UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

IMPLEMENTACIÓN DE UNA HERRAMIENTA TECNOLÓGICA PARA CONTROLAR EL ACCESO A DOCUMENTOS CON INFORMACIÓN CONFIDENCIAL EN UN BANCO

INFORME DE SUFICIENCIA

PARA OBTENER EL TITULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

POMALAZA INGA, DANILO NILTON

LIMA – PERU
2012

DEDICATORIA

Dedico la obtención del mi título de Ingeniero a mis padres Milton Pomalaza y Carmen Inga porque siempre hemos compartido juntos los desafíos y logros que nos han permitido crecer como familia. A mis hermanos y seres queridos por la motivación que representan para mí.

AGRADECIMIENTO

Agradezco a la Universidad Nacional de Ingeniería por brindarme la oportunidad para desarrollarme profesional y personalmente.

INDICE

DESCRIPTORES TEMATICOS

Seguridad de la información

Información Confidencial

Criptografía

Control de Acceso

Herramienta tecnológica

ADRMS

PCI DSS

Ley de Protección de Datos Personales

RESUMEN

El presente informe muestra la implementación de una herramienta tecnológica para controlar los accesos a información confidencial del Banco contenida en documentos digitales.

Se seleccionaron tres herramientas tecnológicas y se evaluaron según los criterios que se definieron para cubrir la necesidad de seguridad de la información. La herramienta de seguridad en documentos Microsoft ADRMS resultó la alternativa escogida.

Para la implementación de la solución ADRMS se tiene dos fases: Implementación de la herramienta y el despliegue de la solución. Dentro de la implementación se selecciono a la Unidad de Tarjetas que maneja información de datos de tarjetas de los clientes para ser protegida debido a que es considera como información confidencial del Banco

Para verificar el uso de la herramienta, se definió un indicador que mide el número de documentos con información sensible que ha sido protegida correctamente en la unidad de tarjetas del Banco; logrando en las 6 últimas semanas los valores esperados para considerar que la unidad está protegiendo adecuadamente los documentos con la Herramienta ADRMS.

INTRODUCCIÓN

La fuga de Información confidencial en las empresas representa un riesgo para la operatividad del negocio, imagen de la empresa y el incumpliendo de leyes y normativas que buscan proteger la información de las personas. En este sentido, El Banco considera que la protección de sus activos, y con ella la sostenibilidad del negocio, debe ser uno de los compromisos más importantes de cara a sus clientes, accionistas y a la sociedad en general.

El Banco reconoce a la información y a los sistemas que la sustentan y procesan, como uno de sus activos más importantes a proteger, y establece como objetivo la gestión efectiva y eficiente de los riesgos a los que se ven sujetos, garantizando un adecuado control interno de los mismos.

En la mayoría de los casos se establecen las medidas de seguridad de índole normativa y tecnológica. El Banco ya tiene un modelo de Clasificación de la Información que le permite identificar la información confidencial del Banco y la normativa que regula su protección. Sin embargo no se contaba con una herramienta tecnológica que le permitiera controlar los accesos a este tipo de información.

ADRMS es una herramienta tecnológica de Microsoft que nos permitirá controlar que solo los usuarios autorizados puedan acceder a los documentos con información confidencial. La herramienta también permite controlar los privilegios que tendrán de los usuarios autorizados sobre los documentos protegidos.

CAPITULO I

PENSAMIENTO ESTRATÉGICO

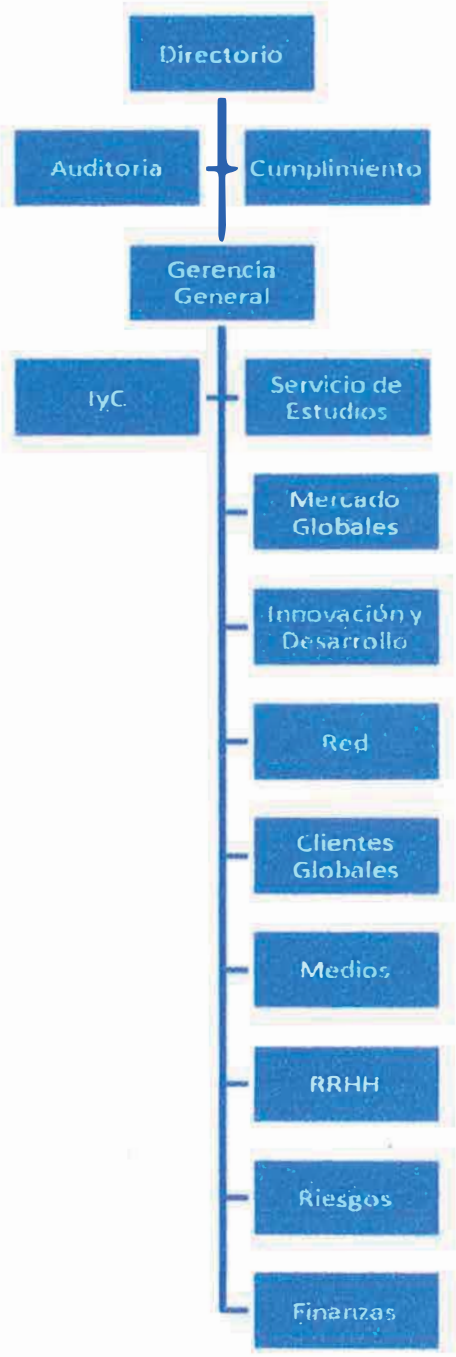
DIAGNÓSTICO FUNCIONAL

ORGANIZACIÓN

El Banco es una entidad financiera cuya sede principal se encuentra en Lima. Es una subsidiaria de Holding Banco SA, la que posee el 92,08% de participación. Holding Banco SA es una empresa peruana formada por el grupo peruano Brescia (50%) y el grupo español Banco (50%). El Banco es una sociedad anónima constituida en 1951, autorizada a operar por la Superintendencia de Banca, Seguros y AFP (SBS). El Banco desarrolla sus actividades a través de una red nacional de 263 oficinas

ORGANIGRAMA

Figura 1: Organigrama del Banco



Fuente: Elaboración propia

CLIENTES

Los clientes del Banco son:

a) Particulares: grandes patrimonios, particulares
b) Empresas: autónomas y pequeñas empresas, grandes empresas, grandes corporaciones, empresas familiares, negocios globales
c) Instituciones:
   - Instituciones públicas, organismos internacionales y empresas y organismos dependientes de alcance nacional, comunitario y local y
   - Instituciones privadas: ONG/fundaciones y asociaciones empresariales)

La participación de mercado del Banco se ha mantenido relativamente constante en los últimos años, posicionándose en segundo lugar tanto en colocaciones como en captaciones, mientras que a nivel patrimonial se ubica en tercer lugar en el sistema financiero.

Figura 3: Participación en el Sistema Bancario

Participación Sistema Bancario* (%)	Banco Continental			
	2008	2009	2010	2011
Créditos Directos	24	23	25	24
Depósitos Totales	22	22	22	24
Patrimonio	18	20	20	19

* No incluye sucursales en el exterior

Fuente: Revista Digital del Banco

El compromiso del Banco con sus clientes: "El cliente como centro del negocio: ofrecerle un servicio de calidad, satisfacer sus necesidades financieras y responder de manera eficaz a sus perspectivas".

PROVEEDORES

La Unidad de Compras del Banco cuenta con un modelo estructurado a partir de una política sostenible de los costes de aprovisionamiento, mejora y transparencia de los procesos y un aumento de la calidad y servicios al usuario. Este modelo es corporativo y se aplica a partir de las directrices del Grupo . Sus principales objetivos con los proveedores son:

- Dinamizar el comercio electrónico facilitando las relaciones comerciales entre empresas y fomentando la accesibilidad, el flujo y la transparencia en las operaciones comerciales de aprovisionamiento.
- Promover y gestionar un adecuado sistema de homologación de los proveedores con el fin de asegurar que los proveedores cuenten con capacidad productiva, técnica, financiera y comercial que garantice la calidad, niveles de servicio y costes previamente establecidos.

La estructura organizativa de Compras está conformada de la siguiente manera:

Gestión de Compras. Equipo constituido por técnicos de Compras que se encargan de recibir y gestionar las solicitudes de aprovisionamiento del Banco según el modelo corporativo.

Almacenes. Función a cargo de tres técnicos: Control de Archivo, Economato y Activo Fijo. Además de dos encargados de controlar los almacenes tanto de Activo fijo como de Economato. Se encargan de recibir la mercadería de los proveedores, controlando cantidad y calidad y efectuando la entrega del

material a cada una de las unidades u oficinas solicitantes. Supervisa el stock y realiza los inventarios a nivel nacional.

Figura 4: Tipología de Proveedores

Fuente: Revista Digital del Banco

PROCESOS

En el Banco se han definido tres grandes familias de Procesos:

a) Procesos Corporativos

Son aquellos procesos que garantizan el cumplimiento de las obligaciones legales y normativa interna, toma decisiones sobre la planificación y control a nivel corporativo y desarrollo de actividades corporativas que no presenta un soporte en los equipos de Negocios.

b) Procesos de Negocio

Son aquellos procesos que comprenden la actividad principal del Banco: captación y fidelización de clientes mediante el asesoramiento y la distribución de productos y servicios.

c) Procesos de Soporte

Son aquellos procesos que aseguran la dotación de los recursos precisos (Humanos, materiales, inmuebles, informáticos) para el correcto desarrollo de la actividad del Banco)

Figura 5: Procesos del Banco

Fuente: Revista Digital del Banco

PRODUCTOS

Los productos se clasifican en:

a) Banca Minorista

El Banco ha querido destacar sus actividades de Banca Minorista intentando un mayor acercamiento con clientes, ampliando su cobertura de servicios bancarios en zonas con potencial de crecimiento.

Atendiendo a su plan de expansión, en el 2006, el banco abrió 4 oficinas comerciales y 3 oficinas especiales. Además, se llevó a cabo un cambio de imagen física de las oficinas, y una campaña de imagen para informar al público de sus nuevos productos.

Así mismo, el banco ha mejorado el proceso de transacciones a través del uso de cajeros automáticos, Internet y vía telefónica.

Los productos más representativos para la Banca Minorista son:

- Depósitos
- Tarjetas
- Préstamos

b) Banca de Empresas e Instituciones

Esta área es la encargada de gestionar la relación del banco con las medianas empresas y los clientes institucionales. A nivel nacional, cuenta con una red de 16 oficinas especializadas en Banca de Empresas y una oficina de Banca Institucional. Además, tiene a su cargo, las unidades de Productos y Servicios Empresariales, Centro de Leasing y Comercio Exterior, las mismas que dan soporte a todas las áreas de negocio del Banco

Los productos más representativos para la Banca de Empresas e instituciones son:

- Financiamientos
- Inversión
- Tarjetas

c) Banca Mayorista Global

En el Perú, la Banca Mayorista Global, abarcan Banca Corporativa, Financiamiento de Comercio Internacional y Mercado de Capitales; y está orientada a atender las necesidades de las empresas multinacionales y los grandes grupos locales.

Los productos más representativos para la Banca Mayorista Global son:

- Comercio Internacional
- Mercado de capitales
- Mercados Globales

DIAGNÓSTICO ESTRATÉGICO

VISIÓN

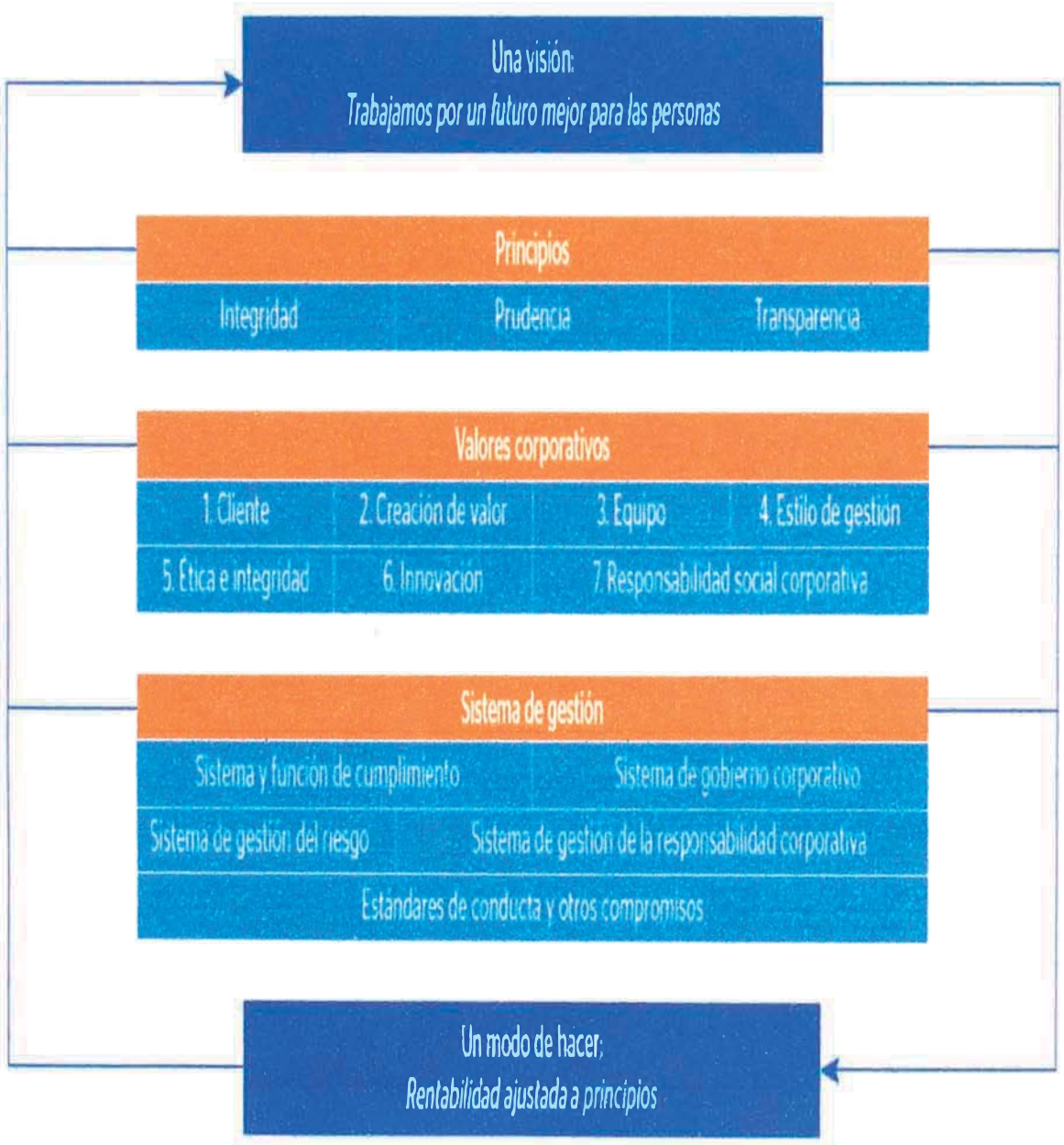
Trabajamos por un futuro mejor para las personas

MISIÓN

El Banco es una empresa que forma parte del Grupo Banco, cuyas actividades se desarrollan en el rubro financiero, teniendo como compromiso principal aportar las mejores soluciones a sus clientes, un crecimiento rentable a sus accionistas y progreso en las sociedades en las que está presente

ESTRATEGIA BASADA EN PRINCIPIOS

Figura 6: Estrategia del Banco



Fuente: Revista Digital del Banco

POSICIONAMIENTO

El Banco define su identidad y posicionamiento de marca corporativa a partir de la combinación de tres ejes básicos, los que resumen la visión del Grupo Banco y son el cimiento sobre el que se construyen su estrategia de negocio, su marca y su reputación:

- Los principios corporativos.
- La prioridad de la innovación.
- Trabajar de personas para personas.

El concepto Adelante simboliza todas las acciones que conllevan a estar un paso más allá en todas y cada una de las actividades del Banco, procurando a sus integrantes una visión de largo plazo.

LA RESPONSABILIDAD CORPORATIVA

Para el Banco, la responsabilidad corporativa (RC) se sustenta en contribuir a la diferenciación de la marca en los diferentes escenarios (económico, político y social) por los que transita la actividad de la empresa. El objetivo principal de la política del Banco es definir comportamientos e impulsar las acciones que permitan crear valor para los grupos de interés (valor social) y para la empresa misma (valor reputacional y valor económico directo). Para lograr esta propuesta el Banco considera que los compromisos y comportamientos han de ser expresión de la visión y de los principios de la empresa y, a su vez, deben responder de la mejor forma posible a las expectativas de los grupos de interés, con el fin de reforzar la estrategia de negocio.

A continuación anotamos los principales compromisos que el Grupo busca cumplir a través de la aplicación de su política de responsabilidad corporativa, en todas y cada una de sus sedes:

- Desarrollar en todo momento su actividad principal de forma excelente.
- Minimizar los impactos negativos derivados de la actividad de negocio.
- Desarrollar "oportunidades sociales de negocio" que generen valor social y valor económico para el Banco.
- Invertir en las sociedades donde el Grupo está presente mediante el apoyo a iniciativas sociales, especialmente las relacionadas con la educación.

ANALISIS EXTERNO

Oportunidades

1. Expansión de una gama de servicios y/o productos a través de la banca electrónica.
2. Bajos niveles de intermediación financiera en el país

AMENAZAS

1. Riesgo de Sobreendeudamiento de los deudores en los segmentos de consumo y microempresas.
2. Incertidumbre sobre el mayor impacto de la crisis internacional de la Zona euro en la Casa Matriz(BANCO)

ANALISIS INTERNO

Fortalezas

1 Respaldo del Grupo BANCO- Banco Bilbao Vizcaya Argentaria

2. Importante participación de mercado en colocaciones y depósitos

3. Eficiencia Operativa

Debilidades

1. Descalce de Operaciones

CAPITULO II

MARCO TEÓRICO Y METODOLÓGICO

LEY DE PROTECCIÓN DE DATOS PERSONALES

Con fecha 3 de julio de 2011 se ha publicado en el Diario Oficial El Peruano la Ley N° 29733 "Ley de Protección de Datos Personales".

La norma, propuesta por el Ejecutivo, consta de un título preliminar con disposiciones generales, otros siete títulos, 40 artículos y disposiciones complementarias finales. Dispone que el tratamiento de los datos personales debe realizarse con pleno respeto de los derechos fundamentales de sus titulares y sólo pueden ser objeto de tratamiento con consentimiento de su titular, salvo ley autoritativa al respecto. En este último caso, precisa la ley, el consentimiento debe ser previo, informado, expreso e inequívoco, y en el caso de datos sensibles, el consentimiento para efectos de su tratamiento debe efectuarse por escrito.

También se indica que las limitaciones al ejercicio del derecho fundamental a la protección de datos personales solo pueden ser establecidas por ley, respetando su contenido esencial y estar justificadas en razón del respeto de otros derechos fundamentales o bienes constitucionalmente protegidos.

En el caso de las comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos, cuando sean de carácter privado o uso privado, solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento del juez o con autorización de su titular, con las garantías previstas en la ley. Asimismo, se señala que se debe guardar secreto de los asuntos ajenos al hecho que motiva su examen y que los datos personales obtenidos con violación de este precepto carecen de efecto legal.

NORMA DE SEGURIDAD DE DATOS DE LA INDUSTRIA DE TARJETAS DE PAGO (PCI-DSS)

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

SEGURIDAD DE LA INFORMACIÓN

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la **confidencialidad**, la **disponibilidad** e **Integridad** de la misma.

a) Confidencialidad

Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. A groso modo, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización.

b) Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

c) Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que lo requieran.

SEGURIDAD Y CRIPTOGRAFÍA

La necesidad de Seguridad de la Información en una organización ha cambiado en las últimas décadas.

Antes del uso de las computadoras, la Seguridad de la Información era proporcionada por medios físicos, por ejemplo el uso de cajas fuertes y por medidas administrativas, como los procedimientos de clasificación de documentos.

Con el uso de la computadora, y más aún con la llegada de Internet, fue indispensable el uso de herramientas automatizadas para la protección de archivos y otro tipo de información almacenada en la computadora, algunas de estas herramientas son los cortafuegos, los Sistemas Detectores de Intrusos y el uso de sistemas criptográficos. Estas herramientas no sólo permiten proteger a la información, sino también a los Sistemas Informáticos que son los encargados de administrar la información.

De la necesidad por proteger a la información y a los sistemas que la administran surge el término de Seguridad Informática.

De acuerdo con las definiciones anteriores para que exista seguridad hay que garantizar las propiedades de confidencialidad, integridad y disponibilidad. Y es aquí donde se utiliza a la criptografía, ya que mediante el uso correcto de sistemas criptográficos se pretende garantizar las propiedades de confidencialidad e integridad. Veamos el siguiente ejemplo que ilustra una comunicación.

Primeramente se muestra lo que idealmente es una comunicación normal, en este caso no existe ningún problema de seguridad informática. El mensaje que se envía se recibe sin alteración alguna.

Figura 7: Comunicación Normal

Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

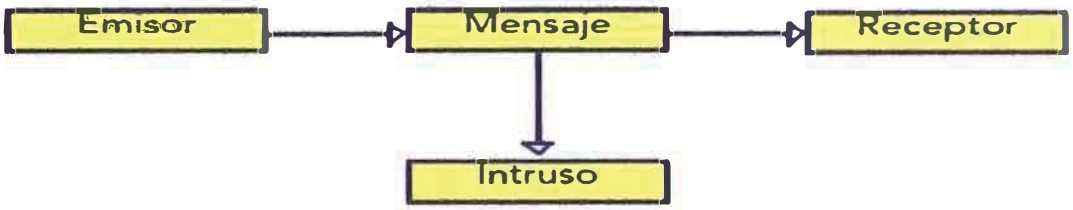
El segundo caso muestra uno de los problemas más grandes que hay, la interrupción de la transmisión del mensaje, que puede ser ocasionada por fallo del canal o de algún elemento del sistema de comunicación, ya sea de forma natural o intencional. Esto es traducido a un problema de disponibilidad.

Figura 8: Comunicación con Interrupción

Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

La interceptación de los datos por un intruso (un intruso es un ente externo al sistema) es algo muy común dentro de las comunicaciones, ya que muchas de las transmisiones son enviadas mediante protocolos que son conocidos por todos y a los mensajes no se les hace ningún tratamiento especial, en otras palabras, viajan tal cual se generan. Lo único que se hace es escuchar todo lo que pasa por el canal sin alterar nada. Este es un problema de confidencialidad.

Figura 9: Comunicación con Interceptación



Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

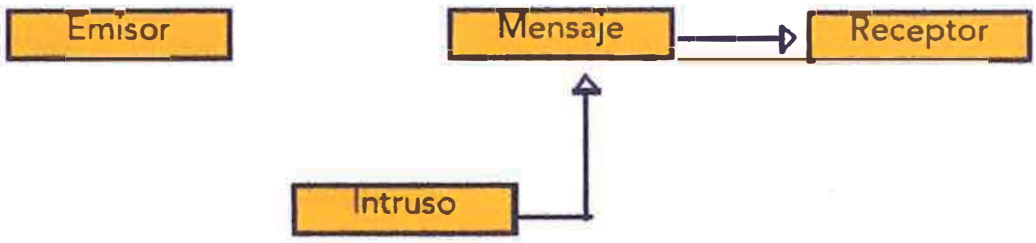
Otro problema en la comunicación es el problema de la falsificación. Esto se produce cuando el intruso captura un mensaje, se adueña de él y de la identidad del emisor y genera un nuevo mensaje con la identidad del emisor. Este es un problema de integridad y confidencialidad.

Figura 10: Comunicación con Falsificación

Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

Finalmente la generación de mensajes se da cuando el intruso genera un mensaje engañando al receptor haciéndolo creer que es un emisor válido. Esto se traduce en un problema de integridad.

Figura 11: Comunicación Apócrifa



Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

Es muy fácil ver como una comunicación y un sistema informático son muy similares, ya que en un sistema informático se procesan, almacenan, envían y reciben datos.

Ahora, si pudiéramos de alguna forma evitar los problemas de disponibilidad, integridad y confidencialidad, tendríamos un sistema "seguro". Para lograr esto tendríamos que aislar al sistema de los intrusos y hacerlo anti-fallos lo cual es prácticamente imposible. Lo que se hace es crear mecanismos que garanticen en cierta medida las propiedades de disponibilidad, integridad y confidencialidad.

La disponibilidad, generalmente, se trata de solucionar con sistemas redundantes.

La confidencialidad se puede lograr usando un mecanismo que, aunque sea robada la información, permita que no se pueda acceder a ésta o garantice de alguna forma que no se pueda llegar a ella, hasta que pierda su valor.

La integridad es más difícil de lograr y se hace con el uso de varios mecanismos que garantizan la identidad de un ente que está autorizado por el sistema para crear o hacer modificaciones a la información, de tal forma que se puede verificar posteriormente quién creó o modificó la información. Además estos mecanismos permiten ver si la información ya creada ha sufrido o no alguna modificación no autorizada.

Los mecanismos para garantizar la integridad y la confidencialidad se implementan con sistemas criptográficos, de ahí la importancia de la criptografía en la seguridad informática en los sistemas actuales.

CRIPTOGRAFÍA

La palabra criptografía proviene en un sentido etimológico del griego Kriptos=ocultar, Graphos=escritura, lo que significaría ocultar la escritura, o en un sentido más amplio sería aplicar alguna técnica para hacer ininteligible un mensaje.

En su clasificación dentro de las ciencias, la criptografía proviene de una rama de las matemáticas, que fue iniciada por el matemático Claude Elwood Shannon en 1948, denominada: “Teoría de la Información”. Esta rama de las ciencias se divide en: “Teoría de Códigos” y en “Criptología”. Y a su vez la Criptología se divide en Criptoanálisis y Criptografía.

En un sentido más amplio, la Criptografía es la ciencia encargada de diseñar funciones o dispositivos, capaces de transformar mensajes legibles o en claro a mensajes cifrados de tal manera que esta transformación (cifrar) y su transformación inversa (descifrar) sólo pueden ser factibles con el conocimiento de una o más llaves.

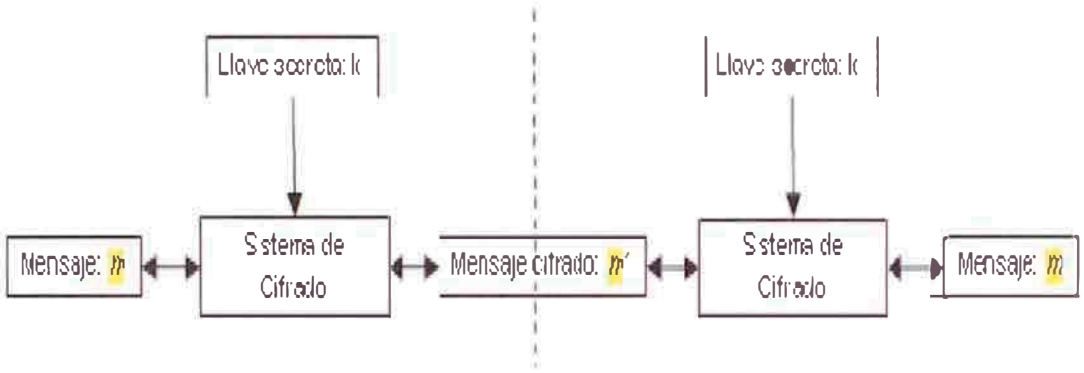
La criptografía moderna se puede clasificar en dos grandes grupos: la criptografía simétrica y la criptografía asimétrica.

En el Anexo I Criptografía se detalla un mayor alcance del desarrollo de la Criptografía hasta la actualidad.

a) Criptografía Simétrica

La criptografía simétrica o de llave secreta es aquella que utiliza algún método matemático llamado sistema de cifrado para cifrar y descifrar un mensaje utilizando únicamente una llave secreta. Se puede observar en la siguiente figura que la línea punteada es el eje de simetría: lo mismo que hay de un lado existe exactamente igual en el otro, esto ilustra el hecho del porqué se le da el nombre de criptografía simétrica.

Figura 12: Criptografía Simétrica



Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

Este tipo de criptografía sólo utiliza una llave para cifrar y descifrar, esto es: si yo cifro un mensaje m con una llave secreta k entonces el mensaje cifrado resultante m' únicamente lo voy a poder descifrar con la misma llave k. Este tipo de llave conocida como secreta se debe de compartir entre las personas que se desea que vean los mensajes.

Con este tipo de criptografía podemos garantizar la confidencialidad porque únicamente quien posea la llave secreta será capaz de ver el mensaje.

El problema con la criptografía simétrica es que si yo quisiera compartir secretos con n personas, para cada persona tendría que generar una nueva llave secreta y la administración personal de todas m llaves sería un caos.

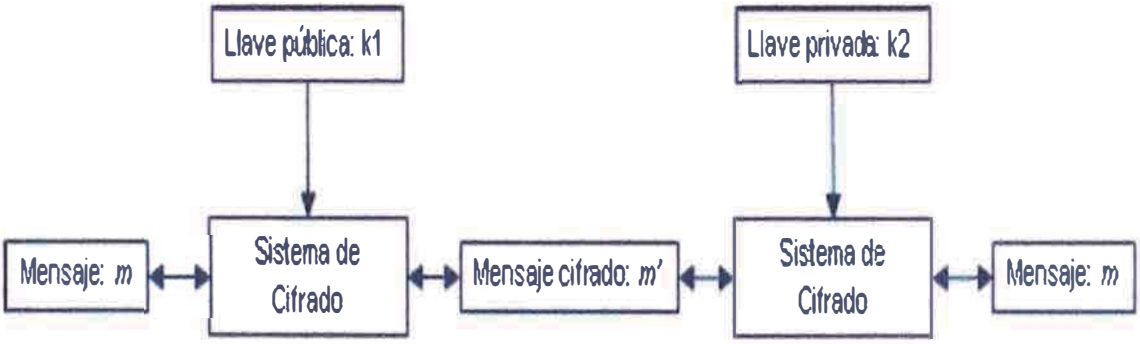
Otro problema asociado con este tipo de criptografía es cómo comparto con otra persona de una forma confidencial e integra la llave secreta.

Estos problemas se resuelven de cierta manera con criptografía asimétrica.

b) Criptografía Asimétrica

Si se observa la siguiente figura, que ilustra la idea de criptografía de llave pública, se puede ver claramente que no existe simetría en ella, ya que de un lado de la figura se cifra o descifra con una llave pública y en el otro lado con una privada. De este hecho es de donde la criptografía asimétrica debe su nombre.

Figura 13: Criptografía Asimétrica



Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

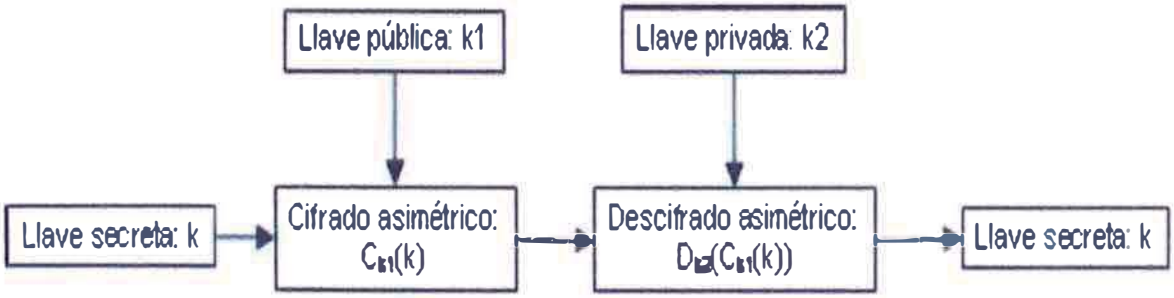
Es importante destacar que para este tipo de criptografía lo que se cifra con una llave se puede descifrar con la otra llave. Es decir, yo puedo cifrar con la llave pública y descifrar con la privada y viceversa. Esto es de gran ayuda ya que el número de llaves que debo de poseer se reduce considerablemente. Si alguien quisiera enviar un mensaje cifrado a n personas, necesitaría saber n llaves públicas una de cada persona, pero si n personas le quiere enviar un mensaje cifrado sólo es necesario que los demás conozcan su llave pública. Así, sólo

tengo que preocuparme de que la llave pública sea de la persona que dice ser. Este es el problema de la criptografía asimétrica, la autenticidad de las llaves públicas.

Algunos ejemplos de este tipo de criptografía son RSA, El Gamal y Curvas Elípticas.

Solución al problema de intercambio de llaves secretas usando criptografía asimétrica: se supone que alguien va a enviar la llave secreta k a una persona para que puedan cifrar entre ellos mensajes. Lo que se hace es que se toma la llave pública de la persona a la que se le va a enviar el mensaje y se cifra con un sistema asimétrico la llave secreta, esto implica que sólo la persona poseedora de la llave privada pueda descifrar lo que se está enviando y con ello tener la llave secreta, tal y como se muestra en la siguiente figura.

Figura 14: Intercambio de llaves secretas



Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

Las dos principales ramas de la criptografía de asimétrica son:

Cifrado de clave pública: un mensaje cifrado con la clave pública de un destinatario no puede ser descifrado por nadie (incluyendo al que lo cifró),

excepto un poseedor de la clave privada correspondiente--presumiblemente, este será el propietario de esa clave y la persona asociada con la clave pública utilizada. Se utiliza para confidencialidad.

Firmas digitales: un mensaje firmado con la clave privada del remitente puede ser verificado por cualquier persona que tenga acceso a la clave pública del remitente, lo que demuestra que el remitente tenía acceso a la clave privada (y por lo tanto, es probable que sea la persona asociada con la clave pública utilizada) y la parte del mensaje que no se ha manipulado. Sobre la cuestión de la autenticidad.

Una analogía con el cifrado de clave pública es la de un buzón con una ranura de correo. La ranura de correo está expuesta y accesible al público; su ubicación (la dirección de la calle) es, en esencia, la clave pública. Alguien que conozca la dirección de la calle puede ir a la puerta y colocar un mensaje escrito a través de la ranura; sin embargo, sólo la persona que posee la clave puede abrir el buzón de correo y leer el mensaje.

Una analogía para firmas digitales es el sellado de un sobre con un sello personal. El mensaje puede ser abierto por cualquier persona, pero la presencia del sello autentifica al remitente.

DIRECTORIO ACTIVO (AD)

Directorio Activo (AD) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

El Directorio Activo permite a los administradores establecer políticas a nivel de empresa, desplegar programas en muchos ordenadores y aplicar actualizaciones críticas a una organización entera.

El Directorio Activo es la pieza fundamental del control de la seguridad de IT e identidad en las organizaciones.

Figura 15: Directorio Activo

Fuente: Estructura del Directorio Activo (Blog Redes Fran-Cisco)

RIGHTS MANAGEMENT SERVICES (RMS)

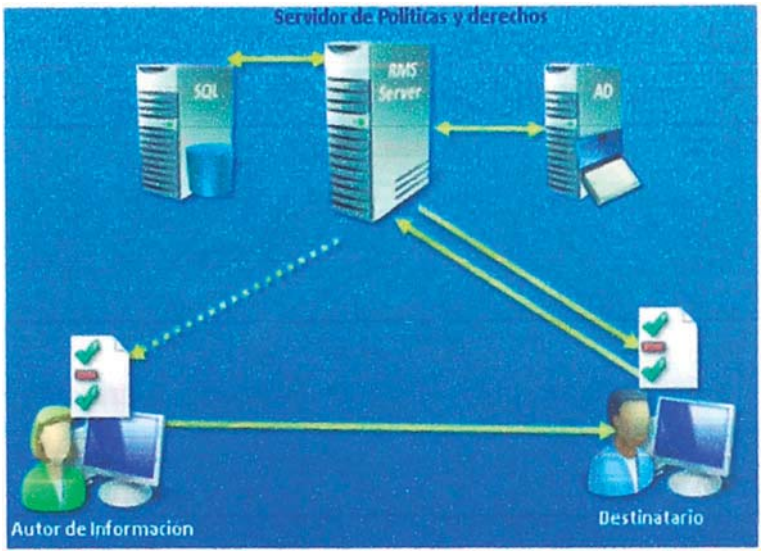
Rights Management Services (Servicios de Administración de Derechos) es una herramienta de Microsoft Windows que utiliza el cifrado y una forma de negación funcionalidad selectiva para limitar el acceso a los documentos, tales como las empresas de e- correo electrónico , Word documentos y páginas web, y las operaciones de los usuarios autorizados pueden realizar en ellos. Las empresas pueden utilizar esta tecnología para encriptar la información almacenada en formatos de documentos de este tipo, ya través de las políticas incluidas en los documentos, evitar que el contenido protegido de ser descifrado, salvo por las personas o grupos específicos, en determinados entornos, bajo ciertas condiciones, y para ciertos periodos de tiempo. Las operaciones específicas, como la impresión, copia, edición, envío y borrado puede ser permitido o no por los autores de contenido para las piezas individuales de contenido, y los administradores pueden implementar plantillas de RMS ese grupo de estos derechos, junto a los derechos predefinidos que se pueden aplicar en masa

SERVICIOS DE GESTIÓN DE DERECHOS (AD RMS)

AD RMS es una tecnología de protección de la información que funciona con aplicaciones compatibles para impedir el uso no autorizado de información digital.

Los propietarios de los contenidos pueden determinar exactamente el modo de uso de la información: quién puede abrirla, modificarla, imprimirla, reenviarla, etc.

Figura 16: ADRMS



Fuente: ADRMS (Blog Redes Fran-Cisco)

AD RMS es una tecnología independiente de formatos y aplicaciones que se implementa en forma de servicios para la creación de soluciones de protección de la información. Puede funcionar con cualquier aplicación compatible con AD RMS, aplicando sobre la información sensible una serie de políticas persistentes. Entre los contenidos que pueden protegerse con AD RMS están, por ejemplo, los sitios Web de intranets, mensajes de correo electrónico y documentos. Las organizaciones pueden diseñar plantillas de derechos de uso del tipo "Confidencial - Solo lectura" que se aplican directamente a los documentos, por ejemplo informes financieros, especificaciones de producto, datos de clientes y mensajes.

PROCESOS DEL ADRMS

ADRMS incluye una serie de funciones básicas que permiten a los desarrolladores añadir medidas de protección de la información a las aplicaciones actuales. Un sistema RMS, que incluye componentes de servidor y de cliente, realiza los siguientes procesos:

a) Licencia de información con protección de derechos:
   Un sistema AD RMS expide certificados de cuentas autorizadas, que identifican a entidades de confianza (por ejemplo usuarios, grupos y servicios) que pueden publicar contenidos protegidos. Estos derechos de uso especifican quién puede acceder a este tipo de contenidos y de qué forma. Cuando un contenido se protege, se genera una licencia de publicación para él. Esta licencia asocia derechos de uso concretos a un bloque específico del contenido, de manera que dicho contenido puede distribuirse. Por ejemplo, los usuarios pueden enviar documentos con derechos restringidos a otros usuarios dentro o fuera de su organización sin que ese contenido pierda los derechos protegidos.

b) Adquisición de licencias para descifrar los contenidos con derechos restringidos y aplicar las políticas de uso.

   Los usuarios que disponen de un certificado de cuenta autorizada pueden acceder a contenidos de acceso protegido utilizando alguna aplicación de cliente compatible con AD RMS que les permita ver y trabajar con dichos contenidos. Cuando un usuario intenta acceder a contenidos protegidos, las peticiones se envían al servidor AD RMS para acceder (o "consumir") ese contenido. Cuando se intenta consumir el contenido protegido, el servicio de

licencia AD RMS del servidor AD RMS expide una licencia de uso exclusivo que lee, interpreta y aplica los derechos de uso y condiciones que se especifican en las licencias de publicación. Los derechos y condiciones de uso son persistentes, y se aplican de forma automática allí a donde viaje el contenido.

c) Adquisición de licencias para descifrar los contenidos con derechos restringidos y aplicar las políticas de uso

Los usuarios que disponen de un certificado de cuenta autorizada pueden acceder a contenidos de acceso protegido utilizando alguna aplicación de cliente compatible con AD RMS que les permita ver y trabajar con dichos contenidos. Cuando un usuario intenta acceder a contenidos protegidos, las peticiones se envían al servidor AD RMS para acceder (o "consumir") ese contenido. Cuando se intenta consumir el contenido protegido, el servicio de licencia AD RMS del servidor AD RMS expide una licencia de uso exclusivo que lee, interpreta y aplica los derechos de uso y condiciones que se especifican en las licencias de publicación. Los derechos y condiciones de uso son persistentes, y se aplican de forma automática allí a donde viaje el contenido.

SEGURIDAD ADRMS

Los usuarios que se consideran entidades de confianza en un sistema AD RMS pueden crear y gestionar archivos protegidos utilizando herramientas de autor muy familiares, dentro de alguna aplicación compatible con AD RMS que incorpore esta tecnología. Además, las aplicaciones compatibles con AD RMS pueden utilizar plantillas de derechos de uso definidas y autorizadas de forma

oficial y centralizada para que los usuarios puedan aplicar, con la máxima facilidad, una serie de políticas de uso predefinidas.

La siguiente tabla enumera los derechos que están disponibles de forma predeterminada cuando se crea una plantilla de directiva de derechos, y da una breve descripción de cómo el derecho se aplica por el cliente de AD RMS es interpretada por comunes AD aplicaciones habilitadas para RMS.

Control total - Si se concede, este derecho permite al usuario ejercer todos los derechos en la licencia, si los derechos están específicamente otorgados a dicho usuario.

Ver - Si este derecho se concede, el cliente de AD RMS permite que el contenido protegido que descifrar. Normalmente, cuando este derecho se concede, la aplicación permitirá al usuario ver el contenido protegido.

Editar - Si este derecho se concede, el cliente de AD RMS permite que el contenido protegido que descifrar y luego vuelve a cifrar con la clave mismo contenido. Normalmente, cuando este derecho se concede, la aplicación permitirá al usuario cambiar el contenido protegido y luego guardarlo en el mismo archivo.

Guardar - Si este derecho se concede, el cliente de AD RMS permite que el contenido protegido que descifrar y volver a cifrar utilizando la clave de un mismo contenido. Normalmente, cuando este derecho se concede, la aplicación permitirá al usuario cambiar el contenido protegido y luego guardarlo en el mismo archivo.

Exportar (Guardar como) - Si este derecho se concede, el cliente de AD RMS permite que el contenido protegido que descifrar y volver a cifrar opcionalmente-con la tecla de un mismo contenido. Normalmente, cuando este derecho se

concede, la aplicación permitirá al usuario utilizar el "Guardar como" para guardar el contenido protegido a un nuevo archivo. Dependiendo de la aplicación, el contenido puede ser salvo sin protección.

Imprimir - Normalmente, cuando este derecho se concede, la aplicación permitirá al usuario imprimir el contenido protegido.

Reenviar - Normalmente, cuando este derecho se concede, la aplicación permitirá a un destinatario de correo electrónico para reenviar un mensaje protegido.

Responder - Por lo general, cuando este derecho se concede, la aplicación permitirá a un destinatario de correo electrónico para responder a un mensaje protegido e incluir una copia del mensaje original.

Responder a todos - Normalmente, cuando este derecho se concede, la aplicación permitirá a un destinatario de correo electrónico para responder a todos los destinatarios de un mensaje protegido e incluir una copia del mensaje original.

Extraer - Normalmente, cuando este derecho se concede, la aplicación permitirá al usuario copiar y pegar información de contenido protegido.

Permitir Macros - Normalmente, cuando este derecho se concede, la aplicación permite al usuario ejecutar macros en el documento o utilice un editor para modificar macros en el documento.

Ver Derechos - Si este derecho se concede, el cliente de AD RMS permite a un usuario para crear una nueva licencia de publicación de la licencia existente, pero la clave de contenido no se conserva.

Editar derechos - Si este derecho se concede, el cliente de AD RMS permite a los usuarios editar los derechos de los usuarios que se asignan por la licencia, manteniendo el mismo contenido fundamental.

BENEFICIOS DEL AD RMS

El despliegue de un sistema de AD RMS proporciona los siguientes beneficios a una organización:

a) Salvaguardar la información confidencial

Las aplicaciones como los procesadores de texto, clientes de correo electrónico y aplicaciones de línea de negocio puede ser habilitado para AD RMS para ayudar a proteger a los usuarios la información confidencial puede definir quién puede abrir, modificar, imprimir, reenviar o realizar otras acciones con la información. Las organizaciones pueden crear plantillas de políticas de uso, como "confidencial - solo lectura" que se puede aplicar directamente a la información.

b) La protección persistente

AD RMS aumenta existentes basados en el perímetro de soluciones de seguridad, como cortafuegos y las listas de control de acceso (ACL), para la protección de una mejor información mediante el bloqueo de los derechos de uso dentro del propio documento, el control de cómo se utiliza la información, incluso después de haber sido abierto por los destinatarios.

c) Tecnología flexible y personalizable.

Los vendedores de software y desarrolladores pueden utilizar AD RMS en cualquier aplicación o habilitar otros servidores, como los sistemas de gestión de contenido o servidores de portales que funcionan en Windows u otros

sistemas operativos, para proteger la información sensible. Ellos están habilitados para integrar la protección de la información en soluciones basadas en servidor, tales como gestión de documentos y registros, los sistemas de archivos y flujos de trabajo automatizados.

CAPITULO III

PROCESO DE TOMA DE DECISIONES

IDENTIFICACIÓN DEL PROBLEMA

CONTEXTO

El Banco considera que la protección de sus activos, y con ella la sostenibilidad del negocio, debe ser uno de los compromisos más importantes de cara a sus clientes, accionistas y a la sociedad en general.

Bajo esta consideración, el Banco reconoce a la información y a los sistemas que la sustentan y procesan, como uno de sus activos más importantes a proteger, y establece como objetivo la gestión efectiva y eficiente de los riesgos a los que se ven sujetos, garantizando un adecuado control interno de los mismos.

El Banco adquiere la responsabilidad de promover y apoyar el establecimiento de medidas técnicas, organizativas y de control que garanticen la confidencialidad de la información

El detalle del Modelo de clasificación de la Información del Banco se encuentra en el anexo II Clasificación de la Información del Banco

PROBLEMA PRINCIPAL

No se ha establecido una medida de seguridad tecnológica para controlar el acceso no autorizado a información confidencial del Banco contenida en documentos digitales.

PROBLEMÁTICA

1. Fuga de información confidencial que se encuentra en los documentos elaborados por la suite de Microsoft (Word, Excel, Power Point) a nivel externo.

   Existe en el Banco un volumen importante de documentos que son de uso de las unidades internas del Banco y que no deben ser enviadas a entidades externas al Banco. La posibilidad de que la información contenida en dichos documentos pueda llegar a terceros no autorizados podría ser perjudicial para el Banco.

2. Fuga de información confidencial que se encuentra en los documentos elaborados por la suite de Microsoft (Word, Excel, Power Point) a nivel interno.

   Existe en el Banco unidades que trabajan con información altamente confidencial y que no debe de ser compartida con otras unidades del Banco sin las autorizaciones y los controles necesarios.

3. Fuga de información confidencial a través de un usuario con privilegios para reenviar, copiar, modificar, imprimir, documentos que no son necesarios para el desempeño de sus actividades.

   Existen unidades en el Banco que tienen la necesidad de trabajar con información confidencial, sin embargo en mucho de los casos no necesitan imprimir los documentos o no necesitan modificarlos; en estos casos sería necesario que estos usuarios tengan solo el privilegio de visualización.

   Se puede reducir el riesgo de posibles fugas de información a través del control de los privilegios que los usuarios tienen sobre los documentos.

Figura 17: Problemática

Fuente: Elaboración Propia

PLANTEAMIENTO DE ALTERNATIVAS DE SOLUCIÓN.

Se evaluaron las diferentes soluciones tecnológicas de seguridad de la Información con las que se contaba, se planteó tres alternativas de solución, las cuales podrían satisfacer las necesidades que se plantearon. A continuación se detallan las tres alternativas

ALTERNATIVA I: IMPLEMENTACIÓN DEL ADRMS (Microsoft Active Directory Rights Management Services)

ADRMS es una tecnología de protección de la información que funciona con aplicaciones compatibles para impedir el uso no autorizado de información digital. Los propietarios de los contenidos pueden determinar exactamente el modo de uso de la información: quien puede abrirla, modificarla, imprimirla, reenviarla, etc. e incluso crear plantillas de aplicación de derechos como por ejemplo "Confidencial - Sólo lectura" que persisten a través de todo el ciclo de vida de los documentos. Estas políticas se aplican incluso cuando los documentos abandonan la red corporativa

VENTAJAS:

- Evita que usuarios no autorizados tanto internos como externos puedan acceder a la documentación que la organización identifique como sensible a través de un proceso de identificación del usuario que intenta acceder al documento.
- Evita que un destinatario no autorizado del contenido restringido reenvíe, copie, modifique, imprima el contenido para uso no autorizado.

- Admite la caducidad de archivo, de forma que el contenido de los documentos, los libros o las presentaciones no se pueda ver con posterioridad a un período de tiempo especificado

ALTERNATIVA II: IMPLEMENTACIÓN POR DOBLE FACTOR PARA AUTENTICACION A COMPUTADORAS PERSONALES MEDIANTE TOKEN

La autenticación por doble factor es un enfoque para la autenticación, que requiere la presentación de "dos o más" de los tres factores de autenticación "" ("algo que el usuario sabe", "algo que el usuario tiene", y "algo que el usuario es"). Para este caso se utilizaría el doble factor:

Algo que el usuario sabe (por ejemplo, contraseña);

Algo que el usuario tiene (por ejemplo, un código generado por un dispositivo TOKEN)

El primer factor de identificación es la contraseña que normalmente utilizamos para poder acceder a los equipos de cómputo. El segundo factor de autenticación es el número que se genera en el TOKEN y que está cambiando en un periodo de tiempo no mayor a un minuto. El usuario para poder acceder a su equipo y a la información sensible que este contiene necesitara de los dos factores de autenticación.

VENTAJAS:

- Eleva el nivel de seguridad en el acceso a los equipos que contienen información altamente sensible.
- Es fácil de utilizar.

- El segundo factor generado por el Token cambia constantemente con lo que no existe riesgo en caso se obtenga el código generado por el Token por un usuario no autorizado.

ALTERNATIVA III: IMPLEMENTACIÓN DE DLP (Data Lost Prevention)

DLP es un producto de software que permite disminuir considerablemente el riesgo de fuga de información mediante la protección de la estación final mediante la creación de políticas que impiden la fuga de información a través de correo electrónico ,Publicaciones Web, Impresiones; Medios Removibles (USB, CD, etc.)

VENTAJAS:

- Monitorea la transferencia de datos confidenciales
- Coloca los datos confidenciales en cuarentena ante posibles fugas de información
- Permite clasificar la información por ubicación, contenido, tipo de archivo.
- Notifica a los administrados los posibles intentos de Fuga de Información

SELECCIÓN DE UNA ALTERNATIVA DE SOLUCIÓN

Para la selección de una de las alternativas de solución se usaron diferentes criterios de los cuales unos tenían mayor relevancia que otros. A continuación se detallarán los criterios usados mostrando su respectivo peso y la valoración obtenida.

Criterio 1: Reducción de los riesgos de fuga de Información (60%)

Este criterio es el más importante debido a que el Banco tiene como objetivo corporativo el reducir el riesgo de fuga de información sensible. Por tal motivo realizaremos una evaluación del cumplimiento de las tres alternativas para reducir los riesgos mencionados inicialmente.

Criterio 2: Facilidad de uso para los usuarios finales. (20%)

El segundo criterio es la facilidad de la aplicación para el usuario final. Se debe considerar la resistencia al cambio que puede representar las actividades que se tengan que desarrollar con la implementación de cada una de las alternativas.

Criterio 3: Costo de Implementación y Mantenimiento. (10%)

El costo de implementación y mantenimiento se debe de considerar aunque no representa un criterio crucial para la evaluación debido a que ya se cuenta con una partida presupuestada para este proyecto.

Criterio 4: Tiempo de implementación. (10%)

El tiempo de implementación debe ser considerar para poder reducir los riesgos identificados de las posibles fugas de información lo antes posible; sin embargo las tecnologías de seguridad de la información se caracterizan por su rápida implementación en el Banco

La metodología que utilizaremos será la de puntuar los criterios de la siguiente manera:

5 = Muy Alto

4 = Alto

3 = Regular

2 = Bajo

1 = Muy Bajo

a) Calculo de la puntuación para el criterio 1

	Problemática 1	Problemática 2	Problemática 3	Promedio
Alternativa I	4	4	4	4
Alternativa II	2	3	1	2
Alternativa III	4	3	2	3

b) Calculo de la mejor alternativa

	Criterio 1	Criterio 2	Criterio 3	Criterio 4	Total
	60%	20%	10%	10%	
Alternativa I	4	3	4	3	3.7
Alternativa II	2	3	3	4	2.5
Alternativa III	3	4	2	2	3

De acuerdo al cuadro la alternativa I es la que mejor se adecua a las necesidades de la organización.

PLANES DE ACCIÓN PARA DESARROLLAR LA ALTERNATIVA DE SOLUCIÓN PLANTEADA

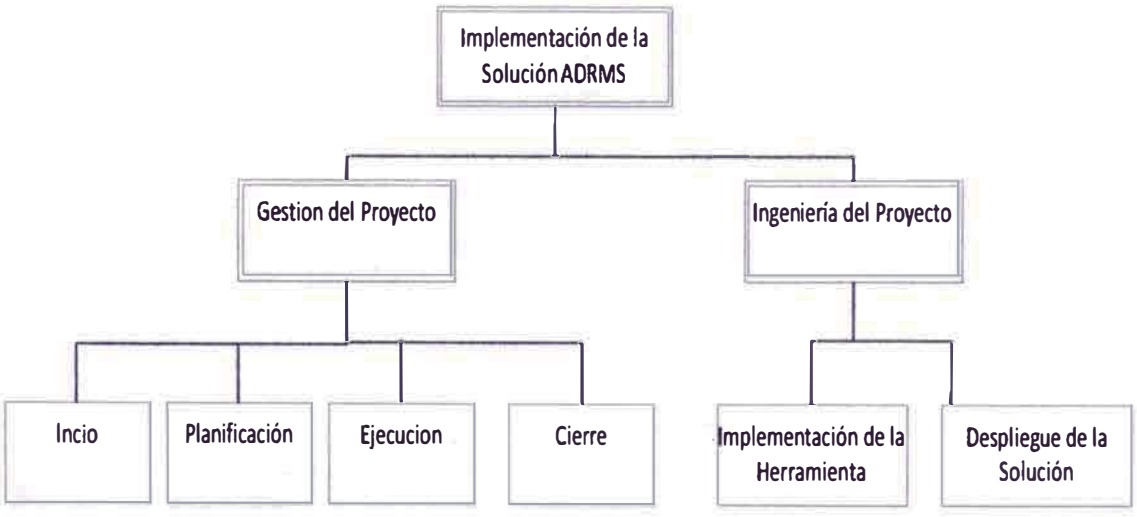
a) Alcance

Los documentos generados en la suite de Microsoft suite de Microsoft (Word, Excel, Power Point) por la Unidad de Tarjetas del Banco que contengan el Número de tarjeta de los clientes.

b) Estructura de Desglose de Trabajo

La estructura de Desglose de trabajo nos indica las fases del proyecto y los principales entregables que se deben de generar.

Figura 18: Estructura de Desglose de Trabajo del Proyecto



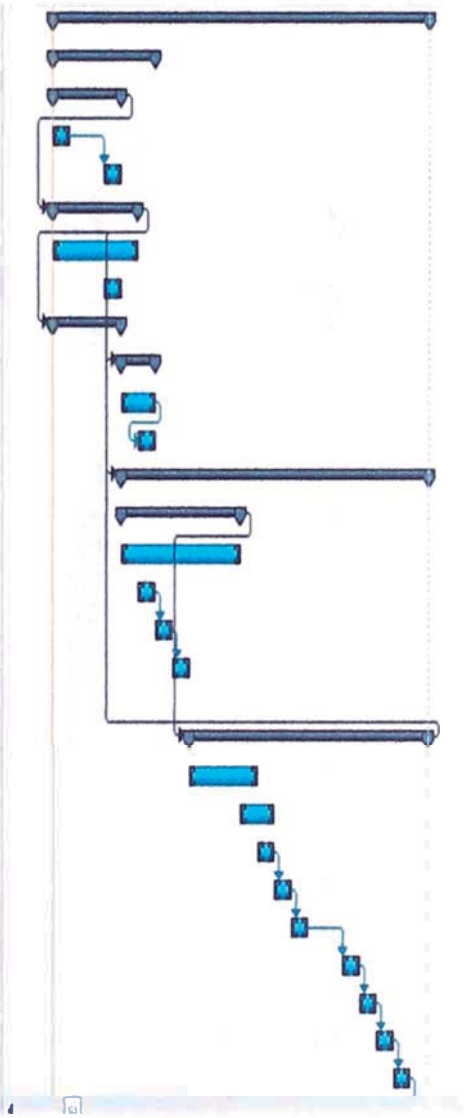
Fuente: Elaboración Propia

c) Cronograma

En el siguiente cronograma se han detallado las actividades que se van a realizar para Implementa la herramienta tecnología ADRMS

Figura 19 Cronograma del Proyecto

	Nombre de tarea	Duración	Comienzo	Fin
1	Implementacion de la solucion ADRMS	16 días	vie 15/06/12	vie 06/07/12
2	Gestion del Proyecto	4 días	vie 15/06/12	mié 20/06/12
3	Inicio	2 días	vie 15/06/12	lun 18/06/12
4	Acta de Inicio de proyecto	1 día	vie 15/06/12	vie 15/06/12
5	Comité de Incio de Proyecto	1 día	lun 18/06/12	lun 18/06/12
6	Planificacion	3 días	vie 15/06/12	mar 19/06/12
7	Plan de Proyecto	3 días	vie 15/06/12	mar 19/06/12
8	Comité de Planificacion de Proyecto	1 día	lun 18/06/12	lun 18/06/12
9	Ejecucion	2 días	vie 15/06/12	lun 18/06/12
12	Cierre	2 días	lun 18/06/12	mié 20/06/12
13	Informe final	2 días	lun 18/06/12	mié 20/06/12
14	Comité de Cierre	1 día	mié 20/06/12	mié 20/06/12
15	Ingenieria del Proyecto	14 días	lun 18/06/12	vie 06/07/12
16	Implementacion de la herramienta	5 días	lun 18/06/12	lun 25/06/12
17	Implementacion de la parte Tecnica	5 días	lun 18/06/12	lun 25/06/12
18	Generacion de los Manuales de Administrador	1 día	mié 20/06/12	mié 20/06/12
19	Generacion de los Manuales de Usuario	1 día	jue 21/06/12	jue 21/06/12
20	Capacitacion de los Administradores del de la herramienta	1 día	vie 22/06/12	vie 22/06/12
21	Despliegue de la Solucion	10 días	vie 22/06/12	vie 06/07/12
22	Identificacion de los procesos de Negocio	2 días	vie 22/06/12	mar 26/06/12
23	Identificacion de los Flujos de Informacion	2 días	mar 26/06/12	mié 27/06/12
24	Definicion de las plantillas de Seguridad	1 día	mié 27/06/12	mié 27/06/12
25	Implementacion de las plantillas	1 día	jue 28/06/12	jue 28/06/12
26	Pruebas de las plantillas	1 día	vie 29/06/12	vie 29/06/12
27	Selección de Flujos para piloto	1 día	lun 02/07/12	lun 02/07/12
28	Ejecucion del Piloto	1 día	mar 03/07/12	mar 03/07/12
29	Modificaciones en las plantillas	1 día	mié 04/07/12	mié 04/07/12
30	Capacitacion en la herramienta	1 día	jue 05/07/12	jue 05/07/12

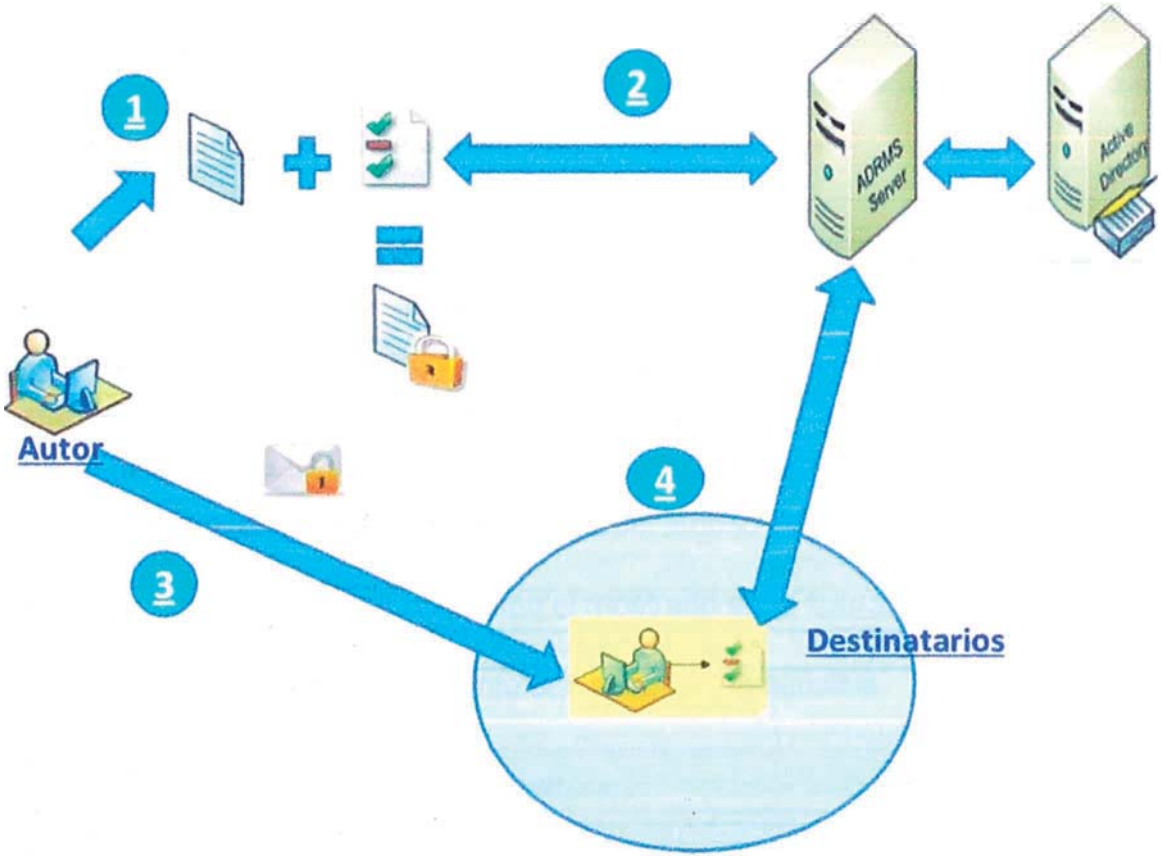


Fuente: Elaboración Propia

FLUJO OPERACIONAL

En el siguiente diagrama se explican los pasos que debe realizar el usuario para el intercambio de información confidencial

Figura 20: Flujo Operacional



Fuente: Elaboración Propia

1.-El autor genera información sensible a proteger.

2.- El autor protege la información utilizando la herramienta ADRMS.

3.- El autor envía la información protegida a otros usuarios.

4.- Los destinatarios abren el documento y se verifican los derechos de estos usuarios sobre la información en el ADRMS.

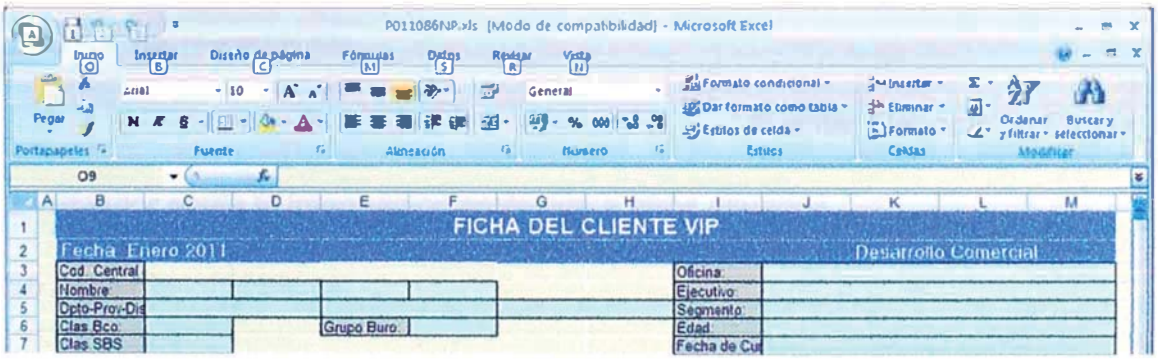
Detalle de los Pasos:

1. El autor genera información sensible a proteger

   El personal de la Unidad de Tarjetas envía vía e-mail documentos información de tarjetas a otras unidades para su gestión. Los documentos son archivos Excel que contienen un listado de los clientes a gestionar con sus respectivos datos personales y datos de tarjeta, lo cual hace que la información se catalogue como sensible y sea prioritario evitar que esta llegue a personas no autorizadas o salga del ámbito del Banco.

   Los usuarios recibían un Excel como el mostrado en la figura.

Figura 21: Documento con información sensible

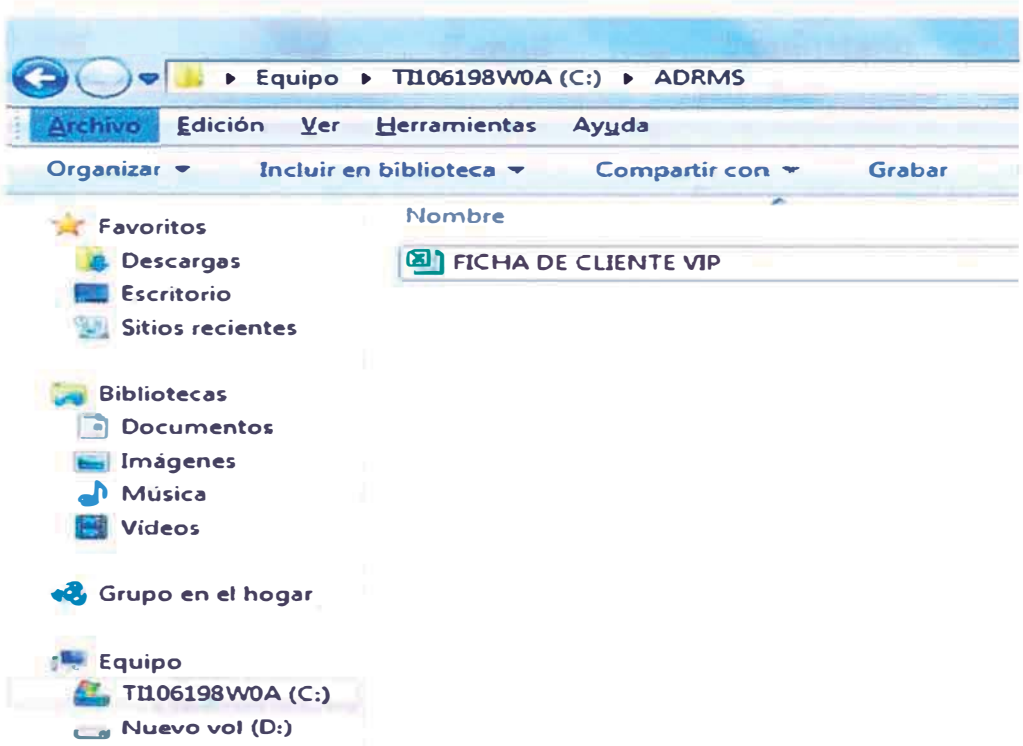


Fuente: Elaboración Propia

2.- El autor protege la información utilizando la herramienta ADRMS.

La unidad de Medios de la Unidad de Medios de Pago coloca el documento generado en una carpeta definida en su computadora y activa la protección de la herramienta ADRMS, con lo cual el todos los documentos que se ubiquen en la carpeta quedan protegidos.

Figura 22: Carpeta seleccionada para la protección de documentos



Fuente: Elaboración Propia

3.- El autor envía la información protegida a otros usuarios.

Se presentan dos casos:

3.1 caso I: Envió a Destinarios No autorizadas

Figura 23: Envió de documentos a destinatarios No autorizados

Fuente: Elaboración Propia

3.2 Caso II: Envió a Destinatario autorizado

Figura 24: Envió de documentos a destinatarios autorizados

Fuente: Elaboración Propia

4.- Los destinatarios abren el documento y se verifican los derechos de estos usuarios sobre la información en el ADRMS.

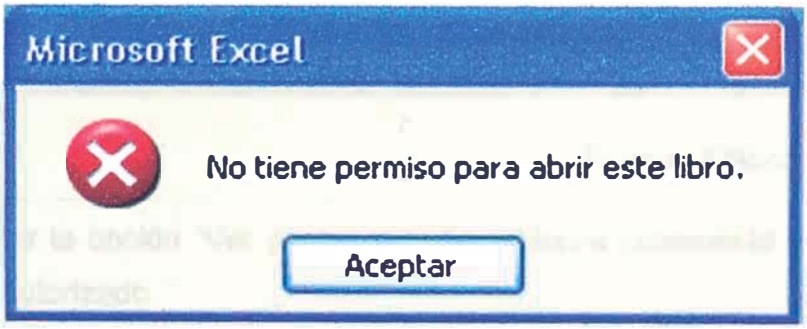
Los destinatarios intentaran al intentar abrir el documento activa el control de acceso ADRMS y realiza una consulta al Directorio Activo para identificar si el destinario está autorizado para acceder al documento. Si el intento de abrir el documento es realizado con un equipo que esta fuera de la red interna del Banco, el usuario será identificado como no autorizado.

Se presentan los dos casos anteriores:

Caso I: Destinario No autorizado intenta abrir el documento

El destinatario no autorizado no podrá abrir el documento y se le mostrara el siguiente mensaje:

Figura 25: Mensaje para usuario No autorizado

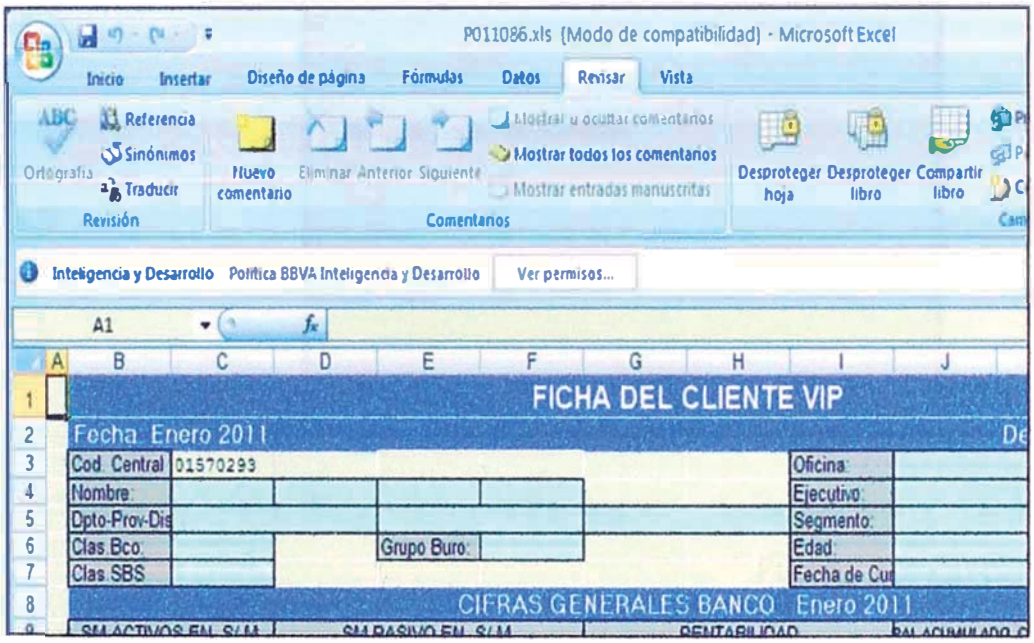


Fuente: Elaboración Propia

Caso II: Destinario autorizado intenta abrir el documento

El Destinatario autorizado si podrá abrir el documento. En la parte superior del documento se mostrara un mensaje con los permisos que tiene el Destinatario sobre el Documento:

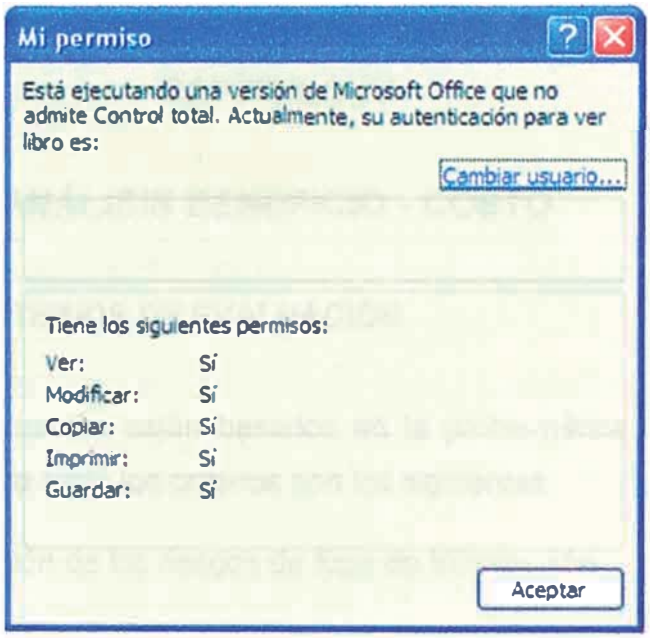
Figura 26: Archivo protegido



Fuente: Elaboración Propia

Al seleccionar la opción "Ver permisos." Se muestra justamente los permisos del usuario autorizado

Figura 27: Mensaje para usuario autorizado



Fuente: Elaboración Propia

CAPÍTULO IV

ANÁLISIS BENEFICIO - COSTO

SELECCIÓN DE CRITERIOS DE EVALUACIÓN

Los criterios de Evaluación están basados en la problemática definida en el capitulo anterior, por lo tanto los criterios son los siguientes:

CRITERIO 1: Reducción de los riesgos de fuga de Información

Este criterio es el más importante debido a que el Banco tiene como objetivo corporativo el reducir el riesgo de fuga de información sensible. Por tal motivo realizaremos una evaluación del cumplimiento de las tres alternativas para reducir los riesgos mencionados inicialmente.

CRITERIO 2: Facilidad de uso para los usuarios finales.

El segundo criterio es la facilidad de la aplicación para el usuario final. Se debe considerar la resistencia al cambio que puede representar las actividades que se tengan que desarrollar con la implementación de cada una de las alternativas.

CRITERIO 3: Costo de Implementación y Mantenimiento.

El costo de implementación y mantenimiento se debe de considerar aunque no representa un criterio crucial para la evaluación debido a que ya se cuenta con una partida presupuestada para este proyecto.

CRITERIO 4: Tiempo de implementación.

El tiempo de implementación debe ser considerar para poder reducir los riesgos identificados de las posibles fugas de información lo antes posible; sin embargo las tecnologías de seguridad de la información se caracterizan por su rápida implementación en el Banco

COSTOS DE LA IMPLEMENTACION

Los costos de la Implementación se muestran en el siguiente cuadro. El valor de los servidores no se considera para los costos del proyecto debido a que el Banco ya contaba con ellos.

Figura 28: Costos del proyecto

CONCEPTOS	PRODUCTO	CANT.	PRECIOS UNIT.	PRECIO TOTAL
Licencias	MS SQL Server Standard 2008 R2	1	$7,331.00	$7,331.00
	Office Professional Plus 2003/2007/2010	40	$520.00	$20,800.00
	Windowns RMS CAL 2008	400	$38.00	$15,200.00
	Windows ADRMS External Connector	1	$18,633.00	$18,633.00
	Windows Server Standard 2008 R2	2	$742.00	$1,484.00
Equipos	1 Servidor para Instalación de ADRMS	1	$0.00	$0.00
	1 Servidor para Base de Datos	1	$0.00	$0.00
Servicios	Capacitación Administrativa	1	$5,000.00	$5,000.00
	Instalación y Configuración de solución ADRMS	1	$29,750.00	$29,750.00
			TOTAL	**$98,198.00**

Fuente: Elaboración Propia

Los costos del proyecto se contabilizaran como parte del presupuesto que el Banco dispone para los proyectos de Seguridad de la Información para el cumplimiento de las Normativas:

- Ley de Protección de Datos Personales
- Norma De Seguridad De Datos De La Industria De Tarjetas De Pago (PCI-DSS)

RESULTADOS DE LA SOLUCIÓN PLANTEADA

Para medir los resultados de la solución planteada se define el siguiente indicador:

Nombre del Indicador: Documentos Protegidos con ADRMS

Formula: (Numero de Documentos Protegidos)/ (Numero de Documentos Revisados)

Frecuencia de la Medición: Semanalmente

Descripción: Se medirá la cantidad de Documentos de la Suite de Microsoft (Word, Excel, Power Point) que son protegidos con la Herramienta ADRMS.

Alcance: Los documentos generados por la unidad de tarjetas que contengan el Número de Tarjeta en su contenido

Procedimiento:

Debido a que se tienen identificados los flujos de información de la unidad de tarjetas con otras unidades del Banco, se realizara revisiones periódicas para verificar que los documentos que contienen el número de tarjeta están protegidos con la solución ADRMS.

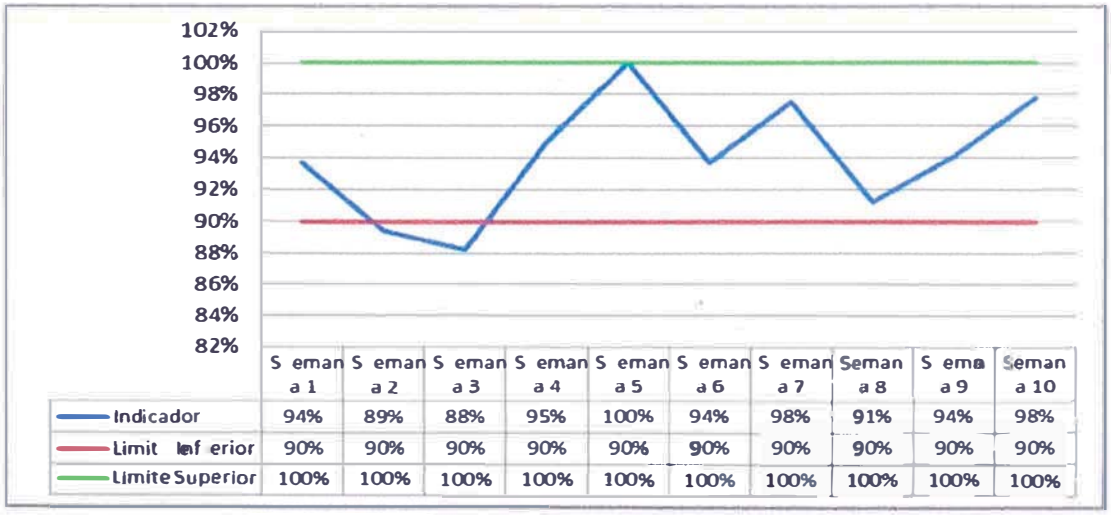
EVALUACIÓN:

Figura 29: Resultado de la medida del Indicador

Semana	Num. de documentos Protegidos	Num. de documentos Evaluados	Indicador	Limite Inferior	Limite Superior
Semana 1	75	80	94%	90%	100%
Semana 2	76	85	89%	90%	100%
Semana 3	75	85	88%	90%	100%
Semana 4	76	80	95%	90%	100%
Semana 5	90	90	100%	90%	100%
Semana 6	89	95	94%	90%	100%
Semana 7	78	80	98%	90%	100%
Semana 8	73	80	91%	90%	100%
Semana 9	80	85	94%	90%	100%
Semana 10	88	90	98%	90%	100%

Fuente: Elaboración Propia

Figura 30: Resultado de la medida del Indicador



Fuente: Elaboración propia

En la semana 1, el indicador fue de 94% de documentos protegidos, sin embargo en las siguientes dos semanas el indicador estaba por debajo de lo esperado debido a que los usuarios estaban en proceso de aprendizaje de la herramienta ADRMS

A partir de la cuarta semana el indicador muestra valores que se encuentran dentro de los límites de control aceptables y se mantiene dentro de los limites de control hasta la decima semana. Con este resultado podemos afirmar que la herramienta ADRMS ha sido implementada satisfactoriamente.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

Podemos mencionar como principales conclusiones lo siguiente:

1. Los documentos que contengan los Números de Tarjeta de los clientes del Banco son considerados como información confidencial y debe de ser protegida según las normativas de la Ley de Protección de Datos y la Norma PCI DSS.

2. La seguridad de la Herramienta ADRMS está basada en la criptografía asimétrica. La criptografía simétrica es un tipo de criptografía moderna que actualmente es una de las más utilizadas para asegurar la confidencialidad de la información que se desee proteger.

3. La implementación de la Herramienta ADRMS debe realizarse en aproximadamente un mes, siendo la fase de despliegue la fase que más tiempo puede consumir.

4. El valor del indicador de Documentos Protegidos con ADRMS dio un giro positivo y se mantuvo dentro de los limites esperados en las seis últimas semanas de su evaluación

RECOMENDACIONES:

1. Se tiene que realizar un constante monitoreo del cumplimiento de que los usuarios de la unidad de Tarjetas estén protegiendo los documentos con la Herramienta ADRMS.

2. Es importante concientizar al personal que utilizara la herramienta ADRMS, de la importancia de proteger los documentos con información confidencial.

3. Actualmente los documentos que salen fuera del Banco y están protegidos con ADRMS no pueden ser accedidos por persona externas. En una etapa posterior se debe trabajar para que se pueda identificar a usuarios que no están dentro del Banco pero que si necesitan tener acceso a los documentos como es el caso de los proveedores.

GLOSARIO

Llave privada

Mitad secreta de un par de claves criptográficas que se utiliza con un algoritmo de clave pública. Las claves privadas se suelen utilizar para descifrar una clave de sesión simétrica, firmar datos digitalmente o descifrar datos que se hayan cifrado con la correspondiente clave pública.

Llave pública

Mitad no secreta de un par de claves criptográficas que se utiliza con un algoritmo de clave pública. Las claves públicas se suelen utilizar para cifrar una clave de sesión, verificar una firma digital o cifrar datos que se pueden descifrar con la clave privada correspondiente.

Cifrado

Proceso de convertir información en un formato que sólo puede leer un receptor específico. El cifrado es un modo efectivo para ayudar a mantener la información protegida. Para descifrar un archivo que se ha cifrado, el receptor debe tener la clave secreta o la contraseña que lo traducirá.

BIBLIOGRAFÍA

Revista Digital del Banco 2007, 2008,2009.

Introducción a la Criptografía - Gibrán Granados Paredes - Coordinación de Publicaciones Digitales. DGSCA-UNAM

Links de páginas web:

http://technet.microsoft.com/es-es/library/cc720205(v=ws.10).aspx

http://technet.microsoft.com/es-es/library/cc706990(v=ws.10).aspx

http://www.microsoft.com/spain/windowsserver2008/roles/apps_ad.mspx

http://www.microsoft.com/spain/windowsserver2008/roles/apps_rms.mspx

http://technet.microsoft.com/en-us/library/cc771234(v=ws.10).aspx

http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

http://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

ANEXO I CRIPTOGRAFIA

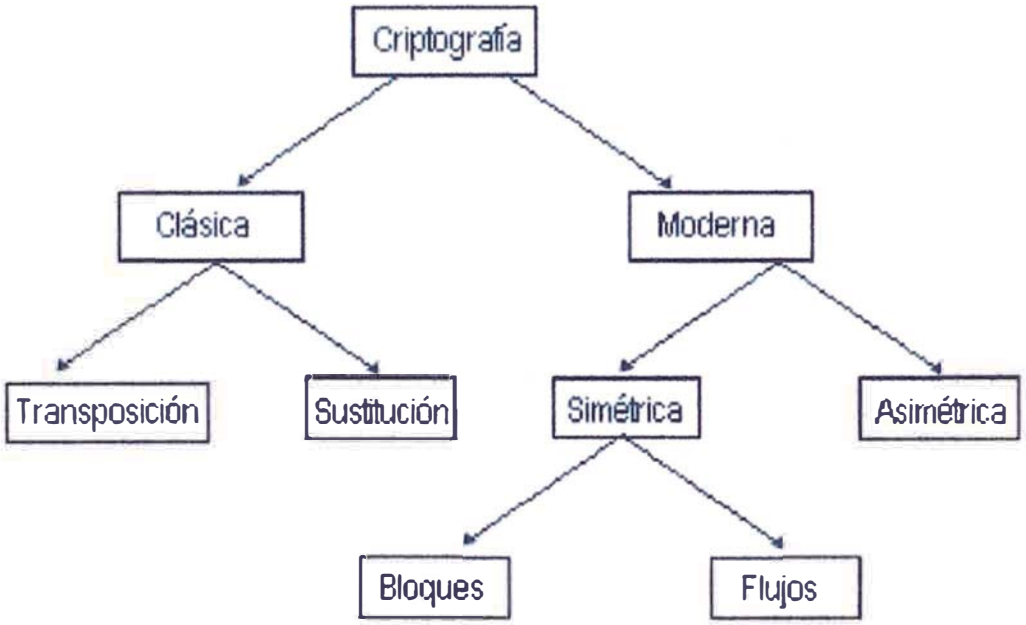
CLASIFICACIÓN DE LA CRIPTOGRAFÍA

La criptografía se puede clasificar históricamente en dos: La criptografía clásica y la criptografía moderna. La criptografía clásica es aquella que se utilizó desde antes de la época actual hasta la mitad del siglo XX. También puede entenderse como la criptografía no computarizada o mejor dicho no digitalizada. Los métodos utilizados eran variados, algunos muy simples y otros muy complicados de criptoanálisis para su época.

Se puede decir que la criptografía moderna se inició después de tres hechos: el primero fue la publicación de la "Teoría de la Información" por Shannon; el segundo, la aparición del estándar del sistema de cifrado DES (Data Encryption Standard) en 1974 y finalmente con la aparición del estudio realizado por Whitfield Diffie y Martin Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifrado, denominado cifrado de llave pública en 1976.

Tanto la criptografía clásica como la moderna se clasifican de acuerdo a las técnicas o métodos que se utilizan para cifrar los mensajes. Esta clasificación la podemos ver en la siguiente figura:

Figura 31: Clasificación de la criptografía



Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

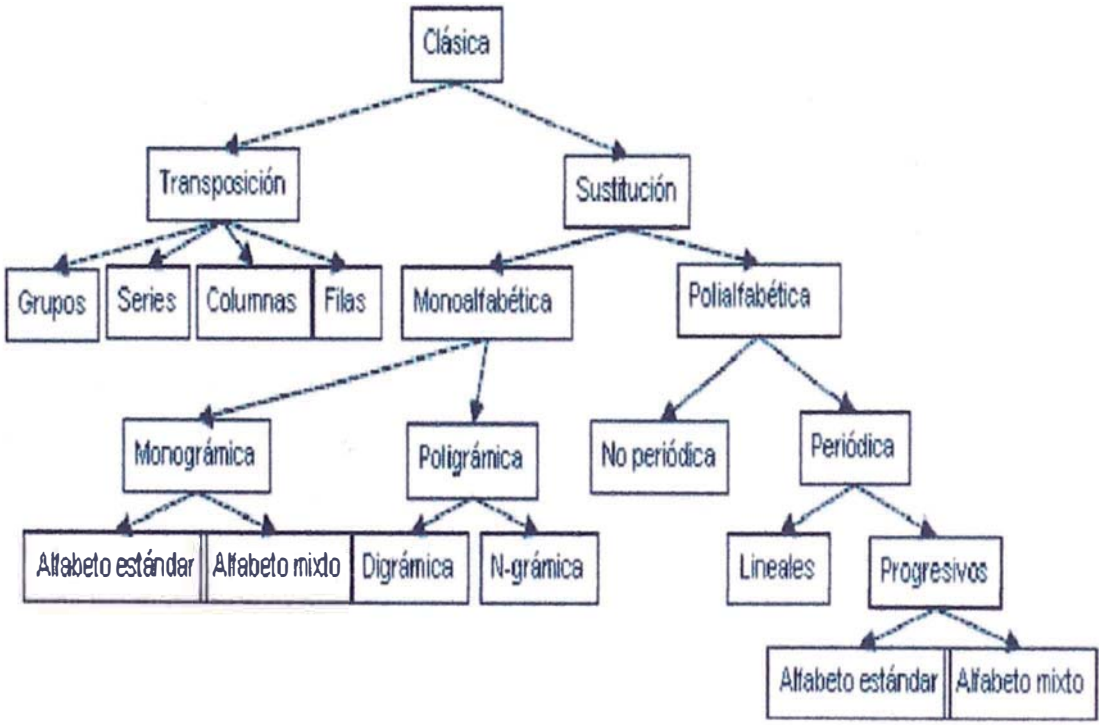
CRIPTOGRAFÍA CLÁSICA

Como ya se mencionó anteriormente, la criptografía clásica es muy antigua. Las técnicas criptográficas eran muy ingeniosas y se usaban para enviar mensajes secretos entre las personas que tenían el poder o en época de guerra para enviar instrucciones. A diferencia de la criptografía moderna, el algoritmo del sistema criptográfico se mantenía en secreto. La criptografía clásica también

incluye la construcción de máquinas, que mediante mecanismos, comúnmente engranes o rotores, transformaban un mensaje en claro a un mensaje cifrado, como la máquina Enigma usada en la Segunda Guerra Mundial.

La siguiente figura ilustra la clasificación de la criptografía clásica:

Figura 32: Clasificación de la criptografía clásica



Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

Los cifradores por transposición utilizan la técnica de permutación de forma que los caracteres del texto reordenan mediante un algoritmo específico.

Los cifradores por sustitución utilizan la técnica de modificación de cada carácter del texto en claro por otro correspondiente al alfabeto de cifrado. Si el alfabeto de cifrado es el mismo que el del mensaje

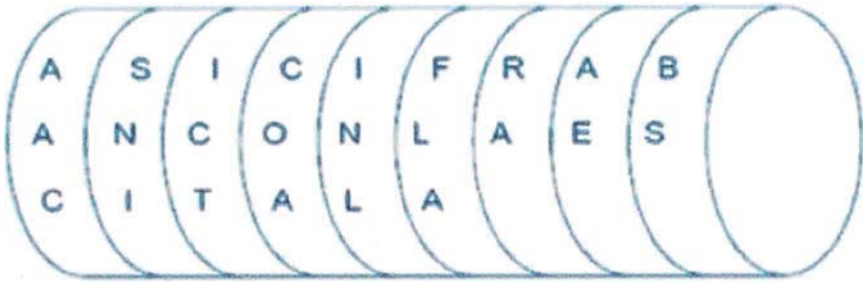
o bien el único, hablamos entonces de cifradores monoalfabéticos; es decir, existe un único alfabeto en la operación de transformación del mensaje en criptograma. Por el contrario, si en dicha operación intervienen más de un alfabeto, se dice que el cifrador es polialfabético.

Es realmente interesante analizar cada una de las técnicas anteriores, en este documento sólo se verán dos técnicas: un cifrado de transposición de grupos, la escítala, y un ejemplo de sustitución monoalfabética, monográmica con el alfabeto estándar, el cifrado César.

LA ESCÍTALA

En siglo V a.c. los lacedemonios, un antiguo pueblo griego, usaban el método de la escítala para cifrar sus mensajes. El sistema consistía en una cinta que se enrollaba en un bastón sobre el cual se escribía el mensaje en forma longitudinal, como se muestra en la siguiente figura:

Figura 33: Escítala



Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

Una vez escrito el mensaje, la cinta se desenrollaba y era entregada al mensajero. Para enmascarar completamente la escritura es obvio que la cinta en cuestión debe tener caracteres en todo su contorno. Como es de esperar, la llave del sistema residía precisamente en el diámetro de aquel bastón, de forma que solamente el receptor autorizado tenía una copia exacta del mismo bastón en el que enrollaba el mensaje recibido y, por tanto, podía leer el texto en claro.

EL CIFRADO CÉSAR

En el siglo I a.c. aparece un método de cifrado conocido con el nombre genérico de cifrado de César en honor al emperador Julio César y en el que ya se aplica una transformación al texto en claro de tipo monoalfabética. El cifrado del César aplica un desplazamiento constante de tres caracteres al texto en claro, de forma que el alfabeto de cifrado es el mismo que el alfabeto del texto en claro, pero desplazado 3 espacios hacia la derecha módulo n, con n el número de letras del mismo. A continuación se muestra el alfabeto y la transformación que

realiza este cifrador por sustitución de caracteres para el alfabeto castellano de 27 letras.

Figura 34: El Cifrador de Cesar

Alfabeto	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fuente: Introducción a la Criptografía - Gibrán Granados Paredes

Así con este alfabeto podemos cifrar el siguiente mensaje:

Mensaje original: MENSAJE DE PRUEBA

Mensaje cifrado: OHPVDM GH SUXHED

Al describir el cifrado de César se utilizó un concepto muy usado en las matemáticas y más en criptografía: el módulo.

El módulo es una operación binaria que se realiza en los enteros positivos y se representa de la siguiente forma: c = a mod b de tal forma que a, b y c son enteros positivos. El valor de c al realizar la operación c = a modulo b es igual al residuo de dividir a entre b. Se puede observar claramente que 0 <= c < b.

Con este antecedente podemos escribir en forma matemática el cifrado de César de la siguiente forma:

Para cifrar

$Ci = (3 + Mi) \bmod 27$

con i= 0,1,...,n ; n = número de letras del mensaje

donde Ci es la letra cifrada y Mi es la letra a cifrar

el alfabeto comienza con A = 0 , B=1, ..., Z=26

Para descifrar

Mi = (Ci - 3) mod 27 = (Ci + 24) mod 27

con i= 0,1,...,n ; n = número de letras del mensaje

donde Ci es la letra cifrada y Mi es la letra a cifrar

el alfabeto comienza con A = 0 , B=1, ..., Z=26

ANEXO II CLASIFICACIÓN DE LA INFORMACION DEL BANCO

El Banco considera que la protección de sus activos, y con ella la sostenibilidad del negocio, debe ser uno de los compromisos más importantes de cara a sus clientes, accionistas y a la sociedad en general.

Bajo esta consideración, la dirección del Banco reconoce a la información y a los sistemas que la sustentan y procesan, como uno de sus activos más importantes a proteger, y establece como objetivo la gestión efectiva y eficiente de los riesgos a los que se ven sujetos, garantizando un adecuado control interno de los mismos.

El Banco adquiere la responsabilidad de promover y apoyar el establecimiento de medidas técnicas, organizativas y de control que garanticen la confidencialidad de la información, dentro de un marco general de gestión de riesgos de seguridad.

OBJETIVO DE CLASIFICACIÓN DE LA INFORMACIÓN

Basados en la experiencia y en incidentes con los que el Grupo ha tenido que lidiar, se ha puesto de manifiesto la necesidad de proteger con mayor esmero aquella información relacionada con incidentes recurrentes, insistiendo en que dichos ataques y las medidas necesarias para mitigarlos son su prioridad, como se muestra en el siguiente gráfico:

A continuación se describen los objetivos estratégicos del Banco en cuanto a la gestión de la seguridad de la información:

Situar al Banco como líder del sector financiero en la gestión de la intencionalidad, es decir, en proteger de forma especial la información objetivo de la delincuencia organizada en cada momento.

Situar al Banco en la media del sector financiero en cuanto a la gestión global de la seguridad de la información, es decir, en el desarrollo y despliegue de medidas organizativas y tecnológicas, la aplicación de estándares internacionales y buenas prácticas, así como en el despliegue tecnológico requerido para la gestión preventiva y proactiva de la seguridad sobre eventos no intencionados, alineándolos con la metodología de clasificación desplegada

Cumplir con la legislación regulatoria aplicable en los países en donde el Banco tenga operaciones; siendo las principales:

- PCI – DSS: Payment Card Industry – Data Security Standard.
- Ley de Protección de Datos Personales

NIVELES DE CLASIFICACIÓN

A continuación se describen los distintos niveles de clasificación de la información definidos en el modelo.

Figura 35: Clasificación de la Información

Fuente: Elaboración Propia

INFORMACIÓN PÚBLICA

La información pública es aquella información que ha sido divulgada o publicada previa autorización.

La información pública será accesible a todo aquel interesado en acceder a ella. Esta información no depende de ningún criterio predeterminado de acceso.

Este tipo de información no requiere de protección especial más allá de la revisión de integridad, ya que su divulgación no supondrá un perjuicio económico.

Así mismo, este tipo de información puede originarse debido a las regulaciones existentes en cada país en donde el BANCO tiene operaciones. Para este

supuesto, se deberá contar con un análisis particular de esta información en lo relativo al cumplimiento de dichas regulaciones.

Por defecto toda información cuyo repositorio sea de dominio público se considerará como información pública.

INFORMACIÓN INTERNA

Información departamental es aquella información necesaria para el correcto desempeño de las funciones y negocios que tiene el Banco por ser una empresa, y cuya divulgación intencionada o accidental podría suponer en algún caso un quebranto económico no significativo. Este tipo de información será accesible por el personal interno del BANCO o ligado contractualmente a él, y no deberá transmitirse ni comunicarse fuera del mismo sin autorización previa.

El nivel de información departamental será considerado como el nivel por defecto para el tratamiento de información no estructurada con el fin de asignar las medidas de seguridad correspondientes y estandarizar la clasificación de la información en todos los procesos operativos del Banco

INFORMACIÓN CONFIDENCIAL

Información confidencial es el tipo de información no estructurada cuya divulgación, alteración o pérdida puede suponer un impacto económico o de imagen muy significativo o crítico para el Banco.

INFORMACIÓN SECRETA.

Información secreta es aquélla que debe ser conocida únicamente por el propietario de la misma.

MEDIDAS DE SEGURIDAD

Las medidas de seguridad a aplicar a la información dependerán de su nivel de clasificación, de si es estructurada o no estructurada y del estadio del ciclo de vida en el que se encuentre.

En la mayoría de los casos podrán establecerse medidas de seguridad de índole tecnológica; sin embargo, en algunas situaciones se deberán establecer medidas de seguridad por medio de normativas de obligado cumplimiento. Por ejemplo, "obligatoriedad de cifrar la información confidencial que se envía por medio de correo electrónico" o "prohibición de enviar información secreta por medio de correo electrónico".

Asimismo, se podrá restringir el acceso de los usuarios a ciertos estadios del ciclo de vida de la información. Por ejemplo, "prohibición de crear información confidencial a usuarios con categoría inferior a X".

En cuanto a la información especial, la aplicación dinámica de medidas de seguridad irá ligada a los requerimientos establecidos por la gestión de la intencionalidad y a las necesidades regulatorias.