

### 2.2.13 FIRMAS DIGITALES

Las firmas digitales permiten garantizar la procedencia de la información mediante el uso de llaves pública y privadas, de tal manera que mediante algoritmos particulares cualquier individuo puede emplear su llave "privada", que solo es conocida por él para firmar la información y el receptor utiliza la llave "pública" correspondiente para verificar quien firmó la información.

Los fundamentos que se garantizan con este mecanismo son:

- Autenticación
- No repudiación
- Integridad

### 2.2.14 CERTIFICADOS DIGITALES

Los certificados digitales permiten a un individuo ser autenticados mediante esquemas de llaves públicas y privadas. Un certificado digital es como una "tarjeta de crédito electrónica" que establece su identidad cuando se está haciendo una transacción en el Web. Ésta es validada por una autoridad de certificación (CA).

Un certificado digital contiene los siguientes datos entre otros:

- Un número de serie
- La fecha de expiración
- La firma digital de la entidad emisora del certificado (para verificar la validez del mismo)
- La llave pública.

Estos certificados son entregados a las personas o entidades que así lo requieran (en este caso, el BR), por compañías especializadas que tienen un alto grado de confiabilidad en el medio de las transacciones electrónicas.

### 2.2.15 INFRAESTRUCTURA DE LLAVES PÚBLICAS (PUBLIC KEY INFRAESTRUCTURE)

Una PKI es una nueva tecnología de seguridad, es la plataforma base para garantizar gran parte de la seguridad del manejo de información electrónica, es por esto que todos los elementos que conformen el manejo de este tipo de documentos deben integrarse y acoplarse muy bien a esta plataforma.

Una PKI es una infraestructura de seguridad de gran alcance con servicios basados en técnicas y conceptos de llaves públicas, sus funciones son:

- Brindar interoperatividad entre sistemas de manera segura .
- Facilitar seguridad en las operaciones electrónicas .

- Fomentar el desarrollo de los mecanismos del Comercio Electrónico.

- Una PKI, cubre aspectos como la administración de las llaves, su registro, su revocación, manejo de llaves históricas, almacenamiento, control, auditorias, entre otros.

Los componentes de una PKI son:

- Autoridad Registro: Se encarga de registrar certificados y llaves nuevas y manejo de solicitudes.

- Autoridad Certificadora: Se encarga de certificar la validez de un certificado, maneja expiraciones y revocaciones.

- Listas de certificados revocados: Listas con los certificados que ya no tienen validez.

- Repositorio de certificados y llaves vigentes: Base de datos con las llaves y certificados vigentes.

- Repositorio de llaves y certificados históricos: Base de datos con las llaves y certificados históricos.

Si se emplea la llave privada del emisor, para firmar digitalmente la información y adicionalmente la llave pública del receptor para encriptar la información, se podrá garantizar los siguientes fundamentos con este mecanismo:

- Autenticación

- Confidencialidad.

- Integridad

- No repudiación

### 2.2.16 SECURE SOCKET LAYER (SSL)

SSL es un protocolo diseñado para adicionar varios aspectos de seguridad a la transmisión de mensajes vía HTTP, el protocolo propio de la comunicación en Internet.

SSL modifica levemente el protocolo TCP/IP, colocando una capa adicional entre las capas de HTTP (protocolo de transferencia de hipertexto) y la de IP (protocolo Internet), garantizando los siguientes fundamentos de seguridad punto a punto:

- Autenticación del cliente y del servidor

- Confidencialidad

- Integridad

- Autenticación

Se define como la propiedad de garantizar la identidad de quien solicita acceso a la información, es decir, la certeza por una de las partes de que aquel con quien se está comunicando sí es quien dice ser. La autenticación en una comunicación cliente-servidor puede ser de las siguientes formas:

- Autenticación del cliente por parte del servidor
- Autenticación del servidor por parte del cliente

Una comunicación con SSL ofrece una autenticación del servidor por parte del cliente. La validación del cliente por parte del servidor es opcional y depende de la configuración del servidor.

Estos certificados son entregados a las personas o entidades que así lo requieran (en este caso, el BR), por compañías especializadas que tienen un alto grado de confiabilidad en el medio de las transacciones electrónicas.

Si un usuario va a entrar en un sitio protegido con un certificado digital, un mensaje con la información del certificado aparecerá. El usuario podrá verificar su validez y decidir su entrada al sitio.

**Confidencialidad**

Se refiere a que la información es solo accesible por aquellos a los cuales se ha autorizado a tener acceso. Un ejemplo de control para garantizar la confidencialidad son los mecanismos de encripción.

Para esto la información se encripta mediante un protocolo de llaves públicas y privadas.

En una comunicación con SSL, los participantes se envían mutuamente sus llaves públicas, y cada emisor encripta los mensajes (paquetes de información) con la llave pública del destinatario y los mensajes que recibe los desencripta con su propia llave privada.

Cuando se manejan certificadas digitales en ambas partes de la comunicación, se utilizan las llaves públicas establecidas en aquellos. De usarse certificados digitales sólo en el servidor, el intercambio de llaves se hace entre la llave pública del servidor y una llave pública preinstalada en el navegador (Netscape, Explorer) del cliente.

Después de que se ha entrado a uno de los sistemas por medio de una carga y una contraseña válidas, la comunicación se encriptará hecho que se notará por un dibujo de candado en una de las esquinas inferiores del navegador:

**Integridad de la información transmitida**

Significa garantizar que la información que llega a su destino exacta y completa, tal cual como fue enviada desde el origen. Es decir, es el hecho de que para cada uno de los paquetes que se transmiten, bien desde la estación del cliente hasta el BR como en sentido inverso, se valida que la información llega intacta mediante la verificación de la firma con que fueron generados.

### 2.2.17 SECURE ELECTRONIC TRANSACTION

SET es un protocolo diseñado para adicionar varios aspectos de seguridad a la realización de transacciones. Este fue soportado inicialmente por Mastercard, Visa, Microsoft, Netscape entre otros. Con SET, un individuo tiene una "billetera electrónica" y una transacción es conducida y verificada usando una combinación de certificados digitales y firmas digitales entre el comprador, el vendedor y el banco de tal forma que asegura la privacidad y confidencialidad. SET hace uso de SSL (Secure Socket Layer), STT (Secure Transaction Technology) y S-HTTP (Secure Hypertext Transfer Protocol). SET utiliza algunos, aunque no todos, los aspectos de una PKI.

Como trabaja SET:

- Asuma que un cliente tiene un browser habilitado para usar SET tal como NetScape o Microsoft Internet Explorer y que el proveedor de la transacción (Banco, almacén, etc) tienen un servidor habilitado para usar SET.

- El cliente obtiene una tarjeta de crédito MasterCard o Visa en cualquier banco.

- El cliente recibe un certificado digital. Este archivo electrónico funciona como una tarjeta de crédito para compras en línea o cualquier otra transacción. Esta incluye una llave pública con una fecha de expiración y está validada por el banco.

- El vendedor también recibe un certificado digital del banco. Este certificado incluye la llave pública del vendedor y la llave pública del banco.

- El cliente realiza una orden por la página Web.

- El browser del cliente recibe y confirma con el vendedor que el certificado del vendedor sea válido.

- El browser envía la información de la orden. Este mensaje es encriptado con la llave pública del vendedor, la información del pago, la cual es encriptada con la llave pública del banco (de tal manera que el vendedor no la puede leer) y la información que asegura que el pago solo puede ser usada con esta orden particular.

- El vendedor verifica la identidad del cliente mediante la firma digital del certificado del cliente. Esto puede ser hecho refiriéndose al certificado del banco o a un tercero.

- El vendedor envía el mensaje con la orden al banco. Esto incluye la llave pública del banco, la información del pago del cliente (la cual el vendedor no puede decodificar) y el certificado del vendedor.

- El banco verifica el vendedor y el mensaje. El banco usa la firma digital del certificado con el mensaje y verifica lo referente al pago.

- El banco firma digitalmente y envía autorización al vendedor, quien puede completar la orden.

Garantizando los siguientes fundamentos de seguridad a nivel transaccional:

- Autenticación
- Confidencialidad
- Integridad
- No repudiación

### 2.2.18 FIREWALLS

Los firewalls son barreras de protección que filtran el acceso a los servidores privados mediante reglas puntuales que habilitan o prohíben el acceso de un punto a otro.

Garantizando los siguientes fundamentos de seguridad:

- Autenticación
- Autorización

### 2.2.19 ANTIVIRUS

Los antivirus son programas que controlan la presencia de programas maliciosos en los sistemas, estos antivirus deben controlar tanto los servidores como las estaciones de trabajo.

### 2.2.20 AUDITORÍAS

Las auditorias son información respecto a quien ejecutó un evento en el sistema, cualquiera que esta sea, según los requerimientos que se estipulen, se debe indicar el momento exacto y el usuario (persona o proceso) que lo realizó.

### 2.2.21 MONITOREO, SISTEMAS DE DETECCIÓN DE INTRUSOS Y DE VULNERABILIDADES

El monitoreo y los sistemas de detección de intrusos y detección de vulnerabilidades son herramientas que permiten realizar labores encaminadas a obtener información respecto a los posibles intrusos que puedan atacar un sistema así como la forma de realizarlo, identificando las vulnerabilidades con el fin de controlarlas y corregirlas.

En términos generales, este tipo de mecanismos permiten ser proactivos en controlar todos los fundamentos de la seguridad informática, ya que las vulnerabilidades y los atacantes que se detecten pueden referirse a cualquiera de ellos.

### 2.2.22 ATENCIÓN DE INCIDENTES

Un esquema de atención de incidentes busca garantizar que se actúa de la forma adecuada en el momento de presentarse un incidente contra cualquiera de los fundamentos de seguridad, tanto

para casos de fallas en los equipos y servicios como para eventualidades que atenten contra la seguridad informática del Banco.

En términos generales, este mecanismo apoya todos los fundamentos de seguridad informática, ya que los incidentes que deben controlarse pueden referirse a cualquiera de los fundamentos.

### 2.2.23 ANÁLISIS DE RIESGOS E IMPACTOS

Mediante los análisis de riesgos se pretende identificar y analizar los riesgos latentes en un sistema y los respectivos impactos sobre éste, es importante realizar este tipo de análisis para ser preventivo en la aplicación de controles, y no esperar que ocurra un incidente para controlarlos.

En términos generales, este mecanismo apoya todos los fundamentos de seguridad informática.

## 2.3 RESPONSABILIDADES DE LOS CLIENTES FRENTE A LOS MECANISMOS DE SEGURIDAD DEL BANCO DE LA REPUBLICA

Los clientes que leen este documento deben hacer sus mejores esfuerzos en entender y documentarse sobre las tecnologías que el Banco ofrece en sus servicios, y que éste implementa una tecnología de seguridad adecuada en la prestación de sus servicios.

## 2.4 ASPECTOS A CONSIDERAR POR PARTE DE LOS CLIENTES

### 2.4.1 PRESUNCIÓN

El cliente tiene plena certeza de que los mecanismos de seguridad del Banco de la República le proveen la seguridad requerida, de tal manera que tiene plena confianza en:

- ✓ El diseño y construcción de las herramientas de seguridad informática así como la selección de los productos de seguridad. De tal manera que se tiene certeza de que el Banco de la República ha puesto todos sus esfuerzos en la mitigación del riesgos de eventuales fallas técnicas, y que la presencia de fallas para efectos legales, se asimila al caso fortuito o de fuerza mayor.

- ✓ La administración del Banco de la República sobre el modelo de seguridad.

- ✓ La vigilancia y control del Banco de la República sobre el modelo de seguridad.

### 2.4.2 EN CUANTO A LOS PERJUICIOS E INDEMNIZACIONES

Los clientes exoneran al Banco de la República de toda responsabilidad en relación con los perjuicios que puedan ocasionarse a terceros o a la entidad que representan por el uso indebido o no autorizado de los mecanismos de seguridad y sus componentes, o del incumplimiento por parte del cliente de las ordenes que sean impartidas utilizando los mecanismos de seguridad. Los clientes se comprometen a indemnizar al Banco de la República por cualquier perjuicio que dichas circunstancias le puedan ocasionar.

### 2.4.3 RESPECTO A LA ENTREGA

Todo mecanismo de seguridad y componentes será entregado a los respectivos clientes mediante documentos denominados "Actas de entrega", donde se estipula claramente el nombre de los usuarios, su documento de identidad, cargo, el mecanismo de seguridad al que está autorizado y el componente que se está entregando. Esta acta formará parte de los contratos de servicio que se hayan firmado por parte de los clientes con el Banco de la República. Esta acta deberá ser firmada por el representante legal de la institución cuya firma debe ir certificada frente a notario público.

Una vez terminado el contrato de servicio con el Banco de la República, nos compromete a hacer la devolución de los componentes entregados.

### 2.4.4 RESPONSABILIDADES

-Uso adecuado de los mecanismos de seguridad: Dado que el cliente conoce las graves implicaciones que podría ocasionar el uso indebido o no autorizado de los mecanismos de seguridad y sus componentes, se obligan a limitar el acceso a estos únicamente a las personas señaladas en las respectivas "Actas de entrega" y a mantener los componentes de los mecanismos de seguridad bajo estrictas medidas de seguridad.

-Respecto a los reglamentos y circulares: Los clientes se obligan a dar estricto cumplimiento a los reglamentos y circulares que establezca el Banco de la República, en relación con los dispositivos de seguridad y con el manejo y utilización de los mecanismos de seguridad y sus componentes.

-Los clientes se comprometen a mantener estricta confidencialidad frente a terceros, respecto a los detalles de los mecanismos de seguridad ofrecidos por el Banco de la República. Y cualquier comunicación que se requiera emitir al respecto debe ser autorizada formalmente por el Banco de la República.

### 2.4.5 EFECTOS LEGALES DE LA INFORMACIÓN

Para todos los efectos legales, las comunicaciones que utilicen los mecanismos de seguridad ofrecidos por el Banco de la República y éste a su vez las haya validado, se consideran auténticas y en consecuencia el emisor de la comunicación responderá plenamente por su contenido. De tal manera que los clientes autorizan al Banco de la República a actuar conforme a las órdenes enviadas mediante la utilización de los mecanismos de seguridad, comprometiéndose a responder por las operaciones que éste ejecute en cumplimiento de tales instrucciones.

### 2.4.6 AUTORIZACIONES

Los clientes autorizan al Banco de la República para monitorear y supervisar toda información que viaje a través de los esquemas de comunicación posibles con el Banco de la República.

# 3 REVISIÓN DEL DOCUMENTO

## 3.1 FRECUENCIA DE REVISIÓN

Este documento deberá revisarse al menos cada tres (3) años, o cuando exista un cambio trascendental en la tecnología de seguridad.

## 3.2 QUIÉNES REVISAN

El Departamento de Seguridad Informática del Banco de la República será la encargada de revisar los tópicos consignados en este documento, con el fin de garantizar su vigencia.

# 4 HISTÓRICO DE CAMBIOS

JCH - Marzo 27 de 2006: Se modifica la versión del documento (versión 2). Se incluyó el concepto de Observancia y se actualizaron los mecanismos de seguridad.

OLR – Mayo 29 de 2007: Se modifica la versión del documento (versión 3). Se modifico Unidad de Seguridad Informática por Departamento de Seguridad Informática. Se elimino el numeral 2.2.17 Virtual Private Network. Se cambio el concepto de acuerdo por documento. Se elimino el capitulo de firmas.

# 5 GLOSARIO

Políticas de seguridad Informática: Son directrices de alto nivel en la cual se expresan valores y objetivos de la organización para proporcionar dirección y soporte a la alta gerencia en los temas relacionados con seguridad informática.

Norma: Es una declaración organizacional que limita las responsabilidades entre diferentes áreas, estableciendo pautas de acción según lo que le correspondan en ámbito de sus funciones.

Estándar: Conjunto de requisitos de obligatorio cumplimiento, que especifican tecnologías y métodos, para implementar las políticas de seguridad informática expuestas por la alta gerencia, establecen un marco de acción coordinado que busca alinear los esfuerzos de la organización para procurar los fundamentos de la seguridad informática.

Instructivos: Define un conjunto de pasos operacionales específicos sugeridos para efectuar una labor particular, que se puede modificar en respuesta a los cambios en la dinámica del negocio y la tecnología. P.e Instructivo para toma de respaldos.