

Minuta del Chat N° 30 – 2005

CLAIN - FELABAN

TEMA	AUDITORIAS A PROVEEDORES DE SERVICIOS DE COMUNICACIONES Y ASPECTOS RELACIONADOS.		
FECHA	04/05/05		
DURACION	1:05		
MODERADORES	Cosme Belmonte y Ricardo Elías		
ASISTENTES			
NOMBRE	APODO	ENTIDAD	PAIS
Silvia Cabrera Sánchez	Silvia	Banco Ganadero	Colombia
william Abril	William	Banco Popular	Colombia
oscar quintero	oscarq	Banco Popular	Colombia
Luiz Ocko	Luiz Ocko	Banco Itau	Brasil
Carlos Caro	ccarog	carlos.caro@ripley.com.pe	Perú
Eduardo ojeda	eojeda	eojeda@bdd.cl	Chile
biviana velez	corfivalle	bvelez@corfivalle.com.co	Colombia
Dario Moreno Calderon	Dario	Banco Popular	Colombia
Cosme Belmonte y Ricardo Elías	Cosme y Ricardo	Banco de la Nación Argentina	Argentina
Martha Lucía Urrego C.	felaban	Felaban	Colombia
Ximena Luna	XimeLu	Produbanco	Ecuador
Alvaro Cuadros	alvarobme	Banco Mercantil	Bolivia
Yolfer Hernandez	Yolfer	yolferh@yahoo.es	Perú

Siendo las 09:20 horas AM (hora Colombia) se comienzan a conectar los integrantes del Comité.

Alcanzándose la lista de los asistentes que previamente se indicaron.

El Chat comienza a las 10:10 horas AM (hora Colombia) presentando una a una las preguntas que se habían enviado en la comunicación preliminar.

INTRODUCCION:

Es común que las Instituciones Bancarias cuenten con una cantidad más o menos importante de Sucursales en ubicaciones geográficas alejadas de su Casa Central, y debido a necesidades de mantener consolidada su operación y/o brindar un mejor servicio a sus clientes deban contar con una Red de Comunicaciones que vincule todas sus filiales.

En aquellas cuyo vínculo no es a través de líneas telefónicas punto a punto, requirieren de la participación de un proveedor con equipamiento dedicado a tal fin.

En los programas de Auditoría de Sistemas resulta necesario auditar a dicho proveedor, debido a las particularidades del servicio del proveedor involucrado es que nos parece conveniente intercambiar las distintas experiencias al respecto, como también aquellas relacionadas con la actividad con sucursales y sus controles.

Este enfoque también debería alcanzar a los correspondientes a Tarjetas de Crédito, Redes de Cajeros Automáticos, etc.

Finalmente el Chateo se enfocó en:

- 1) ¿Existen regulaciones, que obligan a las Áreas de Auditoría de Sistemas auditar a sus proveedores ?
- 2) ¿El área de Auditoría de Sistemas audita a dichos Proveedores ?

- 3) ¿Se exige convenio de confidencialidad con el Proveedor ?
- 4) ¿Dichas auditorías pueden llegar a un nivel de detalle conveniente, ó se limita a información básica que suministra el proveedor ?
- 5) ¿El proveedor adopta una actitud abierta a los requerimientos de Auditoría ?
- 6) ¿Hasta que nivel de información se obtiene ?. Topología, equipamiento incluido, modelos, software involucrado, cantidad de personal, capacitación del personal, aspectos de seguridad lógica/física, etc. ?
- 7) ¿Los Entes Rectores auditan a dichos proveedores ?
- 8) ¿Los proveedores cuentan con servicios de Auditoría externa ?
- 9) ¿Dichos informes producidos por el Ente Rector ó Auditorías externas son suministrados a los Bancos ?
- 10) ¿El Ente Rector le acepta a la Auditoría de Sistemas del Banco como suficientes los informes del punto 9) ?
- 11) ¿El Proveedor suministra facilidades que posibiliten verificar el cumplimiento de los niveles de servicio contratados con el mismo ?. ¿Cuales ?
- 12) ¿La porción de red Wan asignada al Banco por el proveedor está protegida ?
- 13) ¿Que facilidades posee el Banco para proteger la Red Wan, atento que se trata de una red de terceras partes y además compartida ?
- 14) ¿Que tipos de vínculos utilizan: frame relay, X25, etc. ?
- 15) ¿Para dar el servicio en Sucursales el Banco cuenta con servidores con procesamiento por sucursal ó regional, ó está totalmente centralizado ?
- 16) ¿Que esquema de contingencia de vínculos con sucursales posee el Banco ?
- 17) ¿El Banco posee un área que efectúa el monitoreo de la Red Wan ó lo efectúa sólo el proveedor?

Se adjunta resumen ejecutivo del Chateo que incluye preguntas y un resumen condensado de las respuestas.

Se dio por cerrado el Chat N° 30 a las 11:15 AM (hora Colombia), agradeciéndose la participación de todos los integrantes, quedando pendiente el informar el contenido del Chat en la comunidad virtual del CLAIN en el sitio de FELABAN.

CONCLUSIONES GENERALES:

Las regulaciones para las auditorías a proveedores de servicios de comunicaciones y aspectos relacionados, observan un espectro variado dependiendo en parte de la reglamentación dispuesta por los entes de contralor de cada país. Dentro de este marco, se encuentra el caso de Chile donde se detecta un importante grado de regulación, en razón que las exigencias del ente rector obligan a las auditorías a llegar a un suficiente nivel de detalle, con el objetivo de tener conformidad respecto al buen manejo del riesgo operacional por parte del proveedor, efectuando auditorías conjuntas las entidades financieras que tienen un proveedor común. Así también se encuentran otras situaciones en la región donde las regulaciones del país no son tan estrictas y esto dificulta la receptividad del proveedor a ser auditado. Independientemente de ello, en todos los casos, las áreas de auditoría efectúan visitas a los proveedores más representativos y/o calificados como críticos. La diferencia esta dada en cuanto a los niveles de detalle y de receptividad de los proveedores ante el pedido de las auditorías efectuadas por los Bancos

En general se puede decir que los países más avanzados en éste aspecto son aquellos que cuentan con disposiciones taxativas emitidas por el Ente regulador que requiere dicha actividad.

En cuanto a los aspectos de seguridad de los vínculos suministrados, estos se encuentran protegidos, en un ambiente controlado mediante distintos sistemas de detección. El tipo de vínculo mas utilizado es Frame Relay , el procesamiento operativo en su mayoría es centralizado, conteniendo cada solución distintos esquemas de contingencia y en todos los casos las entidades cuentan con sectores para el monitoreo de su red Wan.

RESUMEN EJECUTIVO CHAT N° 30 – 2005

04/05/05

1) ¿Existen regulaciones, que obligan a las Áreas de Auditoría de Sistemas auditar a sus proveedores ?

XimeLu

No existe regulación sobre este aspecto en Ecuador.

corfivalle

Buenos días, en Colombia tampoco existen que yo sepa.

Dario

Para el caso del banco popular de Colombia, no. Eso se da por política interna de la compañía y además cuando se hace la contratación debe dejarse expreso en el contrato de prestación de servicios que el banco se reserva el derecho de efectuar revisiones periódicas (auditorias) a fin de evaluar cumplimiento.

Cosme y Ricardo

La Circular A-3198 del BCRA establece que deben suscribirse contratos formales sobre el alcance y las condiciones de las actividades, donde deben establecerse claramente la “no existencia” de limitaciones para el ente de contralor y a la realización de auditorías periódicas en las instalaciones del proveedor.

¿Cómo es en Chile? Eduardo.

eojeda

En Chile la el regulador, Superintendencia de Bancos, en el ámbito de la administración del riesgo operacional, requiere a las instituciones financieras disponer de información respecto al buen manejo de riesgos operacionales en las empresas que prestan servicios relevantes, en lo principal, seguridad de la información, planes de continuidad de negocios, del proveedor, esta auditoria puede ser efectuada con recursos del banco o contratada con auditores externos.

Luiz Ocko

O Banco Central define no Manual de Supervisão Bancária que deve ser estabelecido um procedimento para assegurar a aderência contínua aos termos firmados no contrato.

2) ¿El área de Auditoría de Sistemas audita a dichos Proveedores ?

Dario

Si, mediante auditoria institucional

XimeLu

No existen auditorías formales, si se efectúan visitas a los proveedores más representativos, por parte del oficial de seguridad informática y el auditor informático

corfivalle

Como dice Dario por política interna la auditoria realiza evaluaciones periódicas a los proveedores calificados como críticos.

Cosme y Ricardo

Si, solo a proveedores críticos.

ejeda

En Chile durante unos años efectuamos auditorias en forma conjunta con otras instituciones financieras, cuando teníamos proveedores comunes, hoy estamos girando hacia la exigencia de auditorias externas del tiempo SAS70.

Luiz Ocko

Sim.

3) ¿Se exige convenio de confidencialidad con el Proveedor ?

Dario

Si, dentro de los contratos.

XimeLu

El proveedor firma un convenio de confidencialidad desde el inicio de la relación con el Banco.

Cosme y Ricardo

La Circular A-3198 del Banco Central de la República Argentina establece que en los contratos a suscribirse deben incluirse compromisos de confidencialidad.

ejeda

En el caso de nuestro banco y entiendo es un estándar de la industria en Chile, los contratos incluyen cláusulas de confidencialidad y responsabilidad ante la divulgación de información, para nosotros es esencial pues tenemos información sujeta a secreto bancario.

Luiz Ocko

Sim, o termo de confidencialidade é parte do contrato de prestação de serviços.

4) ¿Dichas auditorías pueden llegar a un nivel de detalle conveniente, ó se limita a información básica que suministra el proveedor ?

Dario

Se llega al nivel que se requiere sin inconveniente del proveedor, aunque algunas veces con la información inicial que suministra el proveedor es suficiente.

corfivalle

Muchas veces se limita a entrevistas con el proveedor.

XimeLu

Solamente hemos realizado visitas a ciertos proveedores críticos, no hemos realizado auditorías a los proveedores. En los casos en que hemos realizado visitas, no hemos tenido problemas, sin embargo, el proveedor mantiene un sigilo en temas más específicos.

Cosme y Ricardo

Dependiendo del proveedor se obtiene mayor o menor nivel de detalle, a satisfacción de las partes.

ejeda

Las auditorias practicadas en Chile a los proveedores llegan al nivel de detalle, nuestro objetivo es tener conformidad respecto al buen manejo del riesgo operacional por parte del proveedor, lo que por lo tanto incluye la evaluación del control interno del proveedor, entre otros, políticas de selección y mantención de personal, seguridad de instalaciones, software y equipos, planes de contingencia, pruebas de planes de

contingencia, realización de ataques a las instalaciones, en caso de tener acceso por intermedio de la red a los computadores del proveedor, etc.

alvarobme

En el caso de Bolivia no son auditorias completas, son mas bien visitas en las que se tratan de identificar el riesgo presente.

Luiz Ocko

As auditorias estão previstas em contrato e podem chegar a um nível de detalhe conveniente.

5) ¿El proveedor adopta una actitud abierta a los requerimientos de Auditoría ?

Dario

Si, a los que hemos auditado.

corfivalle

Si, en la mayoría de los casos.

alvarobme

Coincido con XimeLu, tenemos mas bien cierto sigilo y reserva en cuanto a su información.

ejeda

Algo más, también en forma periódica hacemos evaluación de la situación financiera del proveedor, en nuestro caso la evaluación se solicita al área de análisis financiero del banco, también verificamos regularmente el cumplimiento de pagos previsional, por parte del proveedor.

Cosme y Ricardo

Dependiendo del proveedor el mismo presta amplia colaboración, ó se limita a suministrar información escrita.

Luiz Ocko

Sim.

6) ¿Hasta que nivel de información se obtiene ?. Topología, equipamiento incluido, modelos, software involucrado, cantidad de personal, capacitación del personal, aspectos de seguridad lógica/física, etc. ?

Dario

Depende del tipo de evaluación, se llega al nivel que se requiera .

alvarobme

Realmente básico.

Luiz Ocko

São obtidas informações referentes à topologia, softwares utilizados, capacitação do pessoal, etc.

ejeda

Nuestra experiencia es que sí, es importante mencionar que la Superintendencia nos obliga a incluir en los contratos con proveedores cláusulas de auditoria, por lo tanto eso está claro desde el inicio de la relación. Lo que ha tenido fuerza es hacer auditorias conjuntas, pues no es lo mismo responder a un banco pequeño, que a un banco grande o a todos los bancos que son clientes del proveedor.

alvarobme

En general Topología y software.

Cosme y Ricardo

En líneas generales se suministra información básica, sin detalles de significación.

6 bis) Eduardo tienen ustedes en Chile, un acuerdo entre Bancos para hacer auditorías conjuntamente?

alvarobme

Dario, estas auditorías las canalizan por su asociación bancaria?

ejeda

Sí lo tenemos, y en el pasado hemos efectuado auditorías en conjunto, pero como les mencioné anteriormente, hoy estamos avanzando en la idea de requerir a los proveedores auditorías practicadas por auditores externos del tipo SAS 70. alvarobme, me imagino que me preguntas a mí, ejeda, efectivamente, las canalizamos por intermedio de la asociación bancaria, tenemos un comité de contralores de la banca, (auditores internos), y es ahí donde trabajamos estos temas en conjunto.

Cosme y Ricardo

En Argentina las Asociaciones Bancarias están trabajando en forma conjunta para auditar a proveedores comunes (Ej. Red Banelco y Link), con la anuencia del Banco Central.

7) ¿Los Entes Rectores auditan a dichos proveedores ?

Dario

Si aunque solamente desde el punto de vista financiero y administrativo y según el ámbito los visita la el ente regulador, superbancaria, supervalores, superintendencia de sociedades entre otros.

alvarobme

Solamente desde el punto de vista financiero. El ente encargado es la Superintendencia de Bancos.

Cosme y Ricardo

Sí en aspectos técnicos, además del financiero y administrativo.

Luiz Oeko

Sim, inclusive os procedimentos estão previstos no manual de supervisão bancária do Banco Central do Brasil.

ejeda

En Chile el ente regulador le exige a los bancos tener la información, existen ciertas empresas de apoyo al giro bancario que sí las visitan, como por ejemplo administradores de tarjetas de crédito y débito bancario, red de cajeros automáticos.

8) ¿Los proveedores cuentan con servicios de Auditoría externa en el área de TI?

Dario

Si en Colombia se denomina Revisoria Fiscal, aunque también se tiene Auditoría Externa por contratos aprobados por las Juntas Directivas.

Luiz Oeko

Sim.

Cosme y Ricardo

Sí. En los Proveedores vinculados a la actividad Bancaria está exigido. Ej.: Redes de Home Banking, etc. En otros es parte de un esquema institucional propio.

alvarobme

Sí.

corfivalle

Los proveedores externos del sector real no tienen obligatoriedad de la existencia de auditorías externas o revisoría fiscal.

ejeda

Los relevantes sí las tienen, redes de cajeros automáticas, administradores de tarjetas, depósitos central de valores, administrador de transferencias electrónica., etc.

9) ¿Dichos informes producidos por el Ente Rector ó Auditorías externas son suministrados a los Bancos ?

alvarobme

No, no existe una regulación que obligue a esto.

Dario

No, solo si hay requerimiento por parte del banco

corfivalle

No.

XimeLu

No.

Luiz Ocko

Estes informes não são enviados porem, pode ser solicitados pelo Banco.

ejeda

En nuestro caso, solo si las requerimos, en general las proporcionan.

Cosme y Ricardo

En general NO, hay información que permiten lectura en el proveedor.

10) ¿El Ente rector le acepta a la Auditoría de Sistemas del Banco como suficientes los informes del punto 9) ?

Dario

No, también en ocasiones solicitan los soportes e informes técnicos a nivel interno.

Luiz Ocko

Sim.

ejeda

Lo evalúan respecto al alcance y calidad, y si pasa esta evaluación lo aceptan.

Cosme y Ricardo

Aceptarían un informe presentado por el conjunto de Bancos a través de las Asociaciones Bancarias. Con el alcance y objetivos de control previamente acordados con el Ente Rector.

11) ¿El Proveedor suministra facilidades que posibiliten verificar el cumplimiento de los niveles de servicio contratados con el mismo ?. ¿cuales ?

Dario

Si, existen reportes mensuales que indican el servicio prestado, así como las interrupciones o demoras en el mismo.

Luiz Ocko

Sim, existe Acordo de Nível de Serviço firmado com o prestador de serviço, que tem como responsabilidade fornecer relatórios mensais com os índices de performance definidos.

XimeLu

Se realiza un monitoreo permanente de los equipos y niveles de servicios de los proveedores.

Cosme y Ricardo

Sí. Suministra información y elementos de monitoreo on-line, como también en algunos casos acceso on-line para reportes de problemas (Particularmente en proveedores de servicios de comunicaciones).

ejeda

Nuestros contratos contienen cláusulas que obligan al proveedor a proporcionar la información, los accesos y facilidades necesarias para verificar los niveles de calidad de servicio, es importante que estos niveles estén bien definidos en los contratos.

12) ¿La porción de red Wan asignada al Banco por el proveedor está protegida ?**Luiz Ocko**

Sim.

XimeLu

Sí, existe un esquema de vlans con algunos proveedores y con otros se maneja Frame Relay.

Cosme y Ricardo

Si.

Dario

Sí, con un sistema de detección de intrusos, firewall, y proxy (symantec web security).

ejeda

Si.

13) ¿Que facilidades posee el Banco para proteger la Red Wan, atento que se trata de una red de terceras partes y además compartida ?**Luiz Ocko**

Sistemas de Firewall e Intrusión Detection System – IDS.

Dario

La red wan del banco no es compartida, los pocos accesos que se tiene para personal externo se tiene controlado mediante sistema de detección de intrusos, firewall, y proxy (symantec web security).

XimeLu

Se manejan esquemas de seguridad en capas.

Cosme y Ricardo

Se cuenta con routers armando una VPN con IpSec.

ejeda

Continuo, y auditoria de sistemas lo verifica periódicamente, ya sea con recursos internos o contratando especialistas externos.

14) ¿Que tipos de vínculos utilizan: frame relay, X25, etc. ?**Dario**

Tcp/ip.

XimeLu

Utilizamos frame relay, metro ethernet.

Luiz Ocko
Frame Relay.

Cosme y Ricardo
Fundamentalmente Frame Relay.

15) ¿Para dar el servicio en Sucursales el Banco cuenta con servidores con procesamiento por sucursal ó regional, ó está totalmente centralizado ?

XimeLu
Centralizado.

Luiz Ocko
O serviço de processamento é centralizado.

Cosme y Ricardo
Casa Sucursal cuenta con un Servidor que vincula la misma con el sistema Central. Dicho servidor puede trabajar desconectado del sistema Central pero con operatividad restringida.

corfivalle
En la operativa del negocio centralizado, pero para correo manejamos servidor por regional.

Dario
Está centralizado en intranet, internet, correo electrónico, antivirus y descentralizado en servicio bancario y plataforma.

ejeda
Centralizado, distribuido, esto quiere decir que existen ciertos aspectos que se verifican y registran a nivel del servidor local y otras a nivel centralizado.

16) ¿Que esquema de contingencia de vínculos con sucursales posee el Banco ?

XimeLu
Poseemos dobles enlaces con diferentes proveedores, en las oficinas más importantes o concentradoras.

Luiz Ocko
Temos links alternativos para o caso de queda na comunicação.

Dario
Copias de seguridad en el sitio y externas, tanto a nivel local como centralizado y planes de contingencia con mediciones de tiempo.

Cosme y Ricardo
Se cuenta con vínculos telefónicos que son activados por el Router de la Sucursal en forma automática en modo dial up y es atendido por equipos Access Server. Para ello cada Servidor de Sucursal posee, además un MODEM.

ejeda
Para fallas de energía, tenemos grupo electrógeno, para comunicaciones enlaces duplicados, y si todo falla, traslado a oficina más cercana, tenemos capacidad de procesar fuera de línea en la oficina

17) ¿El Banco posee un área que efectúa el monitoreo de la Red Wan ó lo efectúa sólo el proveedor?

XimeLu
El Banco tiene un centro de procesamiento que efectúa el monitoreo continuo de comunicaciones.

Dario

El banco posee un área de telecomunicaciones y seguridad de la información quienes monitorean permanentemente la Red.

Luiz Ocko

Monitorizamos a WAN em conjunto com o proveedor.

corfivalle

Contamos con enlaces duplicados adicional a la contingencia que nos presta el proveedor.

Cosme y Ricardo

Sí. Dentro del área de Sistemas, existe un sector responsable de lo atinente a la Red WAN, el que cuenta con equipamiento al efecto, y mantiene contacto con el proveedor.

ejeda

El banco tiene un área que efectúa el monitoreo, para tráfico externo también contamos con los servicios de un proveedor que vigila permanentemente.