



USAID
FROM THE AMERICAN PEOPLE

BRANCHLESS BANKING/MOBILE MONEY: INFORMATION SECURITY

USAID/EL SALVADOR IMPROVING ACCESS TO FINANCIAL SERVICES
PROJECT

JULY 2012

This publication was produced for review by the United States Agency for International Development. It was prepared by Freddy Landivar and Weidemann Associates and submitted by Global Business Solutions, Inc.

BRANCHLESS BANKING/MOBILE MONEY: INFORMATION SECURITY FINAL REPORT

Submitted by:

Global Business Solutions, Inc.

Authored by:

Freddy Landivar, Weidemann Associates, Inc.

Submitted to:

USAID/El Salvador

AID-519-C-12-00001

USAID/El Salvador Improving Access to Financial Services Project

DISCLAIMER

The views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States Government.

CONTENIDOS

- 1. RESUMEN EJECUTIVO.....1
- 2. ANTECEDENTES.....2
- 3. OBJETIVOS Y AGENDA DE LA MISION.....2
 - OBJECTIVO GENERAL.....2
 - OBJECTIVOS ESPECIFICOS.....2
- 4. ACTIVIDADES DESARROLLADAS.....3
- 5. RESULTADOS Y CONCLUSIONES.....3
- ANNEX LIST.....4

I. RESUMEN EJECUTIVO

A raíz del compromiso del Presidente del Banco Central de Reserva de El Salvador para presentar un conjunto de leyes y regulaciones con el fin de fomentar el modelo de “Banca sin Sucursales/Dinero Móvil” para la república de El Salvador, se definió crear un entorno normativo que promueva y supervise efectivamente a todos los actores del sector privado que entraran en activa competencia a raíz del ingreso del modelo mencionado al mercado financiero salvadoreño.

Por lo enunciado y con el apoyo del programa “USAID/Improving Access to Financial Services Program”, se estructuró para representantes del Banco Central de Reserva (BCR) y la Superintendencia del Sistema Financiero (SSF), una serie de visitas a países que ya tienen implementado el modelo mencionado, con el objetivo de que adquirieran familiaridad con los entornos regulatorios. Asimismo, se diseñó una serie de reuniones técnicas y talleres con expertos sobre tópicos referidos al modelo a implementar, donde la presente consultoría, formó parte de ésta serie de actividades proporcionando orientación y guía al BCR y a la SSF en la preparación de normas, reglamentos y directrices sobre la seguridad informática aplicada al Sistema de Pagos Móviles.

En este sentido, para cumplir con las orientaciones y guías enunciadas, se desarrollaron una serie de actividades que culminaron con el enunciado y estructuración de principios de normativa técnica relacionada a la seguridad informática para el Sistema de Pagos Móviles. Estas actividades, en forma general, fueron:

- Desarrollo y estructuración, en el contexto de los servicios financieros móviles, del material referido a tecnología móvil, arquitecturas de comunicación, gestión de riesgos, cadena de valor del servicio financiero móvil, estándares de seguridad e implicancia de la seguridad informática tomando en cuenta los riesgos involucrados.
- Desarrollo de Talleres considerando los tópicos estructurados y detallados en el punto anterior (24 horas aula / 3 Días)
- Asistencia y guía al BCR y SSF en mesas de trabajo (2 días) para elaborar la normativa técnica relacionada a la seguridad informática en el Sistema de Pagos Móviles (Pagos de servicios de bajo valor a través de telefonía móvil y Banca Móvil)

Como resultados de la consultoría efectuada, se desarrollaron y definieron, en forma conjunta con técnicos del BCR y la SSF, las normas técnicas relacionadas a la seguridad informática en el servicios de pagos a través de telefonía celular, mismas que formaran parte de las regulaciones que guiaran el Sistema de Pagos Móviles en El Salvador. Esta normativa técnica, fundada en principios, se estructuró en base a los factores de riesgo tecnológico más críticos en la cadena de valor definida para un mensaje de telefonía móvil, medio a través del cual se realizaran las transacciones financiera de pago. Estos factores se centraron en los siguientes segmentos de la cadena de valor: usuario, transporte/comunicaciones y administración de datos.

Tomando en cuenta lo mencionado y los objetivos trazados para esta consultoría, consideramos que el trabajo fue concluido a plenitud. Mayor detalle será referido en el cuerpo del presente informe, mismo que forma parte de una serie de otros informes que están relacionados al desarrollo de un marco regulatorio para Servicios Financieros Móviles.

II. ANTECEDENTES

Durante la última década las innovaciones tecnológicas han creado nuevos escenarios financieros, donde el sistema bancario ha estado jugando un rol siempre preponderante; sin embargo, esta preponderancia está siendo afectada debido a que las nuevas tecnologías desarrolladas en el ámbito de las telecomunicaciones, está sumando nuevos actores al escenario de la intermediación, como por ejemplo las telefónicas, las empresas de servicios móviles de pago, los mandatarios, etc.

Este nuevo escenario, requiere de marcos directrices que delinee el accionar de los diversos actores en este nuevo escenario, así como también, delinee aspectos referidos a la forma de asegurar que las innovaciones tecnológicas referidas, provean la seguridad, confiabilidad y disponibilidad de la información y de los componentes tecnológicos relacionados.

Asimismo, está por descontado que hoy en día, el desarrollo de estas nuevas tecnologías dentro del campo de la intermediación financiera, presenta modos seguros y más económicos para la interconexión y el flujo de datos; sin embargo, es primordialmente necesario tener presente que las nuevas tecnologías en el campo de las comunicaciones móviles, muestran un potencial para promover la “Inclusión Financiera”, misma que va más allá del simple uso técnico para la interconexión de dispositivos existentes; ésta nueva tecnología, ha creado nuevos canales de suministro de servicios, nuevos instrumentos y nuevos modelos de negocio que permiten brindar servicios financieros a personas que tradicionalmente habían quedado excluidas del sistema financiero formal.

El escenario mencionado muestra un potencial considerable para que los servicios financieros móviles lleguen a más personas, debido a que existen señales de una aceleración en la incorporación de estos servicios en varios países, principalmente latino y centro americanos. La telefonía celular está permitiendo que los operadores móviles participen en la prestación de determinados servicios financieros en varios mercados, aumentando de esta forma la competencia y, simultáneamente, planteando cuestiones de tipo normativo que es necesario encarar debido a la proliferación de distintos modelos de negocio y alternativas tecnológicas que contribuye a la complejidad de este nuevo escenario.

III. OBJETIVOS Y AGENDA DE LA MISIÓN

OBJETIVO GENERAL

El objetivo de la consultoría fue de guiar y orientar a representantes del Banco Central de Reserva y Superintendencia del Sistema Financiero de El Salvador, encargados de preparar las normas, reglamentos y directrices de supervisión para el proyecto “Servicio de Pagos Móviles”, en el enunciado y estructuración de principios de normativa técnica relacionada a la seguridad informática en el servicio de pagos de bajo valor a través de telefonía celular.

OBJETIVOS ESPECÍFICOS

- Estructurar y preparar material para talleres de capacitación sobre el contexto de los servicios financieros móviles, tecnología móvil, arquitecturas de comunicación, gestión de riesgos, mensajerías y su cadena de valor dentro el servicio móvil, estándares de seguridad, implicancia de la seguridad informática tomando en cuenta los riesgos involucrados, etc.
- Desarrollar Talleres considerando los tópicos estructurados y detallados en el punto anterior

- Asistir y guiar al BCR y SSF en mesas de trabajo para elaborar la normativa técnica relacionada a la seguridad informática en el Sistema de Pagos Móviles (Pagos de servicios de bajo valor a través de telefonía móvil y Banca Móvil)

IV. ACTIVIDADES DESARROLLADAS

Las actividades desarrolladas, enmarcadas en los objetivos descritos y cumpliendo los Términos de Referencia (Anexo 1), fueron:

- Estructurar y preparar material para talleres de capacitación sobre el contexto de los servicios financieros móviles, tecnología móvil, arquitecturas de comunicación, gestión de riesgos, mensajerías y su cadena de valor dentro el servicio móvil, estándares de seguridad, implicancia de la seguridad informática tomando en cuenta los riesgos involucrados, etc.
- Impartir talleres en función al Rol de Actividades previamente acordadas con representantes del BCR (Anexo 2), habiéndose estructurado los temas acordados en las siguientes presentaciones:
 - Aspecto conceptuales - Seguridad Informática y Servicios Financieros Móviles – Anexo 4
 - Tecnologías Aplicadas en Servicios Financieros Móviles I, II y III – Anexo 5, Anexo 6, Anexo 7
 - Estándares de seguridad de la información ISO/IEC 27002– Anexo 8
 - Herramienta de gestión de la seguridad y gobierno de TI – COBIT / ISACA– Anexo 9
 - Conceptualización de Riesgos – Anexo 10
 - Conceptos de Firma Digital – Anexo 11
- Desarrollo y definición, en forma conjunta con técnicos del BCR y la SSF, de las normas técnicas relacionadas a la seguridad informática en el servicios de pagos a través de telefonía celular, mismas que formaran parte de las regulaciones que guiaran el Sistema de Pagos Móviles en El Salvador.

V. RESULTADOS Y CONCLUSIONES

El resultado primario fue la estructuración y definición de la normativa técnica relacionada a la seguridad informática en los servicios de pagos a través de telefonía celular, misma que está fundada en principios. Esta estructuración tomó en cuenta los factores de riesgo tecnológico más críticos (usuario, transporte/comunicaciones y administración de datos) en la cadena de valor definida para un mensaje de telefonía móvil, medio a través del cual se realizarán las transacciones financiera de pago. Los enunciados de estos principios normativos se encuentran detallados en el Anexo 3.

Las conclusiones más importantes obtenidas de los talleres fueron:

- La normativa regulatoria debe situarse por encima de la tecnología, debido a que esta última presenta una diversidad de soluciones con una dinámica acelerada, lo cual genera cambios y mejoras continuas que serán difícil de seguir por una normativa que pretende ante todo ser inclusiva en el sector.

- Toda definición debe estar supeditada a análisis de riesgos exhaustivos donde se valore los riesgos en función a su impacto y su beneficio.
- Existe una constante evolución de las tecnologías para la comunicación en telefonía móvil, aspecto que a nivel sistémico/usuario, una migración de tecnologías implicaría para estos mayores costos.
- El eslabón más débil de la cadena de seguridad informática es el factor humano.
- El aspecto primordial para asegurar la integridad y confidencialidad de la información es estructurar un cifrado sólido de datos bajo la premisa End-to-End.

ANNEX LIST

Annex I: Términos de Referencia.....	6
Annex II: Norma Técnica Seguridad Informática en Servicios Financieros Móviles.....	9
Annex III: Cronograma de Actividades.....	12
Annex IV: Conceptualización de Riesgo.....	13
Annex V: Firma Digital.....	51
Annex VI: Aspectos conceptuales Seguridad Informática y SFM.....	71
Annex VII: Tecnologías aplicadas en SFM I.....	104
Annex VIII: Tecnologías aplicadas en SFM II.....	121
Annex IX: Tecnologías aplicadas en SFM III.....	146
Annex X: Estándares de Seguridad de TI Iso 27002.....	166
Annex XI: Herramienta metodológica COBIT.....	226

Annex I: Términos de Referencia

ANNEX I: TERMINOS DE REFERENCIA

SEGURIDAD INFORMÁTICA PARA LOS “SISTEMAS FINANCIEROS MÓVILES”

I. ANTECEDENTES

Durante la última década las innovaciones tecnológicas han creado nuevos escenarios financieros, donde el sistema bancario ha estado jugando un rol siempre preponderante; sin embargo, esta preponderancia está siendo afectada debido a que las nuevas tecnologías desarrolladas en el ámbito de las telecomunicaciones, está sumando nuevos actores al escenario de la intermediación, como por ejemplo las telefónicas, las empresas de servicios móviles de pago, los mandatarios, etc.

Este nuevo escenario, requiere de marcos directrices que delinee el accionar de los diversos actores en este nuevo escenario, así como también, delinee aspectos referidos a la forma de asegurar que las innovaciones tecnológicas referidas, provean la seguridad, confiabilidad y disponibilidad de la información y de los componentes tecnológicos relacionados.

Asimismo, está por descontado que hoy en día, el desarrollo de estas nuevas tecnologías dentro del campo de la intermediación financiera, presenta modos seguros y más económicos para la interconexión y el flujo de datos; sin embargo, es primordialmente necesario tener presente que las nuevas tecnologías en el campo de las comunicaciones móviles, muestran un potencial para promover la “Inclusión Financiera”, misma que va más allá del simple uso técnico para la interconexión de dispositivos existentes; ésta nueva tecnología, ha creado nuevos canales de suministro de servicios, nuevos instrumentos y nuevos modelos de negocio que permiten brindar servicios financieros a personas que tradicionalmente habían quedado excluidas del sistema financiero formal.

El escenario mencionado muestra un potencial considerable para que los servicios financieros móviles lleguen a más personas, debido a que existen señales de una aceleración en la incorporación de estos servicios en varios países, principalmente latino y centro americanos. La telefonía celular está permitiendo que los operadores móviles participen en la prestación de determinados servicios financieros en varios mercados, aumentando de esta forma la competencia y, simultáneamente, planteando cuestiones de tipo normativo que es necesario encarar debido a la proliferación de distintos modelos de negocio y alternativas tecnológicas que contribuye a la complejidad de este nuevo escenario.

2. OBJETIVOS DE LA CONSULTORÍA

2.1. General

El objetivo de la consultoría es coadyuvar al Banco Central de Reserva (BCR) y Superintendencia del Sistema Financiero (SSF), a través de talleres y mesas de trabajo, en el fortalecimiento y consolidación de normas y regulaciones necesarias para promover la “Inclusión Financiera” mediante las transacciones financieras electrónicas, considerando además en este marco directriz, la seguridad informática para los “sistemas financieros móviles”, término que engloba todo el rango de operaciones y transacciones financieras a través de teléfonos celulares.

2.2. Específicos

Desarrollar talleres y conducir mesas de trabajo en temas sobre:

- i. Enfoque metodológico para el análisis de la implicancia de los Servicios Financieros Móviles en el Riesgo Operacional, considerando la cadena de valor de este servicio.
- ii. Enfoque metodológico para el análisis de Riesgo Tecnológico enfocado en los Servicios Financieros Móviles.
- iii. Implicancia de riesgo (vulnerabilidades, amenazas, etc.) en la seguridad informática relacionadas con las tecnologías aplicables a Servicios Financieros Móviles, por ejemplo:
 - NFC - Near Field Communication -
 - USSD - Unstructured Supplementary Service Data –
 - SMS - Short Message Service
 - WAP - Wireless Application Protocol -
 - IVR - Interactive Voice Response

Alguna de estos contempla la seguridad por medio de encriptación desde el chip, como la utilizada en Colombia, tipo SIM Browsing??

- iv. Infraestructuras de seguridad exitosas ya implementadas en Centro y Sur América y cual el marco de referencia de seguridad mínima.
- v. Consideraciones sobre aseguramiento y normalización (COBIT –ISACA-, ISO/IEC 27001, ITIL, PCI-DDS) relacionada a Servicios Financieros Móviles, así como su implicancia referencial en costos, tiempo, recursos y tecnología para su implementación.

Taller : temas *i, ii, iii, iv, v*

Mesas de Trabajo: temas: *i, ii y v*

3. RESULTADOS ESPERADOS

Que, en función a los talleres y mesas de trabajo desarrolladas, se pueda delinear modelos de gestión de riesgos (Operacional y Tecnológico) que permitan, basados en estándares locales e internacionales y buenas prácticas de la industria, generar un marco directriz sobre la Seguridad Informática en los Servicios Financieros Móviles, alineado a las normas y regulaciones necesarias para promover la “Inclusión Financiera” mediante las transacciones financieras electrónicas. Deseable que pueda discutirse los tiempos de adaptación de la tecnología a la regulación, Ej. de pasar de USSD a SIM Browsing.

Recomendaciones para establecer una propuesta de regulación a los Servicios Financieros Móviles, en cuanto a Seguridad de la Información.

4. ÁMBITO DE LAS ACTIVIDADES

Las actividades a desarrollar, sin ser limitativos y siempre que se encuentren enmarcados en los alcances de la consultoría se centraran en:

- i. Desarrollar, en el marco de los servicios financieros móviles, material referido a las nuevas tecnologías, los nuevos actores que están incursionando en el mercado, y la implicancia de la seguridad informática considerando la gestión de los riesgos involucrados.
 - Establecimiento del contexto
 - Identificación de las situaciones con consecuencias de riesgo
 - Análisis y evaluación de riesgos;

- Definición de estrategias para la gestión de los riesgos
 - Generación de modelos de implementación
 - Estrategias de medición y control
 - Generación de informes
- ii. Impartir Talleres considerando los tópicos desarrollados
 - iii. Dirigir y modelar mesas de trabajo en función a los aspectos considerados como objetivos específicos de esta consultoría
 - iv. Desarrollar un informe de conclusiones sobre los aspectos antes mencionados

5. PRODUCTOS ENTREGABLES

- i. Un informe final sobre las actividades desarrolladas, mismo que incluirá las conclusiones sobre las mesas de trabajo desarrolladas, así como recomendaciones generales referidas al objetivo de la presente consultoría. El tono del informe final debe ser de bajo perfil, ya que no es una consultoría.
- ii. Material desarrollado para los talleres y mesas de trabajo referidas a la implicancia de la seguridad informática en el campo de los Servicios Financieros Móviles y su direccionamiento hacia un marco regulatorio.
- iii. Presentaciones y material utilizados durante la capacitación.

6. PLAN DE ACTIVIDADES Y CRONOGRAMA

Ver Anexo

7. PERIODO DE EJECUCIÓN

Inicio de trabajo en gabinete: Mayo 28, 2012

Inicio de trabajo de campo: Junio 6, 2012

**Annex II: Norma Técnica Seguridad
Informática en Servicios Financieros
Móviles**

ANNEX II: NORMA TÉCNICA SEGURIDAD INFORMÁTICA EN SERVICIOS FINANCIEROS MÓVILES

DEFINICIONES

Auditable: Información o datos que cuentan con las características de permitir la reconstrucción, revisión y análisis de la secuencia de eventos que la/los originaron.

Autenticidad: Acción o proceso que tiene por objetivo verificar y asegurar la identificación de una persona o sistema.

Cifrado Sólido: Método de codificación de datos basada en algoritmos probados y aceptados por la industria, extensiones de clave sólidas y prácticas adecuadas de administración de claves.

Confidencialidad: Acceso a la información solo por parte de quienes estén autorizados; característica/propiedad por la que la información no está disponible o revelada a personas, entidades, o procesos no autorizados.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran; característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera un proceso, persona o entidad autorizada.

Estabilidad: Se considera que un sistema informático es estable cuando su nivel de fallos disminuye por debajo de un determinado umbral, que permite generar confianza en su operatividad

No repudio: Capacidad de asegurar la autoría o recepción de un mensaje o transacción, evitando la negación de su existencia, recepción y/o creación

Operatividad: Capacidad de funcionamiento estable y continuo del Sistema de Pagos Móviles.

Privacidad: Es el ámbito de la vida que se desarrolla en un espacio reservado y que la persona tiene derecho a proteger de intromisiones.

Registro electrónico: Anotación en una base de datos digital de los atributos relacionados con la identificación unívoca del usuario del Sistema de Pagos Móviles.

I. PRINCIPIOS GENERALES

A. Respeto a la Seguridad de la Información

La seguridad de la información debe ser lograda mediante la adecuada combinación de políticas, normas, procedimientos, estructura organizacional y herramientas tecnológicas, a efectos que dicha la información cumpla con criterios de confidencialidad, integridad y disponibilidad

B. Respeto a la Gestión de Riesgos

La exposición al riesgo operacional y tecnológico del servicio financiero móvil debe ser determinada a través del establecimiento de un contexto, la identificación, valoración y respuesta a los riesgos, así como de sus actividades de control.

II. PRINCIPIOS ESPECÍFICOS

A. Respeto del Usuario

1. El Sistema de Pagos Móviles debe contemplar la identificación unívoca del usuario a través de un registro electrónico, mismo que considerará como mínimo: el nombre del usuario, el número y tipo del documento de identificación personal, el número de teléfono móvil y el número de cuenta que será vinculada al usuario para el pago y/o recepción de fondos.
2. El acceso a transacciones del Sistema de Pagos Móviles, debe contar con mecanismos que permitan garantizar el cumplimiento de los siguientes criterios: Autenticidad, No Repudio y Confidencialidad.
3. El Administrador del Servicio Financiero Móvil debe establecer e implementar estrategias que permitan informar y capacitar en forma masiva a los usuarios del Sistema de Pagos Móviles respecto a la seguridad y uso adecuado del servicio.
4. El Administrador del Servicio Financiero Móvil debe garantizar la privacidad y confidencialidad de los datos e información del Usuario, considerando prioritariamente su información de acceso al Sistema de Pagos Móviles (usuario/clave) y su información financiera.

B. Respeto a las Comunicaciones

1. Los canales de comunicación del Sistema de Pagos Móviles deben contar con una plataforma tecnológica que comprenda el cifrado sólido de la información en todo su tramo, vale decir de punta a punta (Inicio: Teléfono Móvil – Final: Servidores del Administrador/Entidad Financiera)
2. El Sistemas de Pagos Móviles debe contener mecanismos físicos y lógicos de seguridad que permitan controlar la ejecución de todas las transacciones que se inicien, debiendo tener las condiciones de poder detectar cualquier alteración o intervención a la información transmitida entre el punto en que esta se origine y aquel en la que se reciba.

C. Respeto a la Administración de datos

1. Se debe asegurar que el software aplicativo que gestionara el Servicio Financiero Móvil cumpla criterios de estabilidad y confiabilidad, debiendo contar con niveles de alta disponibilidad, demostrable por medio de una certificación o informe de una firma especializada.
2. Los componentes tecnológicos del Sistema de Pagos Móviles deben garantizar la continuidad de las transacciones ante eventos fortuitos o deliberados, debiendo considerar la aplicación de componentes y procedimientos alternativos que permitan superar los eventos que puedan afectar o interrumpir su normal funcionamiento.

3. Los datos e información registrada en la base de datos del Sistema de Pagos Móviles, sobre las transacciones ejecutadas, deben cumplir los criterios de Integridad, confidencialidad, disponibilidad y ser auditable; debiendo además ser resguardada en el tiempo de acuerdo a las disposiciones normativas vigentes.
4. El sistema de Pagos Móviles debe contar con elementos de trazabilidad que permita el adecuado seguimiento de las transacciones, incluyendo alertas para transacciones sospechosas.
5. El Sistema de Pagos Móviles debe contemplar el cumplimiento de las disposiciones de esta Norma Técnica

Annex III: Cronograma de Actividades

Fecha	Hora	Agenda: Freddy Landivar - Capacitación sobre Seguridad Informática	Número de Participantes	Unidades Participantes	Lugar
6 - Junio	8:30 AM – 10:00 AM	Aspecto conceptuales sobre seguridad informática y Servicios Financieros Móviles	37	BCR, SSF, BDES, BH, BFA, AID, PNUD	Local/PNUD
	10:30 PM – 12:00 M	Contenido de Tecnologías: SMS, USSD, WAP, IVR.			
	1:30 PM – 3:00 PM	Contenido de Tecnologías: Cifrado de información - Particularidades del SIM -Browsing y otras.			
	3:30 PM – 5:00 PM	Alienado de estándares y buenas prácticas sobre seguridad informática (COBIT –ISACA-, ISO/IEC 27001, ITIL, PCI-DDS, etc.) relacionada a Servicios Financieros Móviles.			
7 - Junio	8:30 AM – 10:00 AM	Continuación..... Alienado de estándares y buenas prácticas sobre seguridad informática (COBIT –ISACA-, ISO/IEC 27001, ITIL, PCI-DDS, etc.) relacionada a Servicios Financieros Móviles.	37	BCR, SSF, BDES, BH, BFA, AID, PNUD	Local/PNUD
	10:30 AM – 12:00 M	Enfoque metodológico para el análisis de la implicancia de los Servicios Financieros Móviles en el Riesgo Operacional, considerando la cadena de valor de este servicio.			
	1:30 PM – 3:00 PM	Implicancia de los Servicios Financieros Móviles en el Riesgo Operacional			
	3:30 PM – 5:00 PM	Aplicación del Riesgo Tecnológico (Gobierno y Seguridad de la Información) enfocado en los Servicios Financieros Móviles.			
8 - Junio	8:30 AM – 10:00 AM	Análisis y evaluación de riesgos	37	BCR, SSF, BDES, BH, BFA, AID, PNUD	Local/PNUD
	10:30 AM – 12:00 M	Definición de estrategias para la gestión de los riesgos			
	1:30 PM - 3:00 PM	Estrategias de medición y control, y Generación de informes.			
	3:30 PM - 5:00 PM	Discusión: Tiempos de implementación/adecuación de nuevas tecnologías para la seguridad de la información.			

Además de las actividades de capacitación indicadas en la página anterior, el Sr. Landivar trabajará con grupos pequeños de especialistas el lunes y martes, 11 y 12 de junio.



Annex IV: Conceptualización de Riesgo



CONCEPTUALIZACION DE RIESGOS

Lic. Freddy Landivar P., CISA



AGENDA



- Conceptos de Riesgo
- Personalizando el Riesgo
- Entendiendo el Riesgo
- Gestionando el Riesgo

Conceptos de Riesgo

- Etimología de la palabra “Riesgo”
 - Europa, en el siglo XI, en el latín «riscum», «risichium», «risco», «rischis» => Riesgo
 - Corán, palabra árabe «rizq» => Don fortuito e inesperado, Albur favorable que se corre

griego *rhizikon*

inglés *risk*

italiano *rischio*

portugués *risco*

Catalán *risc*

alemán *risiko* (gefahr)

español *riesgo*

- Definiciones de Riesgo

- La posibilidad de sufrir un daño o pérdida; peligro
- Incertidumbre respecto del valor o estado futuro
- Combinación de la frecuencia o probabilidad que puedan derivarse de la materialización de un peligro
- Es la probabilidad de ocurrencia de un siniestro
- Daño potencial que puede surgir por un proceso presente o suceso futuro

¿Qué es un riesgo?

“La amenaza de que un evento, acción ó falta de acción afecte adversamente la habilidad de una organización para lograr sus objetivos y ejecutar sus estrategias exitosamente”

- Definiciones relacionadas a Riesgo

- **Amenaza:**

- peligro latente con posible manifestación dentro de un período de tiempo, que puede producir efectos adversos

- **Evento:**

- suceso natural o provocado que se describe en términos de sus características, su severidad, ubicación y área de influencia



Conceptos de Riesgo



- **Mitigación:**
 - Planificación y ejecución de medidas dirigidas a reducir o disminuir el riesgo.
- **Prevención:**
 - Medidas y acciones dispuestas con anticipación para evitar que se presente un evento o reducir su incidencia
- **Vulnerabilidad:**
 - Exposición a una amenaza con predisposición intrínseca a ser afectado



Conceptos de Riesgo



- **Resiliencia:**

- Capacidad de absorber un impacto negativo y/o recuperarse una vez hubiere sido afectado por un evento

- **Nivel o intensidad:**

- Medida cuantitativa y/o cualitativa de la severidad de un evento en una unidad de tiempo y lugar.

- **Arriesgar – Peligro (Hazard)**

- Una situación o condición que es probable que cause un daño o pérdida bajo ciertas circunstancias.
- - El peligro es un requisito para el Riesgo exista
- - Arriesgar es una condición no un evento

- **Tolerancia al Riesgo:**
- Niveles de riesgo que son aceptables a una organización
- **Crisis:**
Un evento o situación no planeada que provoca o activa una amenaza a la seguridad, ambiente o reputación de la organización.
- **Gestión de riesgos:**
- proceso que involucra al planeamiento y aplicación de políticas, estrategias, instrumentos y medidas orientadas a impedir, reducir, prever y controlar efectos adversos

● Riesgo e Incertidumbre

- - Riesgo : El resultado puede ser descrito dentro de los límites confidencialmente establecidos

Puede manejar probabilidades

- - Incertidumbre: Un estado no común caracterizado por la ausencia de información relacionada al resultado esperado

No se puede asignar probabilidades a un incertidumbre; i

● Certeza

- Contar con toda la información para tomar decisiones correctas
El resultado es predecible razonablemente



Personalizando el Riesgo

“El riesgo esta en todas partes”,, NOS RODEA

ejemplo: El Riesgo de :

- vivir
- es morir
- amar
- es no ser correspondido
- navegar
- hundirse



Por



Personalizando el Riesgo



Podemos
eliminar el
riesgo

?

Podemos
evitar el
riesgo

Personalizando el Riesgo

- Un pensamiento:

Aquel que no arriesga nada

No hace nada

No tiene nada

Y no es nada iiii



Personalizando el Riesgo



- Tipos de riesgos personales

Riesgos físicos

Riesgos emocionales

Riesgos Financieros

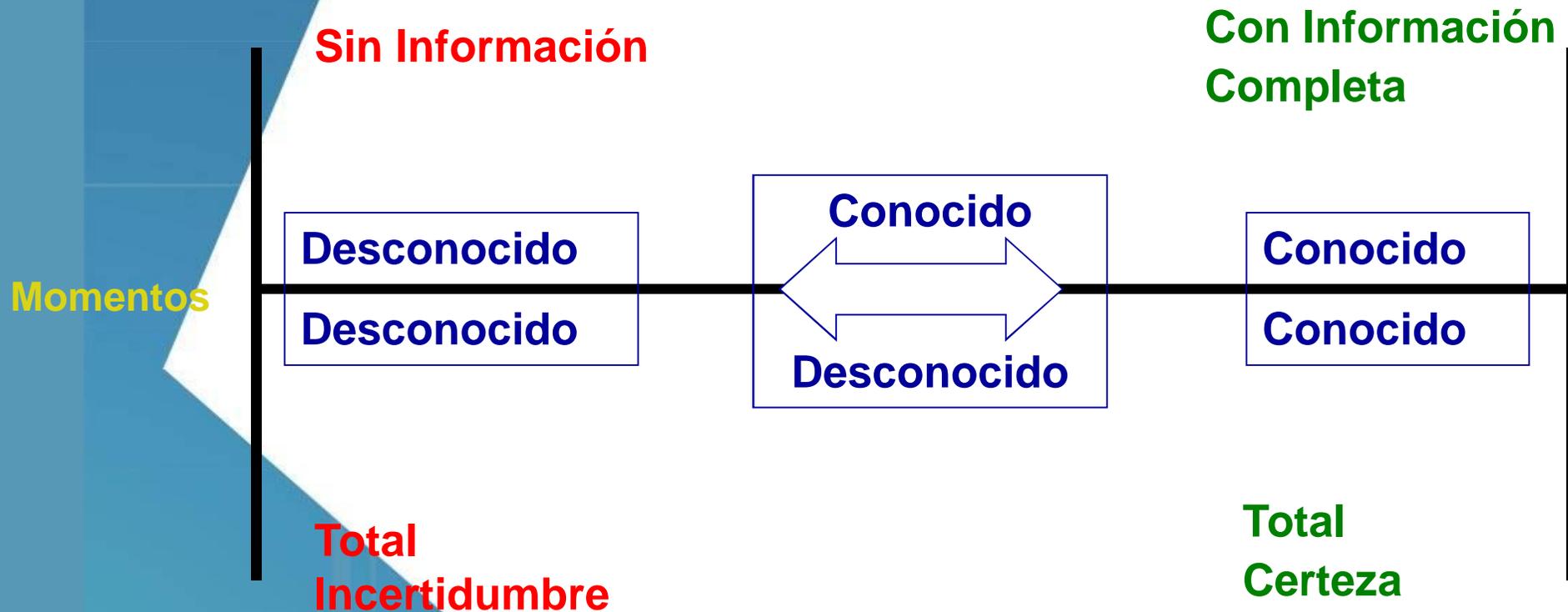
Personalizando el Riesgo

- Porque las personas asumen riesgos
- Ganancias
- Reconocimientos
- Beneficios
- Desafíos
- Estupideces



Entendiendo el Riesgo

- El Espectro del Riesgo (en un proyecto cualquiera)





Entendiendo el Riesgo



- **Riesgos Known/known:**
 - Todos sobre la situación es conocido
- **Riesgos know/unknow:**
 - Identificado, evaluado, y cuantificados los riesgos se desarrolla un plan de contingencia para cubrirlo
- **Riesgos unknow/unknow**
 - No identificados, imposibles de predecir y cubrir



Entendiendo el Riesgo



- **Factores de Riesgo (en un proyecto) – Preguntarse??**
 - **Evento**
 - **Que puede pasar para disuadir o afectar la ejecución de un proyecto?**
 - **Probabilidad**
 - **Como probablemente el evento ocurrirá?**
 - **Impacto**
 - **Cual el costo?**
 - **Cual las posibles ganancias?**



Entendiendo el Riesgo



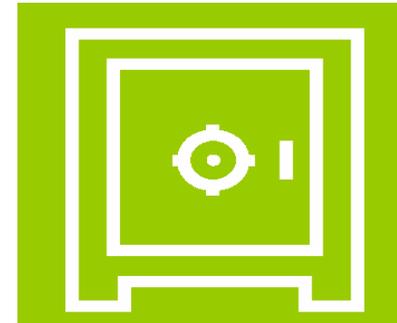
- El Riesgo esta en función a:
 - Eventos -> Probabilidades - > Impacto
 - RES = Risk Event Status

RES= Probabilidad x Amount at stake

Gestionando el Riesgo



**Tecnología de
Información**

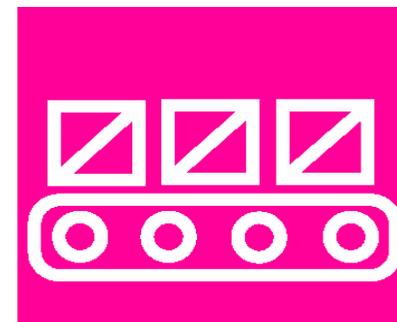


**Financieros y
Tesorería**

Tipos de riesgos que se gestionan



**Prevención y
Detección de
Fraudes**



**Procesos de
Negocio**

Gestionando el Riesgo

Estrategia

La estrategia establece los lineamientos específicos sobre los cuales debe llevarse a cabo la operación

Tecnología

Como área que determina los sistemas informáticos que soportan los procesos y almacenan la información generada



Gente y Organización

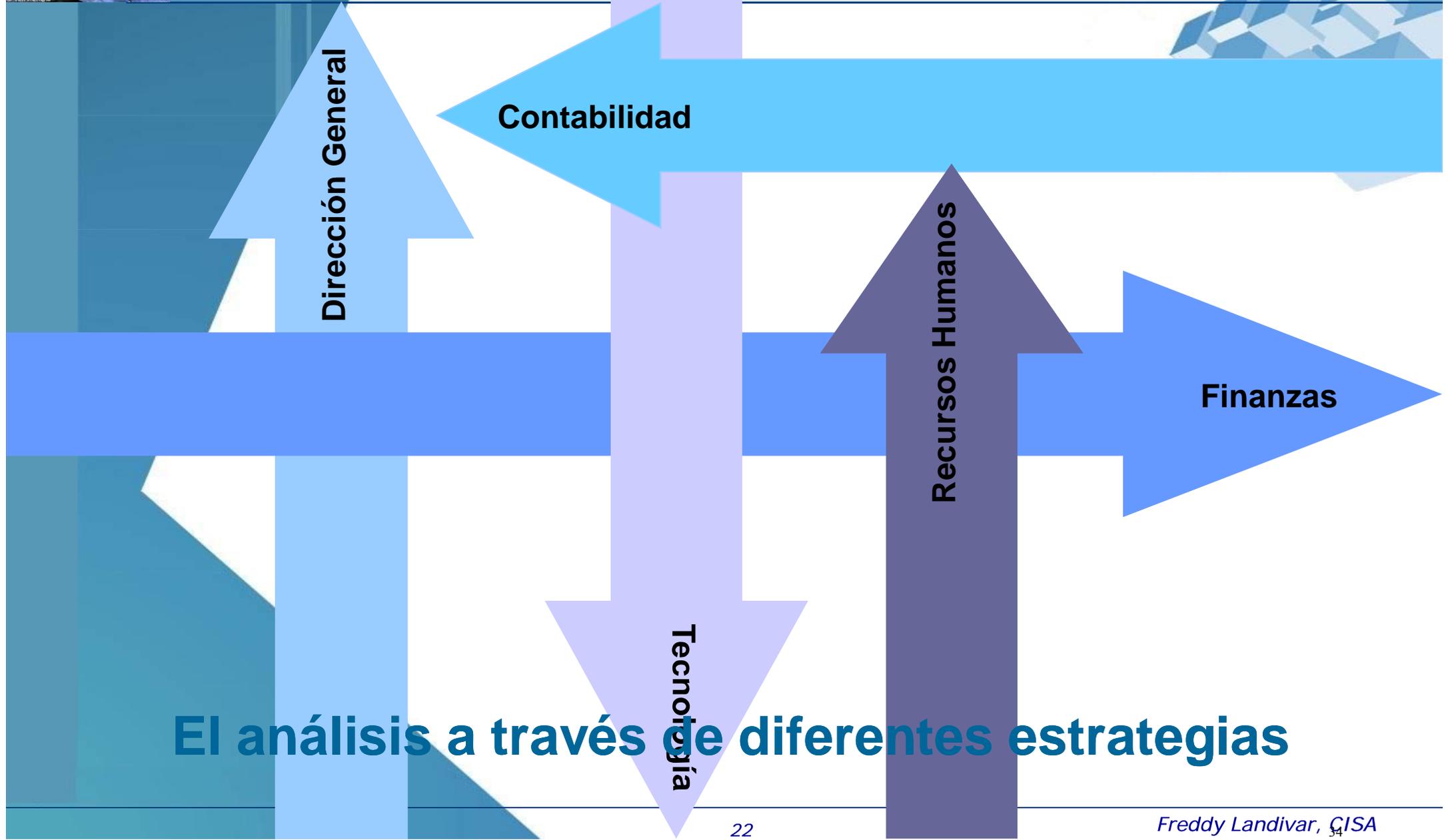
La gente y la organización necesarias para lograr el objetivo de la Compañía

Procesos

Los procesos de operación establecidos sobre los cuales deben de realizarse todas las actividades de sus integrantes

la gestión de riesgos desde 4 ópticas

Gestionando el Riesgo



El análisis a través de diferentes estrategias

Ponencia :

70% a 90%
de todos los problemas y
cuestionamientos
son
predecibles y prevenibles

Que es un Proyecto

- Es un emprendimiento temporal para crear un producto o servicio, producto de
 - Nuevas tecnologías
 - Incrementar la especialización
 - Relaciones contractuales complejas
 - Ampliación de políticas e implicancia social
 - Creación de leyes y regulaciones
 - Globalización



Gestionando el Riesgo en un Proyecto

Que es una Gestión de Proyecto

La aplicación de conocimientos, herramientas y técnicas para proyectar y administrar actividades y asegurar su consecución

Gestionar un Proyecto = Gestionar riesgos



Gestionando el Riesgo en un Proyecto

Que es una Gestión de Riesgos

- Es el proceso sistemático de identificar, analizar y responder a riesgos en un proyecto. Incluye acciones para maximizar los eventos positivos y minimizar los negativos
- La preparación por posibles eventos con anticipación en lugar de responder cuando ocurran



Gestionando el Riesgo en un Proyecto

Cual es la meta (GOAL) en la Gestión de Riesgos en un proyecto?

- Pronosticar e identificar las diferentes fuentes de riesgo a un proyecto, especialmente aquellos con las mayores impactos, y buscar reducir sus consecuencias y probabilidades

Las fuentes comunes de Riesgos

- Cambios en los requerimientos
- Errores de diseño u omisión
- Equivocaciones entre la gente del proyecto
- Roles no entendibles o pobremente definidos
- Insuficiente habilidades (skill) del equipo
- Falsas suposiciones
- Rendimiento de los subcontratistas

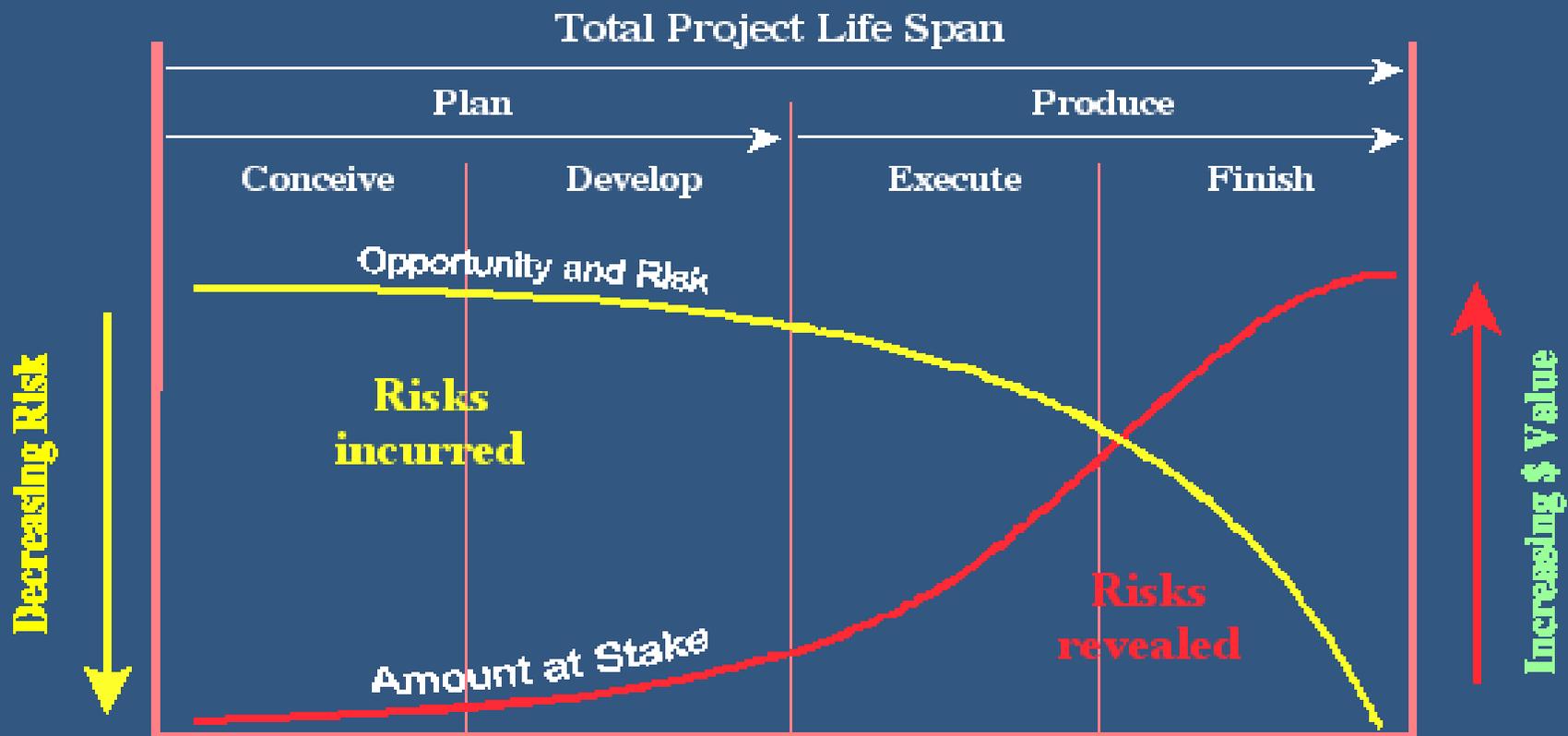
Cuán Riesgoso es el proyecto?

- Es diferente de otros anteriores?
- El alcance no está bien definido?
- Existe carencia de algunos datos técnicos ?
- Los costos, planificaciones y ejecuciones no están expresados en términos claros?
- El diseño no fue considerado por el usuario?

Gestionando el Riesgo en un Proyecto

El Riesgo en un Proyecto

Opportunity/Risk vs. Amount at Stake



Pasos comunes para Gestionar Riesgos

- Planificación para la Gestión de Riesgos
- Identificación de riesgos
- Análisis Cualitativo
- Análisis Cuantitativo
- Planificación de replica ante Riesgos consumados
- Monitorear y Controlar el Riesgo

Planificación para la Gestión de Riesgos

- Decida como abordar la gestión del riesgo para un proyecto en particular
 - Como
 - Que
 - Quien
 - Cuando
 - Cuanto Tiempo
 - Cual el costo



Identificación de Riesgos

- Cuales son las cosas que pueden ir mal?
- Cuales son las posibles causas para que las cosas vayan mal?
- Si van mal, cual serían las consecuencias'





Gestionando el Riesgo en un Proyecto

Análisis Cualitativo

- Realizar un análisis del riesgo y condiciones para priorizar el riesgo que tendrá el mayor impacto en el proyecto





Gestionando el Riesgo en un Proyecto

Análisis Cuantitativo

- Evaluar e interactuar con riesgos para valorar los posibles rangos que afecten al proyecto
- Medir la probabilidad y las consecuencias del riesgo y estimar su impacto a los objetivos del proyecto





Gestionando el Riesgo en un Proyecto

Planificación de replica ante Riesgos consumados

- Desarrollar procedimientos y técnicas para resaltar oportunidades y reducir las amenazas a los objetivos del proyecto



Monitorear y Controlar el Riesgo

- Monitorear el riesgo residual y nuevos riesgos que puedan aparecer durante el proyecto
- Ejecutar un plan de reducción
- Evaluar la efectividad de las respuestas a los riesgos, desarrollado durante la etapa de planificación



Preguntas



Freddy Landivar P, CISA, CRISC
flandivar@bdoberthin.com

Annex V: Firma Digital

-
-
-



FIRMA DIGITAL

Que es la Firma Digital?

- Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.
- La firma digital es un instrumento con características técnicas y normativas, esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen

Cómo se crea la firma digital?

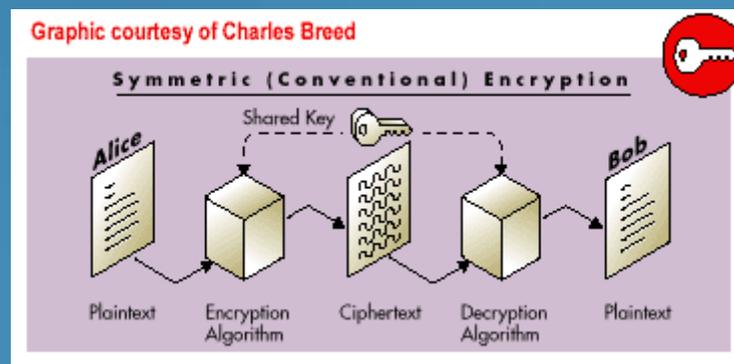
- La firma digital se crea utilizando la técnica de criptografía asimétrica, permitiendo la identificación del signatario; permitiendo garantizar la integridad del contenido y detectar cualquier modificación ulterior.

¿Qué es la criptografía?

- La criptografía es un arte mediante el cual un mensaje legible es convertido en un texto incomprensible y después devuelto a su forma original

¿Qué es la criptografía simétrica?

- Aplicando una clave sobre un texto, se le convierte en incomprensible y volviendo a aplicarla (pero en sentido simétricamente inverso) el texto incomprensible recupera su legibilidad.

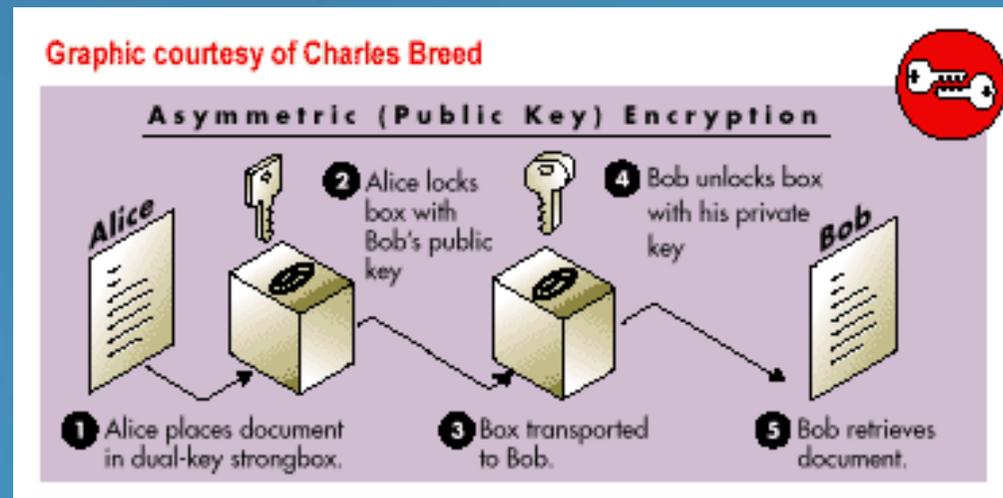


Que es la criptografía asimétrica?

- Es una modalidad del arte criptográfico que, a diferencia del método simétrico tradicional, no utiliza la misma clave para cifrar y descifrar un mensaje sino que utiliza dos claves diferentes: una para cifrar el mensaje y otra (que no es la “inversión” de la primera) para descifrarlo.

Que es la criptografía asimétrica?

- También se le llama “criptografía de clave pública” porque sólo una de estas claves es privada y secreta. La otra es necesariamente de conocimiento público.



¿Qué es una función HASH?

El código ASCII asigna un número a cada letra o signo de puntuación

65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
!	"	#	\$	%	&	'	()	*	+	,	-	.	/

Es una clave simétrica estándar internacional.
La utilizan, por ejemplo, todos los ordenadores.

¿Qué es una función HASH

Podemos substituir cada letra de un texto por su código ASCII

E	n		u	n		r	i	n	c	ó	n		d	e	
69	110	32	117	110	32	114	105	110	99	243	110	32	100	101	32
l	a		M	a	n	c	h	a		d	e		c	u	y
108	97	32	77	97	110	99	104	97	32	100	101	32	99	117	121
o		n	o	m	b	r	e		n	o		q	u	i	e
111	32	110	111	109	98	114	101	32	110	111	32	113	117	105	101

¿Qué es una función HASH

Podemos utilizar los códigos ASCII de un texto para hacer cualquier cálculo

E	n		u	n		r	i	n	c	ó	n		d	e	
69	110	32	117	110	32	114	105	110	99	243	110	32	100	101	
-1312			224			990			-15840			-6868			-22806
	l	a		M	a	n	c	h	a		d	e		c	
32	108	97	32	77	97	110	99	104	97	32	100	101	32	99	
-7372			-4365			1144			6500			6831			2738
u	y	o		n	o	m	b	r	e		n	o		q	
117	121	111	32	110	111	109	98	114	101	32	110	111	32	113	
-444			-8658			1254			7590			8927			8669
														-11399	

Aquí, cada tres caracteres, con sus códigos ASCII, se opera

$$(1^{\circ}-2^{\circ}) * 3^{\circ}$$

La suma de los resultados es una **función HASH** que identifica perfectamente el texto.

¿Qué es una función HASH

Cualquier modificación en el texto provoca un cambio en el valor de la función HASH

E	n		u	n		r	i	n	c	o	n		d	e	
69	110	32	117	110	32	114	105	110	99	111	110	32	100	101	
		-1312	224			990			-1320			-6868		-8286	
	l	a		M	a	n	c	h	a		d	e		c	
32	108	97	32	77	97	110	99	104	97	32	100	101	32	99	
		-7372	-4365			1144			6500			6831		2738	
u	y	o		n	o	m	b	r	e		n	o		q	
117	121	111	32	110	111	109	98	114	101	32	110	111	32	113	
		-444	-8658			1254			7590			8927		8669	

Por ejemplo, al substituir “**rincón**” por “**rincon**” sin acento, el valor HASH ha pasado de -11.399 a 3.121

¿Qué es una función HASH

Ejemplo



Ana envía un mensaje a Benito.
Al final del mensaje le añade el valor HASH del texto según una función en la que se han puesto previamente de acuerdo.



Benito recibe el mensaje y calcula el valor HASH. Si coincide con el que ha dicho Ana puede estar seguro de que el mensaje no ha sido modificado.

¿Qué es una función HASH

Conclusión

Los textos enviados electrónicamente pueden deformarse, bien por la intervención de terceras personas, o bien por errores en la transmisión.

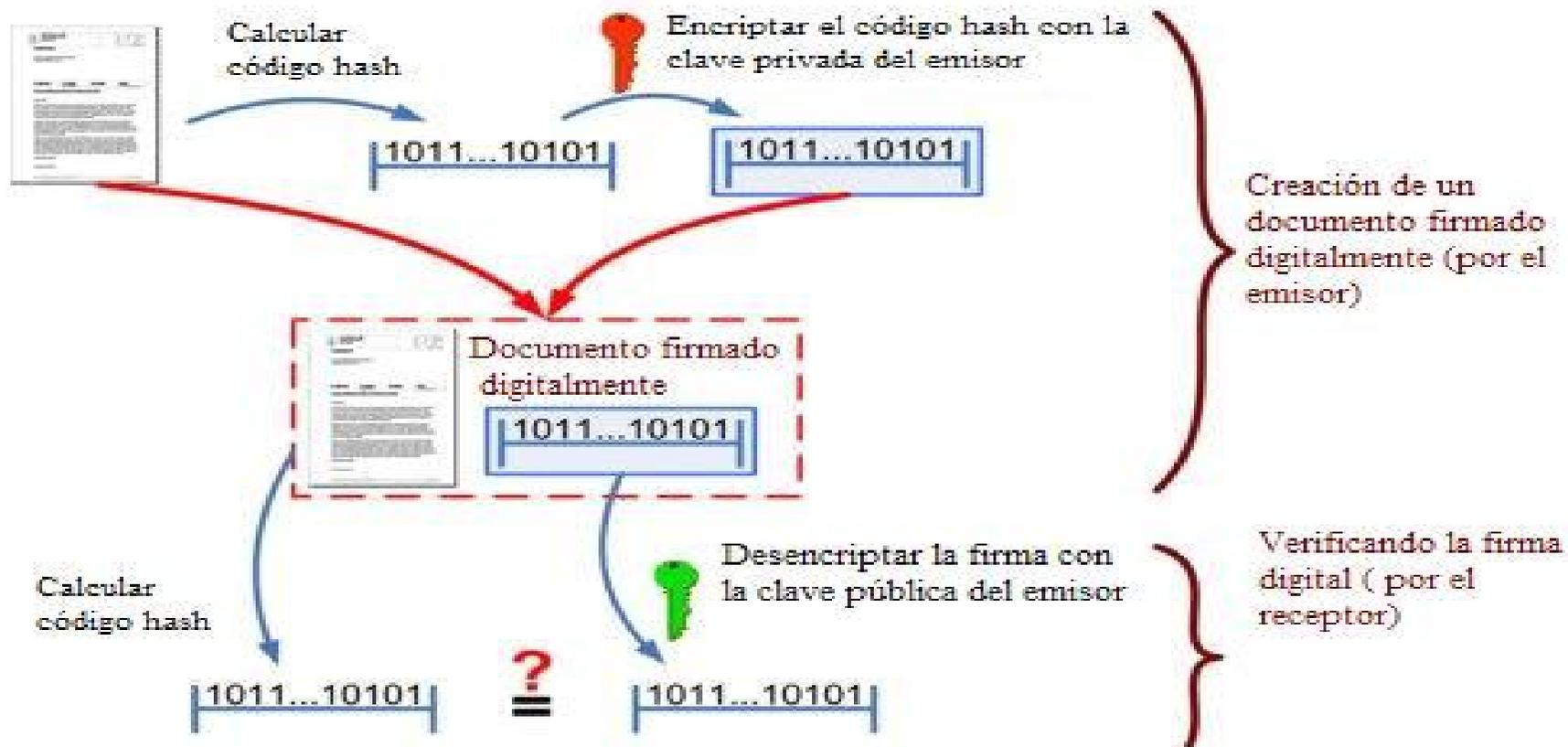
Las funciones HASH sirven para garantizar la integridad de los textos

¿Qué es el Certificado Digital?

- Un Certificado Digital es un documento electrónico emitido por una empresa denominada “Entidad de Certificación” a nombre del titular del Certificado. Contiene la clave pública del titular del certificado y está “colgado” en una página electrónica de libre acceso.

¿Qué es y Cómo funciona la firma digital?

Creando y verificando una firma digital



Si el código hash calculado no concuerda con el resultado de la firma digital desencriptada, o el documento fue modificado después de hacer la firma, o la firma no fue generada por la clave privada del emisor del documento

¿Es todo esto suficiente para certificar la autoría del mensaje?

- No, para evitar que los certificados sean falsos es necesario que las claves públicas de todos los usuarios estén “colgadas” en documentos electrónicos totalmente confiables. Los Certificados Digitales emitidos por Entidades de Certificación debidamente acreditadas por la Autoridad Competente constituyen, por ley, documentos confiables.

Importancia de la Firma Digital

- Tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica

-
-
-

Aplicaciones 1

- Contratos comerciales seguros
- Cobranza electrónica
- Mensajes de autenticidad segura

Concepto Legal

- Es aquella firma electrónica que utilizando una técnica de criptografía asimétrica, permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su control, de manera que está vinculada únicamente al signatario y a los datos a los que refiere, lo que permite garantizar la integridad del contenido y detectar cualquier modificación ulterior, tiene la misma validez y eficacia jurídica que el uso de una firma manuscrita, siempre y cuando haya sido generada por un Prestador de Servicios de Certificación Digital debidamente acreditado que se encuentre dentro de la Infraestructura Oficial de Firma Electrónica”

-
-
-



Gracias

Annex VI: Aspectos conceptuales

Seguridad Informática y SFM



ASPECTO CONCEPTUALES SOBRE SEGURIDAD INFORMÁTICA Y SERVICIOS FINANCIEROS MÓVILES

Freddy Landivar CRISC, CISA

Mayo, 2012





AGENDA

- I. EL CONTEXTO DE LA SEGURIDAD INFORMÁTICA**
- II. EL CONTEXTO DE LOS SERVICIOS FINANCIEROS MÓVILES**

El contexto de la seguridad informática

- i. Conociendo la Seguridad Informática
- ii. Aspectos básicos a considerar para gestionar la Seguridad Informática
- iii. Entendiendo la Gestión de Riesgos





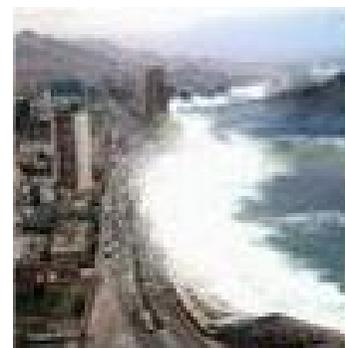
Seguridad Informática





Seguridad de la Información

Protección contra
pérdida y
modificación,
motivada
generalmente por
interés común





Protección de datos

Protección de los derechos personales de los individuos respecto a sus datos, siendo su motivación generalmente Jurídica





Objetivos de la Seguridad Informática

- **Garantizar condiciones y características de datos e información**
 - Confidencialidad: Acceso autenticado y controlado
 - Integridad: Datos completos y no modificados
 - Disponibilidad: Acceso garantizado

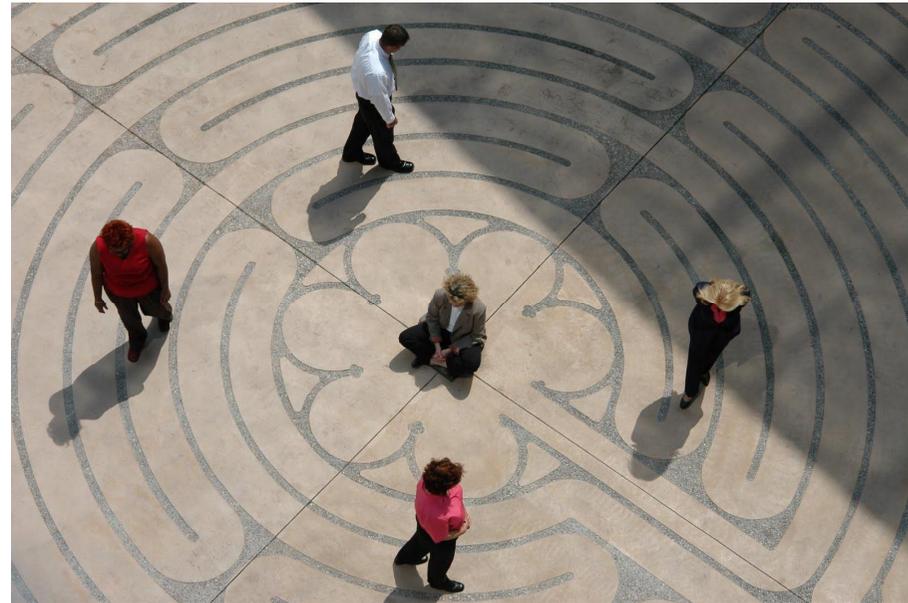
- **Gestión de las amenazas**
 - Conocerlo
 - Clasificarlo
 - Protegerse contra daños





Aspectos básicos a considerar para la Seguridad Informática

- Sus Componentes
- Su Clasificación
- Sus Retos
- Sus Premisas





Componentes de la Información

- Datos / Información
 - Financieros, Documentos ofimáticos, Llamadas telefónicas, Correo electrónico, Base de Datos, ...
- Hardware / Infraestructura
 - Centro de datos, Equipos de red, Computadoras, Memorias portátiles, Celulares, ...
- Recursos Humanos
 - Personal Informático, Administración, Comités de Coordinación,...
- Sistemas
 - Aplicativos, Software Ofimático, SO, ...





Clasificación y Flujo de Información

- Identificar tipo de datos e información y clasificar
 - Confidencial (acceso restringido: personal interno autorizado)
 - Privado (acceso restringido: personal interno)
 - Sensitivo (acceso controlado: personal interno y externo)
 - Público

- Análisis de flujo de información
 - Observar cuáles instancias manejan que información
 - Identificar grupos externos que dependen o están interesados en la información
 - Determinar si se deben efectuar cambios en el manejo de la información.



Retos de la Seguridad

- Recibir la atención adecuada
 - Involucramiento Directriz
 - Formar parte de la estrategia Empresarial
 - Asignación de Costos
 - Afrontar la Ignorancia, falta de conocimiento y negligencia
 - Cumplimiento de normas y estándares





Retos de la Seguridad

- Cambiar paradigmas errados de TI
 - Asumir que los datos se encuentran en el centro de datos
 - No reconocer el valor de los datos de los dispositivos móviles
 - Tratar los portátiles y dispositivos móviles como activos de la empresa que nunca se utilizan para uso personal, creyendo que los datos de la compañía nunca llegan a los sistemas domésticos
 - No tratar a los dispositivos móviles como si fueran equipos de mesa





Retos de la Seguridad



.....

- Adoptar los medios de comunicación sociales sin análisis y protección
- Centrarse en la protección frente a la detección y respuesta
- Falta de concienciación
- Falta de registro y seguimiento de las infracciones de seguridad
- Prepararse sólo para el cumplimiento de normativas
- Suponer que todo está bien



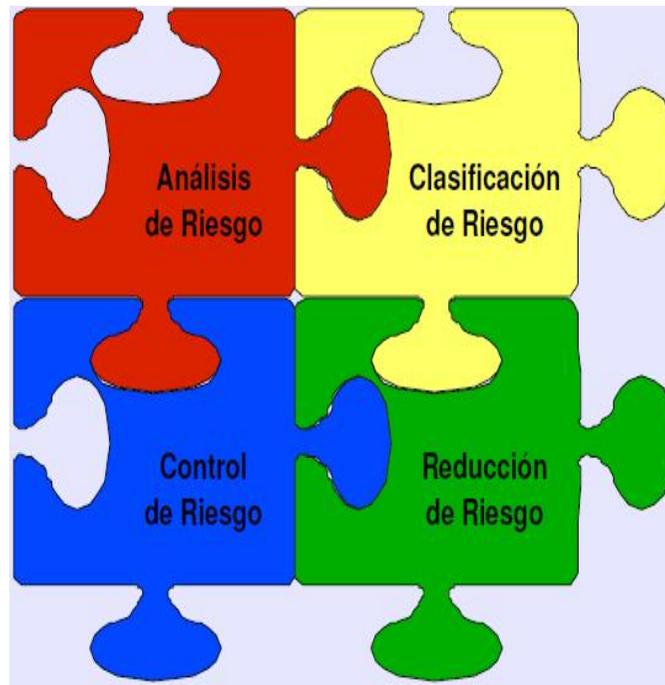


Retos de la Seguridad

- **Proceso dinámico y permanente**
 - Seguimiento de control y sanciones
 - Adaptar medidas a cambios de entorno
 - Capacitación del personal
 - Documentación.



Gestión del Riesgo



- **Políticas**
- **Normas**
- **Procedimientos**
- **Estructura Organizacional**

**C
O
N
T
R
O
L**

Vulnerabilidades

- Ambiental / Físicas
 - Desastres naturales, Ubicación, Capacidad técnica, Materiales...
- Económica
 - Escasez y mal manejo de recursos
- Socio / Conductiva
 - Relaciones, Comportamientos, Métodos,
 - Conductas...
- Institucional / Política
 - Procesos, Organización, Burocracia,
 - Corrupción, Autonomía.



Amenazas

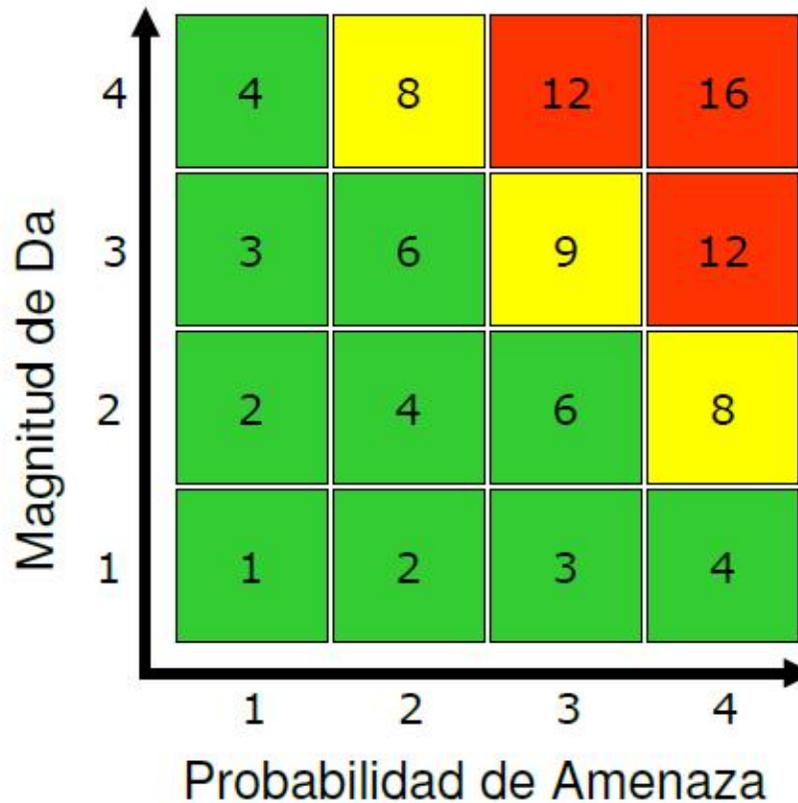
- Criminalidad (común y política)
 - Allanamiento, Sabotaje, Robo / Hurto, Fraude, Espionaje, Virus, ...
- Sucesos de origen físico
 - Incendio, Inundación, Sismo, Polvo Sobrecarga eléctrica, Falta de corriente, ...
- Negligencia y decisiones Institucionales
 - Falta de reglas, Falta de capacitación, No cifrar datos críticos, Mal manejo de contraseñas, ...





Análisis de Riesgo

Riesgo = Probabilidad de Amenaza * Magnitud de Daño



Alto Riesgo (12-16)
Medio Riesgo (8-9)
Bajo Riesgo (1-6)

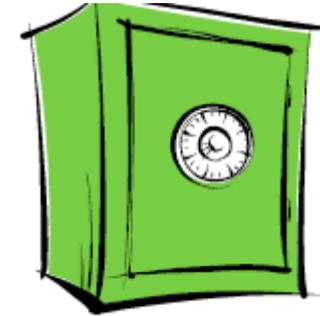
Valores:
1 = Insignificante
2 = Baja
3 = Mediana
4 = Alta



Análisis de Riesgo

- **Valorar la Probabilidad de Amenaza**
 - Consideraciones
 - Interés o la atracción por parte de individuos externos
 - Nivel de vulnerabilidad
 - Frecuencia en que ocurren los incidentes
 - Valoración de la probabilidad
 - Alto Medio Bajo
- **Determinación del Impacto y sus consecuencias**
 - Pérdida de información
 - Terceros tienen acceso a la información
 - Información ha sido manipulada o está incompleta
 - Información no está disponible
- **Medición**

- **Medidas físicas y técnicas**
 - Construcciones de edificio, Control de acceso, Planta eléctrica, Antivirus, Datos cifrados, Contraseñas inteligentes, ...
- **Medidas personales**
 - Contratación, Capacitación, Sensibilización, ...
- **Medidas organizativas**
 - Normas y reglas, Seguimiento de control, Auditoría, ...





Mitigación del Riesgo

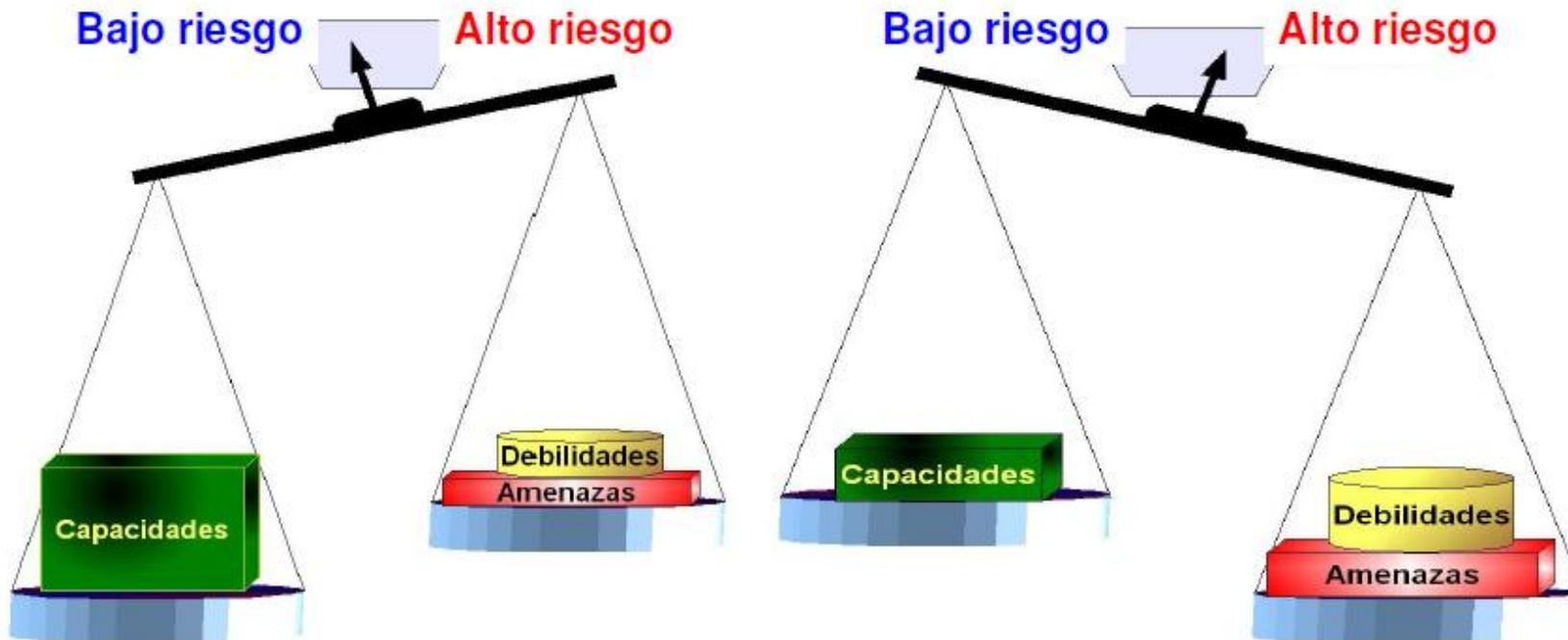
- Medidas de acuerdo al grado de riesgo
 - Medio riesgo: Medidas parciales para mitigar daño
 - Alto riesgo: Medidas exhaustivas para evitar daño
- Verificación de funcionalidad
 - Respaldo por coordinación
 - Esfuerzo adicional y costos vs. beneficio
 - Evitar medidas pesadas o molestas
- Fundamental en normas y reglas “Framework”
 - Actividades, frecuencia y responsabilidades
 - Publicación



Clasificación de Riesgo

Seguro, pero exceso de atención

Inseguro, poca atención





El riesgo siempre existe

Riesgo Inherente



¡Nada es 100% seguro!



El contexto de los Servicios Financieros Móviles

- i. Incursión de los SFM
- ii. El móvil como Instrumento Primario
- iii. Los Riesgos que Conlleva
- iv. La Seguridad Informática en los SFM

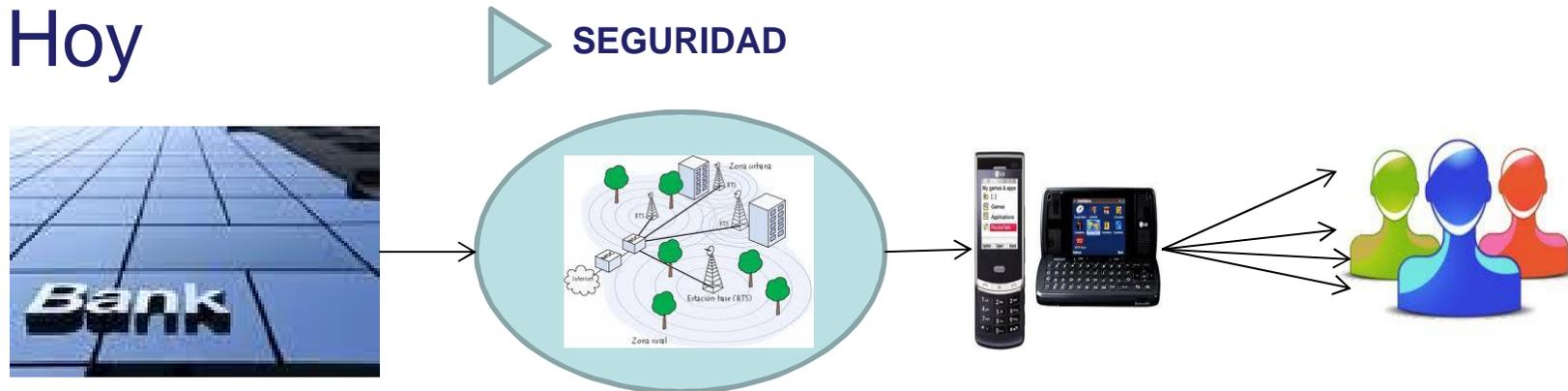


La incursión de los SFM

➤ Antes



➤ Hoy



- NUEVOS CANALES DE SUMINISTRO DE SERVICIOS
- NUEVOS INSTRUMENTOS
- NUEVOS MODELOS DE NEGOCIO



INCLUSIÓN

La Herramienta Primaria



Un canal de suministro de servicios

- Prestar servicios financieros electrónicos paralelamente con otros canales (ATM, Puntos de Venta, etc.)
- Interactuar directamente con el consumidor final y/o con las nuevas redes de agentes que prestan servicios al consumidor final (**comodatos**).



DISMINUYE COSTOS POR SvFin

Un instrumento de pago

- Transmite instrucciones de pago entre el agente pagador y el beneficiario desde y hacia distintos tipos de cuenta (generalmente bajo regulación)
- Genera servicios que involucra la creación y emisión de nuevos instrumentos de pago tales como el dinero electrónico (sin regulación).



Instaura Riesgos

Los Riesgos que Conlleva



Instaura Riesgos

Riesgos Prudenciales

Surgen con la creación de nuevos instrumentos de pago tal el caso del dinero electrónico emitido por entidades no bancarias

Riesgos Operativos

Surgen de la utilización de teléfonos móviles como un nuevo canal de servicios implicando la **Seguridad Informática**

- ❖ Riesgos de Banca Electrónica
- ❖ Riesgos por el uso de dispositivos móviles y de canales móviles.



La Seguridad Informática en los SFM....

- El éxito para instaurar SMF requiere no sólo de una **interfaz amigable**, sino también de una **seguridad probada** que de confianza al cliente



Lamentablemente:

- Internet creó desconfianza por la gran cantidad de limitaciones de seguridad



..., y

... La Seguridad Informática en los SFM

- Otras dos tendencias que se solapan han exacerbado aún más las cuestiones de seguridad'

- ✓ El uso de herramientas colaborativas y nuevas formas de interacción interna
- ✓ La arquitectura “cloud”, donde algunos procesos antes internos, se convierten en algo parcialmente externo al “Firewall” y, implicando a la seguridad





...La Seguridad Informática en los SFM

- El Riesgo crece...cualquier falla de la seguridad informática puede tener graves implicancias para las empresas involucradas,

- ✓ Riesgo Legal
- ✓ Riesgo Reputacional
- ✓ Riesgo Operacional, etc.



- Pero, la amenaza es particularmente más aguda para las empresas de servicios financieros, dado que el almacenamiento y el intercambio de dinero constituyen el núcleo de su negocio





La clave ... La Proactividad

- **Identificar y asegurar los activos de TI en sí mismos, no solamente el perímetro**
 - Es más efectivo asegurar los datos o los activos en sí mismos, donde quiera que residan y viajen.
 - Deben incorporarse capacidades tecnológicas de defensa y resistencia en toda la organización, no solamente en componentes
- **Desarrollar una cultura de seguridad**
 - Las EF deben definir claramente las estructuras de dirección de la seguridad informática, considerando: responsabilidades, supervisión y monitoreo
- **Prestar mayor atención a las aplicaciones**
 - Medir y gestionar la resistencia de una aplicación ante ataques, así como su capacidad de **gestionar información confidencial**,
 - Realizar pruebas exigentes para confirmar su proceso con riesgo reducido, considerando el ciclo de vida de desarrollo de sistema,



La clave ... La Proactividad

- **Comprobar y volver a comprobar la identidad del usuario**
 - La gestión de la identidad es una prioridad para la seguridad a raíz de la convergencia de varias tendencias como: robo de identidad; clonaciones, el e-procurement, ataques a identificación y claves, etc.
- **Prestar atención a la seguridad de los dispositivos móviles.**
 - Si bien muchas tecnologías móviles subyacentes son similares a las que dan soporte a la banca por Internet, se deben considerar otras tendencias.
- **Desarrollar una aguda toma de conciencia ante la situación.**
 - Las IF deben entender todo el panorama relacionado con los riesgos y su gestión (identificar, medir, determinar, controlar, monitorear)
 - Se debe considerar principalmente el Riesgo Operacional (eventos externos, eventos internos, recursos humanos, tecnología)
 - Generar concientización en torno al impacto potencial de este servicio
 - Adoptar estándares probados y buenas prácticas



Preguntas ??

Fuentes:

- Propia
- Protejete wordpress
- Whitepapers Kaspersky Lab
- Juan J. Senin, El Rol de la Seguridad en SMF

Annex VII: Tecnologías aplicadas en SFM I



TECNOLOGÍAS APLICADAS EN SERVICIOS FINANCIEROS MÓVILES (I)

Freddy Landivar CRISC, CISA

Mayo, 2012



AGENDA

- I. LA EVOLUCIÓN DEL MÓVIL
- II. LA SEGURIDAD EN COMUNICACIONES MÓVILES



La evolución del Móvil

- Martin Cooper pionero en esta tecnología “el padre de la telefonía celular” - primer radioteléfono en 1973
- 1983 se pone en operación el primer sistema comercial en la ciudad de Chicago
- La tecnología inalámbrica tuvo gran aceptación, por lo que a los pocos años de implantarse se empezó a **saturar el servicio**, por lo que hubo la imperiosa necesidad de desarrollar e implementar otras formas de **acceso múltiple al canal y transformar los sistemas analógicos a digitales** para darle cabida a más usuarios.
- Todo este crecimiento se ha categorizado por generaciones.



Las Generaciones G

- **La primera generación 1G**
 - La 1G de la telefonía móvil apareció en 1979
 - Se caracterizó por ser analógica y estrictamente para voz.
 - La calidad de los enlaces de voz era muy baja, velocidad [**2400 bauds**],
 - La transferencia entre celdas era imprecisa,
 - Tenían baja capacidad [basadas en FDMA, Frequency Division Multiple Access]
 - La seguridad no existía.
 - La tecnología predominante de esta generación es AMPS (Advanced Mobile Phone System)..

Las Generaciones G

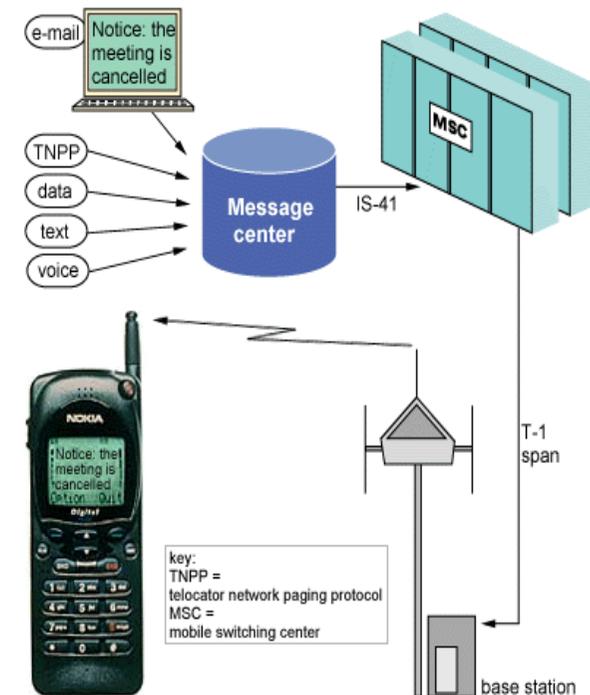
➤ La segunda generación 2G

- Apareció en 1990 y se caracterizó por ser digital.
- El sistema 2G utiliza protocolos de codificación más sofisticados y son los sistemas de telefonía celular usados en la actualidad.
- Las tecnologías predominantes son:
 - GSM (Global System for Mobile Communications)
 - TDMA (Time Division Multiple Access - Multiplexación) IS-136 /TIA/EIA-136 o ANSI-136
 - CDMA (Code Division Multiple Access)
 - PDC (Personal Digital Communications)- aplicado en Japón.



Las Generaciones G

- Los protocolos empleados soportan velocidades de información mas altas para voz pero limitados en comunicaciones de datos.
- Se pueden ofrecer servicios auxiliares tales como datos, fax y **SMS [Short Message Service]**.
- La mayoría de los protocolos de 2G ofrecen **diferentes niveles de encriptación**.
- Se le conoce también como PCS (Personal Communications Services).





Las Generaciones G

- **La generación 2.5 G**
- Es más rápida y más económica.
- Fue tecnología de transición de 2G a 3G
- Ofrece características extendidas para ofrecer capacidades adicionales como
 - GPRS (General Packet Radio System)
 - HSCSD (High Speed Circuit Switched Data),
 - EDGE (Enhanced Data Rates for Global Evolution),
 - TDMA IS-136B,
 - CDMA IS-95B, entre otros..





Las Generaciones G

- **La tercera generación 3G**
 - Tipificada por convergencia de voz y datos con acceso inalámbrico a Internet, aplicaciones multimedia y transmisión de datos a mayores velocidades.
 - Los protocolos empleados están enfocados para aplicaciones mas allá de la voz tales como audio (MP3), video en movimiento, video conferencia y acceso rápido a Internet
 - Los sistemas 3G alcanzan velocidades de hasta 384 Kbps permitiendo una movilidad total a usuarios viajando a 120 kilómetros por hora en ambientes exteriores y alcanzará una velocidad máxima de 2 Mbps permitiendo una movilidad limitada a usuarios caminando a menos de 10 kilómetros por hora en ambientes estacionarios de corto alcance o en interiores.

- **La cuarta generación 4G**
 - Está basada completamente en el protocolo IP, siendo un sistema de sistemas y una red de redes, que se alcanza gracias a la convergencia entre las redes de cables e inalámbricas.
 - Esta tecnología es usada por modems inalámbricos, celulares inteligentes y otros dispositivos móviles.
 - La principal diferencia con las generaciones predecesoras será la capacidad para proveer velocidades de acceso mayores de 100 Mbps en movimiento y 1 GB en reposo
 - El WWFR (Wireless World Research Forum) trabaja en que 4G sea una fusión de tecnologías y protocolos y no sólo un único estándar,





La Seguridad en comunicaciones móviles....

- Asegurar que la comunicación entre dos agentes se mantenga **confidencial y privada** evitando la interceptación por terceras personas para usos indebidos.
- Para el paso a la comunicación digital de la telefonía móvil primero se utilizó el estándar de segunda generación **(2G) GSM** que significa “Groupe Special Mobile”.
- Este sistema fue desarrollado por el Instituto Europeo de Estándares en Telecomunicaciones ETSI e incluyo un **conjunto de protocolos criptográficos** para proporcionar tanto **confidencialidad como autenticación**.
- Se utilizan los siguientes algoritmos:
 - **A3**: algoritmo de autenticación que se implementa dentro de la SIM de forma que entre los operadores puedan inter-operar entre sí sin revelar sus algoritmos de autenticación ni sus claves móviles (referido como Ki)



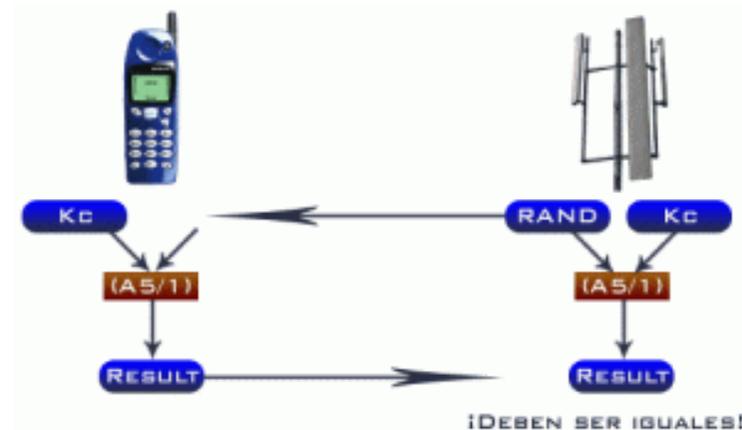
La Seguridad en comunicaciones móviles....

- **A5:** algoritmo de cifrado de voz. Permite que la conversación vaya encriptada. Se trata de un algoritmo cifrador de flujo con una clave de 64 bits.

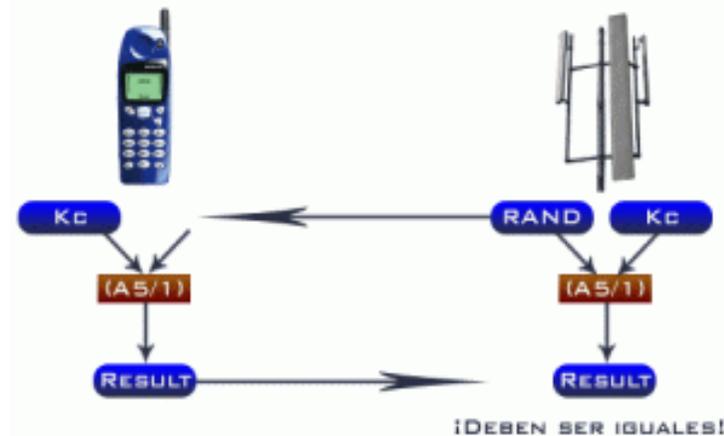
Se implementan en hardware para asegurar una velocidad rápida. Hay dos versiones, denominadas

- A5/1 creado en 1981 usado por Europa y Estados Unidos con un cifrado menos fuerte y
 - A5/2 creado en 1982 usado por el resto de países considerados de no confianza para tener un cifrado más fuerte
- **A8:** algoritmo que genera claves tanto para autenticación (A3) como para encriptación (A5)
 - **COMP128:** algoritmo que permite funcionar a los A3 y A8. Es un algoritmo que implementa una función HASH que sirve para garantizar que el mensaje no ha sido modificado

- Su funcionamiento paso a paso:



- El teléfono toma de la tarjeta (SIM) una clave almacenada en su interior (K_i)
- A continuación, el teléfono toma ciertos datos aleatorios que se intercambian entre éste y la estación base más cercana. El paquete de datos se conoce como random seed.
- El conjunto clave+semilla es transformado mediante el algoritmo de autenticación A3.
- El resultado de dicha transformación es enviada a la estación base.



- La estación base autentica la identidad del llamante. Es decir, toma los datos de semilla aleatoria y la clave del teléfono K_i (que están almacenados a disposición de dicha estación) y realiza la comprobación.
- Si la estación base ha quedado satisfecha con los resultados de la comprobación, da vía libre a la comunicación.
- Toma la clave del teléfono K_i y una semilla aleatoria para crear una clave de sesión K_c , de 64 bits de longitud. Esa clave es usada para encriptar la comunicación, gracias al algoritmo A5



La Seguridad en comunicaciones móviles....

- Otro sistema de comunicación móvil muy utilizado en la telefonía 3G es el **UMTS** (Universal Mobile Telecommunications System)
 - Esta basado en tecnología GSM (Global System for Mobile Communications)
 - Es un sistema de acceso múltiple por división de código de banda ancha.
 - Es multi-servicio y multi-velocidad es decir ofrece distintos servicios a distintas velocidades.
 - Las características del sistema de seguridad son las siguientes:
 - i. Seguridad de acceso a la red: proporciona a los usuarios acceso seguro a los diferentes servicios 3G y protege contra ataques al enlace que hay de acceso vía radio.
Se divide en:
 - sistema de confidencialidad,



La Seguridad en comunicaciones móviles....

- sistema de autenticación del usuario,
 - confidencialidad al usuario,
 - cifrado de los datos,
 - comprobación de la integridad de los datos (evitar terceras conexiones),
 - identificación del equipo del usuario y
 - cifrado de la red.
- ii. Seguridad del dominio de red: es el conjunto de características de seguridad que permite a los nodos del dominio del proveedor intercambiar de forma segura datos de señalización y protege contra ataques en la red fija de naturaleza alambica.



La Seguridad en comunicaciones móviles....

- iii. Seguridad del dominio de usuario: permiten el acceso seguro a la estación móvil. Los tipos de estación móvil o MS se pueden clasificar atendiendo a sus capacidades de servicio más que a sus características físicas.
- iv. Seguridad del dominio de aplicación: características de seguridad que permiten a las aplicaciones del dominio de usuario y del dominio del proveedor intercambiar mensajes de forma segura.
- v. Visibilidad y configuración de la seguridad: esto permite al usuario informarle de si las características de seguridad se encuentran operativas o no y si el uso y provisión de los servicios depende de la característica de seguridad.



Preguntas ??

Fuentes:

- Propia
- Eveliux
- Wikipedia

Annex VIII: Tecnologías aplicadas en SFM II



TECNOLOGÍAS APLICADAS EN SERVICIOS FINANCIEROS MÓVILES (II)

Freddy Landivar CRISC, CISA

Mayo, 2012



AGENDA

- I. LA TARJETA SIM**
- II. TECNOLOGÍA SMS**
- III. TECNOLOGÍA USSD**



La Tarjeta SIM - Generalidades

- La tarjeta SIM (Subscriber Identity Module)
 - Es componente clave en las redes GSM
 - Almacena principalmente y de forma segura la clave de servicio del suscriptor usada para identificarse ante la red (K_i)
- Tiene diferentes tamaños
 - Tarjeta SIM,
 - Mini-SIM,
 - Micro-SIM.





La Tarjeta SIM - Generalidades

- Tiene diferentes capacidades de Memoria
 - La básica (GSM 11.11) 2-3 KB, espacio usado casi directamente por el teléfono.
 - La con aplicaciones adicionales (GSM11.14) disponibles con varias capacidades de almacenamiento diferente, de 16 KB hasta 128 KB
 - La “Large Memory SIM” (‘SIM de Memoria Grande’), del orden de 128 a 512





La Tarjeta SIM - Generalidades

- Una interfaz relaciona los ocho contactos metálicos visibles con el lector del móvil y este alimenta eléctricamente a la tarjeta y transmite los datos para operar
- Esta arquitectura se basa en estándares ISO/IEC 7816 e ISO/IEC 7810, que define:
 - La forma física,
 - La posición de las formas de los conectores eléctricos,
 - Las características eléctricas
 - Los protocolos de comunicación, y otros





La Tarjeta SIM - Generalidades

- Las tarjetas SIM almacenan información específica de la red, usada para **autenticar e identificar** a los suscriptores en ella
 - El **ICCID** (Integrated Circuit Card ID) identificación internacional de la tarjeta (18 dígitos)
 - El **IMSI** (International Mobile Subscriber Identify) Identidad Internacional del Suscriptor Móvil secreta (protegida con PIN/PUK – 4 dígitos)
 - La clave de autenticación **Ki** (Authentication key) (16 bytes) usado para autenticar las tarjetas SIM en la red móvil, asignada por el operador en la personalización.
 - Otras como el número del SMSC (centro de servicio de mensajes cortos), el nombre del proveedor de servicio (SPN), los números de servicio de marcado (SDN) y las aplicaciones de servicios de valor añadido (VAS).





La Tarjeta SIM - Generalidades

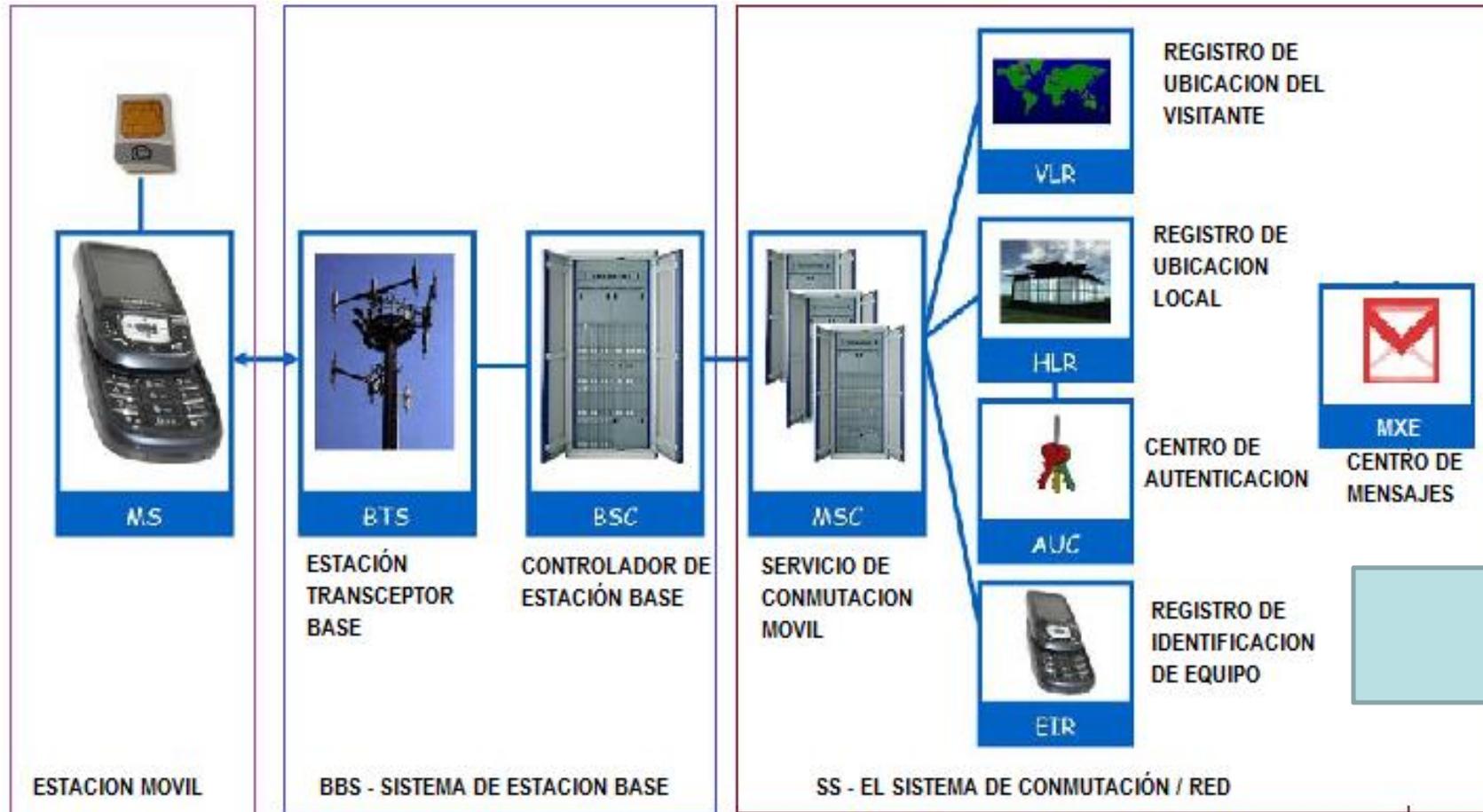
➤ Proceso de autenticación

- a. Al encender el teléfono se envía su IMSI al operador de la red solicitando acceso y autenticación.
- b. El operador de la red busca en su base de datos el IMSI y la clave de autenticación (Ki) relacionada.
- c. El operador de la red genera un número aleatorio (RAND) y lo firma con la Ki de la SIM, generando así un número conocido como **SRES_1** (*Signed Response 1*, 'Respuesta Firmada 1').
- d. El móvil cliente de la red envía el RAND a la tarjeta SIM, que también lo firma con su Ki y envía el resultado (SRES_2) de vuelta al operador de la red.
- e. El operador de la red compara su SRES_1 con el SRES_2 generado por la tarjeta SIM. Si los dos números coinciden la SIM es autenticada y se le concede acceso a la red.





La Arquitectura GSM





La Tecnología SMS

- Un mensaje SMS es una cadena alfanumérica de hasta 140 caracteres , cuyo encapsulado incluye una serie de parámetros en su payload (carga útil o cuerpo del mensaje)

- Parámetros de los SMS
 - Fecha de envío (también llamada *timestamp*);
 - Validez del mensaje en tiempo (de hora a semana)
 - Número de teléfono del remitente y del destinatario;
 - Número del SMSC que ha originado el mensaje;
 - Este modo se asegura el correcto procesamiento del mensaje en el SMSC y a lo largo de toda la cadena





La Tecnología SMS

- En principio, se emplean para enviar y recibir mensajes de texto normal
- Hoy existen extensiones del protocolo básico que permiten incluir otros tipos de contenido, dar formato a los mensajes o encadenar varios mensajes de texto para permitir mayor longitud
- En GSM existen varios tipos de mensajes de texto SMS:
 - mensajes de texto "puros",
 - mensajes de configuración
 - mensajes WAP -Wireless Application Protocol,
 - notificaciones de mensajes MMS - Multimedia Messaging System.





La Tecnología SMS

- Se generan dos tipos de mensaje - **Mensajes MT-SM (de llegada al teléfono) y MO-SM (originados en el teléfono)**
- En principio se definieron como unidireccional operador-abonado **MT-SM** (Mobile Terminated-Short Message)
- Con la **MO-SM** (Mobile Originated) se permitió la comunicación bidireccional por SMS



La Tecnología SMS

- Los mensajes de texto son procesados por un **SMSC** o centro de mensajes cortos (*Short Message Service Center*) - MXE
 - que se encarga de recibir y almacenar los mensajes cortos enviados por los usuarios (MO-SM) o por otras fuentes (avisos del operador, buzón de voz, sistemas de publicidad, alertas de correo electrónico...) hasta que puedan ser enviados;
 - verificar los permisos para enviar mensajes, en comunicación con el HLR de origen
 - verificar si el usuario al que se envía el mensaje está operativo o no, mediante consulta al VLR de destino;
 - verificar periódicamente el estado de los usuarios que tienen mensajes pendientes.
 - Interconecta con el resto de elementos de la red GSM



La Tecnología SMS

Envío y recepción vía radio de los SMS

- Los mensajes cortos hacen un uso extremadamente eficaz de la red de radio, y son enviados y recibidos en cualquier momento, incluso durante una llamada.
- Debido a su pequeño tamaño, los SMS **no necesitan que se asigne un canal de radio al usuario**. Estos se insertan en la información de señalización de la propia red, en los time slots reservados para este fin.
- Algunos operadores han implementado el transporte de los mensajes SMS a través del protocolo de paquetes GPRS en lugar del canal de señalización, incrementando la velocidad de transmisión y la capacidad del sistema,





La Tecnología SMS

El camino de un MO-SM

- El usuario de la red genera un mensaje corto (MO-SM)
- El HLR donde está registrado el usuario decide si puede o no enviar mensajes; si todo está en orden,
- El MSC al que está conectado el usuario recibe el mensaje, envía la información necesaria al VLR para su posterior tarificación y después lo remite al SMSC de origen
- El SMSC convierte en MT-SM
- El SMSC informa del estado del mensaje y devuelve un informe de recepción al MSC y al usuario. En la pantalla del usuario se advierte: “mensaje enviado”.
- Si el usuario lo ha solicitado, recibirá posteriormente un mensaje de estado confirmación de recepción



La Tecnología SMS

El camino de un MT-SM

- El SMSC que ha recibido el mensaje lo almacena en su base de datos y solicita al VLR del usuario la información de localización;
- Si el usuario destino está disponible, el SMSC envía al MSC el mensaje, indicando en que parte del BSS debe ser entregado; si no lo está, se almacena en el SMSC durante su periodo de vigencia;
- Si el usuario destino está disponible, el MSC envía un aviso al VLR al que está conectado el usuario destino (que puede ser o no de su operador) para indicarle que va a entregarse un mensaje;
- El VLR avisa al terminal del usuario y verifica si está conectado a la red (en zona de cobertura);



La Tecnología SMS

Otras aplicaciones del SMS

- Concursos y sorteos de diversa índole.
- Otro de los usos lúdicos que más se está extendiendo es el uso de micropagos por SMS en Internet para poder tener acceso a contenidos u opciones restringidas de determinadas webs.
- Pero también se utiliza en el ámbito industrial como elemento de comunicación entre máquinas y personas, a través de módulos de telecontrol por SMS (envío de SMS con el estado o las alarmas que se producen y respuesta a las mismas - M2M)
- En el **ambiente doméstico**, ya son muchos los que abren la puerta de su garaje mediante una llamada perdida desde su móvil a un módulo de telemando GSM. Lo mismo se puede hacer con la calefacción, riego, lavadora o las persianas.

➤ **SFM**

16



La Tecnología USSD

- USSD, (Unstructures Supplementary Services Data) es un protocolo de transmisión de mensajes que forma parte del sistema GSM de telefonía
- Sus Funcionalidades
 - Se trata de una utilidad basada en **SESIONES TRANSACCIONALES DIRECTAS** en las que no existe riesgo de pérdidas ni duplicidades , siendo la transmisión **EN TIEMPO REAL**
 - Permite el **acceso** y la comunicación en **zonas de mínima cobertura**, ya que las comunicaciones a través del protocolo USSD pueden realizarse en condiciones en las que no es posible enviar mensajes SMS o realizar llamadas.
 - Este canal ofrece un servicio de mensajería móvil que, a **diferencia del SMS**, abre una sesión '**HEAD – TAIL**' (**EXTREMO A EXTREMO**), que permite diferentes operaciones y que no se corta hasta que éstas finalizan.
 - Permite realizar transacciones monetarias en segundos permitiendo el realizar pagos con el teléfono celular.



La Tecnología USSD

- De igual forma permite a los usuarios de teléfonos móviles, con **capacidades MMS**, enviar mensajes que combinen texto, imágenes, gráficos y sonido en un único mensaje rico en contenidos, directamente a otro terminal MMS, a direcciones de e-mail o incluso a teléfonos móviles no MMS, lo que permite una completa solución MMS, extremo a extremo, que incluye el centro de mensajería multimedia, además de otros servicios de comunicación.
- Posibilita **la recarga virtual** de saldo, en las **agentes /comodatos** permitiendo agregar dinero a su cuenta móvil de forma rápida, segura y eficaz.
- De igual forma, este canal hace posible el funcionamiento de los **Puntos de Venta Inalámbricos**, que cambiaran la forma de realizar pagos y transacciones, gracias a este novedoso sistema de pago.



La Tecnología USSD

Su funcionamiento

- A diferencia de SMS, los mensajes **no se almacenan**
- El **tiempo de respuesta** total en aplicaciones interactivas es **menor** ya que no es un servicio de almacenamiento y reenvío, sino que está **orientado a conexión**, la sesión permanece abierta hasta que el usuario, la aplicación o el timer la liberan.
- Los mensajes de texto alcanzan los 182 caracteres de longitud
- **USSD no compite con SMS, sino que lo complementa.**
- Usa para comunicación una **analogía** con protocolos de comunicación de internet (**TELNET**)
- Los requerimientos de ancho de banda son mucho menores que los necesitados por los servicios WAP, pero mayores a los que necesita SMS.



La Tecnología USSD

- El protocolo USSD ha tenido mejoras técnicas a lo largo de su aparición
 - USSD fase 1 que solamente permitía sesiones iniciadas por el terminal móvil, PUSH, donde no había un **mecanismo de diálogo**.
 - USSD Fase 2 que es el presente estado del estándar, que permite a la red enviar operaciones USSD hacia la MS, así como también combinar operaciones iniciadas por la red y el terminal móvil, con el fin de intercambiar datos en una manera de diálogo Push-Pull
- Las arquitecturas de las redes GPRS y UMTS conservan los elementos núcleo de la red GSM como son: la MSC, HLR y VLR, permitiendo la incorporación del protocolo USSD en la evolución hacia tercera generación de los servicios móviles



La Tecnología USSD

- La presisa es que en **M-COMMERCE** se debe garantizar la autenticidad, privacidad, integridad y no repudio (no phishing) en las comunicaciones
 - Las redes GSM tienen como ventaja a su favor el empleo de firmas digitales a diferencia de otras tecnologías como TDMA o CDMA, haciendo de esta forma que una transacción con USSD sea totalmente fiable,
 - La tarjeta SIM que identifica al abonado frente al operador es un buen medio de almacenamiento para albergar claves privadas y dado que éstas no salen de la tarjeta.
- La tarjeta SIM cumple un papel fundamental del lado cliente en cuanto a la seguridad, ya que en USSD es posible la implementación de funciones criptográficas, es decir cifrado y/o firma digital, en la programación de la SIM.
- Se pueden desarrollar aplicaciones utilizando las definidas en la librería “Java Card de SUN o en la API de Windows for Smart Card de Microsoft.



Preguntas ??

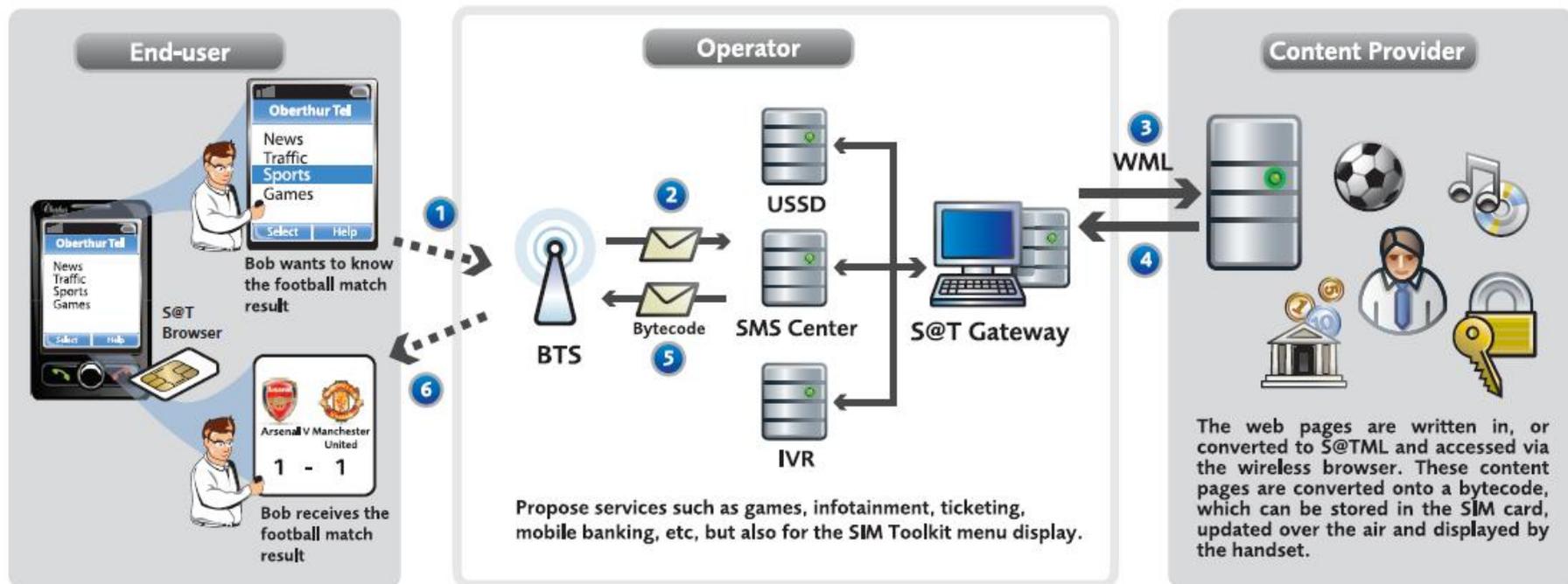
- LAS COMUNICACIONES HOY
- UN HACKER DE 26 AÑOS ROMPE EL CIFRADO DE LOS TELÉFONOS MÓVILES GSM
- ¿LA NORMA A ELABORAR APOYARA O TRUNCARA ESTE AVANCE?



Sim Browsing

Sim Browsing

Scenario of S@T Browsing





Preguntas ??

Annex IX: Tecnologías aplicadas en SFM

III



TECNOLOGÍAS APLICADAS EN SERVICIOS FINANCIEROS MÓVILES (III)

Freddy Landivar CRISC, CISA

Mayo, 2012



AGENDA

I. OTRAS TECNOLOGÍAS

- SIM BROWSING
- SIM APPLICATION TOOLKIT
- WAP
- IVR
- J2ME
- NFC

II. CONCEPTOS DE SEGURIDAD

SIM BROWSING

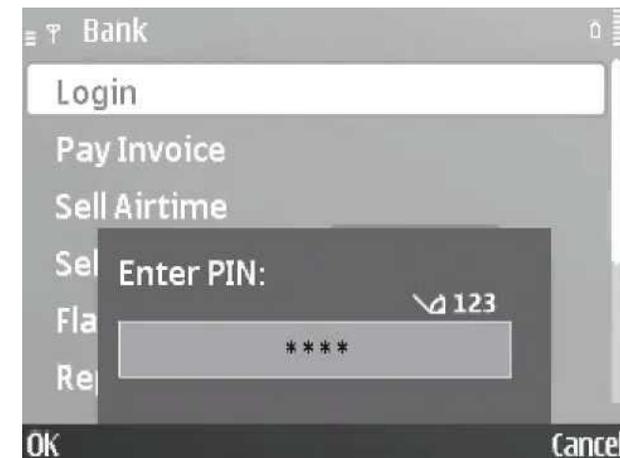


- SIM BROWSING no es más que un navegador ligero cargado en la tarjeta SIM de un teléfono móvil.
- Se basa en la estructuración de un XML en el teléfono y permite la comunicación a un puerto de navegación
- XML - eXtensible Markup Language es un lenguaje que permite definir la gramática de lenguajes específicos, siendo un estándar para el intercambio de información estructurada entre diferentes plataformas.
- Se puede usar en bases de datos, editores de texto, hojas de cálculo y casi cualquier cosa imaginable



SIM BROWSING

- El XML puede permanecer cargada y almacenada en la tarjeta SIM, ó puede ser descargada dinámicamente a pedido.
- La ventaja es que interconexión con el teléfono móvil es través del **mismo protocolo** que se utiliza para las funciones del teléfono, **permitiendo que los menús y mensajes sean consistentes** con los otros menús y mensajes en el teléfono.
- Para utilizar las funcionalidades SIM Toolkit recogidas en la especificación GSM 11.14 correspondiente a la Fase 2, se requieren **tarjetas y terminales capaces de** soportar esta opción





SIM BROWSING

El circuito es:

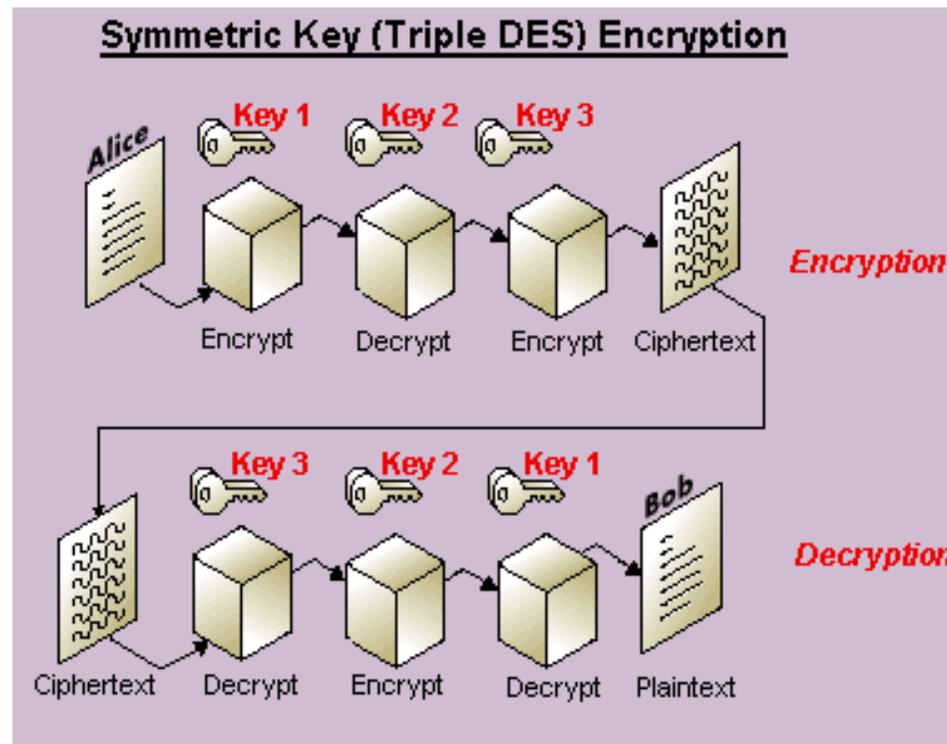
- El usuario solicita un sitio web (http-url)
- El XML configura la dirección URL del http y el SIM Browser empaqueta esta solicitud en un mensaje SMS y lo envía al SMSC
- El SMSC desempaqueta el mensaje y lo reenvía al modulo servidor de aplicaciones
- El servidor de aplicaciones responde con un XML, mismo que es convertido y empaquetado en un mensaje SMS y enviado al teléfono móvil a donde el SIM Browser desempaqueta el mensaje y lo muestra al usuario



La comunicación con el gateway (SMSC) de la telefónica es via SMS, pero el SIM Browser es quien controla la comunicación

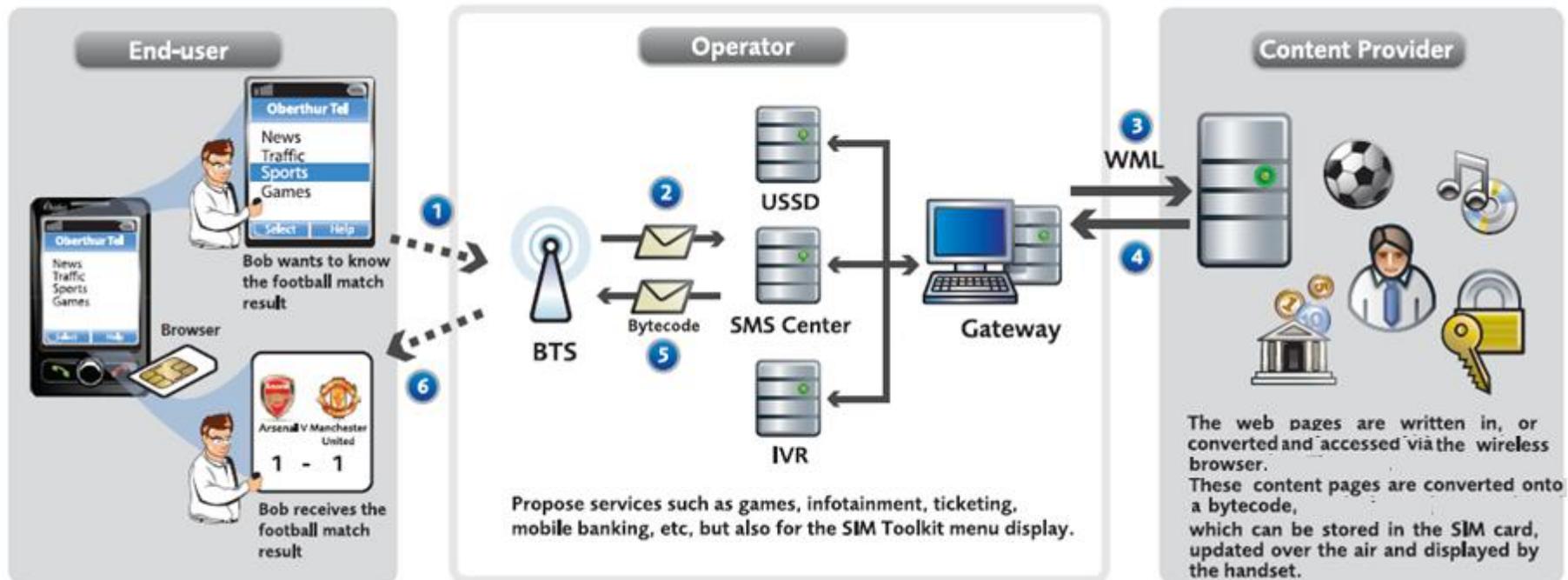
SIM BROWSING

Considerando que el SIM Browser se ejecuta en la SIM card, esta ya tiene acceso al plugin de seguridad 3DES de la SIM card y puede encriptar datos sensibles o and can encrypt data such as passwords o generar valores MAC para comprobar la integridad de los mensajes



SIM BROWSING

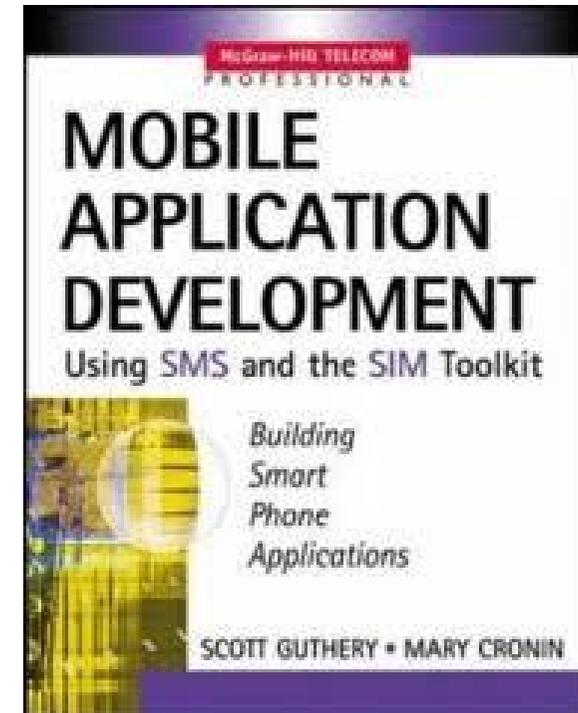
Diagrama Sim Browsing





SIM APPLICATION TOOLKIT (SAT)

- Consisten en una serie de procedimientos y comandos que extienden las funciones del interfaz entre el teléfono GSM y la tarjeta SIM.
- Permiten una comunicación integrada entre la SIM y el terminal, lo cual permite programar nuevos servicios con independencia de los fabricantes de tarjetas y teléfonos.



SIM APPLICATION TOOLKIT (SAT)

- Permite personalizar los servicios de cada abonado a través del teléfono móvil; siendo posible:
 - programar aplicaciones en la tarjeta SIM para visualizar una serie de menús
 - automatizar procedimientos en el terminal.
- Siguiendo las instrucciones en pantalla se podrá:
 - ordenar operaciones bancarias sin necesidad de realizar una llamada
 - solicitar mediante un mensaje corto los titulares de las últimas noticias sin tener que recordar el código que corresponde a ese servicio.



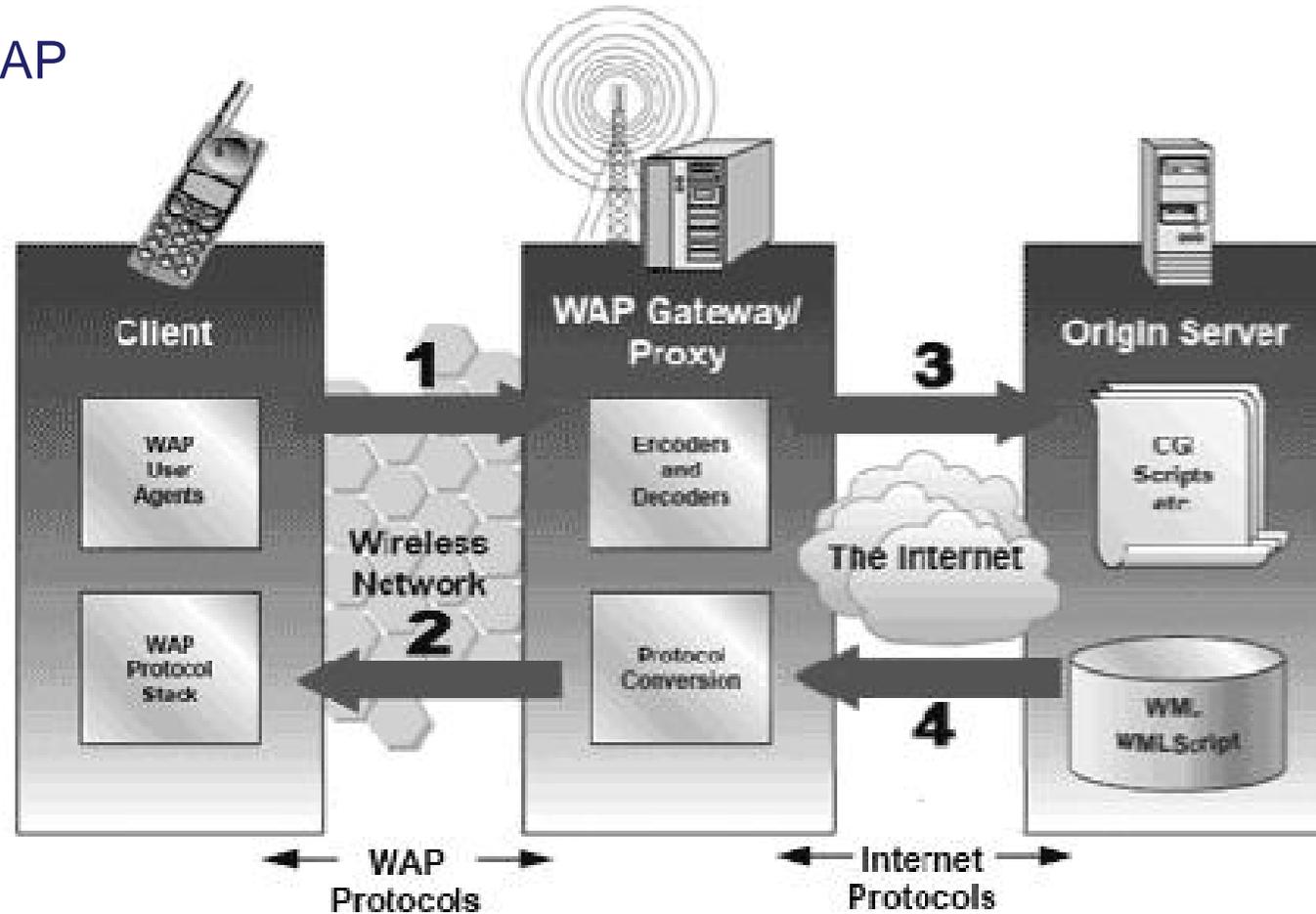
WAP

- **Wireless Application Protocol** o **WAP** (protocolo de aplicaciones inalámbricas) es un estándar para aplicaciones que utilizan las comunicaciones inalámbricas
- Son especificación de un **entorno de aplicación** y de un conjunto de **protocolos de comunicaciones** para normalizar el modo en que los dispositivos inalámbricos, pueden utilizar para acceder a correos electrónicos, grupos de noticias y otros
- La Navegación WAP generalmente es **activado** por el proveedor del servicio de telefonía móvil con un **costo de por medio**
- La oferta de información vía WAP es preparada exclusivamente para aquellos que deseen navegar por medio del celular, son **versiones especiales de sitios** creados para navegantes WAP



WAP

➤ Flujo WAP



- 1 -- WSP Request (URL)**
- 2 -- WSP Response (Binary WML)**
- 3 -- HTTP Request (URL)**
- 3 -- HTTP Response (WML)**

IVR

- IVR Interactive Voice Recognition, es un sistema de Respuestas de Voz Interactiva
- Permiten procesar las llamadas entrantes mediante la reproducción de mensajes pre-grabados con los que los clientes interactúan oprimiendo las teclas del teléfono de acuerdo a las opciones que el sistema IVR ofrece
- El IVR recopila la información tecleada y pasa al ACD (Automatic Call Distribution) o sistema de distribución de llamadas y este procede de acuerdo a la opción marcada





J2ME

- **Java Micro Edition** es un subconjunto de la plataforma JAVA , que orientada a proveer una colección certificada de APIs (**application programming interface**) de desarrollo de software para dispositivos con recursos restringidos.
- Está orientado a productos de consumo como PDAs, Teléfonos móviles o electrodomésticos
- Java ME se ha convertido en una buena opción para crear aplicaciones y juegos en teléfonos móviles debido a que se puede emular en un PC durante la fase de desarrollo y luego subirlos fácilmente al teléfono.
- Al utilizar tecnologías JAVA el desarrollo de aplicaciones las convierte en completamente portables



NFC

- **NFC (Near Field Communication (NFC))** es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos. Es una extensión del estándar ISO 14443 RFID
- Su punto fuerte está en la velocidad de comunicación (casi instantánea) sin necesidad de emparejamiento previo.
- Como contrapartida, el alcance de la tecnología NFC es muy reducido, pues se mueve como máximo en un rango de los **20 cm.**
- La interconexión es transparente al usuarios y es capaz de enviar y recibir información al mismo tiempo.



- Funciona en dos modos:
 - **Activo**, en el que ambos equipos con chip NFC generan un campo electromagnético e intercambian datos.
 - **Pasivo**, en el que solo hay un dispositivo activo y el otro aprovecha ese campo para intercambiar la información.
- Su aplicabilidad:
 - **Identificación:** el acceso a lugares donde es precisa una
 - **Recogida/intercambio de datos:** utilizando etiquetas RFID (Identificación por radiofrecuencia) almacena y recupera datos remotos
 - **Pago con el teléfono móvil:**



- **Riesgos y amenazas de seguridad.** Los ataques detectados son similares a los registrados en otras tecnologías.
 - **Sniffing o eavesdropping:** técnica con la que un atacante podría escuchar los datos que se comunican entre ambos dispositivos, el emisor y el receptor.
 - **Corrupción de datos:** ataque de denegación de servicio (DoS) en el que se modificarían los datos con intención de impedir la comunicación entre dispositivos.
 - **Modificación de los datos:** similar al anterior, pero manteniendo la validez de los datos.
 - **Man in the middle:** en un ataque MitM, las dos partes que se comunican son engañadas pensando que se comunican entre sí de manera segura mientras el atacante está entre ellas comunicándose con ambas

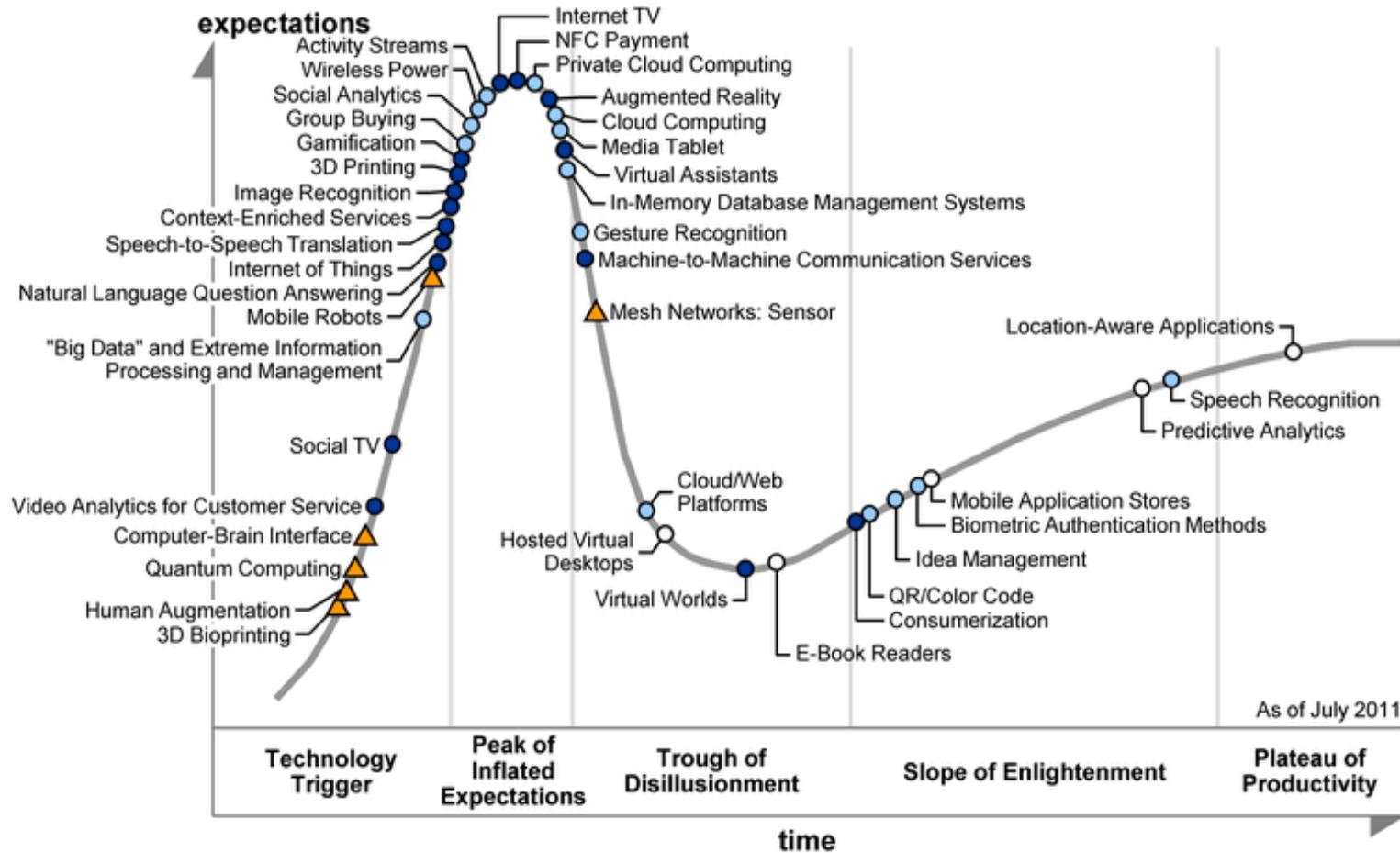
- **La seguridad**

- Cifrado
- Almacenamiento en tarjetas USIM Universal Subscriber Identity Module (3G) y tarjetas SD Secure Digital



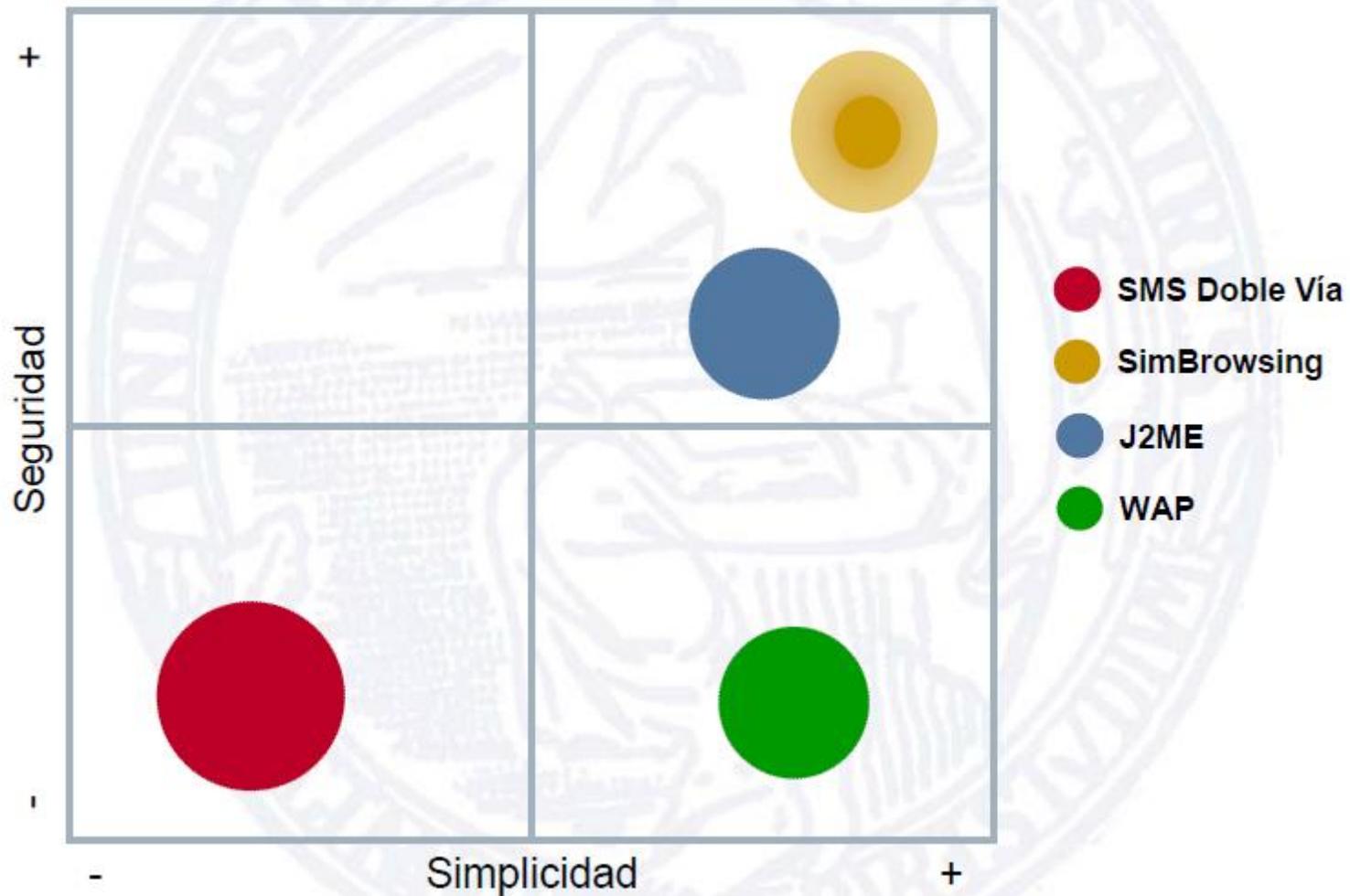


NFC





NFC





Conceptos de seguridad a gestionar

- **Integridad de datos.** Es alcanzada con la criptografía electrónica que le asigna una identidad única, cualquier cambio se identifica
- **Autenticación** Se gestiona con un sistema de autenticación usando el sistema de firma PKI el cual verifica la firma digital mas su origen, verificación efectuada en forma conjunta. Un HASH (algoritmo criptográfico) genera la firma digital
- **No repudio** Se gestiona incorporando una firma digital de una tercera parte, quien corrobora las identidades
- **Authorization and Delegation** Se gestiona con Certificados de autoridad criptográficos
- **Auditing and Logging** Registro de logs efectuados para su auditoria
- **Management.** Procesos administrativos normados (Manipulación, suscripción est)



Preguntas ??

Annex X: Estándares de Seguridad de TI

Iso 27002



ESTÁNDARES Y BUENAS PRÁCTICAS SOBRE SEGURIDAD INFORMÁTICA ISO-IEC 27002

Freddy Landivar CRISC, CISA

Mayo, 2012



AGENDA

- I. LA EVOLUCIÓN DEL MOVIL**
- II. LA SEGURIDAD EN COMUNICACIONES MOVILES**



Áreas asociadas a la seguridad





Las buenas practicas – ISO 27002

Tenemos 2 normas fundamentales:

- **17799 → 27002 : NORMALIZACION (Mejores Prácticas)**

Homologada en Argentina IRAM-ISO/IEC 27002

- **27001: Sistema de Gestión de Seguridad de la Información (CERTIFICACION)**

Homologada en Argentina IRAM-ISO/IEC 27001

Las certificaciones son con: BS 7799-2 ó ISO 27001



Las buenas practicas – ISO 27002

Está organizada en 11 capítulos en los que se tratan los distintos criterios a ser tenidos en cuenta en cada tema para llevar adelante una correcta:

GESTION DE SEGURIDAD DE LA INFORMACION

Alcance:

- **Recomendaciones para la gestión de la seguridad de la información**
- **Sirve de Base para el desarrollo de las políticas de seguridad en las organizaciones**



Objetivo

Preservar la:

● confidencialidad:

accesible sólo a aquellas personas autorizadas a tener acceso.

● integridad:

exactitud y totalidad de la información y los métodos de procesamiento.

● disponibilidad:

acceso a la información y a los recursos relacionados con ella toda vez que se requiera.



Dominios

- 1. Política de Seguridad**
 - 2. Organización de Seguridad**
 - 3. Gestión de Activos**
 - 4. Seguridad de los Recursos Humanos**
 - 5. Protección Física y Ambiental**
 - 6. Gestión de Comunicaciones y Operaciones**
 - 7. Control de Accesos**
 - 8. Adquisición, Desarrollo y Mantenimiento de Sistemas**
 - 9. Gestión de los Incidentes de Seguridad**
 - 10. Gestión de la Continuidad del Negocio**
 - 11. Cumplimiento**
-



A que se refiere “La Información”

La información = activo comercial

Tiene valor para una organización y por consiguiente debe ser debidamente protegida.

“Garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades”

“La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados”



Formas y medios de distribución

- **Impresa,**
- **escrita en papel,**
- **almacenada electrónicamente,**
- **transmitida por correo o utilizando medios electrónicos,**
- **presentada en imágenes, o**
- **expuesta en una conversación.**



La gestión de la seguridad de la Información

Implementando un conjunto adecuado de “CONTROLES”:

- **Políticas**
- **Mejores Prácticas**
- **Normas**
- **Procedimientos**
- **Planes**
- **Estándares Tecnológicos**
- **Estructuras Organizacionales**
- **Software**
- **Hardware**



Como establecer los requerimientos de seguridad

● **Evalúan los riesgos:**

- **se hace un relevamiento de los activos,**
- **se identifican las amenazas a esos activos,**
- **se evalúan vulnerabilidades y probabilidades de ocurrencia,**
- **se estima el impacto potencial y**
- **se determina el nivel de riesgo de cada activo.**

● **Evalúan los Requisitos legales, normativos, reglamentarios y contractuales que deben cumplir:**

- **la organización,**
- **sus socios comerciales,**
- **los contratistas y los prestadores de servicios.**



La selección de controles

“Los controles pueden seleccionarse sobre la base de la Norma ISO 27002, de otros estándares, o pueden diseñarse nuevos controles para satisfacer necesidades específicas según corresponda”

Costo de implementación vs. riesgos a reducir y las pérdidas monetarias y no monetarias

Revisiones periódicas de:

- **Riesgos**
- **Controles implementados**



La selección de controles

- **Controles “esenciales” desde el punto de vista legal:**
 - ➔ **protección de datos y confidencialidad de información personal**
 - ➔ **protección de registros y documentos de la organización**
 - ➔ **resguardo de derechos de propiedad intelectual**
 - ➔ **protección contra los delitos informáticos**

- **Controles considerados como “práctica recomendada” de uso frecuente en la implementación de la seguridad de la información:**
 - ➔ **documentación de la política**
 - ➔ **asignación de responsabilidades en materia de seguridad**
 - ➔ **concientización, capacitación y entrenamiento**
 - ➔ **comunicación de incidentes relativos a la seguridad**
 - ➔ **administración de la continuidad de los negocios**



Factores críticos de éxito

- **política de seguridad, objetivos y actividades que reflejen los objetivos de la empresa;**
- **una estrategia de implementación de seguridad que sea consecuente con la cultura organizacional;**
- **apoyo y compromiso manifiestos por parte de la gerencia;**
- **un claro entendimiento de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos;**
- **comunicación eficaz de los temas de seguridad a todos los gerentes y empleados;**
- **capacitación del área de TI.**



Factores críticos de éxito

- **distribución de las políticas y estándares de seguridad de la información a todos los empleados y contratistas;**
- **Concientización, capacitación y entrenamiento adecuados;**
- **un sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información y para brindar sugerencias tendientes a mejorarlo.**



Dominio 1 – Política de Seguridad

Nivel gerencial debe:

- **aprobar y publicar la política de seguridad**
- **comunicarlo a todos los empleados**



Dominio 1 – Política de Seguridad

Debe incluir:

- **objetivos y alcance generales de seguridad**
- **apoyo expreso de la dirección**
- **breve explicación de los valores de seguridad de la organización**
- **definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información**
- **referencias a documentos que puedan respaldar la política**



Dominio 1 – Política de Seguridad





Dominio 1 – Política de Seguridad

Es política de la compañía:

● **Eficacia:**

Garantizar que toda la información utilizada es necesaria y útil para el desarrollo de los negocios.

● **Eficiencia:**

Asegurar que el procesamiento de la información se realice mediante una óptima utilización de los recursos humanos y materiales.

● **Confiabilidad:**

Garantizar que los sistemas informáticos brindan información correcta para ser utilizada en la operatoria de cada uno de los procesos.



Dominio 1 – Política de Seguridad

● Integridad:

Asegurar que sea procesada toda la información necesaria y suficiente para la marcha de los negocios en cada uno de los sistemas informáticos y procesos transaccionales.

● Exactitud:

Asegurar que toda la información se encuentre libre de errores y/o irregularidades de cualquier tipo.

● Disponibilidad:

Garantizar que la información y la capacidad de su procesamiento manual y automático, sean resguardados y recuperados eventualmente cuando sea necesario, de manera tal que no se interrumpa significativamente la marcha de los negocios.



Dominio 1 – Política de Seguridad

● Legalidad:

Asegurar que toda la información y los medios físicos que la contienen, procesen y/o transporten, cumplan con las regulaciones legales vigentes en cada ámbito.

● Confidencialidad:

Garantizar que toda la información está protegida del uso no autorizado, revelaciones accidentales, espionaje industrial, violación de la privacidad y otras acciones similares de accesos de terceros no permitidos.



Dominio 1 – Política de Seguridad

● Autorización:

Garantizar que todos los accesos a datos y/o transacciones que los utilicen cumplan con los niveles de autorización correspondientes para su utilización y divulgación.

● Protección Física:

Garantizar que todos los medios de procesamiento y/o conservación de información cuentan con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado.

● Propiedad:

Asegurar que todos los derechos de propiedad sobre la información utilizada por todos sus empleados en el desarrollo de sus tareas, estén adecuadamente establecidos a favor de la compañía.



Dominio 2 – Organización de la Seguridad

Infraestructura de seguridad de la información:

- **Debe establecerse un marco gerencial para iniciar y controlar la implementación.**
- **Deben establecerse adecuados foros de gestión de seguridad que asignen responsabilidades para cada usuario en la organización.**
- **Se debe establecer una fuente de asesoramiento especializado en materia de seguridad y contactos con organizaciones externas**



Dominio 2 – Organización de la Seguridad

Foros de Gestión: Comité de Seguridad

- **aprobar la política de seguridad de la información**
- **asignar funciones de seguridad**
- **actualizarse ante cambios**
- **coordinar la implementación**
- **definir metodologías y procesos específicos de seguridad**
- **monitorear incidentes de seguridad**
- **lidera el proceso de concientización de usuarios**



Dominio 2 – Organización de la Seguridad

Principales roles y funciones:

Sponsoreo y seguimiento

- Dirección de la Compañía
- Foro / Comité de Seguridad

Autorización

- Dueño de datos

Definición

- Área de Seguridad Informática
- Área de Legales

Administración

- Administrador de Seguridad

Cumplimiento directo

- Usuarios finales
- Terceros y personal contratado
- Área de sistemas

Control

- Auditoría Interna
- Auditoría Externa



Dominio 2 – Organización de la Seguridad

Seguridad frente al acceso por parte de terceros:

- **El acceso por parte de terceros debe ser controlado.**
- **Debe llevarse a cabo una evaluación de riesgos: determinar las incidencias en la seguridad y los requerimientos de control.**
- **Los controles deben ser acordados y definidos en un contrato con la tercera parte.**



Dominio 2 – Organización de la Seguridad

Tipos de terceros:

- **personal de mantenimiento y soporte de hardware y software**
- **limpieza, "catering", guardia de seguridad y otros servicios de soporte tercerizados**
- **pasantías de estudiantes y otras designaciones contingentes de corto plazo**
- **consultores.**



Dominio 3 Gestión de activos

- **Hacer un Inventario de los Activos de Información**
- **Designar a un propietario para cada uno de ellos**
- **Hacer la Clasificación de la información**



Dominio 3 Gestión de activos

Inventario:

“Cada activo debe ser claramente identificado y su propietario y clasificación en cuanto a seguridad deben ser acordados y documentados, junto con la ubicación vigente del mismo”

Ejemplos:

● recursos de información:

bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada;

● recursos de software:

software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios;



Dominio 3 Gestión de activos

Designar a un propietario para cada recurso de información:

- **Identificarse claramente los diversos recursos y procesos de seguridad relacionados con cada uno de los sistemas.**
- **Designar al responsable de cada recurso o proceso de seguridad y se deben documentar los detalles de esta responsabilidad.**
- **Los niveles de autorización deben ser claramente definidos y documentados.**



Dominio 3 Gestión de activos

Clasificación de la información:

Garantizar que los recursos de información reciban un apropiado nivel de protección.

Se debe utilizar un sistema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de tratamiento especial.

La información debe ser clasificada para señalar:

- **la necesidad,**
- **las prioridades y**
- **el grado de protección.**



Dominio 3 Gestión de activos

Pautas de clasificación:

Considerar las necesidades de la empresa con respecto a la distribución (uso compartido) o restricción de la información, e incidencia de dichas necesidades en las actividades de la organización.

La información deja de ser sensible o crítica después de un cierto período de tiempo.

La clasificación por exceso ("over classification") puede traducirse en gastos adicionales innecesarios para la organización.



Dominio 3 Gestión de activos

La información y las salidas de los sistemas que administran datos clasificados deben ser rotuladas según su valor y grado de sensibilidad para la organización.

Se debe considerar el número de categorías de clasificación.

La responsabilidad por la definición de la clasificación debe ser asignada al propietario designado de la información.



Dominio 4 –Seguridad de los RRHH

Seguridad en la definición de puestos de trabajo y la asignación de recursos

Las responsabilidades en materia de seguridad deben ser:

- explicitadas en la etapa de reclutamiento,**
- incluidas en los contratos y**
- monitoreadas durante el desempeño como empleado.**



Dominio 4 –Seguridad de los RRHH

Capacitación del usuario

Garantizar que los usuarios están al corriente de las amenazas e incumbencias en materia de seguridad de la información, y están capacitados para respaldar la política de seguridad de la organización en el transcurso de sus tareas normales.



Dominio 4 –Seguridad de los RRHH

Respuesta a incidentes y anomalías en materia de seguridad

Minimizar el daño producido por incidentes y anomalías en materia de seguridad, y monitorear dichos incidentes y aprender de los mismos.



Dominio 4 –Seguridad de los RRHH

Proceso disciplinario

Debe existir un proceso disciplinario formal para los empleados que violen las políticas y procedimientos de seguridad de la organización.



Dominio 5 – Protección física y ambiental

Impedir accesos no autorizados, daños e interferencia a:

- **Sedes**
- **Instalaciones**
- **Información**



Dominio 5 – Protección física y ambiental

- **Perímetro de seguridad física**
- **Controles de acceso físico**
- **Seguridad del equipamiento**
- **Suministros de energía**
- **Cableado de energía eléctrica y de comunicaciones**
- **Mantenimiento de equipos**
- **Seguridad del equipamiento fuera del ámbito de la organización**
- **Políticas de escritorios y pantallas limpias**
- **Retiro de bienes**



Dominio 5 – Protección física y ambiental

Ejemplos:

● Suministro de energía:

Asegurar el suministro permanente de corriente eléctrica, instalando UPS y generadores alternativos. Asegurar el combustible necesario para dichos generadores.

● Escritorios y pantallas limpias:

Sobre los escritorios no deben de quedar papeles sensibles.

Las pantallas deben quedar protegidas con protectores de pantalla con contraseña.

● Retiro de bienes:

Establecer políticas de retiros de bienes de la compañía, ya sea por reparación, mantenimiento, trabajos fuera de la oficina, etc.



Dominio 6 – Gestión de Operaciones y Comunicaciones

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

- **Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información.**
- **Se debe implementar la separación de funciones cuando corresponda.**
- **Se deben documentar los procedimientos de operación**



Dominio 6 – Gestión de Operaciones y Comunicaciones

Separación entre instalaciones de desarrollo e instalaciones operativas

Deben separarse las instalaciones de:

- **Desarrollo**
- **Prueba**
- **Operaciones**

Se deben definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.



Dominio 6 – Gestión de Operaciones y Comunicaciones

Procesos / Procedimientos de:

- **Planificación y aprobación de sistemas**
- **Protección contra software malicioso**
- **Mantenimiento back up**
- **Administración de la red**
- **Administración y seguridad de los medios de almacenamiento**
- **Acuerdos de intercambio de información y software**



Dominio 7 – Control de accesos

Requerimientos de negocio para el control de accesos:

- **Coherencia entre las políticas de control de acceso y de clasificación de información de los diferentes sistemas y redes**

Administración de accesos de usuarios:

- **Se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información.**



Dominio 7 – Control de accesos

- **Administración de accesos de usuarios**
- **Administración de privilegios**
- **Responsabilidades del usuario**
- **Control de acceso a la red**
- **Camino forzado**
- **Autenticación de usuarios para conexiones externas**
- **Monitoreo del acceso y uso de los sistemas**



Dominio 7 – Control de accesos

Ejemplo:

Camino forzado:

“Forzar” al usuario a seguir una ruta de menú preestablecida hasta llegar al recuso y/o transacción solicitada sin la posibilidad de evitar algún paso previo.



Dominio 8 – Adquisición, desarrollo y mantenimiento de sistemas de información

Requerimientos de seguridad de los sistemas.

Asegurar que la seguridad es incorporada a los sistemas de información.

- **Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información.**



Dominio 8 – Adquisición, desarrollo y mantenimiento de sistemas de información

Seguridad en los sistemas de aplicación

Se deben diseñar en los sistemas de aplicación, **incluyendo las aplicaciones realizadas por el usuario**, controles apropiados y pistas de auditoría o registros de actividad, incluyendo:

- la validación de datos de entrada,
- procesamiento interno, y
- salidas.



Dominio 9 – Gestión de los incidentes de seguridad de la información

Garantizar que los eventos de seguridad de la información y las debilidades asociadas a los sistemas de información sean comunicados para que puedan ser corregidos en tiempo y forma.

- **Reporte de eventos de seguridad de la información**
- **Reporte de las debilidades de la seguridad**
- **Gestión de incidentes y mejoras**
- **Recolección de evidencia**



Dominio 10 – Gestión de la continuidad del negocio

Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos del negocio de los efectos de fallas significativas o desastres.

- **Se debe implementar un proceso de administración de la continuidad del negocio**
- **Se deben analizar las consecuencias de desastres, fallas de seguridad e interrupciones del servicio.**



Dominio 10 – Gestión de la continuidad del negocio

- **Se deben desarrollar e implementar planes de contingencia para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos.**
- **Los planes deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.**
- **La administración de la continuidad del negocio debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.**



Dominio 10 – Gestión de la continuidad del negocio

Principales etapas:

- **Clasificación de los distintos escenarios de desastres**
- **Evaluación de impacto en el negocio**
- **Desarrollo de una estrategia de recupero**
- **Implementación de la estrategia**
- **Documentación del plan de recupero**
- **Testing y mantenimiento del plan**



Dominio 11 – Cumplimiento

- **Impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.**
- **Garantizar la conformidad de los sistemas con las políticas y estándares de seguridad de la organización.**
- **Maximizar la efectividad y minimizar las interferencias de los procesos de auditoría de sistemas.**



Dominio 11 – Cumplimiento

Recolección de evidencia:

La evidencia presentada debe cumplir con las pautas establecidas en la ley pertinente o en las normas específicas del tribunal en el cual se desarrollará el caso:

- **Validez de la evidencia: si puede o no utilizarse la misma en el tribunal**
- **Peso de la evidencia: la calidad y totalidad de la misma**



Dominio 11 – Cumplimiento

- **Adecuada evidencia de que los controles han funcionado en forma correcta y consistente durante todo el período en que la evidencia a recuperar fue almacenada y procesada por el sistema.**

Para lograr la validez de la evidencia, las organizaciones deben garantizar que sus sistemas de información cumplan con los estándares o códigos de práctica relativos a la producción de evidencia válida.



Dominio 11 – Cumplimiento

Revisiones de la política de seguridad y la compatibilidad técnica:

Garantizar la compatibilidad de los sistemas con las políticas y estándares (normas) de seguridad de la organización.



Dominio 11 – Cumplimiento

Auditoria de sistemas:

Optimizar la eficacia del proceso de auditoria de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Deben existir controles que protejan los sistemas de operaciones y las herramientas de auditoria en el transcurso de las auditorias de sistemas.



Dominio 11 – Cumplimiento

Relación entre RIESGOS y DELITOS informáticos:

Delitos tradicionalmente denominados informáticos

Delitos convencionales

Infracciones por “Mal uso”



Dominio 11 – Cumplimiento

Principales Leyes relacionadas con la Seguridad Informática

- **Protección de Datos Personales – “Habeas Data”**
- **Firma Digital.**
- **Propiedad intelectual / Software Legal**
- **Regulación de las Comunicaciones Comerciales Publicitarias por Correo Electrónico – “Antispam”**
- **Delitos Informáticos**
- **Confidencialidad de la Información y productos protegidos**



Preguntas ??

Fuentes:

- Propia
- J. Eterovic Seguridad Informatica
- Wikipedia

Annex XI: Herramienta metodológica COBIT



COBIT®

Freddy Landivar P., CRISC, CISA

Agenda

- Introducción
- Visión General
- Marco Referencial
- Guías de aplicación
 - Guías de Auditoría

Introducción al COBIT®

- *¿Por qué la TI necesita de un marco estructural de control? (Framework)*
- *¿Quiénes necesitan de un Framework?*
- *¿Por qué y cómo se aplica COBIT como Framework?*

¿Por qué la TI necesita un Framework?

- Dependencia creciente sobre la información y los sistemas que proveen
- Las vulnerabilidades crecientes y un amplio espectro de amenazas
- La necesidad de seguir normativas y estándares
- El potencial de TI para cambiar organizaciones y hábitos, crear nuevas oportunidades y reducir gastos

Las organizaciones que comprenden y administran los riesgos asociados con las nuevas tecnologías tienen mas probabilidades de éxito

Se necesita un Framework

1. Para asegurar que TI :

- Provea valor
 - costo, tiempo y funcionalidad sean como se espera
- No provea sorpresas
 - los riesgos sean mitigados
- Apoye el desarrollo
 - nuevas oportunidades e innovaciones de proceso, productos y servicios

2. La alta dirección pueda tener a TI bajo control

¿Quiénes necesitan de un Framework?

- **Junta de Directores y Ejecutivo**
 - Para asegurarse que la administración de TI esta siguiendo e implementando la dirección estratégica definida para TI
- **Administración de TI**
 - Para tomar decisiones de inversión
 - Para balancear el riesgo y controlar la inversión
 - Para mediciones de referencia en TI (Benchmark)
- **Usuarios**
 - Para obtener confianza sobre la seguridad y el control de productos y servicios TI adquiridos interna o externamente
- **Audidores**
 - Para substantiar sus opiniones respecto a los controles internos
 - Para recomendar sobre controles mínimos necesarios

¿Por qué y cómo se aplica COBIT®?

- COBIT nace como una respuesta a necesidades
- Considera las normas internacionales más importantes
- Se ha convertido en el estándar de facto para el control de TI
- Se enfoca en los requerimientos del negocio
- Esta orientado a procesos



Visión General del COBIT®

Que es el Cobit ?

Control
OBjectives
for **I**nformation
and Related **T**echnology

*Gobierno, Control y Auditoría de la
Información y su Tecnología Relacionada*

¿Quiénes esta detrás del COBIT®?



IT Governance Institute

*ISACA - Information systems
audit and control association*



*Information Systems
Audit and Control
Association*

***Reconocida como líder mundial en el
gobierno, control y evaluación de TI.***

Antecedentes COBIT®

Su Integración :

COBIT integra y concilia normas existentes como:

COSO (Committe Of Sponsoring Org. of the Treadway Commission)

ISO (International Standars Organization)

NIST (National Institute of Standars and Technology)

DTI (Departament of Trade and Industry of the U.K)

ITSEC (Information Technology Security Evaluation Criteria - Europa)

TCSEC (Trusted Computer Evaluación Criteria - Orange Book - E.U)

IIA SAC (Institute of Internal Auditors - Systems Auditability and Control)

IS (Auditing Standars Japón)

Marco Referencial COBIT®

Sus Características

- Enfocada al Negocio – *(business-focused)*
- Orientada a Procesos – *(process-oriented)*
- Basado en controles y unidades de medición *(controls-based and measurement-driven)*

Marco Referencial COBIT®

Su Principio



"Para proveer la información que la organización necesita para alcanzar sus objetivos, los recursos de TI necesitan ser administrados por procesos naturalmente agrupados"

Marco Referencial COBIT®

Requerimientos del negocio



Requerimientos de Calidad	Calidad (cumplimiento de requerimientos) Costo (dentro del presupuesto). Oportunidad (en el tiempo indicado)	CRITERIOS BASICOS <ul style="list-style-type: none"> 📄 Efectividad 📄 Eficiencia 📄 Confidencialidad 📄 Integridad 📄 Disponibilidad 📄 Cumplimiento 📄 Confiabilidad
Requerimientos Financieros (COSO)	Efectividad y eficiencia operacional. Confiabilidad de los reportes financieros. Cumplimiento de leyes y regulaciones.	
Requerimientos de Seguridad	Confidencialidad Integridad Disponibilidad	

CobiT combina los principios contenidos por modelos conocidos, como COSO, SAC y SAS

Marco Referencial COBIT®

Criterios Básicos de la Información



Efectividad

Se refiere a la información que es relevante para el negocio y que debe ser entregada de manera **correcta, oportuna, consistente y usable**.

Eficiencia

Se refiere a la provisión de información a través del **óptimo** (más productivo y económico) uso de los recursos.

Confidencialidad

Relativa a la protección de la información sensible de su **revelación no autorizada**.

Integridad

Se refiere a la **exactitud y completitud** de la información, así como su **validez**, en concordancia con los valores y expectativas del negocio.

Marco Referencial COBIT®

Criterios Básicos de la Información



Disponibilidad

Se refiere a la que la información debe estar **disponible** cuando es requerida por los procesos del negocio ahora y en el futuro. Involucra la **salvaguarda** de los recursos y sus capacidades asociadas.

Cumplimiento

Se refiere a **cumplir** con aquellas leyes, regulaciones y acuerdos contractuales, a los que están sujetos los procesos del negocio.

Confiability

Se refiere a la **provisión** de la información **apropiada a la alta gerencia**, para operar la entidad y para ejercer sus responsabilidades financieras y de cumplir con los reportes de su gestión.

Marco Referencial COBIT®

Recursos de TI



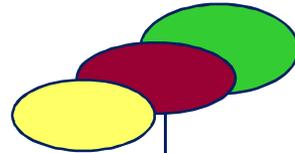
- **Aplicaciones** – Se entiende como la suma de procedimientos manuales y automatizados
- **Datos** - En su sentido más amplio, externos e internos, estructurados y no estructurados, gráficos, sonidos etc.
- **Infraestructura** – Se refiere a la tecnología e instalaciones que permite el procesamiento de las aplicaciones (hardware, sistemas operativos, administrador de base de datos, redes, multimedia, etc., y el ambiente que los aloja y respalda)
- **Recursos Humanos** – Se refiere al personal requerido para planificar, organizar, adquirir, implementar, distribuir, soportar, monitorear y evaluar la información de los sistemas y sus servicios. Pueden ser internas, tercerizadas o contratadas a requerimiento.

Marco Referencial COBIT®

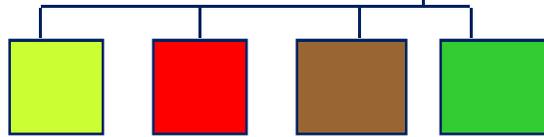
Procesos de TI



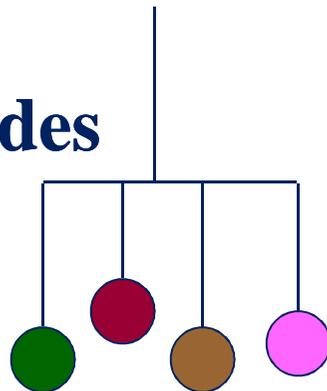
Dominios



Procesos



Actividades o tareas



Agrupación natural de procesos, normalmente corresponden a una responsabilidad organizacional

Conjuntos de actividades unidas con delimitación o cortes de control.

Acciones requeridas para lograr un resultado medurable
Las Actividades tienen un ciclo de vida mientras que **las tareas** son discretas.



Marco Referencial COBIT®

Su Orientación Natural



Dominios TI

- Administración
- Desarrollo
- Operaciones
- Control

Agrupamiento natural de procesos, usualmente correspondiendo a un dominio organizacional de responsabilidad

Procesos de TI

- Estrategia de TI
- Operaciones de computadora
- Respuesta a incidentes
- Aceptación de Pruebas
- Cambios de dirección
- Planes de contingencia

Serie de actividades unidas con cortes de control naturales

Actividades TI

- Registrar problemas
- Analizar
- Proponer soluciones
- Monitorear soluciones,
- Etc.

Acciones necesarias para alcanzar resultados medibles. Las actividades tienen un ciclo de vida, mientras que las tareas son discontinuas

Marco Referencial COBIT®



- **Planeación y Organización - PO**
(Planning and Organization)
- **Adquisición e implementación - AI**
(Acquisition and Implementation)
- **Entrega y Soporte - ES**
(Delivery and Support)
- **Monitoreo y Evaluación - ME**
(monitor and evaluate)

Marco Referencial COBIT®



Planeación y Organización

➤ Tópicos

- Abarca aspectos estratégicos y tácticos
- Contribuye con el logro de los objetivos del negocio
- Considera actividades de planificación, comunicación y administración de la visión estratégica

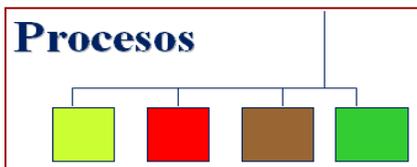
➤ Referencias

- ¿TI y la estrategia del negocio están alineadas?
- ¿La empresa está consiguiendo el uso óptimo de los recursos de TI?
- ¿Todos en la organización comprende los objetivos de TI?
- ¿Los riesgos de TI están comprendidos y administrados?
- ¿La calidad en TI es apropiada para las necesidad del negocio?

Marco Referencial COBIT®



Planeación y Organización



1. Definir un plan estratégico de TI
2. Definir la arquitectura de información
3. Determinar la dirección tecnológica
4. Definir la organización y relaciones de la Función TI
5. Administrar la inversión en TI
6. Comunicación de la directrices Gerenciales
7. Administración del Recurso Humano
8. Asegurar el cumplimiento d requerimientos externos
9. Evaluación de Riesgos
10. Administración de Proyectos
11. Administración de Calidad

Marco Referencial COBIT®



Adquisición e Implementación

➤ Tópicos

- Identificación, desarrollo o adquisición de soluciones de TI
- Implantación e integración en el proceso de negocio
- Cambios y mantenimiento de los sistemas existentes para garantizar la natural continuidad del ciclo de vida para estos sistemas

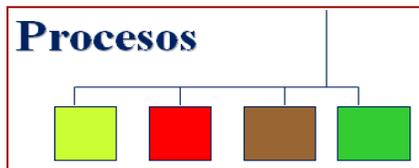
➤ Referencias

- ¿Los proyectos son soluciones que cubren las necesidades del negocio?
- ¿Los proyectos se entregan a tiempo y dentro del presupuesto?
- ¿Los sistemas trabajarán apropiadamente cuando se implementan?
- ¿Los cambios se ejecutaron sin interrumpir las operaciones en curso de la empresa?

Marco Referencial COBIT®



Adquisición e Implementación



1. Identificación de soluciones
2. Adquisición y mantenimiento de SW aplicativo
3. Adquisición y mantenimiento de arquitectura TI
4. Desarrollo y mantenimiento de Procedimientos de TI
5. Instalación y Certificación de sistemas
6. Administración de Cambios

Marco Referencial COBIT®



Entrega y Soporte

➤ Tópicos

- Prestación efectiva de los servicios requeridos (operaciones tradicionales, seguridad y continuidad, capacitación, etc.)
- Procesos de soporte necesarios
- Procesamiento real de los datos por los sistemas de aplicación

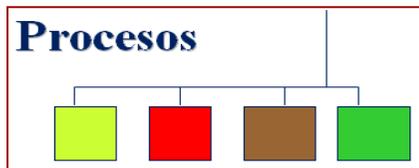
➤ Referencias

- ¿Los servicios de TI están acorde con las prioridades del negocio?
- ¿Los gastos de TI son optimizados?
- ¿Existe seguridad en el ambiente?
- ¿Existe integridad, disponibilidad, confiabilidad en la información?

Marco Referencial COBIT®



Entrega y Soporte



1. Definición del nivel de servicio
2. Administración del servicio de terceros
3. Administración de la capacidad y el desempeño
4. Asegurar el servicio continuo
5. Garantizar la seguridad del sistema
6. Identificación y asignación de costos
7. Capacitación de usuarios
8. Soporte a los clientes de TI
9. Administración de la configuración
10. Administración de problemas e incidentes
11. Administración de datos
12. Administración de Instalaciones
13. Administración de Operaciones

Marco Referencial COBIT®



Monitoreo y Evaluación

➤ Tópicos

- Evaluar regularmente todos los procesos de TI para determinar su calidad y el cumplimiento de los requerimientos de control
- Seguimiento de la gerencia sobre los procesos de control de la organización
- Garantía independiente provista por la auditoría interna y externa u obtenida de fuentes alternas

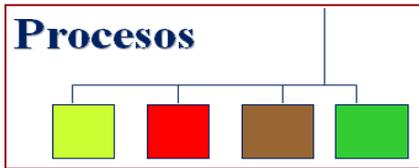
➤ Referencias

- ¿El rendimiento de TI puede ser medido y los problemas pueden ser detectados a tiempo?
- ¿Las áreas críticas están operando adecuadamente?

Marco Referencial COBIT®



Monitoreo y Evaluación



1. Seguimiento de los procesos
2. Evaluación de lo adecuado del control Interno
3. Obtener aseguramiento independiente
4. Proveer una auditoría independiente



Marco Referencial COBIT®

Como se relacionan



- ➔ Datos
- ➔ Aplicaciones
- ➔ Infraestructura
- ➔ RRHH

- ➔ Planeación y Organización
- ➔ Adquisición e Implementación
- ➔ Entrega y Soporte
- ➔ Monitoreo y Evaluación

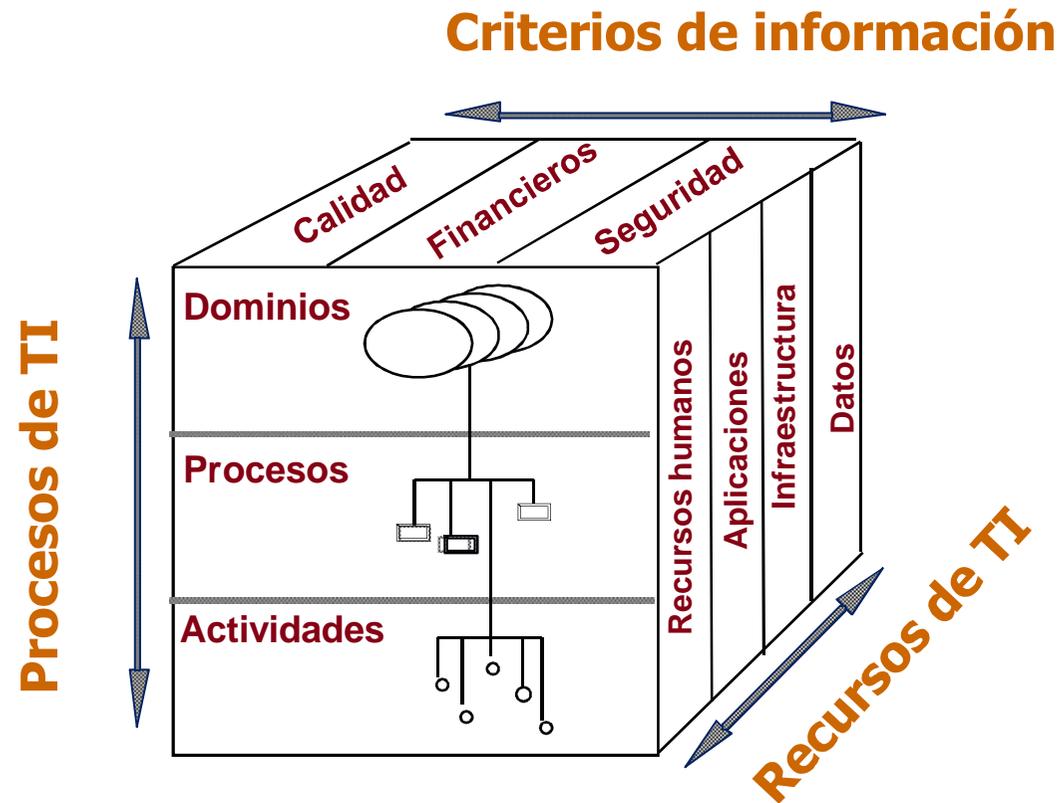
- ➔ Eficacia
- ➔ Eficiencia
- ➔ Confidencialidad
- ➔ Integridad
- ➔ Disponibilidad
- ➔ Cumplimiento
- ➔ Confiabilidad

Marco Referencial COBIT®



Guías de Aplicación COBIT®

Los componentes de un ambiente TI



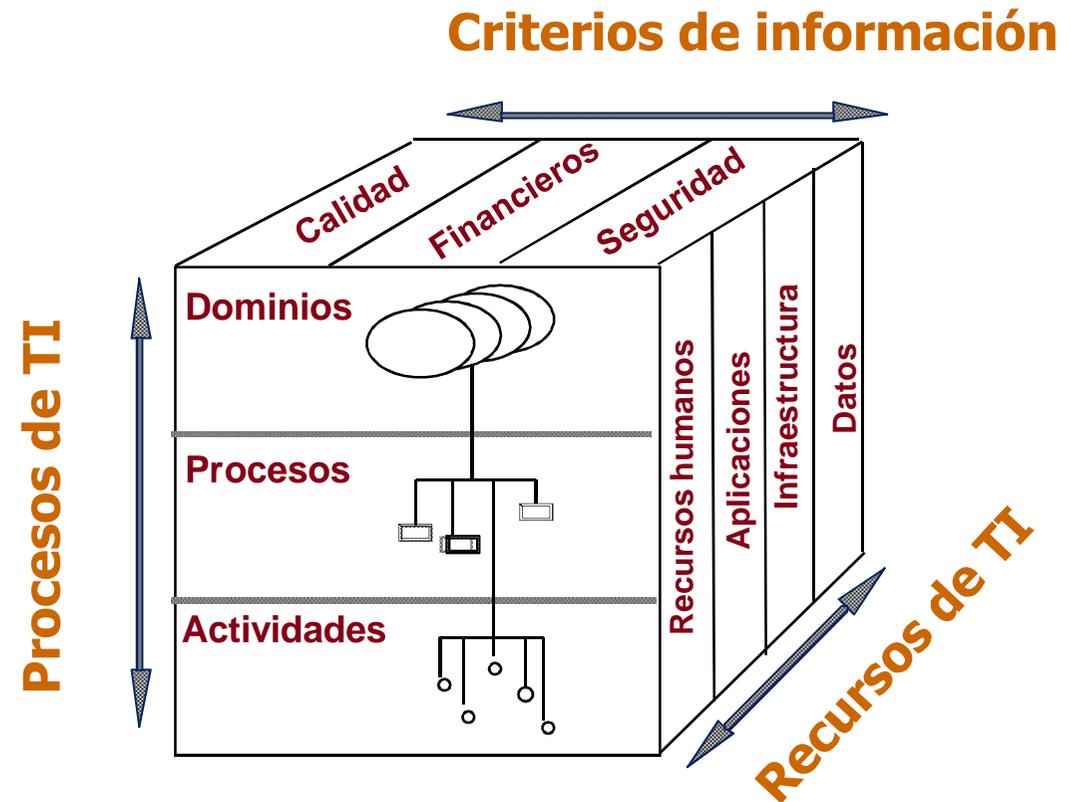
El cubo de COBIT

Guías de Aplicación COBIT®

Perspectivas diferentes - Enfoques diferentes

Para Directores

Pueden interesarse en un enfoque de calidad, seguridad o fiduciario (traducido por el marco referencial en siete requerimientos de información específicos)

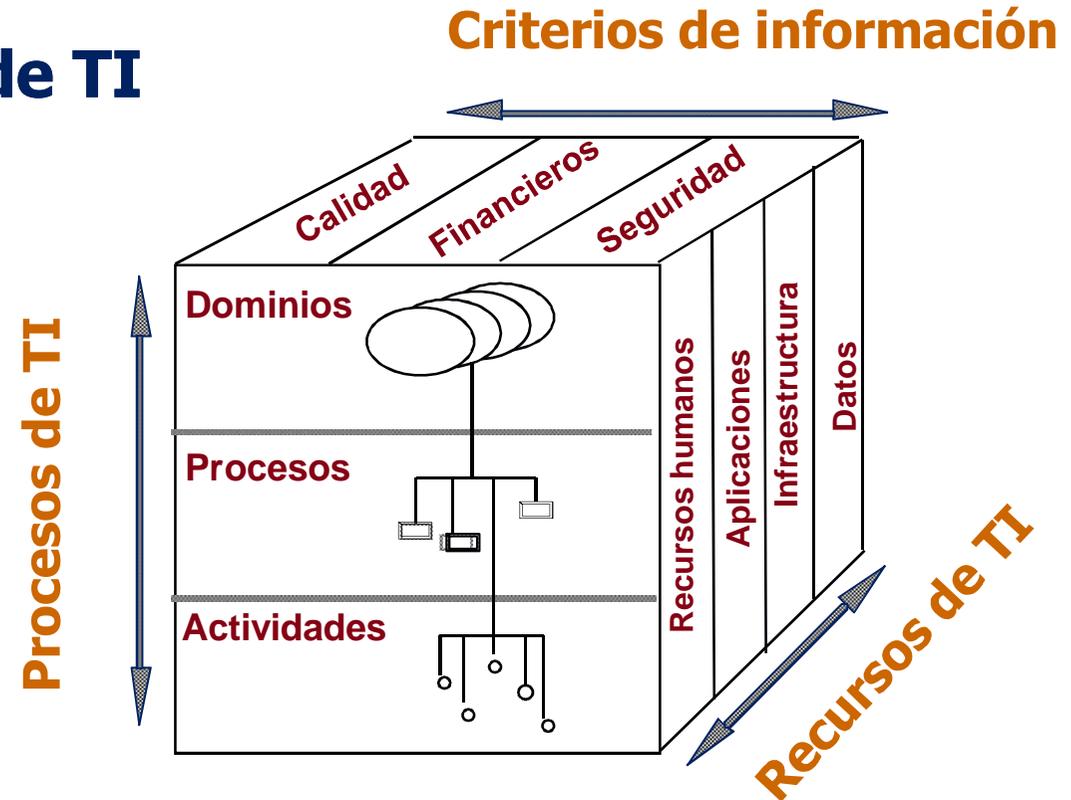


Guías de Aplicación COBIT®

Perspectivas diferentes - Enfoques diferentes

Para un Administrador de TI

Un Administrador de TI puede desear considerar recursos de TI por los cuales es responsable



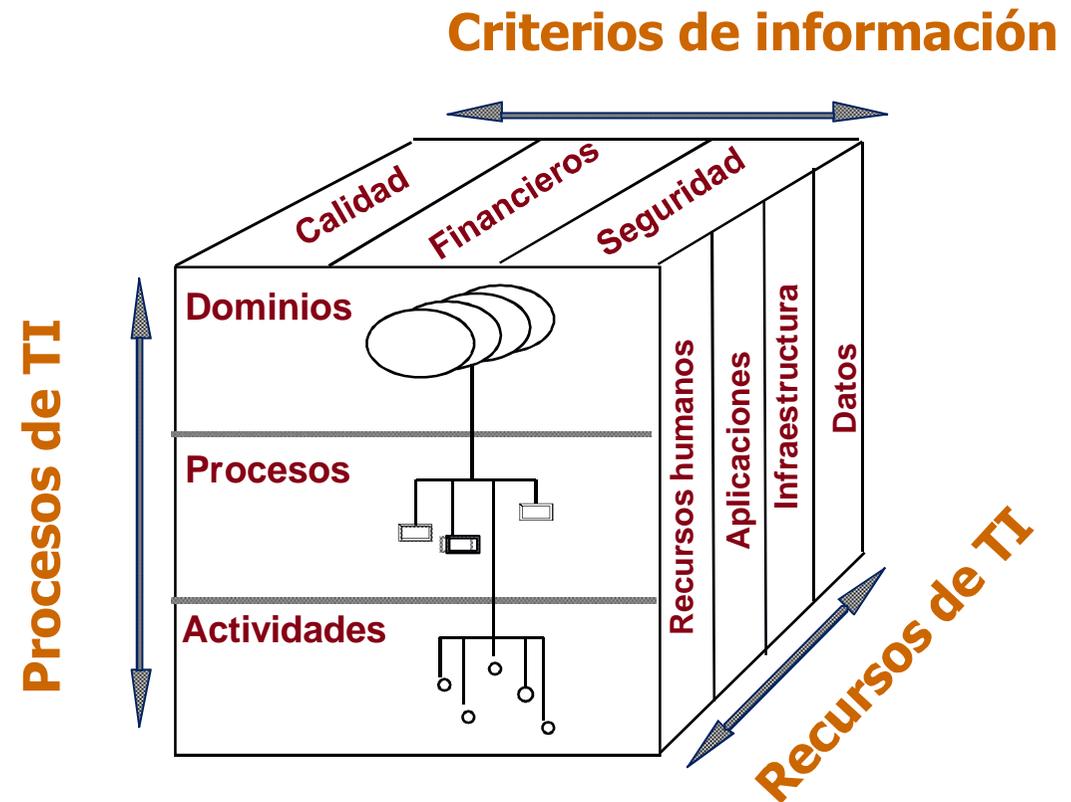
Guías de Aplicación COBIT®

Perspectivas diferentes - Enfoques diferentes

Para Propietarios de procesos o Auditores

Propietarios de procesos, especialistas de TI y usuarios pueden tener un interés en procesos particulares

Los auditores podrán desear enfocar el marco referencial desde un punto de vista de cobertura de control



Productos Importantes del COBIT®

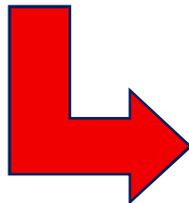
Guías de Auditoría

Relación guías de auditoría y Objetivos de Control

➤ **Obtener un entendimiento**

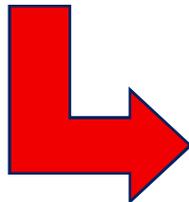
Colecte información de respaldo del negocio sobre riesgos, infraestructura, etc.

➤ **Evaluar la adecuación de controles**



Objetivo de el Control contrastado para verificar que los controles ya implementados son pertinentes para el negocio y la administración conoce sobre su vigencia

➤ **Asegurar el cumplimiento**



Objetivo de Control contrastado para probar y/o medir si los controles están implementados, y que los objetivos de control están presentes y operando satisfactoriamente

➤ **Substanciar el Riesgo**

Respalde objetivos del negocio faltantes, perdidos, etc., debido a la ausencia de un adecuado control

¿Preguntas?



Gracias



Freddy Landivar, CRISC CISA
freddylandivar@gmail.com