Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de posgrado

Tema
Aplicación de Métricas de Seguridad Informática

Título

Implementación de Métricas de Seguridad Informática en Instituciones Bancarias de Tamaño Medio que operan en Argentina

Autor: Ing. Sis. Emiliano José Fausto
Director de tesis: Dr. Raúl Saroka

Año
2011

Cohorte
2009

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Nombres y Apellido: Emiliano José Fausto
Número de documento: 29.438.583

Resumen

El trabajo se centra en Métricas de seguridad informática que responden a los niveles Estratégico, Táctico y Operativo. Consta de una primera parte teórica, que analiza la bibliografía disponible del tema a nivel internacional, y luego una segunda parte, que presenta un análisis descriptivo de implementaciones en entidades bancarias-financieras del mercado Argentino.

Para ello se realizó un análisis exhaustivo de los distintos estándares, normas, libros y artículos que tratan sobre el tema de Métricas de Seguridad Informática, como así también lo vinculado al área de seguridad informática en general (principalmente en el ámbito financiero-bancario). Algunos de estos indicadores, son considerados herramientas para el área de gerencia alta, y otros son útiles para el área de gestión media. Estos contribuirán a la toma de decisiones y la planificación de la seguridad informática basada en una mayor adhesión a los lineamientos del negocio.

Adicionalmente, se realizó un trabajo de campo con el objeto de observar la aplicabilidad real de las métricas de seguridad en tres entidades bancarias de tamaño medio que operan en Argentina, y se validó la factibilidad técnica y la utilidad real de las mismas.

En este trabajo se describen una serie de métricas de métricas de Seguridad Informática que aplican entidades financieras locales, para ejemplificar indicadores que apunten a los niveles estratégico, táctico y operativo, y su validación empírica en instituciones bancarias.

Tabla de contenidos

Declaración Jurada de origen de los contenidos 2

Resumen 3

Tabla de contenidos 4

Introducción 7

Antecedentes públicos sobre métricas de SI 9

Capítulo 1 19

Concepto de Métricas vinculadas a la Tecnología Informática 19

Evolución de las métricas 20

Utilidad de las métricas 21

Usuarios de las métricas 22

Capítulo 2 24

Métricas y su inserción en la empresa 24

Caso 1: El Tablero de Comando 24

Caso 2: British Airways 25

Capítulo 3 28

Aplicación en el ámbito de la Seguridad Informática 28

Cinco características de las buenas métricas de SI 29

Capítulo 4 31

La Seguridad Informática en las Entidades Financieras 31

¿Qué medir en una organización financiera/bancaria? 31

1) Cumplimiento Regulatorio y Marco Normativo 32

2) Gestión de Identidades 33

3) Seguridad de la Infraestructura Tecnológica 33

4.1 Cumplimiento Regulatorio y Marco Normativo 34

¿Qué tener en cuenta al momento de medir el Cumplimiento Regulatorio y Marco Normativo? 34

Métricas propuestas 35

4.2 Gestión de Identidades 39

¿Qué tener en cuenta al momento de medir la Gestión de Identidades? 40

Métricas propuestas 40

4.3 Seguridad de la Infraestructura Tecnológica 52

¿Qué hay que tener en cuenta al momento de medir la seguridad de la IT? . 52

Métricas propuestas 53

Capítulo 5 63

Trabajo de Campo 63

Indicadores ESTRATÉGICOS (Directorio) 64

Indicadores TÁCTICOS (Gerencias Medias) 75

Indicadores OPERATIVOS (Grupo de trabajo de Seguridad Informática) 92

Conclusiones 119

Recomendaciones 123

Bibliografía 125

Anexo I: Gestión de Identidades 127

Anexo II: Cumplimiento Regulatorio y Marco Normativo 133

Anexo III: Seguridad de la Infraestructura Tecnológica 143

Anexo IV: Comunicación “A” 4609 (Banco Central de la Rep. Argentina) 147

Anexo V: Sistema MEP (Medio Electrónico de Pagos) 148

Anexo VI: Método de Evaluación C.A.M.E.L. 150

Anexo VII: Comunicación “A” 5374 (Banco Central de la Rep. Argentina).....157

Introducción

Las entidades bancarias dependen cada día más de la tecnología para la realización de las actividades que dan sustento al negocio, y esta dependencia, cada vez mayor, es la que genera un gran desafío, puesto que siempre surgen nuevas amenazas y riesgos cuyo impacto sobre la organización podría ser muy perjudicial. En este marco de trabajo, la Seguridad Informática dentro de las entidades bancarias, forma parte integral de la competencia del área gerencial.

La carencia de los servicios de Tecnología Informática o Comunicaciones, para una entidad bancaria o financiera, es un impedimento total para la continuidad de su actividad laboral normal. Por otra parte, sería una gran pérdida de imagen y confiabilidad si parte, o toda, la información confidencial que maneja la entidad se viera comprometida, fuese accedida o modificada sin autorización (ya sea intencionalmente o no) por empleados del banco o por externos.

Es entonces que la Seguridad Informática cumple un rol fundamental en las entidades bancarias, y es así que está tomando cada vez mayor importancia en la administración de estas instituciones. Constituye una función imprescindible para asegurar la continuidad del negocio mediante la protección de los servicios de Tecnología Informática y Comunicaciones.

Dentro de las diferentes áreas de la entidad bancaria, el área de seguridad informática tiene una labor diaria que conlleva cierto trabajo operativo. Por ejemplo, realizar un análisis de los listados con cada uno de los accesos denegados a ciertos documentos restringidos. Este tipo de información, en general, no sirve a un gerente de área para tomar decisiones tácticas. Es por ello que a medida que la cantidad de controles de seguridad comenzaron a ser cada vez mayores, y el número de eventos de inseguridad informática dentro de las entidades bancarias creció sustancialmente, fue necesario adecuar el concepto de Métricas de Seguridad.

Los Indicadores de Seguridad están basados en el concepto análogo de los *Key Performance Indicators* (de ahora en adelante KPI) o también conocidos como Indicadores Clave de Desempeño.

Los KPI miden el nivel de desempeño de un proceso de negocio, de manera tal que se sepa de forma rápida si se está cumpliendo, o no, con el objetivo fijado. También se podría hablar de KPI como una métrica que mide el rendimiento de cierto componente tecnológico por ejemplo, el consumo en porcentaje de una memoria RAM computacional.[1]

De igual forma que los KPI miden el desempeño de objetos puntuales o de procesos de negocio complejos, los Indicadores Clave de Seguridad (también llamados *Key Security Indicators*, o por sus siglas KSI) miden el nivel de cumplimiento o no de determinados controles y procedimientos vinculados a la Seguridad Informática de la entidad; por ejemplo, algunos indicadores de seguridad son:

- Virus detectados y eliminados a tiempo,
- Ataques externos neutralizados (realizados por fuera del perímetro de la red),
- Tiempo de respuesta promedio para la solución de un incidente de Seguridad Informática (que cause la detención de un servicio crítico).

También existen indicadores más complejos, cuyo cálculo involucra información proveniente de distintas aplicaciones, sistemas operativos y entornos de trabajo. Estos últimos indicadores son los más interesantes para el área gerencial, puesto que en conjunto y combinados muestran información que da cuenta de la situación de un aspecto del negocio o área, pero resumido en un solo indicador.

[1] Se sabe que si el consumo de la misma llega al 100%, el sistema operativo comenzará a realizar un proceso de *Swapping*, el cual implica un intercambio de datos repetitivamente entre el disco rígido y la memoria RAM, un concepto vinculado al de la memoria virtual. El problema es que el rendimiento de los procesos que corren en el equipo se va a ver afectada de manera negativa, puesto que la velocidad que tiene la memoria RAM (digital) no es la misma que la del disco rígido (mecánica).

A nivel teórico, este trabajo tiene como propósito revisar la mayor parte de la documentación existente al momento sobre Métricas de Seguridad Informática y presentar de manera general las fortalezas y limitaciones de cada publicación.

Posteriormente, se realizará un relevamiento de campo en entidades financieras argentinas, para conocer a qué nivel se aplican las métricas de seguridad en la actualidad.

Finalmente, otro aporte del presente trabajo es llenar parte del vacío que existe en el campo disciplinar a nivel práctico, brindando casos concretos sobre la implementación de indicadores del área de Seguridad Informática a distintos niveles organizativos. Dichas métricas tienen base en la implementación empírica de la métrica por parte de la entidad, y en la realización de un enlace con la documentación analizada, como así también de la experiencia propia del maestrando.

Antecedentes públicos sobre métricas de SI

A medida que se fue difundiendo el uso de métricas clave en el campo de la Seguridad Informática y en la Seguridad de la Información en general, es que los organismos más reconocidos internacionalmente publicaron documentos, estándares e incluso guías de mejores prácticas para la implementación de controles y mediciones vinculados a las métricas de Seguridad.

Del BS7799 a la serie de estándares ISO 27000[2]

Hace algunos años no existía la tendencia de certificar procesos, o sistemas de gestión. Por ello, la ISO 9000 vino a redefinir en el año 2000 la certificación de los sistemas de gestión de calidad, mediante la norma ISO 9001:2000, donde se incorpora el modelo PDCA (*Plan–Do–Check–Act*, por sus siglas en inglés).

[2] http://seguinfo.wordpress.com/2007/09/02/la-evolucion-del-estandar-iso-27001/

Hasta antes del año 2005, no existía una norma ISO que permitiera certificar a una organización en cuanto a sus prácticas y políticas de Seguridad Informática; las únicas normas utilizadas en ese momento eran las inglesas (BS) y españolas (UNE). Hasta el 2005, el estándar más conocido en el entorno de seguridad informática era el ISO 17799, pero con la limitación de ser un "código de prácticas" (*Information technology –Security techniques– Code of practice for information security management*). En el momento que se publica su última revisión, se anuncia el desarrollo de una serie de estándares ISO 27000, dedicada exclusivamente a la seguridad de la información. Con esto se le da un nuevo alcance a la seguridad, porque no sólo es llevar una metodología de mejores prácticas, sino establecer un estándar certificable de forma similar al ISO 9000. El primero de esa serie en publicarse fue el ISO 27001.

El estándar ISO 27001 nace como consecuencia de años de trabajo, como lo demuestra la siguiente cronología:

Año	Publicación / Suceso
1980	Estándar de Shell
1985	Código de práctica (PD0003)
1993	Código de prácticas
1993	Grupo industrial del trabajo
1995	BS 7799 – 1
1998	BS 7799 – 2
1999	Revisión BS 7799 – 1 y BS 7799 – 2
2000 (Diciembre)	ISO/IEC 1779:2000
2001	Revisión BS 7799 – 2
2002 (Septiembre)	Revisión 7799 – 2
2004 (Marzo)	UNE 71502
2005 (Junio)	ISO/IEC 17799:2005
2005 (Octubre)	ISO/IEC FDIS 27001:2005
2007 (Abril)	ISO/IEC FDIS 27003:2007

Los aportes más importantes a la familia ISO 27001 vienen, principalmente, de los

estándares británicos BS7799-1 (*Information Technology. Code of Practice for Information Security Management*) y BS7799-2 *(Information Security Management Systems – Specification with Guidance for Use*).

La familia completa de la ISO 27000 está formada por los estándares mencionados a continuación:

ISO/IEC	Descripción
27000	Vocabulario y definiciones (*Information Technology – Information Security Management – Fundamentals and Vocabulary).*
27001	Especificación de la estructura metodológica (basada en el BS7799-2:2002) (*Information Technology – Security Techniques- Information Security Management Systems – Requirements).*
27002	Código de prácticas (*Code of Practice for Information Security Management)*. Actualmente ISO/IEC 17799:2005, publicado el 15 de junio de 2005
27003	Guía de implementación (ISMS *Implementation Guidance).* Publicado el 1ro de Febrero del 2010
27004	Métricas y medidas (*Information Security Management Measurement*). En desarrollo
27005	La administración del Riesgo (Basado en BS 7799 – 3) (*Information Security Risk Management,* basado e incorporado a ISO/IEC 13335 MICTS part 2). En desarrollo
27006	Requerimientos para organismos de acreditación de Sistemas de Gestión de Seguridad de la Información (*Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems).*

Las certificaciones han pasado a ser necesarias, para demostrar la existencia de un sistema de gestión de seguridad de la información que asegure procesos consistentes. En el campo de la seguridad informática, estas buenas prácticas brindan una ventaja competitiva a las organizaciones que las implementan, y se mejora el aseguramiento de todos los sistemas de información que cada día

cobran una mayor importancia para sustentar la toma de decisiones y salvaguardar así el activo más importante de una organización: la información.

SANS (System Administration, Networking, and Security Institute)

Shirley Payne liberó en junio del 2006 un breve documento[3] en el cual cubrió (según la óptica del SANS) los aspectos básicos a tener en cuenta relativos al tema de Métricas de Seguridad.

Este documento viene asociado a un curso que se dicta en el instituto llamado: *"SANS SEC410 IT Security Audit & Control Essentials course"*, y en el cual, basándose en los comentarios de Diane Frank[4] (entre otros autores), expresan que inicialmente los líderes de seguridad en las empresas notaron que era necesario mantener un programa para la gestión de la seguridad informática, y luego, al pasar los años, notaron que no habían creado a la par mediciones que dieran cuenta de la efectividad real del mismo, y de las medidas que involucraba; es por ello que destacan la importancia de las Métricas de Seguridad.

En el artículo liberado hace unos años por el SANS la autora comenta, entre otras, cosas la dificultad de generar métricas de seguridad; por un lado, porque no había ningún tipo de documentación hasta el momento que indicara "qué medir", "cómo medirlo", "para qué medir", etc., y, por otro, porque en general el área de Seguridad Informática en las empresas (quienes las tenían, que no eran la mayoría) estaban en sus primeros años, recién asentando sus bases. Tener un área que se dedique específicamente a la seguridad de la información convertía a las empresas en pioneras del tema, pero había aún un arduo trabajo por realizar en materia de concientización, capacitación, y desarrollo del área.

Comenta, también, el valor de las métricas de seguridad, como respuesta a las preguntas clave que se hicieron desde siempre muchas organizaciones:

[3] http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55
[4] http://fcw.com/articles/2000/06/19/agencies-seek-security-metrics.aspx

- ¿Estamos hoy más seguros de lo que estábamos ayer?
- ¿Cómo nos comparamos contra la competencia en esta materia?
- ¿Estamos lo suficientemente seguros?

Estas preguntas son las que se hace cada responsable de área hasta el día de hoy. Como bien comenta la autora, armar un programa que permita recolectar información para responderlas certeramente, es todo un reto. Y de hecho, al día de hoy no se cuenta con una metodología de trabajo que pueda responderlas con una completa exactitud.

A pesar de esta dificultad, propone una forma de armar el programa basada en una metodología de siete pasos, entre los cuales se definen los objetivos del programa y las métricas a generar, se desarrollan las estrategias para generar esos indicadores y cómo serán luego utilizados, o sea, como los van a reportar y los umbrales a definir, así como un último paso que indica repetir todo el proceso una y otra vez para refinarlo y mejorarlo en cada ciclo.

Por último, da una conclusión dónde indica, en resumen, que el artículo si bien puede ser tenido en cuenta para la generación de un programa siguiendo la metodología propuesta, es simplemente una primera aproximación al tema de métricas de seguridad. El SANS propone hasta el día de hoy tomar el curso *"SANS SEC410 IT Security Audit& Control Essentials course"* dónde se exponen los conceptos en profundidad y la metodología se explica detalladamente para poder implementarla.

NIST (National Institute of Standards and Technology)

En el año 2008 el NIST también ingresó al ruedo de las métricas de seguridad, al emitir una guía de implementación práctica titulada: *"NIST Special Publication 800-55 Revision 1"*[5] en la cual se exponen los lineamientos detallados que permiten desarrollar, seleccionar e implementar ciertas mediciones que puedan ser

[5] http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

utilizadas tanto para mejorar el nivel operativo del área de Seguridad Informática, como así también para alinear las decisiones con los programas y misión establecidos.

La guía tiene base en otras publicaciones previas del NIST y, de las cuales, ésta pretende ser una actualización y un documento que además las vincula teniendo en cuenta las mediciones para saber, si las medidas tomadas siguiendo los documentos anteriores están siendo efectivas y corregir los desvíos que pudiese llegar a haber. Entre las publicaciones previas tenidas en cuenta están las siguientes:

- NIST SP 800-53A[6] *"Guide for Assessing the Security Controls in Federal Information Systems"*, la cual fue liberada en el año 2008, y sirve como guía para crear planes de evaluación de seguridad útiles que no sean meros *check-lists*, sino realmente planes basados en programas efectivos para mejorar la seguridad de la información en la organización.
- NIST SP 800-30[7] *"Risk Management Guide for Information Technology Systems"*, liberada en Julio del 2002, da cuenta de la administración de riesgos en todo sentido, desde la identificación, valoración hasta finalmente tomar las acciones necesarias para reducirlo a un nivel aceptable y acordado con el directorio. La publicación contiene la teoría de administración de riesgos de la TI, así como un detalle práctico de implementación de un programa de gestión de riesgos en TI.
- NIST SP 800-53[8] *"Recommended Security Controls for Federal Information Systems"*, el propósito de la publicación es proveer las guías necesarias para seleccionar y especificar controles de seguridad para los sistemas de información que tienen vinculación con agencias gubernamentales, de

[6] http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf
[7] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
[8] http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

forma tal de cumplir con la regulación FIPS 200 [9] [10]. Está actualizada a enero del 2010.

La orientación de la publicación NIST SP 800-55 sobre métricas de seguridad, como todas aquellas en las que se basa la misma, es a la realización de "mediciones" numéricas puntuales que den cuenta del trabajo operativo del área, alineándolo con la misión de la misma y armando programas consistentes dentro de un plan general de trabajo. Lo que las cataloga en un vertical más bien técnico y no estratégico o de negocio.

ISACA (Information Systems Audit and Control Association)

En el año 2008, la asociación ISACA publicó un artículo escrito por C. Warren Axelrod[11], en el cual el autor daba cuenta de los distintos tipos de mediciones que existían hasta el momento, y señalando para cada uno de ellos sus pros y contras.

En esta primera publicación que hace ISACA sobre "Métricas de Seguridad" habla también de los programas de métricas en general, y de lo que el autor denomina el enfoque tradicional, que según él no sirve realmente para la toma correcta de decisiones.

Warren dice: "Es mejor tomar buenas decisiones de seguridad basado en estimaciones menos precisas de valor y riesgo, que tomar decisiones pobres de seguridad avalado por métricas precisas pero inadecuadas"[12].

[9] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
[10] ***Federal Information Processing Standards*** (**FIPS**, en español Estándares Federales de Procesamiento de la Información) son estándares anunciados públicamente desarrollados por el gobierno de los Estados Unidos para la utilización por parte de todas las agencias del gobierno no militares y por los contratistas del gobierno.
[11] http://www.isaca.org/Journal/Past-Issues/2008/Volume-6/Pages/Accounting-for-Value-and-Uncertainty-in-Security-Metrics1.aspx
[12] Texto original: *"It is better to make good security decisions based upon less-precise estimates of value and risk than to make poor security decisions supported by precise, though inaccurate, metrics."*

Entonces, el autor plantea la dificultad que hay en encontrar una métrica de seguridad acertada y con bajo margen de error, pero a la vez, la ventaja que trae basarse en ella para tomar una decisión. A continuación se describen las categorías en las que encasilla las métricas, así como sus ventajas y desventajas:

Categoría de la Métrica	¿Qué dice?	¿Qué no dice?
Existencia	Es del tipo exacta, y nos indica si existe o no algo en la compañía, ayuda a responder a preguntas como: "¿Tiene Ud. un programa de actualizaciones de sistemas operativos implementado?"	Incluso si la respuesta fuese "SI", no sabríamos la calidad, periodicidad, y demás características fundamentales del objeto en cuestión
Ordinal	A veces no podemos medir numéricamente algo, entonces optamos por responder con una probabilidad ALTA, MEDIA, BAJA	Este tipo de mediciones son por lo general subjetivas
Puntuación	Se define una escala de 1 a 10, o se establece 1-Alta, 2-Media, 3-Baja	Este tipo de medida es tan subjetiva como la Ordinal
Numérica	Responden a preguntas tales como "¿En cuántos sistemas se aplicaron correcciones de software el último mes?", los resultados podrían ser analizados a través del tiempo para obtener reportes de tendencias	No siempre pueden usarse teniendo en cuenta la misma población objeto de estudio, o mismo podría ser que disminuya el número de correcciones aplicadas en cada mes, pero el número de vulnerabilidades vaya en aumento
Porcentaje	Ayuda a responder una pregunta como "¿Qué	El problema es que quizá el 99% de equipos fueron

	porcentaje de sistemas fueron actualizados el último mes?". Esto ayuda mucho más porque da cuenta de los equipos actualizados por sobre el total existente	actualizados, pero en ese 1% no actualizado correctamente en el último mes es dónde se alberga la información más importante, o el que está más expuesto a amenazas externas, etc.
Valor de la pérdida	Nos ayudaría para expresar el valor de la pérdida que tuvo la compañía por incurrir por ejemplo en una vulnerabilidad explotada	Este tipo de métricas es tan subjetiva como lo que uno quiera involucrar en ella
Incertidumbre	Es una estimación estocástica o probabilística de un evento	La especificación de las distribuciones de probabilidad son altamente subjetivas

Tabla 1 - C. Warren Axelrod, "Accounting for Value and Uncertainty in Security Metrics", ISACA, 2008 [13]

Por último, el autor recomienda, armar planes y programas de medición de la seguridad dentro de la compañía, más allá de todas las limitaciones o parte negativa que tienen cada una de las categorías. Advierte también lo difícil que es definir métricas que realmente sirvan para la correcta toma de decisiones, plantea que finalmente es todo parte de un esfuerzo continuo por mejorar día a día las mediciones y métricas en las cuales se basa el área.

Este artículo es útil para tener una idea de las categorías en las que se dividen las métricas y cuáles son los aspectos a favor y en contra de cada una de ellas, siempre teniendo en cuenta su orientación operativa.

[13] http://www.isaca.org/Journal/Past-Issues/2008/Volume-6/Pages/Accounting-for-Value-and-Uncertainty-in-Security-Metrics1.aspx

OWASP (The Open Web Application Security Project)

En octubre del 2006[14], la organización OWASP realizó una presentación en Seattle donde dio a conocer la importancia de las métricas en el ámbito de la seguridad informática; citó en ella el estado del arte sobre métricas de seguridad en aquel momento y dio a conocer lo que sería luego un proyecto[15] del OWASP para identificar y proveer a la comunidad un conjunto de métricas de seguridad para aplicaciones.

La idea finalmente es lanzar documentación avalada por la organización, que sea fruto del debate de todos los miembros que forman parte de la comunidad OWASP, y nutrirse entre ellos para ir madurando las métricas propuestas, armando así un conjunto de métricas que esté disponible para todas aquellas personas que quieran desarrollar o mantener aplicaciones Web soportados sobre una base sólida de métricas de seguridad informática.

Este tipo de métricas son importantes para tener en cuenta al momento de adquirir (o desarrollar) aplicaciones Web en la entidad, y a nivel técnico son uno de los estándares más consultados por los especialistas de seguridad.[16]

[14] https://www.owasp.org/images/4/49/OWASPAppSec2006Seattle_Security_Metrics.ppt
[15] https://www.owasp.org/index.php/Monitor_security_metrics
[16] http://arctecgroup.net/pdf/0703-OWASPMetrics.pdf

Capítulo 1

Concepto de Métricas vinculadas a la Tecnología Informática

Existen muchas definiciones de la palabra *métrica* vinculadas específicamente a métricas de TI, siendo la más completa y aceptada a nivel profesional aquella que dan Maizlitsh y Handler, distinguiéndolas en dos tipos: cuantificadoras de valor y aquellas usadas para medir rendimiento:

> "Hay dos tipos fundamentales de métricas que deben ser consideradas antes de comenzar con la tarea de gestionar la TI: entrega de valor y proceso de mejora. Entrega de valor consiste en reducir costos, incrementar las ganancias, incrementar la producción, reducir el tiempo de cada ciclo y reducir el riesgo. La mejora de procesos se refiere al desarrollo para mejorar el proceso de gobernar la TI. Mientras los dos tipos de métricas son similares y en muchos puntos se interrelacionan, las métricas de procesos se focalizan en la efectividad. ¿Está mejorando el proceso? ¿Está el proceso proveyendo valor al negocio? ¿Este valor agregado es percibido por los usuarios? ¿Está el proceso expandiendo su alcance? Cada día más, los líderes buscan microscópicamente en las métricas para eliminar toda aquella actividad que no da valor agregado a la empresa, y enfocarse en aquellas actividades que sí lo hacen." [17]

Otros conceptos ligados a las métricas son:

- Medición o Medida: es asignar un valor a un atributo de una entidad en un momento específico en el tiempo.
- Entidad: es cualquier objeto (tangible o intangible) sobre la cual se puede realizar una medición. La misma cuenta con atributos.

[17] B. Maizlitsh y R. Handler, IT Porftfolio Management: Step by Step, John Wiley & Sons, 2005, p. 53.

- Atributos: Son las propiedades o características de las entidades, que pueden ser medidos cuantitativa o cualitativamente por una persona o sistema automatizado.

Evolución de las métricas

Así como la TI evoluciona y sigue un proceso de mejora continua (análogo al círculo de Edward Deming o también llamado PDCA); hay un concepto muy interesante que comenzó a surgir hace unos años en el área de Seguridad Informática (y de la TI en general); se lo llama "Visión Holística", o también lo nombran algunos autores como "Visibilidad Total".

Este paradigma incorporado al área de Sistemas de Información en las empresas, plantea la diferencia entre los esquemas clásicos de trabajo con verticales acentuados y diferenciación marcada entre áreas de una empresa, en contraste con tener indicadores que lleven cuenta de una visión global del negocio o de los servicios que presta.

En algunas publicaciones del CIO de Tango/04 Computing Group, Raúl Cristian Aguirre, explica claramente de la siguiente forma *el concepto de* Visibilidad Total en las empresas: *"se trata de una necesidad ineludible para conservar y mejorar los niveles de servicio, agregar valor al negocio, reforzar la seguridad y acelerar el proceso de toma de decisiones, maximizando el rendimiento de los recursos"*.

Profundizando en detalle sobre la documentación del tema, se entiende que: lo que plantea esta nueva concepción es que las métricas que interesan al área directiva, son las que están más vinculadas al negocio (o al servicio que brindan); o sea, que ya no solamente basta con tener números que nos digan la cantidad de bloqueos de cuentas de usuarios que hubo en el mes; ni la cantidad de tickets que se lograron resolver en tiempo; ni tampoco el porcentaje de cumplimiento de una norma regulatoria; porque se puede tener un 99% de cumplimiento correcto en todos los controles de auditoría, y ese 1% restante es tan grave que derive en una multa severa o problemas legales para la empresa por irregularidades financieras.

El concepto de visión holística, está ligado a la necesidad actual de tomar en cuenta la mayor cantidad de variables a la hora de gestionar un área dentro de una organización, para hacerlo de manera más eficiente. Se sabe que el negocio bancario tiene ciertos lineamientos u objetivos estratégicos que deben perseguirse de forma unísona por toda la empresa (y que son propios de este tipo de vertical de compañías); entonces para que la gestión de la organización sea coherente y simplificada, se deberá contar con métricas que indiquen al gerente de cada área cuan alineada está la misma al negocio (sin tener en cuenta los indicadores definidos para la correcta gestión operativa del área).

Entonces, sería prudente tener indicadores de nivel táctico, encargados de alertar al gerente del área de Seguridad Informática si las decisiones que se toman están alineadas al negocio o no; de forma que nunca haya un aislamiento del área respecto del resto de la empresa.

Teniendo una visión total, o visión integral es que se puede trabajar sinérgicamente desde todas las áreas, y para ello es importante crear ciertas métricas bajo esta filosofía, lo que requerirá inevitablemente de mayor interacción entre áreas, y más cooperación entre todo el personal de la compañía para lograr el éxito.

El éxito del área de Seguridad Informática será la prevención de incidentes, y en los casos que no puedan prevenirse, mitigarlos de alguna forma; como así también asegurar al directorio que todas las situaciones que podrían llevar riesgo al negocio y/o a los directivos están razonablemente controladas; o al menos limitadas a las menores consecuencias posibles.

Utilidad de las métricas

Uno de los objetivos de utilizar métricas de Seguridad Informática, es contar con indicadores que permitan reflejar el estado de situación de la seguridad informática del negocio.

Otro conjunto de indicadores permiten a la gerencia media una visión clara del trabajo operativo de cada área. Esta serie de métricas de nivel medio brindan al CSO una mayor visualización del estado global del área de seguridad informática para la toma de decisiones.

Por consiguiente, la utilización adecuada de estos indicadores permitiría al gerente de seguridad informática evitar costos económicos y problemas legales a la alta gerencia, por la infracción de puntos críticos de leyes o normativas (Sarbanes-Oxley, BCRA 4609, etc.).

Usuarios de las métricas

Las métricas se utilizan en todos los niveles de la organización, probablemente importarán más (y serán más útiles) en los niveles gerenciales medios y altos que en los operativos.

Para armar cada métrica se podrían estar recolectando decenas de mediciones que abarquen distintos ámbitos, estos valores se ponderan según criterios establecidos, y por último el gerente medio cuenta con un valor que dé cuenta de un aspecto importante de la compañía, para tomar decisiones tácticas en el área.

El autor Verne Harnish en su libro *"Mastering the Rockefeller's Habits"*, plantea que las métricas deben usarse en todo momento para llevar la organización al éxito y que ésta nunca decaiga en su ritmo de mejora. El autor propone una gestión global de la empresa basada en tres pilares:

- Objetivos
- Datos
- Ritmo

El segundo punto (Datos) se refiere a la información con la que se debe contar para conocer el estado de los distintos aspectos de la organización; los cuales no tienen que ser grandes cantidades de estadísticas, gráficos históricos, reportes, y un sinfín de textos que si bien pueden ser interesantes no permiten tomar ninguna decisión. El concepto que el autor da respecto de estos "Datos" es prácticamente

el de “métricas”; o sea, significa tener valores que den cuenta de un aspecto clave de la empresa (o del área a gestionar) en una única representación.

Este último concepto está ligado a la diferenciación que hace Jim Collins en su libro *“Good to best”* respecto de contar con excesiva información versus una métrica o un conjunto de ellas que den conocimiento del negocio de un solo pantallazo; dice: “Lo que las métricas hacen, es proveernos de conocimiento en lugar de información. Este conocimiento nos da visibilidad de las actividades que hacemos para mejorar nuestra organización, y saber si realmente dan resultados.”[18]

[18] En el texto original dice: *“What metrics do is get us knowledge instead of information. This knowledge gives us visibility into the “improvement” activities we are doing in our organization to see if they are actually working.”*

Capítulo 2

Métricas y su inserción en la empresa

La utilización de métricas claves en tableros de comando balanceados para la gestión de una empresa es relativamente nueva, pero se puede afirmar que las métricas en sí mismas no son un desarrollo moderno y que se vienen usando en distintas industrias desde hace muchos años atrás.

A continuación, dos casos de aplicación de métricas para su uso en rangos corporativos alto y medio:

Caso 1: El Tablero de Comando

Cuadro de mando deriva del concepto francés: *"tableau de bord"*, que traducido de manera literal, significaría algo similar a tablero de mando o cuadro de instrumentos.

A partir de los años 80, es cuando el Cuadro de Mando pasa a ser, además de un concepto práctico, una idea académica, ya que hasta entonces el entorno empresarial no sufría grandes variaciones, la tendencia del mismo era estable, las decisiones que se tomaban carecían de un alto nivel de riesgo.

Para entonces, los principios básicos sobre los que se sostenía el Cuadro de Mando ya estaban estructurados, es decir, se fijaban objetivos en la entidad, cada uno de éstos eran llevados a cabo mediante la definición de unas variables clave, y el control era realizado a través de indicadores.

La evolución del tablero de mando que se originó en los ochenta, fue creciendo hacia el tablero de mando **integral** en los noventa, donde el concepto de Cuadro de Mando Integral[19] – CMI (*Balanced Scorecard – BSC*) fue presentado en el número de enero/febrero de 1992 de la revista Harvard Business Review, con base en un trabajo realizado para una empresa de semiconductores. Sus autores,

[19] http://www.balancedscorecard.org/BSCResources/AbouttheBalancedScorecard/tabid/55/Default.aspx

Robert Kaplan y David Norton, plantean que el CMI es un sistema de administración o sistema administrativo (*management system*), que va más allá de la perspectiva financiera con la que los gerentes acostumbran evaluar la marcha de una empresa.

Al tener en cuenta esto, cuando se desean tomar decisiones importantes en un área, o dentro de una empresa (decisión multitarea) teniendo en cuenta los distintos factores o perspectivas que integran el tablero de mando integral, se hace menester contar con estas métricas generales que den sustento a la decisión que se está por tomar.

Caso 2: British Airways

Si se quiere hacer una analogía por referencia respecto del uso de métricas para la gestión correcta de una organización, uno de los casos de éxito más conocidos es el de la aerolínea British Airways, la cual realizó en los años 80 un estudio (asesorada por consultores externos) sobre qué métricas deberían tener en cuenta para medir y corregir todo lo que fuese necesario de manera tal de mejorar la experiencia final de sus clientes, de sus empleados, y principalmente dar un vuelco positivo en las finanzas.

Los consultores que estaban realizando el trabajo, venían con idea de implementar distintas métricas que en su conjunto tuviesen en cuenta la perspectiva financiera, la perspectiva de los clientes, el aprendizaje y crecimiento de los empleados y los procesos internos; o sea, aspectos que se aplicaban al tablero de control balanceado; y para la sorpresa del personal de British Airways, no se definieron cientos de métricas para cumplir con la recolección de información de estos indicadores, sino que se construyó un número reducido de métricas (KPI – *Key Performance Indicators*) que ayudarían a la empresa a vincular estas perspectivas de forma centralizada y mediante esta información permitir a los directivos de la empresa tomar decisiones sobre dónde poner el foco de atención, dónde corregir desvíos, dónde invertir la mayor cantidad de recursos para cumplimentar los objetivos generales de la compañía. Dentro de los

indicadores creados, el KPI principal fue: “Puntualidad en las salidas de los vuelos”.

Y una vez que se había definido este KPI como el principal y más importante indicador a nivel global, el proyecto arrancó y el señor Lord King [20] (gerente general de la compañía por esos años) se había tomado muy en serio apoyar el proyecto y ser el promotor de llevarlo adelante y que sea tenido en cuenta en todos los estratos. Entonces, si un vuelo no salía a tiempo, el señor Lord King llamaba de forma personal al encargado responsable de la demora del vuelo para pedir explicaciones de por qué estaba saliendo tarde dicho vuelo. Obviamente, a nadie le gustaba recibir la llamada del gerente general con el consecuente problema que eso podría generar en su carrera en la empresa y además en su crecimiento profesional; por ello todos se esforzaban por cumplir con el KPI propuesto de “Puntualidad en las salidas de los vuelos” [21] [22]

La tozudez en la persecución de este KPI realmente dio un giro drástico en la caída de imagen que tenía British Airways, y finalmente posicionó a la empresa en el pensamiento del público usuario como entre una de las mejores y más recomendadas compañías aéreas del mundo, puesto que:

- Los empleados trabajaban más distendidos porque no tenían que lidiar con clientes enojados por retrasos en los vuelos
- La empresa no incurría en costos adicionales, porque no tenían que pagar noches de hotel, ni comidas compensatorias para los pasajeros que veían demorado su vuelo de un día para otro con una noche de por medio
- La promoción que se realizaba de boca en boca por toda la gente que estaba contenta y confiada que su vuelo saldría a horario, y efectivamente así era
- No se malgastaba combustible extra (puesto que un piloto que nota que está llegando tarde a destino, tiende a acelerar durante el resto del viaje

[20] http://www.nytimes.com/2005/07/13/business/worldbusiness/13king.html
[21] http://www.britishairways.com/cms/global/microsites/ba_reports0809/pdfs/KPIs.pdf
[22] Escrito en inglés sería: *“Punctuality – Ready to go”*

para compensar el tiempo perdido en la salida y esto conlleva un desgaste mayor de combustible)

- No se desperdiciaba alimento del que se servía a bordo del aeroplano (puesto que la comida caliente que se sirve durante el vuelo, estaba pensada y preparada para comerse en algunas horas, pero si este tiempo se excedía, la misma debía ser desechada)
- Muchos profesionales del rubro aéreo altamente capacitados, al notar este cambio, querían formar parte del personal de British Airways

Esta historia que se remonta a los años ochenta, si bien no vinculada de forma directa con la seguridad informática, marca la importancia de lo que una métrica bien elegida para medir un aspecto clave del negocio, puede ayudar en la gestión de una organización. Muchas otras empresas (no solamente vinculadas al rubro del aerotransporte) tomaron caminos similares, armando tableros de comando balanceados, y realizando el análisis respectivo para tener en cuenta solamente un bajo número de métricas clave.

Capítulo 3

Aplicación en el ámbito de la Seguridad Informática

En el área de Seguridad Informática el tema de las métricas, KPIs y KSIs (*Key Security Indicators*) es relativamente novedoso, y dependiendo el nivel de la métrica tiene mucha aplicación y utilidad para la toma gerencial de decisiones. Las métricas pueden ser un valor numérico ponderado o bien, pueden ser un indicador que se escalara desde los niveles operativos hasta alcanzar un nivel estratégico y de planificación, por ejemplo los proyectos en proceso que precisan del apoyo del área de Seguridad Informática. Incluso, podrían quedar expresadas en formato numérico para el seguimiento del día a día operativo del área de Seguridad Informática.

En los casos de indicadores que tengan impacto directo en el negocio, el directorio podrá tomar decisiones basándose en métricas claves del estado de la Seguridad Informática de la compañía. Estas métricas podrían informar, entre otras cosas, sobre los posibles proyectos de mitigación de riesgo entre los cuales podrá elegir, qué aspecto de la SI mejora en la compañía y los costos de cada uno (tiempos, personal, recursos financieros, etc.).

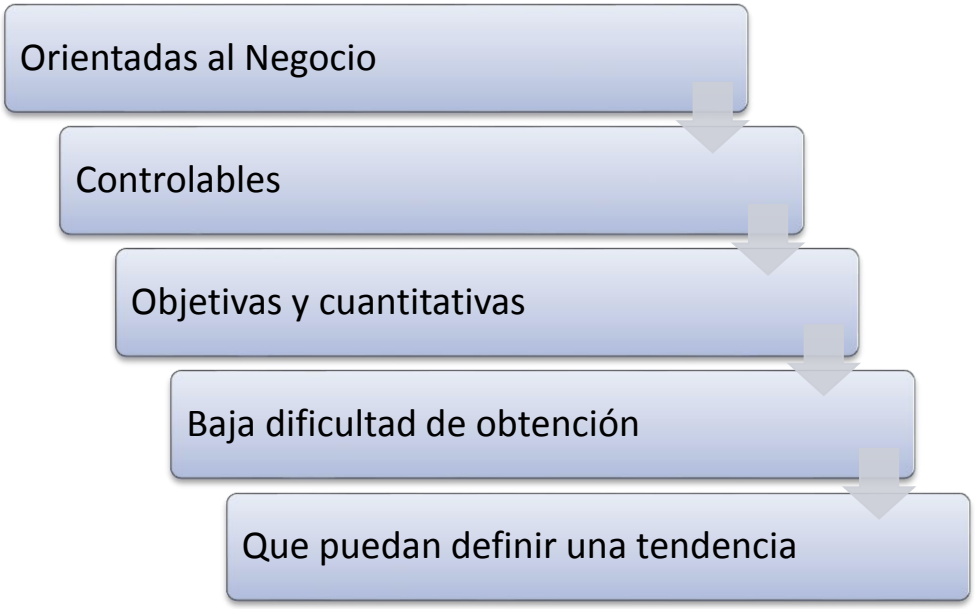
Para que las acciones realizadas en la compañía (respecto de la Seguridad Informática) sean en beneficio del negocio y no vayan en contra o colisionen con los objetivos globales de la entidad, es imprescindible que las métricas de alto nivel creadas, lo hagan teniendo en cuenta una visión integral de los servicios que provee la compañía.

Adicionalmente, las métricas que se planteen desde el área de Seguridad Informática, tienen que tener como meta final perseguir los objetivos generales de la organización, es decir, deben estar alineadas en gran medida con los objetivos propuestos por la alta dirección. Este último, es uno de los puntos clave al momento de crear una métrica de seguridad de alto nivel, que sea recolectada de

manera periódica, medida sistemáticamente, analizada por el área y por último tenida en cuenta para la toma de decisiones.

Cinco características de las buenas métricas de SI

Cómo dice Jeffrey Wheatman (de Gartner) en su artículo titulado: *"Five required Characteristics of Security Metrics"*[23], hay una gran cantidad de características y factores que determinan el valor y relevancia de una métrica de Seguridad Informática, pero mínimamente deben contar con las siguientes cinco características:



Orientadas al Negocio. Es esencial, puesto que los altos niveles de la empresa están más interesados en saber qué ha hecho la seguridad informática para ayudarlos a lograr sus objetivos, más que en saber "cómo" se ha hecho en detalle cada una de esas cosas.

[23] http://www.gartner.com/id=1665315

De todas formas, aunque la métrica no sea consumida por el nivel directivo, sino por gerencias medias o rango operativo, su meta final debe estar alineada con los objetivos de la compañía.

Controlables. Para que las métricas sean efectivas en demostrar que el equipo de seguridad informática alcanza sus objetivos, deben medir factores que puedan ser controlados por procesos o herramientas.

Objetivas y cuantitativas. Deben estar debidamente medidas, y los resultados deben ser claros e imparciales, puesto que en muchas ocasiones serán las bases de la toma de decisiones. Su cálculo y valor debe ser sencillo de entender, incluso por gerentes o directivos que no tengan un alto grado de conocimiento de la seguridad informática.

Baja dificultad de obtención. Para que entreguen valor, deben ser fáciles de obtener y analizar. Si las métricas toman mucho tiempo y esfuerzo al momento de recolectarse, entonces su valor decae.

Que puedan definir una tendencia. Si apuntamos a indicadores de nivel estratégico, es preciso pensarlas de manera tal que con ellas se pueda armar una presentación a los directivos, donde puedan ver la tendencia de las métricas de seguridad informática simplificadamente.

Capítulo 4

La Seguridad Informática en las Entidades Financieras

El avance de la tecnología en lo que respecta a entidades financieras y sus clientes, está cambiando la forma de hacer negocios. Ningún banco de Argentina que quiera brindar un buen nivel de atención a clientes y empresas puede prescindir del servicio de HomeBanking [24] y Banca Empresaria.

Asegurar los medios informáticos en los que se sustenta esta nueva forma de hacer negocios se torna imprescindible. Y no solo por políticas internas de la entidad financiera, sino porque son uno de los segmentos de la industria que más normas nacionales e internacionales deben cumplimentar, so pena de sanciones legales o económicas.

En este contexto de trabajo, las métricas de seguridad informática aplicadas sobre entidades financieras proveen facilidad para controlar la correcta adhesión a las políticas, programas, normas y leyes establecidas que rigen para la entidad y minimizar así el riesgo informático.

¿Qué medir en una organización financiera/bancaria?

Para el desarrollo de este trabajo, se han seleccionado ciertos pilares considerados básicos de la seguridad informática, que a su vez tienen injerencia sobre el rango operativo, táctico y estratégico.

Para la selección de estos pilares, se tuvieron en cuenta, la experiencia laboral del maestrando (trabajando como analista y liderando varios proyectos de Seguridad Informática en clientes de América Latina y Estados Unidos); trabajos de distintos autores reconocidos en el ámbito de la seguridad informática y normativas nacionales e internacionales.

[24] Cómo lo indica el BCRA en su publicación: http://www.bcra.gov.ar/pdfs/snp/SNP0165.pdf, el HomeBanking: “Es un servicio que brindan la gran mayoría de los bancos importantes, públicos y privados, de manera gratuita, a través de sus páginas Web. Es factible su ingreso y operatividad las 24 horas de todos los días, los únicos requisitos son: poseer una cuenta corriente o caja de ahorro y obtener una clave personal. Se pueden realizar casi todas las operaciones que se hacen en los cajeros automáticos, incluso hay más posibilidades.”

Un breve detalle de los pilares sobre los cuales se desarrollaron los indicadores es el siguiente:

1) **Cumplimiento Regulatorio y Marco Normativo** (También conocido como *"Compliance", "Regulatory Compliance", o "IT Compliance"*).

   En términos generales, se habla de *compliance* significando conformidad. Esta conformidad será a una regla, especificación, política, estándar o ley. El Cumplimiento Regulatorio describe el objetivo permanente que persiguen las instituciones bancarias, realizando su mayor esfuerzo, para asegurarse que el personal está consciente de las leyes y regulaciones relevantes que aplican en la institución (y específicamente en su puesto de trabajo), y realiza así, todos los pasos necesarios para cumplir con ellas.

   Debido al creciente número de regulaciones y a la necesidad que tienen las instituciones bancarias y financieras de apegarse a su cumplimiento, es que cobra mucha importancia tener en cuenta este pilar. [25]

   El propósito del *compliance* es monitorear, detectar y corregir [26] cualquier riesgo que se presente respecto del incumplimiento, parcial o total, de las obligaciones regulatorias (sean estas internas o externas) que aplican a la entidad en cuestión.

   En Argentina, todos los bancos e instituciones financieras deben cumplir obligatoriamente (so pena de sanción por incumplimiento) con la Comunicación "A" 4609 *(Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología Informática y sistemas de*

[25] http://www.gartner.com/it-glossary/regulatory-compliance/. Regulatory compliance is concerned with laws that a business must obey, or risk legal sanctions, up to and including prison for its officers.
http://en.wikipedia.org/wiki/Regulatory_compliance. In general, compliance means conforming to a rule, such as a specification, policy, standard or law. Regulatory compliance describes the goal that corporations or public agencies aspire to in their efforts to ensure that personnel are aware of and take steps to comply with relevant laws and regulations. Due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls. [1] This approach is used to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity from resources.

[26] No siempre se podrá o querrá corregir un determinado riesgo, pero es clave de todas formas tener conocimiento de cada uno de ellos que se tome la decisión de evitarlos, mitigarlos, transferirlos o aceptarlos.

información); emitida por el Banco Central de la República Argentina (desde ahora abreviado como BCRA) el 27 de diciembre del 2006. [27]

2) **Gestión de Identidades** (También conocido como *"Access Management"*, *"Identity Management"*, "Gestión de Accesos", "Gestión de Derechos", "Solicitud de acceso / autorización a los componentes tecnológicos").

   Se denomina Gestión de Identidades al sistema integrado de políticas de seguridad, junto a los procesos de la organización en su conjunto, que pretende facilitar y controlar el acceso a las distintas aplicaciones de negocio, así también como a los distintos recursos y activos.

   La catalogación de los servicios de TI, junto a los usuarios disponibles y sus distintos niveles de autorización será definida por el área de Seguridad Informática basada en el análisis de los servicios TI existentes en la organización, la lista nominal del personal, los roles necesarios y el entendimiento minucioso de cada una de las aplicaciones y recursos informáticos de la compañía.

   El propósito de la gestión de identidades, es brindar a los usuarios autorizados el derecho a utilizar un servicio; denegando el acceso a este servicio a los usuarios que no estén autorizados. [28]

3) **Seguridad de la Infraestructura Tecnológica** (También conocido como "Seguridad TI", "IT Security", "Seguridad Tecnológica").

   La Seguridad Tecnológica en una empresa se define como un conjunto de reglas, planes y acciones que permiten asegurar la información contenida en uno o varios sistemas de la empresa.

   La infraestructura tecnológica es el conjunto de hardware y software sobre el que se asientan los diferentes servicios que la entidad financiera o banco necesita tener en funcionamiento para poder llevar a cabo toda su actividad. El conjunto de hardware consta de elementos tan diversos como

[27] http://www.bcra.gov.ar/pdfs/comytexord/A4609.pdf / Ver anexo IV en este mismo trabajo.
[28] Para mayor información sobre el tema dirigirse al Anexo II, en este mismo trabajo.

los grandes ordenadores que hacen de servidores de aplicaciones, los elementos de red como *routers* o *firewalls*, los ordenadores personales, las impresoras, los aires acondicionados, los estabilizadores de corriente de las salas de máquinas, los sensores, las cámaras, los teléfonos, etc. El conjunto de software incluye los sistemas operativos, aplicaciones críticas del negocio, las bases de datos, los servidores de aplicaciones o las herramientas de ofimática.

El objetivo de medir la Seguridad Tecnológica es proteger el conjunto de estos componentes para asegurar la integridad, disponibilidad y confidencialidad de la información en ellos contenida y/o transmitida.[29] [30]

Cada pilar tiene sus propias características, por ende, se proponen en este trabajo métricas específicas de cada uno de ellos. Se desarrolla cada indicador informando a qué pilar corresponde, y se presenta información sobre cómo podría llevarse a cabo la recolección de los datos necesarios para su cálculo, el procesamiento de estos datos.

4.1 Cumplimiento Regulatorio y Marco Normativo

¿Qué tener en cuenta al momento de medir el Cumplimiento Regulatorio y Marco Normativo?

Lo más importante de la medición en este pilar es tener en cuenta los puntos incumplidos y que signifiquen un riesgo alto para la entidad.

Cada regulación que aplique a las entidades bancarias y financieras, deberá ser cumplida en su totalidad para evitar sanciones económicas y legales, pero ciertas veces el incumplimiento de alguno o varios puntos se fundamentan en una razón de costo/beneficio, el cual es considerado por el directorio una vez informado.

[29] http://www.linalco.com/seguridad-tecnologica-linux.html
[30] http://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html

En este pilar, se tendrá en cuenta uno de los principios conocidos de la Seguridad Informática respecto del negocio y la economía de la empresa, que dice: *"no tiene sentido invertir más dinero en proteger un activo, que lo que vale el activo mismo".*

Métricas propuestas

Métrica:
Observaciones de puntos de auditoría de Seguridad Informática de Riesgo Alto

¿Qué mide?
Detalla las observaciones realizadas por alguna auditoría (interna o externa), donde se hayan encontrado puntos incumplidos respecto a normativas o leyes vigentes. Este tipo de inseguridades informáticas debieran representar un riesgo alto para el negocio. Y se considerarán de riesgo alto, los puntos observados que puedan implicar pérdidas económicas, problemas legales o reducción positiva de la imagen de la compañía.

¿Para qué medir las observaciones?
Es necesario puntualizar las observaciones abiertas que no están debidamente solucionadas, por un lado porque ya fueron detectadas por un tercero, el cual seguramente deja claro el riesgo informático que existe por no tener control sobre esta brecha de seguridad; y por otro lado, son importantes porque probablemente respondan a un riesgo conocido y analizado (incluso, puede estar descrito el riesgo de su incumplimiento) por la comunidad informática. Se miden para que la alta gerencia tome conciencia de la existencia de las mismas y el área de seguridad informática pueda actuar en consecuencia.

¿Cuándo medir las observaciones?
En cada auditoría realizada (sea esta interna o externa), y se actualizarán cada vez que los analistas de seguridad informática trabajen en resolver estos puntos pendientes (este trabajo realizado, debiera ayudar a mitigar en gran medida el riesgo latente).

¿Quién ve esta métrica?
El gerente del área de Seguridad Informática y el Directorio.

¿Cómo se miden las observaciones?

Se contabilizan en cada auditoría, se clasifican y solamente se dejarán las de riesgo ALTO. El resto seguirán su proceso habitual y se irán resolviendo bajo los canales y tiempos normales de trabajo. La medición debe ser realizada manualmente.

Detalles de la Métrica

En esta métrica se expresa puntualmente cualquier riesgo de seguridad informática que pueda devengar en pérdida de datos confidenciales, dinero o prestigio de la entidad financiera.

Es muy común que las auditorías que detectan estos problemas, sean contratadas a empresas consultoras que se dedican a realizar este tipo de relevamientos y su desarrollo no quede únicamente en manos del área de Seguridad Informática o Auditoría Interna.

Métrica:

Abuso de sitios web restringidos, descargas de software ilegal, control de SPAM

¿Qué mide?

- La cantidad de conexiones abiertas (entrantes/salientes) que tienen los equipos de la red,
- un primer grupo de los usuarios que mayor cantidad de MB están transfiriendo,
- un segundo grupo de usuarios que mayor cantidad de correos enviaron,
- un tercer grupo que representa a los que mayor cantidad de correos recibieron.

¿Para qué medir las observaciones?

Según encuestas realizadas por diversas consultoras y empresas de seguridad informática los problemas de la descarga ilegal de software, o la navegación por sitios web infectados con troyanos, malware o spyware siguen con tendencia en alta durante estos últimos años. Que un empleado descargue una aplicación ilegal, o bien que ingrese a un sitio en internet para usar un juego online podría poner en riesgo a la red entera de la entidad financiera y no solo a su PC.

Por ejemplo, podría convertir a los equipos y servidores de la empresa en participantes de una *botnet* [31], haciendo que desde la misma entidad financiera se re-transmitan virus, hagan robo de identidad, o envíen correos basura.
Medir este tipo de tráfico en la entidad es una necesidad puesto que en mayor o menor medida todos los empleados requieren del uso de internet para desarrollar su trabajo diario.

¿Cuándo medir las observaciones?
Diariamente, y reportarlo mensualmente.

¿Quién ve esta métrica?
El área de Seguridad Informática, junto al área de Recursos Humanos, quiénes oportunamente podrían dar información al Directorio

¿Cómo se miden las observaciones?
Con software de filtrado de Internet y lectura de logs de dispositivos de *networking*

Notas de la Métrica
Es importante la medición del tráfico entrante/saliente que se hace desde un equipo de la red, no solamente para detectar si está descargando archivos de gran tamaño (que podría ser por ejemplo una imagen de un CD ó DVD) sino también para conocer si se está subiendo información de la entidad o de su labor diaria a algún sitio de archivado de información en la nube (por ejemplo, *DropBox* [32]).
Se hace menester contar con algún software de filtrado *web* [33], que permita llevar el control de los sitios que intentan visitar los empleados dado que muchos de ellos no son necesarios para desempeñar correctamente sus funciones y debiera estar

[31] Fuente: http://cxo-community.com/articulos/blogs/blogs-seguridad-informatica/2142-ataques-de-seguridad-botnet.html
Bot: es una pieza de software que puede de manera autónoma ejecutar una tarea “en nombre de” una persona o entidad.
Botnet: es una cantidad de computadores conectados en Internet, sus propietarios pueden no ser conscientes de ello. Estos computadores están en condiciones de realizar transmisiones (las cuales pueden incluir código malicioso, *spam*, virus, etc.) hacia otros computadores conectados también a la red.
[32] https://www.dropbox.com/
[33] Uno de los más utilizados en Argentina es el WebSense: http://www.issecurity.com.ar/site/index.php/productos/websense

deshabilitados. En este filtrado se pueden incluir las descargas de cierto tipo de archivos (programas ejecutables, librerías dinámicas *dll*, de un tamaño mayor a cierto número de MB, comprimidos o encriptados).
Sería interesante tener vinculada esta métrica a los programas de concientización de seguridad informática que dicte el área de seguridad informática y al seguimiento por parte de los gerentes.

Métrica:
Estado general de seguridad del sistema MEP (Medio Electrónico de Pagos)

¿Qué mide?
La seguridad general del sistema MEP, el cual es supervisado bajo rigurosos controles del BCRA, y sirve para realizar transacciones interbancarias, transacciones transfronterizas (principalmente en dólares), liquidación de saldos y pagos judiciales entre otras operaciones.

¿Para qué medir las observaciones?
Para evitar incurrir en cualquier falta grave que pueda ser detectada por el BCRA en sus controles periódicos. Este sistema es de uso obligatorio para entidades financieras que quieran operar con cuentas corrientes registradas en el BCRA.

¿Cuándo medir las observaciones?
Las mediciones deben ser en tiempo real para detectar prontamente cualquier actividad anormal que termine en incumplimiento regulatorio, o riesgo de sufrir algún tipo de pérdida monetaria inmediata.

¿Quién ve esta métrica?
El gerente del área de seguridad informática, y oportunamente informará a sus superiores en caso de detectar anomalías

¿Cómo se miden las observaciones?

A través de la lectura de los archivos de Log propios de la herramienta MEP brindada por el BCRA.

Detalles de la Métrica

El MEP[34] es un sistema desarrollado y operado por el BCRA, las entidades financieras y las Cámaras Electrónicas de Compensación (C.E.C.). Permite que las instituciones autorizadas realicen transferencias en tiempo real a través de las cuentas corrientes que tienen registradas en el BCRA, y dispongan de información en tiempo real acerca de los saldos disponibles en cada una de sus cuentas. (Es importante destacar el carácter irrevocable de las transacciones efectuadas a través del sistema, según lo expresa el BCRA).

CAMEL[35] es un método de evaluación, que consiste en medir y analizar cinco parámetros fundamentales: Capital, Activos, Manejo Corporativo, ingresos y Liquidez. Del análisis efectuado, se ponderan los cinco dominios y se extrae un puntaje del 1 al 5. Puntualmente, el capítulo de Activos y Management de la metodología CAMEL, se desarrollan en parte sobre los activos de información, su infraestructura técnica, puntos de control y auditoría implementados y cumplimiento de regulaciones y normas; es por ello que este indicador de MEP cobra importancia, dado que mide una de las Operaciones más críticas de una entidad financiera, como ser, las transacciones electrónicas de clientes e interbancarias.

4.2 Gestión de Identidades

La gestión de identidades es una metodología de trabajo que permite realizar la gestión del ciclo de vida de las identidades y el control de acceso a los distintos recursos de la entidad con el objetivo de evitar/mitigar riesgos, reducir costos y permitir que el negocio evolucione de manera segura, flexible y escalable.

Continuamente, las entidades financieras, deben enfrentarse a modificaciones regulatorias en las leyes y normas que les aplican, por lo que una gran velocidad

[34] Para un mayor detalle de MEP, dirigirse al Anexo V en este mismo trabajo
[35] Para mayor detalle de CAMEL, dirigirse al Anexo VI en este mismo trabajo

de adaptación de gestión de identidades y control de acceso se hace imprescindible.

Por otro lado, los bancos cuentan con gran cantidad de aplicativos de software sobre los cuales deben gestionar el correcto acceso de cada empleado a las funciones y módulos específicos que requieren para su trabajo, esta tarea se haría casi imposible de realizar sin una buena política de gestión de identidades implementada. O por lo menos llevaría una gran cantidad de horas de los analistas de seguridad, que es un tiempo que se luego les faltaría para poder analizar incidentes de seguridad que impliquen mayor riesgo a la entidad.

¿Qué tener en cuenta al momento de medir la Gestión de Identidades?

Los indicadores de gestión de identidades pueden ser varios, dependerán en gran medida de la organización, de su forma de trabajo habitual y de las demandas de información que haga la alta gerencia, pero hay determinadas métricas claves que son comunes a todas las compañías financieras y bancos. Las mismas se basan generalmente en:

- la **cantidad** de peticiones realizadas al área de seguridad informática.
- el **canal de ingreso** (telefónico, correo electrónico, personalmente, automático, CRM).
- la **complejidad** de la solicitud (más compleja si involucra varias aplicaciones, servicios de software o diferentes permisos a otorgar dentro de cada componente; más sencilla si solamente impacta una sola aplicación y un solo perfil de usuario).

Métricas propuestas

Métrica: Solicitud de Acceso (a aplicaciones / servicios de software de la entidad) Definición de Solicitud de Acceso: Se entiende solicitud de acceso a cada petición que efectúa un solicitante para hacer uso de una aplicación de software perteneciente a la entidad bancaria o financiera en

cuestión.

Esta solicitud contendrá mínimamente:

- Identificación del solicitante
- Aplicación / servicio (al que desea acceder)
- Tareas a realizar / características a utilizar (dentro de dicha aplicación o servicio de software)
- (Opcionalmente) Fecha de expiración del permiso de acceso

El personal del área de Seguridad Informática tendrá que basarse en la identificación del solicitante para conocer el alcance de las tareas de su puesto y, en base a ello, seguir adelante o no con el proceso de otorgar los permisos solicitados sobre el componente tecnológico en cuestión.

En base a las características solicitadas para utilizar de la aplicación, se determinarán los permisos mínimos necesarios a otorgarle al solicitante en la plataforma tecnológica solicitada.

Adicionalmente, tendrá que tener en cuenta la fecha de expiración del permiso, si es que no fuese una solicitud permanente; para que una vez cumplido el tiempo se remuevan los permisos brindados.

¿Qué mide?

La cantidad y tipo (complejidad, canal de ingreso) de las solicitudes de acceso recibidas por el área de Seguridad Informática

¿Cuándo se mide?

Se propone una medición diaria. Para la obtención de conclusiones, mensualmente se realizarán los cálculos pertinentes de tipo sumatoria y promedio.

¿Quién ve esta métrica?

El gerente del área de Seguridad Informática

¿Para qué se mide?

Para tener un dato preciso de la cantidad de solicitudes de acceso que ingresan al área cada día, y de las que se resuelven. Esto da a conocer una medida del ancho de banda

diario que se puede resolver, y un número con el promedio de tipo y cantidad de casos que ingresan al área diariamente.

Se valida además el canal de ingreso para diferenciar principalmente una petición manual en contraposición a una alerta automática de intento de acceso no autorizado previamente a un componente tecnológico.

¿Por qué se mide?

Porque es preciso saber si la cantidad de peticiones solicitadas está siendo evacuada de forma correcta cada día, o en los N días subsiguientes (dependiendo el acuerdo de nivel de servicio vigente). Seguramente la cantidad de días será tal que no interfiera negativamente en la operatoria normal de la entidad bancaria / financiera.

Posibles conclusiones a obtener

Analizando los resultados y números de la métrica, se podrá conocer:

1) Si se obtiene diariamente, a lo largo de un cierto período de tiempo, se podrían establecer los tiempos medios de resolución de cada tipo de solicitud, lo que ayudaría a negociar o renegociar los tiempos acordados con otras áreas.
2) El valor del ratio Solicitudes_Abiertas / Solicitudes_Cerradas, el cual tiene que estar siempre cercano a 1, si diese un valor muy por encima, está indicando que el equipo de trabajo del área de Seguridad Informática no está pudiendo resolver a tiempo las peticiones que ingresan al área.
3) En qué parte del proceso de atención del requerimiento se invierte más tiempo. Esto es importante puesto que a partir de conocer cada etapa del proceso por la que transita un requerimiento desde que se abre el ticket en el sistema de gestión de incidencias hasta que se le da curso, nos es posible determinar cuánto tiempo se tarda en cerrarlo y en qué etapa del proceso consume la mayor parte del tiempo.

   Así, si notamos que la mayor parte del tiempo se pierden en el análisis inicial, será hora de pensar si realmente los técnicos que están dando curso a cada requerimiento tienen el nivel de capacitación necesario para interpretar lo que se solicita y decidir rápidamente si se da o no lugar al pedido.
4) Si la cantidad de personal del área está adecuadamente definida con respecto a la cantidad de requerimientos solicitados al área. Incluso sabiendo que el área

puede estar sujeta de tener que cumplir un tiempo acordado con otra área, (proveedor externo, usuarios finales) al no estar cumpliéndolos se incurriría en el algún tipo de penalidad. Al tener conocimiento de las métricas propuestas en el punto anterior, el gerente del área de Seguridad Informática podría sacar como conclusión si es que se están pagando multas por incumplimiento de los tiempos de servicio acordados y si el monto de ellas supera en dinero lo que saldría incorporar a más analistas de seguridad informática.

5) Teniendo en cuenta si los requerimientos son manuales o automáticos, y el porcentaje en que se dan cada uno, se podría llegar a pensar en la forma de automatizar ciertas peticiones para que no quiten tiempo a los analistas de seguridad del área y por otro lado, se resuelvan más rápido. Aquí es importante también que al haber analizado el "tipo" de requerimiento, podríamos entender cuáles son pasibles de ser automatizados (puesto que no implican un riesgo a la compañía) y cuales obligatoriamente tienen que pasar por el visto bueno de un analista.
6) Al conocer el TOP 5 de las aplicaciones y tipo de requerimiento solicitado se puede intentar bajar los tiempos de los mismos, o mejorar el proceso o circuito específicamente para la atención de estos, dando lugar así a una mejora en la percepción del usuario final respecto del área de Seguridad Informática.

Evaluación de la métrica

Dada la implicancia en la actividad operativa que puede traer aparejada la demora en la concesión de un requerimiento solicitado por un empleado, esta métrica se calificará como "Aceptable" si más del 95% de los requerimientos se resuelven dentro de los plazos acordados según el contrato interno de acuerdo de servicio (SLA – *Service Level Agreement*).

Y será calificada como "No aceptable", si se excede del 5% de roturas del contrato acordado.

Para que esto no suceda, es importante que la entidad cuente con una cabeza de equipo (podría ser el responsable del área, u otra persona designada a tales fines) que pueda manejar las excepciones (para resolver tickets que están cercanos a pasarse del tiempo estimado de resolución) y que de manera periódica evalúe la capacidad de resolución del

equipo de trabajo versus la demanda de requerimientos que se solicitan al área.

Métrica:

Intentos no autorizados de acceso a Datos Confidenciales

Descripción de intento de acceso:

Basándose en el rol que desempeña cada empleado en la entidad financiera o bancaria, debe poseer acceso a determinada información. De esta forma es que puede desempeñar sus tareas habituales asignadas.

Para regular el acceso a datos confidenciales, o que por su naturaleza no pueden ser accedidos por todos los niveles de la empresa, se establecen controles de seguridad.

Estos controles tienen por objetivo rechazar preventivamente los intentos de acceso a recursos de software por parte de usuarios que no estén debidamente autorizados; y por otro, alertar al área de seguridad informática en el momento que este tipo de incidentes se produzcan.

El área de seguridad informática con la alerta de un intento fallido, o autorización revocada automáticamente, debería:

- Identificar a la persona física (en caso de ser factible) que intentó utilizar un recurso para el cual sus funciones no lo requieren, o directamente no lo permiten
- Identificar el dispositivo o terminal desde la cual se intentó realizar el acceso
- Analizar la transacción completa que se intentó realizar
- Investigar si hubo finalmente acceso o no a información confidencial (total o parcial) y de qué tipo (solo lectura, modificación, eliminación)
- Avisar al responsable inmediato superior a dicho empleado
- Dar parte a las gerencias medias involucradas o gerencia superior del incidente ocurrido y del alcance de los hechos (esto no se da en todos los casos, pero dependiendo de la gravedad del incidente podría ser necesario)
- Revisar el conjunto de medidas preventivas, detectivas y/o correctivas asociadas a dicho control, y en todo caso evaluar su creación/modificación, en caso que no lo haya hecho aún

Este tipo de alertas está indicada como obligatoria en la comunicación “A” 4609, donde dice: “3.1.4.5. Alertas de seguridad y software de análisis. Las entidades financieras deben implementar funciones de alertas de seguridad y sistemas de detección y reporte de accesos sospechosos a los activos de información, y contar con monitoreo constante de los accesos a recursos y eventos críticos, que reporten a los administradores sobre un probable incidente o anomalía en los sistemas de información. Asimismo, se considera una sana práctica de seguridad la detección en tiempo real de los eventos o intrusiones, así como la utilización de herramientas automatizadas para el análisis de la información contenida en los registros operativos, de seguridad y de auditoría. De esta manera, se reducirá el volumen de los datos contenidos en los reportes, minimizando los costos relacionados con su almacenamiento y tareas de revisión.”

¿Qué mide?

Los intentos de acceso no autorizados (sea por personal interno a la entidad o por terceros) a datos confidenciales, los cuales conllevan un riesgo potencial

¿Cuándo se mide?

Se propone una medición constante en tiempo real y un reporte mensual, de los recursos que contengan información confidencial para la organización, y sin previa autorización hayan intentado ser accedidos. Esta métrica tendrá únicamente en cuenta documentación, bases de datos e información que esté vinculada de manera directa a la alta gerencia, o que atenten directamente contra la seguridad informática de la entidad y puedan devengar en una pérdida de imagen de la misma.

¿Quién ve esta métrica?

El gerente del área de Seguridad Informática, quien podría informar al Directorio si cree conveniente ante un intento fallido o falta grave

¿Para qué se mide?

Para tener información mensual de intentos fallidos de acceso a información clave de la

entidad, mejorar los controles cada mes, alertar a cargos superiores del incidente y adaptar los controles en base a las tendencias que se vayan detectando.

Adicionalmente, para cumplimentar con la comunicación “A” 4609 y la comunicación “A” 5374, esta segunda se centra específicamente sobre canales electrónicos e indica sobre la gestión de incidentes:

“[…] 6.2.5. Gestión de Incidentes (GI). Proceso relacionado con el tratamiento de los eventos y consecuentes incidentes de seguridad en Canales Electrónicos, su detección, evaluación, contención y respuesta, así como las actividades de escalamiento y corrección del entorno técnico y operativo.

6.3.2.2.5. Gestión de Incidentes. Complementariamente a lo indicado en el punto 6.2.5., las entidades deben arbitrar los esfuerzos necesarios para contar en sus organizaciones o a través de terceros bajo coordinación y control propio, con equipos de trabajo especializado en la atención, diagnóstico, análisis, contención, resolución, escalamiento e informe de los incidentes de seguridad de todos sus Canales Electrónicos, de manera formal e integrada. […]”

¿Por qué se mide?

Porque el área de seguridad informática es la encargada de crear, actualizar y mantener correctamente configurados los controles de seguridad lógica y de acceso a la información confidencial de la entidad.

Además el área de seguridad informática es la que tendría que brindar o denegar el acceso a estos recursos confidenciales a cada empleado, o grupo de empleados basándose en las funciones de sus cargos.

Se mide también, porque si ocurriesen una gran cantidad de incidentes en un período medido, o se detecta una tendencia en alta respecto de determinada información que es tratada de acceder sin autorización, el primero que debería enterarse y tomar acciones correctivas es el gerente de seguridad informática junto a su equipo de trabajo.

Posibles conclusiones a obtener

1) Lo principal es la medición de la calidad del sistema de gestión de identidades implementado, el cual debe contar con controles de seguridad lógica y perimetral que impidan el acceso efectivo a ciertos recursos catalogados como críticos.
2) En base a los accesos detectados (y que no deberían haberse permitido) se

mejora el control, o se crea uno nuevo que sea una variante del anterior si fuese necesario. Intentando además, encontrar patrones de intentos de acceso.

3) Recolectando todos los intentos revocados de acceso y agrupándolo según distintas variables (área origen, servidores destino, tipo de plataforma afectada, grado de confidencialidad del recurso comprometido, rango horario del incidente, etc.) se pueden observar tendencias de incidentes, y en base a ello, atacar de manera prioritaria los problemas que signifiquen mayor impacto sobre la entidad.
4) Ante una falta grave en reiterados períodos de medición por parte de un empleado en particular, se podrían tomar acciones legales contra el mismo.
5) Si se repitiesen reiterados accesos no autorizados por cierto sector de la entidad, se deberá alertar del comportamiento sospechoso a la alta gerencia.

Métrica:

Acceso de programadores al código fuente del sistema de producción

Cómo dictamina la Comunicación “A” 4609 del Banco Central de la República Argentina en la sección 2.5.4, un empleado no puede desempeñar dos o más roles que sean incompatibles entre sí (debería existir siempre “contraposición de intereses”). Esta incompatibilidad se basa en la segregación de funciones que debe existir en la entidad.
Específicamente, quienes realicen el “Análisis de Sistemas / Programación”, no podrán ser las mismas personas que hagan las “Implementaciones”. Así, es que los programadores de Software no deberán tener acceso a modificar absolutamente ningún código de programación en ambiente productivo.
La Comunicación 4609 define:

- Análisis de Sistemas / Programación: diseño y desarrollo de los sistemas aplicativos, de acuerdo con las necesidades del negocio y del usuario.
- Implementaciones: puesta en producción de sistemas aplicativos.

Y expresamente indica que quien desempeñe una actividad no puede realizar la otra.

Asociado a esto, también indica en el capítulo 5, respecto de los cambios de software en producción: “5.8. Control de cambios a los sistemas productivos. A fin de minimizar el riesgo de actualizaciones accidentales en el entorno productivo, ingresar programas no

probados y evitar accesos no autorizados a los datos, las entidades financieras deben definir un adecuado esquema de separación entre sus ambientes informáticos de procesamiento (desarrollo, prueba y producción). Se deberá asegurar que los analistas y programadores de sistemas no tengan acceso al entorno productivo, ni los operadores accedan al ambiente ni a las herramientas utilizadas para el desarrollo y el mantenimiento de los sistemas de aplicación, de acuerdo con el cuadro del punto 2.5.4. sobre segregación de funciones. El proceso de actualización de nuevas versiones de sistemas deberá ser estrictamente controlado y realizado por personal que no tenga relación con el área de desarrollo y mantenimiento, mediante mecanismos que garanticen la correspondencia entre los programas "fuentes" y los programas "ejecutables". Asimismo, las nuevas versiones y las modificaciones de los programas aplicativos deben someterse a procedimientos formales de revisión, registro y aprobación, antes de la implementación definitiva en el ambiente de producción. En los casos de implementaciones de sistemas informáticos adquiridos, desarrollados o mantenidos por servicios externos, se deben registrar adecuadamente los cambios efectuados, verificando que todos los programas “fuentes” en custodia se correspondan con los programas “ejecutables”, antes de su puesta operativa en el ambiente de producción.”

¿Qué mide?

La detección del acceso a producción por parte de un programador para realizar modificaciones sobre el software bancario, ya sea por error (involuntario) o con conocimiento de causa

¿Cuándo se mide?

El control debe ser realizado en tiempo real, existen varias herramientas de software que nos permitirían cumplir con este control [36]

¿Quién ve esta métrica?

El gerente del área de Seguridad Informática (quien deberá comunicarlo al Gerente de

[36] La empresa Tango/04 por ejemplo, ofrece la posibilidad de implementar este tipo de controles con su solución VISUAL Message Center http://www.tango04.com/products/knowledgemodules/multiplatform-security-knowledge-module

Desarrollo) y eventualmente ante un incidente o problema de continuidad al directorio

¿Para qué se mide?

Para cumplir con la comunicación “A” 4609 del BCRA respecto de Gestión de Identidades, Segregación de funciones y Control de cambios a los sistemas productivos.

¿Por qué se mide?

Porque la segregación de funciones y ambientes fue ideada para proveer mayor seguridad funcional a las entidades que las respeten. Puntualmente, esta separación que no permitiría acceder a los desarrolladores a trabajar en sistemas productivos, está explícita en la comunicación “A” 4609 del BCRA. Más allá de ser ya conocida en todo el ambiente de Seguridad Informática como una buena práctica, por el gran riesgo que conlleva realizar pruebas sobre entornos productivos.

Posibles conclusiones a obtener

1) El punto más crítico es conocer en el momento, si alguien del equipo que realiza desarrollos está accediendo a modificar código en los sistemas productivos; y de aquí luego se podría analizar a lo largo del tiempo para saber si fue un incidente puntual aislado en el tiempo, o se nota cierta tendencia o periodicidad en los actos.

   Si se encuentra que este incidente se repite varias veces en un lapso de tiempo, o bien están mal diseñados los procesos y de ahí que se provoque que este incidente se dé con frecuencia, o bien se detecta un patrón sospechoso que deberá ser reportado al directorio.
2) Si es detectado este incidente, habrá que analizar cuál fue el impacto del mismo. Si hay posibilidades de deshacerlo o habrá que comunicar al directorio las consecuencias y luego tomar las medidas respectivas con el área de Desarrollo de Software (sea esta interna o tercerizada).

Evaluación de la métrica

En caso de demostrar que se hicieron modificaciones al código de algún aplicativo, y se aplicaron al ambiente de producción sin haber seguido el protocolo definido que indica

que primero se prueba en desarrollo, luego en Pre-producción (o también llamado ambiente de QA o *Testing*) y dado el visto bueno, recién ahí pasar los cambios al entorno productivo; la métrica se considerará "No aceptable".
De igual forma, la métrica tomará el valor "No aceptable", si se realizasen cambios en el código de aplicativos directamente sobre entornos productivos.
Idealmente para que este tipo de incidentes no ocurran, es importante promulgar e implementar una correcta división de entornos y permisos a los usuarios.
La métrica será "Aceptable", si en el período analizado no se encuentran incidentes que infrinjan este procedimiento definido.

Métrica:
Cuentas de usuario genéricas / Cuentas inactivas por más de 90 días

Dice la comunicación "A" 4609:
" 3.1.4.2. Estándares de acceso, de identificación y autenticación, y reglas de seguridad. Se deben implementar métodos de identificación y autenticación para controlar el acceso lógico a los sistemas y servicios informáticos, los que dependerán de la criticidad y el valor de los datos a proteger, debiéndose considerar: [...]

- la no utilización de denominaciones de usuario genérico para perfiles asignados a personas físicas;
- la identificación única (ID) de usuarios;
- la eliminación de las cuentas de usuario inactivas por un período mayor a 90 (noventa) días; […] "

Se entiende por cuentas genéricas, todas aquellas que son utilizadas por dos o más personas (ya sean de la entidad o de un proveedor externo a la misma).
La identificación única de usuarios, consiste en establecer una relación de uno a uno entre el usuario del sistema y el sistema.
Es una práctica relativamente habitual, que cuando un proveedor externo de la entidad comienza a realizar algún trabajo que requiera permisos de conexión a la red de la compañía durante un período de tiempo extenso, se le cree una cuenta para su comodidad de trabajo y velocidad en los tiempos de implementación; pero ocurre en

reiteradas oportunidades que luego el proveedor deja la entidad (al finalizar su implementación/proyecto por ejemplo) y su cuenta sigue inactiva pero nunca es eliminada del sistema de cuentas de la compañía. A las cuentas que están creadas, pero con imposibilidad de hacer uso de los servicios se las conoce como “inactivas”.

¿Qué mide?
La detección de la existencia de cuentas de usuario genéricas o inactivas

¿Cuándo se mide?
La creación de cuentas de usuario en las distintas aplicaciones, debe estar siempre bajo el visto bueno del área de Seguridad Informática. Si por algún motivo, otra área tiene acceso a realizar el ABM de cuentas de usuario, es preciso medir diariamente su actividad. De todas formas, se realiza un reporte mensual que de información sobre las cuentas inactivas de más de 90 días, y un reporte trimestral que contraste cada cuenta existente en el sistema contra la nómina de empleados de la entidad.

¿Quién ve esta métrica?
El gerente del área de Seguridad Informática.

¿Para qué se mide?
Para asegurar que no hay cuentas de usuario genéricas activas, o cuentas con más de 90 días de inactividad.

¿Por qué se mide?
Respecto de las cuentas genéricas, es evidente que ante un eventual incidente de seguridad, la misma no tiene asociada una persona física que se haga responsable por el hecho. Llegado este caso, se debería responsabilizar el encargado del área que posee la cuenta, o bien, el problema recaerá sobre el área de Seguridad Informática (por permitir la existencia de una cuenta genérica).
Sobre las cuentas inactivas por más de 90 días, se supone que si están inactivas durante ese período de tiempo sin que nadie reclame su activación, es que no se precisan para la operatoria diaria, más aún, es probable que pertenezcan a algún proveedor que

finalizó su proyecto, personal que ya no desempeña estas tareas, o un ex empleado de la entidad.

Posibles conclusiones a obtener

1) Si es que se están usando cuentas genéricas en la entidad. Acción que va en contra de las prácticas recomendadas en la mayoría de los estándares de seguridad informática. E incluso este accionar iría en contra de lo planteado como obligatorio en la comunicación "A" 4609 del BCRA.
2) La tendencia a la creación y utilización de este tipo de cuentas de usuario genéricas, y luego analizar por qué para determinar la causa raíz. Quizá sea una mala gestión de procesos de las áreas, simplificación de tareas, etc.
3) Indirectamente puede estar vinculado al sistema de *Single-Signon* y su implementación, como lo propone el BCRA en la Comunicación "A" 4609.
4) Si hay cuentas que permanecieron inactivas por más de tres meses, y que deban ser eliminadas para brindar mayor seguridad a la entidad.

Evaluación de la métrica

Será "Aceptable" en el caso que no existan cuentas de usuarios o aplicativos que no estén vinculadas a una persona física; y además que no haya en ninguno de los aplicativos, sistemas operativos o bases de datos, cuentas con más de 90 días de inactividad (ya sean de exempleados, consultores externos, creadas con fines de prueba, etc.).

En caso de infringir estos requisitos, la métrica será evaluada como "No aceptable".

4.3 Seguridad de la Infraestructura Tecnológica

¿Qué hay que tener en cuenta al momento de medir la seguridad de la IT[37]?

Controlar la seguridad física del edificio, cómo así de todos los elementos que componen la Infraestructura tecnológica de la entidad es parte fundamental de un buen programa de seguridad informática.

[37] IT: Infraestructura Tecnológica

Tener controlados los elementos de la IT, permite principalmente:

- Afrontar un accidente (de tipo natural, ataque, incidente de seguridad, etc.) sin perder la continuidad del negocio
- Restringir el acceso físico a la información a personal no autorizado
- Asegurar la disponibilidad e integridad de la información y de los canales a través de los cuales se transmite
- Reducir los riesgos de robo o pérdida de información contenida en dispositivos físicos

Métricas propuestas

Métrica:
Acceso a las instalaciones controladas

¿Qué mide?
Los intentos fallidos de acceso a las instalaciones controladas de la entidad.

¿Para qué medir las observaciones?
Para controlar, analizar y modificar si hace falta los permisos de acceso físico que tiene cada empleado a ciertas instalaciones controladas (sobre todo en las que se realiza el procesamiento de los datos críticos). O bien, para detectar accesos no autorizados a instalaciones con información o bienes críticos para el negocio.
El BCRA en su comunicación “A” 4609 indica que el directorio es el responsable de velar por la seguridad física de los activos de información, dice explícitamente: “3.2. Implementación de los controles de seguridad física aplicados a los activos de información. Los recursos humanos, los equipos, los programas, los archivos y los datos que involucran a las operaciones y procesos de la tecnología de la información representan uno de los activos críticos de las entidades financieras. El Directorio, o autoridad equivalente, es el responsable primario por la existencia de distintos niveles de seguridad física en correspondencia con el valor, confidencialidad y criticidad de los recursos a proteger y los riesgos identificados.
Los datos y equipos considerados críticos deben ser instalados en ambientes conforme a estándares y normas nacionales e internacionales pertinentes, que protejan a los mismos

contra fuego, calor, humedad, gases corrosivos, acceso indebido, desmagnetización y todo otro tipo de evento que pueda afectarlos.

El Directorio, o autoridad equivalente, debe considerar el uso de sistemas de monitoreo centralizado en todas las facilidades, con el objetivo de lograr un control preventivo y correctivo de fallas en la seguridad. Además, se valorará la inclusión de dispositivos de video y grabación de eventos en aquellas áreas con mayor concentración de activos de información.

[...]

3.2.2. Acceso físico a las instalaciones del centro de procesamiento de datos. Las instalaciones deben tener apropiados controles de acceso, por medio de los cuales se permita sólo el ingreso al área de procesamiento de datos a personal autorizado.

Se valorizará la existencia de varios niveles de acceso para los distintos recintos del centro de procesamiento de datos, basados en las definiciones de necesidad de acceder, en relación con la función o actividad primaria del personal interno o externo a la entidad financiera que solicite el ingreso. Todos los accesos, de rutina o de excepción, deben ser registrados por mecanismos que permitan la posterior revisión de los siguientes datos como mínimo: nombre completo, relación (interno o externo), en caso de ser externo deberá constar quién ha autorizado el acceso, motivo, hora de ingreso y hora de egreso."

¿Cuándo medir las observaciones?

Su recolección debe ser continua, y el reporte de accesos no autorizados debiera ser mensual.

¿Quién ve esta métrica?

El gerente de seguridad informática, el supervisor de la persona que intentó acceder a la instalación sin autorización, y eventualmente el directorio en caso que haya ocurrido algún incidente de seguridad que así lo amerite.

¿Cómo se miden las observaciones?

Desde el sistema que administra el control de acceso de tarjetas, ayudándose (en caso de contar con el recurso) con las cintas de grabación de las cámaras de video.

Posibles conclusiones a obtener

1) El control podría hacerse más en profundidad y correlacionando otros eventos, por ejemplo, para analizar a detalle que quien inicia sesión en su computadora y no haya pasado la tarjeta a la entrada del edificio. Indicando así que alguien está usando ese usuario indebidamente, o se están compartiendo cuentas, o la persona no está efectuando correctamente su ingreso al edificio.
2) Podría estar pasando que un intento fallido reiterado de cierto empleado a una instalación indique que esta persona esté intentando vulnerar el control impuesto o que realmente por su rol y actividades precise hacer uso de la instalación; si esta persona tiene que entrar, pedirá la tarjeta a un compañero que sí tenga acceso, incurriendo en una brecha y riesgo de seguridad aún mayor.

Métrica:
Capacidad de la red para soportar el servicio de HomeBanking

¿Qué mide?
El porcentaje del ancho de banda utilizado por sobre el disponible, y la cantidad de usuarios nuevos del servicio que se espera recibir.

¿Para qué medir las observaciones?
Porque la seguridad de la información debe garantizar confidencialidad, integridad y a la vez “disponibilidad” de los recursos críticos en la organización. Es por ello que deberían efectuarse los controles necesarios para asegurar la disponibilidad de suficiente capacidad de red para cumplir con las demandas del negocio. Haciendo además un análisis de la tendencia de uso a futuro en la entidad.
El BCRA, en su comunicación A 4609, dice explícitamente: “El Directorio o autoridad equivalente de la entidad [...] es el responsable primario del establecimiento y la existencia de un área que gestione la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas para todos los canales electrónicos por los que las entidades financieras realizan el ofrecimiento de sus productos y servicios. [...]
Los procedimientos que deben llevarse a cabo para el desarrollo de la tarea y control de

las áreas de sistemas de información, los cuales involucran al Directorio, Consejo de Administración o autoridad equivalente, Gerencia General, Gerencia de Sistemas de Información (SI) y personal de la entidad, deben estar diseñados para proveer un grado razonable de seguridad en relación con el logro de los objetivos y los recursos aplicados en los siguientes aspectos: [...] 1.5. **Disponibilidad**. Los recursos y la información, ante su requerimiento, deben estar disponibles en tiempo y forma."

Y en la comunicación A 5374, que se centra sobre Canales Electrónicos (entre ellos el HomeBanking), indica: "6.3.3. De la responsabilidad sobre los Canales Electrónicos. 6.3.3.1. El Directorio o autoridad equivalente de la entidad, es el responsable primario de la gestión de seguridad informática de la operatoria de los Canales Electrónicos desde el primer momento en que sus clientes se suscriben a los servicios ofrecidos por su intermedio o reciben medios de pago emitidos por ellas o en su nombre para su uso dentro de los alcances establecidos en el acuerdo de prestación.".

Estas dos declaraciones, hacen claramente responsable al directorio o gerencia general sobre la Disponibilidad de la información (el activo más importante de la entidad). En el caso de la métrica puntual, se centrará en la disponibilidad de red propia de uno de sus servicios al público usuario, llamado HomeBanking. Sabiendo que una gestión deficiente de los equipos de red (*routers, firewalls, hubs*, etc.) así como de las líneas de comunicación que los conectan, daría como resultado un problema en el servicio.

¿Cuándo medir las observaciones?

Los logs se pueden recolectar diariamente.

¿Quién ve esta métrica?

El gerente de Seguridad Informática, el gerente de Redes y Comunicaciones, el gerente de Marketing y el gerente de Sistemas e Infraestructura, quienes elevan al Directorio el resultado. Si del resultado del *"Capacity Planning"* que se realice se detecta que habrá un faltante del recurso, se debería realizar la respectiva propuesta

¿Cómo se miden las observaciones?

Recolectando información sobre el uso de red, actividad de usuarios, tendencias pasadas, informes solicitados al área de redes y marketing de la empresa, asesorándose con los PM (*Project Managers*) de la institución sobre proyectos futuros que impacten en

el ancho de red necesario.

Detalles de la Métrica

La idea fundamental es evitar una denegación de servicio para los servidores críticos de la empresa que soportan el servicio de HomeBanking; sería recomendable dividir entre tráfico entrante y saliente si se deseara además hacer un análisis de red para el soporte de los servicios d Banca Empresaria y Cotizaciones online. Una caída abrupta del ancho de banda disponible en la compañía entera hará que el negocio probablemente no tenga Disponibilidad de información en el momento preciso.

Si, por ejemplo, el sitio de HomeBanking (ya sea para personas físicas o Banking Empresas) dejase de prestar servicio, se produciría una cierta pérdida de dinero e imagen para la institución.

Si los servicios de red estuviesen tercerizados, entonces es importante que las mediciones tengan en cuenta los niveles de acuerdo de servicio (SLA – *Service Level Agreement*) contratados con cada proveedor.

Evaluación de la métrica

En la medida en que se rompan los números acordados en el acuerdo de nivel de servicio acordado (SLA), esta métrica tomará el valor: “No aceptable”.

Por el contrario, si todos los valores estuviesen dentro del acuerdo pactado, será evaluada como “Aceptable”.

Métrica:

Ciclo de tiempo para recuperación ante desastres

¿Qué mide?

El tiempo medio desde que se produce un desastre hasta que los procesos críticos del negocio están activos nuevamente

¿Para qué medir las observaciones?

La importancia reside en la correcta realización y verificación de los planes de continuidad del negocio. Entre ellos se incluyen también los planes de contingencia,

recuperación de desastres, etc.

Por un lado está el marco legal, donde la comunicación “A” 4609 del BCRA establece un capítulo dedicado a la continuidad del procesamiento de datos, de hecho indica que debieran hacerse pruebas del plan de contingencia periódicamente e informar los resultados al Directorio: “4.6. Pruebas de continuidad del procesamiento de datos.

El plan de continuidad de procesamiento de datos debe ser probado periódicamente, como mínimo una vez al año. Las pruebas deben permitir asegurar la operatoria integral de todos los sistemas automatizados críticos –de acuerdo con los análisis de riesgo previos-, a efectos de verificar que el plan está actualizado y es eficaz. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente del plan mencionado.

Deberá evidenciarse la existencia de un cronograma formal de pruebas que indicará cómo debe probarse cada elemento del plan, y la fecha en la cual cada una de las pruebas deberá ser efectuada. En las pruebas deben participar las áreas usuarias de los procesos de negocio, quienes deben verificar los resultados de las mismas. Se deberá documentar formalmente su satisfacción con el resultado de la prueba como medio para asegurar la continuidad de los procesos de negocio en caso de que ocurra una contingencia. La auditoría interna de la entidad también deberá conformar la satisfacción por el resultado de las mismas a tal efecto.

El informe realizado por las áreas usuarias y de auditoría interna deberá ser tomado en conocimiento por el Directorio, o autoridad equivalente de la entidad, y mantenido en archivo para su control posterior por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.”

Y por otro lado, hay un factor financiero, dado que ciertos procesos considerados críticos del negocio representan una pérdida económica a la compañía por cada minuto que no están operativos; por ejemplo, un servicio de cotización online que permita a clientes finales, o asesores de seguros solicitar un presupuesto para asegurar su auto o casa.

¿Cuándo medir las observaciones?

En cada una de las pruebas de DR y BCP (*Disaster Recovery y Business Continuity Plan*)

¿Quién ve esta métrica?

El directorio y el área de Seguridad de la Información.

¿Cómo se miden las observaciones?

En parte serán estimaciones o cálculos predictivos, puesto que si ocurriese un desastre natural no se puede medir de ante mano ni prevenir exactamente el impacto final en las instalaciones de la compañía. Pero también será importante probar empíricamente los planes de continuidad y las pruebas de contingencia periódicamente, con el afán de capacitar al personal debidamente y de medir el tiempo que lleva el ciclo entero desde que comienza a afectar uno o más servicios hasta que todo está operativo nuevamente, ya sea en esquema de contingencia o en su vuelta a producción. Se debería ir midiendo cada paso o etapa, para luego entender donde ajustar los tiempos en caso que alguna fase lleve proporcionalmente mucho más tiempo que el resto.

Posibles conclusiones a obtener

1) Sería interesante medir el tiempo estimado en poner nuevamente al negocio activo luego de ocurrido un desastre, y un objetivo sería ir reduciendo ese tiempo al mínimo, sin incurrir en un costo que sea más alto que el de no tener activo cierto dicho proceso crítico del negocio.
2) Habría que analizar a qué tipos de desastre puede enfrentarse la organización, y su probabilidad de ocurrencia. Por ejemplo, analizar situaciones como desastres naturales, incendios accidentales, tormentas e inundaciones, amenazas ocasionadas por el hombre, disturbios, sabotajes internos y externos deliberados; y para cada una de ellas tener un aproximado del riesgo que representaría a cada activo crítico de la entidad y la forma de que su pérdida afecta al negocio.

Métrica:

Seguridad en dispositivos personales

¿Qué mide?

La cantidad de incidentes de seguridad en dispositivos personales de los empleados que se conecten a la red de la entidad

¿Para qué medir las observaciones?

Porque cada vez más el personal utiliza dispositivos como teléfonos inteligentes, *tablets*, *notebooks/netbooks*; y es muy común que dentro de estos equipos transporte información propia de la entidad o software malicioso (de manera intencionada o no).

El riesgo se incrementa, porque son dispositivos móviles que circulan dentro y fuera de la empresa (por su carácter de uso personal).

¿Cuándo medir las observaciones?

Se miden diariamente para armar el informe, y se reportan trimestralmente

¿Quién ve esta métrica?

El gerente de Seguridad Informática, gerente de Redes y Comunicaciones y gerente de Sistemas de Información

¿Cómo se miden las observaciones?

Mediante logs de antivirus, logs de *software antispyware*, reportes del área de Mesa de Ayuda.

Detalles/Conclusiones de la Métrica

Esta métrica está asociada al término BYOD (por sus siglas en inglés *Bring Your Own Device*). Este término fue introducido por Ballagas, Rohs, Sheridan y Borchers[38] en el año 2004, y luego en el 2009 la empresa INTEL[39] (lo siguieron en el 2011 Unisys, VMWare y Citrix) lo hizo más conocido cuando notó la tendencia creciente de sus empleados de planta de traer sus propios dispositivos personales a la compañía.

Una encuesta llevada a cabo por la empresa Fortinet[40], durante mayo/junio del año pasado en más de quince países, dio a conocer que cerca del 74% (casi tres cuarta parte) de los encuestados incurre en esta práctica normalmente.

El riesgo mayor viene dado porque el 42% de los encuestados cree que parte de la pérdida de datos o la entrada de software malicioso a la compañía pudo haber sido

[38] http://www.vs.inf.ethz.ch/publ/papers/rohs-byod-2004.pdf
[39] http://www.gartner.com/technology/topics/byod.jsp
[40] http://www.fortinet.com/press_releases/120619.html

consecuencia del BYOD. Lo más preocupante es que esta práctica posiblemente no pueda ser erradicada, dado que un 36% de encuestados reconoce que infringió o infringiría una prohibición en esta materia.

Adicionalmente, la consultora Gartner encuestó a 2.000 CIOs, y concluyo que en el año 2016, el 38% de los empleadores pedirán a los trabajadores que tengan un equipo que lo usen en el entorno de trabajo. Esta cifra aumentará hasta el 50% para 2017[41].

Por lo expuesto anteriormente, es recomendable plantear políticas de aseguramiento de la información mediante la encriptación de datos en los dispositivos, planes de concientización, configuración adecuada de las políticas de seguridad y privacidad de estos dispositivos, entre otros. Y de aquí que esta métrica cobra sentido si se registra un alza en los incidentes detectados por Mesa de Ayuda o el área de Infraestructura Tecnológica o Seguridad Informática en sus aplicaciones Antivirus.

Métrica:

Acceso y disponibilidad de los Cajeros Automáticos (ATM)

¿Qué mide?

El correcto acceso y la disponibilidad operativa de los cajeros automáticos.

¿Para qué medir las observaciones?

Para estar enterados sí la comunicación entre los servidores centrales y los cajeros automáticos es exitosa, y además, conocer el estado de salud operativa de los mismos.

¿Cuándo medir las observaciones?

Se deben realizar mediciones en tiempo real.

¿Quién ve esta métrica?

El gerente de Seguridad Informática, el Gerente de Redes y Comunicaciones, y el Gerente de Sistemas. Luego se puede elevar un informe resumido donde se indique el Nivel de Servicio al que se ha comprometido al banco, y el Nivel de Servicio real que se

[41] http://www.gartner.com/newsroom/id/2466615

brindó al nivel directivo por sucursal y en total global.

¿Cómo se miden las observaciones?

Se integra un modelo de monitorización de lectura de Logs en tiempo real, con el sistema nativo en los cajeros que provee dicha información.

Posibles conclusiones a obtener

Las TAS (Terminales AutoServicio) están conectadas a los servidores centrales del banco de diversas formas. En algunos bancos se usa la red RedLink, en otros Banelco y en otras entidades se usan líneas redundantes contratadas a distintos proveedores de internet como ser Telecom, Telefónica, Telmex, iPlan, etc.

En este último caso, cada año se verifican los contratos de nivel de servicio acordado con cada proveedor a fin de saber si se renueva el contrato, o se cancela y se convoca a otro proveedor para el servicio; esta medición estaría dando cuenta de la calidad de atención a los usuarios finales, y la confiabilidad que tiene el banco respecto de sus cajeros electrónicos. Dado que si están con mucho tiempo de "*outage*", los clientes tienden a ir hacia el cajero más próximo (sea o no del banco en cuestión).

Evaluación de la métrica

En la medida en que se rompan los números acordados en el acuerdo de nivel de servicio acordado (SLA), esta métrica tomará el valor: "No aceptable".

Por el contrario, si todos los valores estuviesen dentro del acuerdo pactado, será evaluada como "Aceptable".

Capítulo 5

Trabajo de Campo

En tres entidades bancarias[42] de tamaño medio que operan en el mercado financiero argentino se analizó la aplicación de las siguientes métricas pertenecientes a distintos niveles organizativos, y los resultados de la implementación se detallan a continuación. Cabe destacar que todas las métricas implementadas son las que están definidas teóricamente en este mismo trabajo en el capítulo 4.

- Indicadores ESTRATÉGICOS
  - Estado general de seguridad del sistema MEP (Medio Electrónico de Pagos)
  - Incumplimiento de las normativas o leyes vigentes
- Indicadores TÁCTICOS
  - Acceso y disponibilidad de los Cajeros Automáticos (ATMs)
  - Solicitud de Acceso (a aplicaciones / servicios de software de la entidad)
  - Capacidad de la red para soportar el servicio de HomeBanking
- Indicadores OPERATIVOS
  - Intentos no autorizados de acceso a Datos Confidenciales
  - Abuso de sitios web restringidos, descargas de software ilegal, control de SPAM
  - Acceso de programadores al código fuente del sistema de producción
  - Cuentas de usuario genéricas / Cuentas inactivas por más de 90 días

[42] Las mismas no serán nombradas para mantener la confidencialidad acordada antes de iniciar este trabajo

Indicadores ESTRATÉGICOS (Directorio)

Métrica aplicada:

Estado general de seguridad del sistema MEP (Medio Electrónico de Pagos) [43]

Experiencia práctica:

MEP es un sistema provisto por el BCRA para Medio Electrónico de Pagos. La aplicación MEP provee información de la actividad de usuarios, tanto usuarios comunes como administradores. Esta información está almacenada en una base de datos y posee diferentes tablas de las cuales se tuvieron en cuenta las siguientes tres:

- bc05_administradores_log
- bc03_usuarios_log
- movimientos_log

Estas tres tablas almacenan información acerca de la actividad de usuarios administradores, actividad de usuarios comunes y movimientos respectivamente. Uno de los detalles al implementar este control sobre MEP, fue que las dos primeras tablas tienen los datos del día en curso, es decir que diariamente se depuran de forma automática y no tienen un campo del tipo *timestamp* lo que imposibilita una lectura incremental de las mismas.

Al estar imposibilitada la lectura incremental por fecha, se aplicó una solución alternativa que fue poner *triggers* sobre las tablas. Un *trigger* sobre la tabla bc05_administradores_log y otro sobre la tabla bc03_usuarios_log, el objetivo de estos *triggers* es que para cada registro que se inserte sobre las tablas

[43] La definición teórica de la métrica se encuentra en la página 39, en este mismo trabajo

mencionadas el mismo se inserte en nuevas tablas [44] agregando un campo *timestamp* para poder realizar una lectura incremental y cronológica. Las tablas a crear tendrán los mismos campos que sus respectivas de MEP con el agregado del campo fecha y estarán alojadas en una base de datos distinta a la del sistema MEP. En la tabla de movimientos esto no fue necesario.

En resumen, se debió:

- Crear base de datos B04_APLICACIONES
- Crear tabla MEP_usuarios_log
- Crear tabla MEP_administradores_log
- Crear el Trigger en base bc05_administradores_log
- Crear el Trigger en base bc03_usuarios_log

Los comandos ejecutados para la creación de tablas y triggers fueron los siguientes:

Objeto	Detalles	Script
Tabla MEP_usuarios_log	Actividad de usuarios dentro de la aplicación	CREATE TABLE [dbo].[MEP_usuarios_log]([pk_codigo] [int] IDENTITY(1,1) NOT NULL, [cod_usuario] [char](8) NOT NULL, [id_sesion] [varchar](8) NOT NULL, [hora_inicio] [char](8) NOT NULL, [hora_cierre] [char](8) NOT NULL, [usuario_cierre] [char](8) NOT NULL, [fecha] [char](10) NULL, CONSTRAINT [PK_MEP_usuarios_log] PRIMARY KEY NONCLUSTERED ([pk_codigo] ASC) ON [PRIMARY]) ON [PRIMARY]

[44] Programado por Esteban Bietti, consultor de Barcelona/04 para el áre de Servicios Profesionales.

Tabla MEP_administradores_log	Actividad de usuarios administradores dentro de la aplicación	CREATE TABLE [dbo].[MEP_administradores_log]([pk_codigo] [int] IDENTITY(1,1) NOT NULL, [cod_usuario] [char](8) NOT NULL, [hora_tarea] [varchar](19) NOT NULL, [tipo_tarea] [char](2) NULL, [descripcion_log] [char](50) NULL, CONSTRAINT [PK_bc05_administradores_log] PRIMARY KEY CLUSTERED ([pk_codigo] ASC)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]) ON [PRIMARY]
trigger en la base bc05_administradores_log		CREATE TRIGGER [dbo].[B04_MEP_ADMINISTRADORES] -- Cambiar este nombre si se necesita cambiar el nombre del trigger por algun otro ON [dbo].[bc05_administradores_log] AFTER INSERT AS BEGIN insert into B04_MEP_ADMINISTRADORES.dbo.bc05_administradores_log (cod_usuario,hora_tarea,tipo_tarea,descripcion_log) select pk_cod_usuario, convert(varchar(10),getdate(),111)+' '+pk_hora_tarea,bc05_tipo_tarea,bc05_descripcion_log from inserted END
trigger en base bc03_usuarios_log		CREATE TRIGGER [B04_MEP_USUARIOS] -- Cambiar este nombre si se necesita cambiar el nombre del trigger por algun otro ON [dbo].[bc03_usuarios_log] AFTER INSERT AS BEGIN insert into B04_APLICACIONES.dbo.MEP_usuarios_log (cod_usuario,id_sesion,hora_inicio,hora_cierre,usuario_cierre, fecha) select Pk_cod_usuario, Pk_id_sesion, bc03_hora_inicio, bc03_hora_cierre, bc03_usuario_cierre,convert(char(10),getdate(),111) from inserted END

Ejemplos de Logs del sistema MEP[45]:

LOG DE ACTIVIDAD DE USUARIOS

[45] Los archivos aquí expuestos son del año 2007, pero la esencia del control es la misma con los datos al día de hoy, y se prefirió no ponerla por temas de privacidad. Asimismo, muchos de los datos han sido modificados aleatoriamente por las mismas razones.

```
1> 2> 1> 2> 3>  Pk_cod_usuario   Pk_id_sesion     bc03_hora_inicio bc03_hora_cierre bc03_usuario_cierre
 --------------- --------------- --------------- --------------- --------------------
 usuarioMEP1      19274638        19:37:46        19:53:51        usuarioMEP1
 usirMEP22        200543870       20:05:08        20:18:45        uaerMEP2
 admep121         19541281        19:54:19        19:54:50        adgepg721
 en003            085345275       08:53:52        08:54:05        Kerberos
 admep126         102154257       10:11:52        10:25:27        admeg326
 userMEP23        102847429       10:28:47        10:36:14        userMEP23
 userMEP23        10523353        10:52:02        10:53:20        userMEP23
 userMEP23        11022649        11:11:06        11:03:46        userMEP23
 userMEP23        11322744        11:32:27        11:34:13        userMEP23
 userMEP23        122225690       12:12:56        12:14:25        userMEP23
 userMEP4         12384352        12:38:14        14:18:36        TimeOut
 userMEP23        14520083        14:52:03        14:53:49        userMEP23
 userMEP23        15233851        15:26:28        15:27:38        userMEP23
 userMEP4         16130021        16:13:12        18:06:53        TimeOut
 enarg003         15552333        15:55:20        15:55:41        Kerberos
 userMEP23        163223401       16:32:10        16:34:15        userMEP23
 ususarioMEP1     164023594       16:40:35        19:17:12        TimeOut
 usserMEP4        180943586       18:09:45        19:03:19        userMEP4
 usesrMEP2        190543318       19:05:03        19:40:43        TimeOut
 usuaaioMEP1      19274570        19:27:45        0               0
 userMEP22        195554321       19:55:57        0               0
 usuarioMEP11     122534358       12:25:36        16:34:54        TimeOut
 userMEP24        144053390       14:40:59        16:03:23        TimeOut

(23 rows affected)
1> 2> 1>
```

LOG DE ACTIVIDAD DE ADMINISTRADORES

```
1> 2> 1> 2> 3>  Pk_cod_usuario   Pk_hora_tarea    bc05_tipo_tarea bc05_descripcion_log
 --------------- --------------- --------------- ----------------------------------------------------------------------------------------------------
 admep141         19:54:33        25              MEP TODOS
 admep121         19:54:45        30              MEP CIERRE
 admep166         10:22:21        30              MEP CIERRE
 admep166         10:22:30        28              MEP APERTURA: XX/XX/XXXX
 admep166         10:22:47        24              MEP TODOS
 admep136         10:25:22        31              MEP ACTUALIZACION TABLAS MEP
 admep171         19:54:33        25              MEP TODOS
 admep181         19:54:45        30              MEP CIERRE
 admep196         10:22:21        30              MEP CIERRE
 admep196         10:22:30        28              MEP APERTURA: XX/XX/XXXX
 admep196         10:22:47        24              MEP TODOS
 admep196         10:25:22        31              MEP ACTUALIZACION TABLAS MEP
 admep101         19:54:45        30              MEP CIERRE
 admep196         10:22:21        30              MEP CIERRE
 admep186         10:22:30        28              MEP APERTURA: XX/XX/XXXX
 admep176         10:22:47        24              MEP TODOS
 admep166         10:25:22        31              MEP ACTUALIZACION TABLAS MEP
```

LOG DE MOVIMIENTOS

mp18_movimientos_log

```
1> 2> 1> 2> 3>

Pk_fecha_hora_log
Pk_nro_movimiento
Pk_nro_intento
```

Pk_operatoria
Pk_cod_usuario
mp18_tipo_movimiento
mp18_entidad_deudora
mp18_cuenta_deudora
mp18_entidad_acreedora
mp18_cuenta_acreedora
mp18_importe
mp18_moneda
mp18_contacto_apynom
mp18_contacto_tipo
mp18_contacto_via
mp18_contacto_via_tipo
mp18_campos
mp18_checksum

11/11/XXXX 14:33:05 29 0 DL1 l0067334 E 7 7 285 285
104853.10 ARP C.A.E. BC 6329-0000
TE 28506551300655019228 21;30644718979;VAR;VARIOS;00700160200000038120 66;30549220955;AUTOMOTORES
JUAN MANUE;SI; 12253658
11/11/XXXX 17:01:42 99 0 DL0 L0067334 C 7 7 16 16
120000.00 ARP C.A.E. BC 6329-0000
TE 01688881000006072601 91;30500846301;VAR;VARIOS;00709990200000449603 15;30500846301;ABBOTT
LABORATORIES AR;SI; checksum
11/11/XXXX 17:23:44 141 0 DL1 L0067334 C 7 7 17 17
896596.63 ARP C.A.E. BC 6329-0000
TE 01704703200000000049791;30530589265;VAR;VARIOS;00709990200000591106 64;30592238892;B T U S A;SI;
checksum
11/11/XXXX 17:23:44 142 0 DL0 L0067334 C 7 7 299 299
1044000.00 ARP C.A.E. BC 6329-0000
TE 29900000000000139300 06;30501086246;VAR;VARIOS;00700764200000015938 22;30501086246;BENITO RORORO
E HIJOS;SI; checksum
11/11/XXXX 17:23:44 143 0 DL0 L0067334 C 7 7 309 309
1075000.00 ARP C.A.E. BC 6329-0000
TE 30900002010003100449 66;30685376349;VAR;VARIOS;00700764200000107770 42;30685376349;ORANGE
ORANGE S A;SI; checksum
11/11/XXXX 17:23:44 144 0 DL7 L0067334 C 7 7 34 34
1514023.97 ARP Villé Jose E BC 6329-2333
TE bco patagonia sudameris sa soc dep lombard ahorro dolar cuit 30500006613 cta 100070829 cbu
03400104081000708290 07; checksum
11/11/XXXX 17:23:52 145 0 DL7 L0067334 C 7 7 17 17
3024041.09 ARP Villé Jose E BC 6329-2333
TE fba renta pesos fci bco frances cuit 30500003193 cbu 01704932200000000439 84;
checksum
11/11/XXXX 17:23:53 146 0 DL7 L0067334 C 7 7 72 72
10116794.52 ARP Villé Jose E BC 6329-2333
TE bco rio soc dep super fondo ahorro pesos fci cuit 30500008454 cta 214946 cbu 0720000720000002149 68;
checksum
11/11/XXXX 17:28:10 137 0 DT0 l0067334 E 7 7 325 325
170239.90 ARP Romina Irma M BC 6329-2672
TE Rendicion cobranza diaria del dia 08-02-XXXX - Fideicomiso Financiero Galicia Prendas Comerciales I o-DBSA -
Cuenta Recaudadora Nro 101132330008 CBU 3250000200- 011323300089;
16403594
11/11/XXXX 17:46:49 163 0 DL1 L0067334 C 7 7 265 265
147672.80 ARP C.A.E. BC 6329-0000
TE 26504007020400543766 85;30591195200;VAR;VARIOS;00700993200000002426 19;30516868119;ODFJELL
TERMINALS TAGS;SI; checksum
11/11/XXXX 17:50:11 173 0 DL4 l0067334 E 7 7 389 389
1701225.51 ARP Villé Jose E BC 6329-2333
TE ORDEN SERVICIO ELECTRONICO DE PAGO SA CUIT 30659863789;
16403594
11/11/XXXX 17:50:41 150 0 DR1 l0067334 E 7 80007 15
80015 11962.14 USD C.A.E. BC 6329-0000
TE 01509094110000003419 38;30693184947;VAR;VARIOS;00709990310097513488 21;33506737449;NIDERA S A;
16403594
11/11/XXXX 17:01:33 73 0 DL1 L0067334 C 7 7 93 93
2334.12 ARP C.A.E. BC 6329-0000 TE
09303445215002019370 46;27101057017;VAR;VARIOS;00709990200000495958 22;30540385102;MOLINO NUEVO SA;SI;
checksum
11/11/XXXX 17:01:34 74 0 DR1 L0067334 C 7 80007 15
80015 2694.94 USD C.A.E. BC 6329-0000
TE 01509094110000003419 38;30693184947;VAR;VARIOS;00701194310097500531 17;33708110049;ALICAMPO SRL;
checksum
11/11/XXXX 14:27:43 28 0 DL0 l0067334 E 7 7 11 11

```
100000.00 ARP C.A.E. BC 6329-0000
TE 01105995200000052584361;30709753424;VAR;VARIOS;00709990200000060545853;30709753424;JOSE J CHEDIACK
S A I;SI; 12253658
 11/11/XXXX 14:27:49 30 0 DL0 l0067334 E 7 7 17 17
110000.00 ARP C.A.E. BC 6329-0000
TE
01704895200000000032065;30599298173;VAR;VARIOS;00701682200000000506755;30599298173;ESTABLECIMIENTO MADERE;SI;
12253658
 11/11/XXXX 14:27:53 31 0 DL0 l0067334 E 7 7 387 387
200000.00 ARP C.A.E. BC 6329-0000
TE 38700031008016001619O4;30503926365;VAR;VARIOS;00701095200000000919999;30503926365;ZF SACHS
ARGENTINA SA;SI; 12253658
 11/11/XXXX 14:27:59 32 0 DL0 l0067334 E 7 7 72 72
200000.00 ARP C.A.E. BC 6329-0000
TE 07202614200000000300586;30503926365;VAR;VARIOS;00701095200000000919999;30503926365;ZF SACHS
ARGENTINA SA;SI; 12253658
 11/11/XXXX 14:28:03 34 0 DL0 l0067334 E 7 7 301 301
1000000.00 ARP C.A.E. BC 6329-0000
TE 30100013300000010081715;30532847547;VAR;VARIOS;00701118200000000005528;30532847547;BAZAR AVENIDA
S A;SI; 12253658
 11/11/XXXX 14:32:59 27 0 DL1 l0067334 E 7 7 34 34
90000.00 ARP C.A.E. BC 6329-0000 TE
03401510001000008840O9;33677414419;VAR;VARIOS;00700252200000003212217;30573785742;MULTIRADIO SA;SI;
12253658

(352 rows affected)
1> >2
```

Comentarios/Conclusiones:

Una vez que se pudo salvar el problema de que ciertas tablas claves para la monitorización del sistema MEP no contaban con la fecha para poder hacer una auditoría que tenga en cuenta este dato clave, se llevó adelante la planificación de reportes mensuales con la siguiente información:

1) **Reporte "MEP - Movimientos y Respuesta"**

   Campo 1: Nro de movimiento

   Campo 2: Nro de intento

   Campo 3: Operatoria

   Campo 4: Fecha y hora de envio

   Campo 5: Nro de transacción

   Campo 6: Fecha y hora de transacción

   Campo 7: Saldo actualizado

   Campo 8: Estado

   Campo 9: Repuesta

2) **Reporte "MEP – Log de Movimientos"**

Campo 1: Fecha y hora de log

Campo 2: Operatoria

Campo 3: Código de Usuario

Campo 4: Tipo de movimiento

Campo 5: Importe

Campo 6: Moneda

Campo 7: Apellido y nombre del contacto

3) **Reporte "MEP – Log de Movimientos por entidad"**

Campo 1: Fecha y hora de log

Campo 2: Número de movimiento

Campo 3: Número de intento

Campo 4: Operatoria

Campo 5: Código de Usuario

Campo 6: Tipo de Movimiento

Campo 7: Entidad deudora

Campo 8: Entidad acreedora

Campo 9: Cuenta acreedora

Campo 10: Importe

Campo 11: Moneda

Campo 12: Apellido y nombre del contacto

Campo 13: Tipo de contacto

Campo 14: Vía de Contacto y Tipo

Y alarmas en tiempo real para el aviso inmediato de la ocurrencia de los siguientes eventos:

1) Blanqueo de clave
2) Desbloqueo de clave

3) ABM de Usuarios
4) Asignación de perfiles de usuarios
5) Habilitación de usuario
6) ABM de operatoria

Esto permitió al Gerente de Seguridad Informática tener una supervisión completa de uno de los sistemas críticos de transacciones electrónicas de la entidad bancaria. Y adicionalmente, en caso de detectar una alerta (se configuró la llegada de un correo electrónico por cada ocurrencia de alguno de los seis eventos antes mencionados) en tiempo real, y validar que fuese un incidente anormal, podía asignar a su equipo de trabajo a investigarlo antes del cierre diario del sistema; de forma de tomar acciones durante ese mismo día contable.

Métrica aplicada:

Incumplimiento de las normativas o leyes vigentes [46]

Experiencia práctica:

Esta métrica se basa en un informe mensual obligatorio del “Seguimiento de Observaciones”, y quizá lo que más despertó el interés en los gerentes de alto rango fue su formato de presentación en una suerte de tablero de comando.

Una de las dificultades de esta métrica, es su obtención. La misma se realiza de forma manual y precisa varias horas para su desarrollo. Solamente se pudieron automatizar los indicadores gráficos para mostrar a directores y al área de seguridad informática.

La institución cuenta con un *software* de gestión de auditoría donde se vuelcan, de forma centralizada, todos los puntos de distintas comunicaciones y leyes que debe cumplir la entidad.

[46] La definición teórica de la métrica se encuentra en la página 36, en este mismo trabajo.

Este *software,* permite insertar el detalle de las posibles medidas a tomar para mitigar / eliminar / delegar el riesgo inherente del incumplimiento, así como también los posibles problemas que traería el no tomar ninguna de dichas acciones propuestas. [47]

Con un *software* de monitorización en tiempo real, se accedió a la base de datos de dicho aplicativo y se realizaron consultas agrupadas por mes. Estas consultas comparaban:

- Una lista de los puntos de auditoría a cumplir por la entidad
- Detalle de los puntos incumplidos [48]
    - Mes de detección del punto de auditoría
    - Entidad que regula su cumplimiento
    - Riesgos por incumplimiento
    - Acciones a tomar para su mitigación o prevención [49]
    - Mes del próximo control de auditoría
    - Fecha comprometida de resolución (si la hubiese)

En el caso de esta entidad financiera, fue muy importante detectar el mes en donde una auditoría (interna o externa) detectaba el incumplimiento, y por ello en la consulta a la base de datos se agruparon todos los puntos por MES.

Para una rápida visualización, se asignaron colores a cada mes, que reflejan el estado de situación del *compliance*, y las acciones tomadas por el sector de seguridad informática para cubrir con los puntos. Cada mes tiene un ícono que refleja el estado en el que se encuentra la resolución de los controles de seguridad:

- **Verde**: Finalizado (Existe un control, y una acción de resolución asociada)

[47] Por cuestiones de confidencialidad no fue posible obtener documentación del software, así como capturas de pantalla ni acceso a su base de datos con contenido productivo.
[48] Y que cuya categorización sea Alta o Crítica. Se tuvieron en cuenta únicamente los puntos que pudiesen traer problemas legales o económicos.
[49] Solamente en los casos que el punto ya estaba analizado y se tenía certeza de cómo actuar para corregir la vulnerabilidad.

- **Amarillo**: Pendiente parcialmente (La acción está en proceso de finalización)
- **Azul**: Pendiente de generación de información para la métrica (mes que aún no se realizó el control)
- **Rojo**: Pendiente de regularización (hay controles que aún no tienen una acción realizada)

La siguiente es una imagen de la sección superior izquierda del plasma de 42" ubicado en la sala de seguridad informática (tomada en Abril del 2012):

Puede notarse que para el mes en curso, todavía había puntos de auditoría incumplidos que fueron detectados ese mes y que no tenían acciones de resolución vinculadas a los mismos.

Para el resto de meses siguientes se dejó el color AZUL, puesto que aún no se habían relevado los puntos pendientes ni su estado de desarrollo.

En una entrevista con el CISO, al hablar de estas métricas y cómo las entendía él, y cómo las mostraba a su jefe, expresó: *"La idea es tener una visión de más largo plazo (6 meses o más), viéndolo como Gerencia, es decir, no solo desde la detección de un problema (control), sino hasta que se realice una acción en correspondencia con el incidente. Pero eso nos va a llevar un tiempo de trabajar con esto, y tener históricos mensuales de años anteriores… cosa que hoy no tenemos aún. En el fondo, lo que yo quiero es que con el tiempo, se puedan madurar los controles para lograr un grupo de Semáforos de la Gerencia con los indicadores más importantes respecto de cumplimiento.*

Ahora esta información la puede ver todo el banco porque está ubicada en un plasma de 42" en el centro del quinto piso, por un lado está buenísimo porque da visibilidad del trabajo que se hace en el área de seguridad informática para cumplir con todo lo que se le demanda en cuanto a auditoría, y por otro lado hay meses que es un quemo porque tenemos todo en rojo y los más curiosos se acercan a preguntar porque está en rojo y si es peligroso que estemos así.

Yo creo que esto también sirve al equipo de motivador, porque los incita a mantener un ritmo de trabajo continuo para que todo esté en verde y nadie se les acerque a preguntarles cuándo lo van a solucionar."

Comentarios/Conclusiones:

Si bien la recolección de información para preparar esta métrica lleva bastante tiempo, según comentó el CISO la utilidad de la misma es altísima para ellos. Además, este es uno de los indicadores que interesan a directivos y como tal ayuda a la gerencia de seguridad informática a dar visibilidad de su trabajo y a justificar ciertos proyectos que operen de forma directa sobre mejoras de *compliance*.

Indicadores TÁCTICOS (Gerencias Medias)

Métrica aplicada:

Acceso y disponibilidad de los Cajeros Automáticos (ATMs) [50]

Experiencia práctica:

El Cajero Automático también conocido como ATM (*Automatic Teller Machine*) [51], es un dispositivo cuya principal finalidad es dispensar efectivo a los clientes, sin embargo, también proporciona servicios adicionales como la consulta de saldos, traspasos entre cuentas propias y de terceros, pagos de servicios, entre otros.

El objetivo del banco es tener los Cajeros Automáticos donde los clientes lo requieren, brindándoles mayor comodidad y seguridad.

Ante un eventual problema que involucre la disponibilidad de los cajeros automáticos el personal del banco debe actuar de forma inmediata (sobre todo en los períodos de atención crítica definidos en los calendarios). La entidad pone de manifiesto que ha habido históricamente problemas de denegación de servicio donde no se pudo detectar el origen de los mismos, pero saben que en la medida que los clientes usen cada vez más los ATMs es prioridad tenerlos siempre disponibles, dado que hay momentos donde la actividad de los Cajeros Automáticos se torna crítica y prescindir de ellos sería aceptar que el banco pierde imagen, confiabilidad, calidad de servicio al cliente, comisión sobre ciertas operaciones, se incrementa el trabajo en línea de cajas, etc.

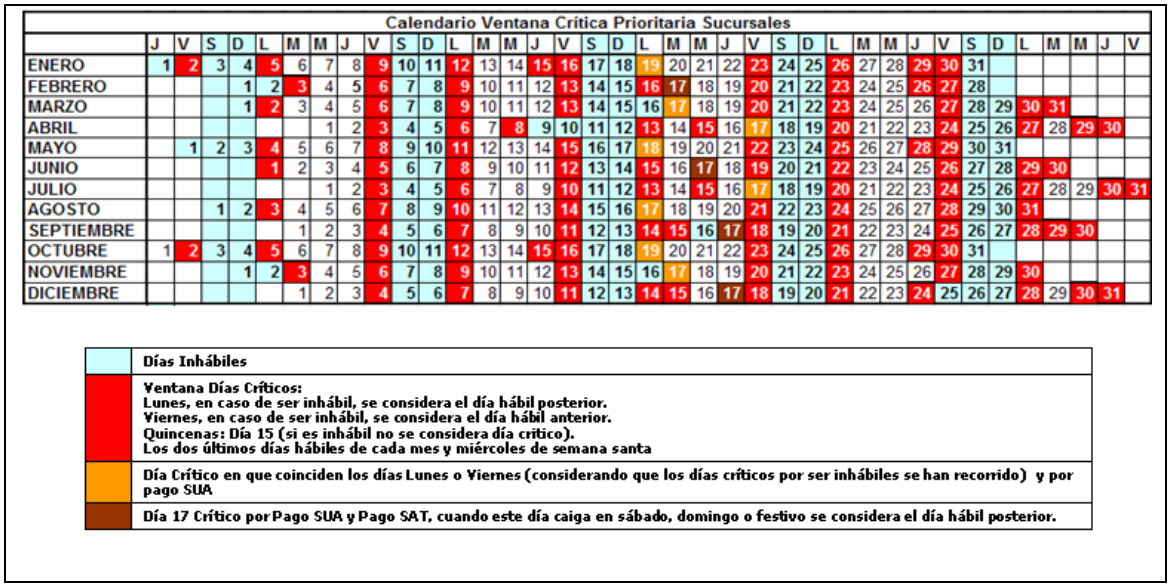
[50] La definición teórica de la métrica se encuentra en la página 61, en este mismo trabajo
[51] El Banco Central de la República Argentina en su comunicación "A" 5374 los define de la siguiente forma: *"Cajeros Automáticos (ATM). Comprende a las redes, dispositivos, entornos informáticos, operativos y de servicio destinados al usuario de servicios financieros, que se basan en la utilización de los dispositivos conocidos cómo Cajeros Automáticos o ATM ("Automated Teller Machine") en sus distintas modalidades: Dispensadores de Efectivo, Kioscos Digitales, entre otros y que permitan por lo menos, la extracción de efectivo sin intervención de un operador humano."*

Por esta razón, se hizo necesario armar primero un sistema calendarizado de cada cajero/sucursal, días de la semana y horarios (para dividir los momentos que son críticos de los que no lo son) de la siguiente forma:

Días Normales	
Ventana General del Servicio	Lunes a Viernes: 08:30 a 20:00 hrs.
Ventana Crítica del Servicio (Ponderación del 90%)	Lunes a Viernes: 08:30 a 17:00 hrs.
Ventana No Crítica (Ponderación del 10%)	Lunes a Viernes 17:00 a 20:00 hrs.

Días Críticos	
Ventana General del Servicio	Lunes a Viernes: 08:30 a 20:00 hrs.
Ventana Crítica del Servicio (Ponderación del 30%)	Lunes a Viernes: 08:30 a 12:00 hrs. Lunes a Viernes: 16:00 a 17:00 hrs.
Ventana Crítica Prioritaria del Servicio (Ponderación del 60%)	Lunes a Viernes 12:00 a 16:00 hrs. Días Críticos -Ver Calendario 2011
Ventana No Crítica (Ponderación del 10%)	Lunes a Viernes 17:00 a 20:00 hrs.

Calendario 2011



Calendario Ventana Crítica Prioritaria Sucursales

	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V
ENERO	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						
FEBRERO				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28						
MARZO				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31			
ABRIL							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
MAYO		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31					
JUNIO					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
JULIO							1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
AGOSTO			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
SEPTIEMBRE						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
OCTUBRE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31						
NOVIEMBRE				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30				
DICIEMBRE						1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	

	Días Inhábiles
	Ventana Días Críticos: Lunes, en caso de ser inhábil, se considera el día hábil posterior. Viernes, en caso de ser inhábil, se considera el día hábil anterior. Quincenas: Día 15 (si es inhábil no se considera día crítico). Los dos últimos días hábiles de cada mes y miércoles de semana santa
	Día Crítico en que coinciden los días Lunes o Viernes (considerando que los días críticos por ser inhábiles se han recorrido) y por pago SUA
	Día 17 Crítico por Pago SUA y Pago SAT, cuando este día caiga en sábado, domingo o festivo se considera el día hábil posterior.

Los Cajeros Automáticos del banco están distribuidos a nivel nacional y se pueden clasificar en 3 tipos: Cajeros de Sucursal, Cajeros Remotos Públicos y Cajeros Remotos en Empresas.

Cajeros Automáticos en Sucursales.

Su característica principal es que forman parte de la sucursal, pero con acceso al público independiente, están ubicados en zonas geográficas con alto volumen de clientes, su objetivo es desahogar transacciones de la sucursal que fácilmente pueden realizarse a través de ellos.

Estos cajeros generalmente son operados por los apoderados de la propia sucursal en donde están situados, por lo que el papel que desempeñan los apoderados es determinante para que estén disponibles todo el tiempo.

Cajeros Automáticos Remotos Públicos.

Ubicados, sin la presencia de sucursal, en zonas con alto tráfico tales como: centros comerciales, supermercados, aeropuertos, negocios específicos, etc., con atención al público en general. El principal objetivo es acercar el servicio a los

clientes y a no clientes de la institución, en los centros de consumo para su comodidad y seguridad.

Este tipo de cajeros son operados por empresas especializadas de traslado de valores.

Cajeros Automáticos Remotos en Empresas.

Están ubicados en su mayoría dentro de las instalaciones de ciertas empresas, algunos tienen acceso al público, pero la gran mayoría tiene acceso restringido solo para el personal de la empresa en cuestión. Su principal objetivo es dar servicio a los empleados de la empresa donde se encuentran, generalmente asociados a beneficios y asociaciones o negocios con dicha compañía.

Son operados por empresas especializadas en traslado de valores.

Una vez que se determinaron los tipos de cajeros, los horarios críticos (días, horas, días especiales), y las formas de conexión entre los cajeros y las oficinas centrales de la institución, se implementó un sistema de medición de red que alerta en tiempo real los eventos de desconexión de alguna de las líneas contra los cajeros automáticos; y reportes mensuales sobre el estado general de conectividad contra los mismos.

En el reporte se tiene en cuenta un SLA (*Service Level Agreement*) determinado para cada tipo de cajero, y cada sucursal (dependiendo mayoritariamente de la cantidad de transacciones que normalmente realiza cada Cajero y Sucursal en general); y además tiene en cuenta, en lugares con líneas redundantes:

> **NO DISPONIBLE:** Si todos los medios de comunicación contra la sucursal/cajero están indisponibles.
>
> **ADVERTENCIA:** Si se mantiene conectividad contra los dispositivos pero no es del 100% de sus vínculos.

CORRECTO FUNCIONAMIENTO: Si todos los vínculos contra los dispositivos están activos y funcionando de manera correcta.

Ejemplo de Reporte mensual:

SUCURSALES	Meta	Ene	Feb	Mar	10
Total Redes	0.38	0.36	0.32	0.20	0.29

CANALES	Meta	Ene	Feb	Mar	10
Cajeros Automáticos	4.20	3.01	3.43	2.75	3.06
[illegible]	0.85	0.01	0.38	0.04	0.14
[illegible]	0.85	0.01	0.38	0.12	0.17
[illegible]	0.50	0.07	0.30	0.11	0.16
[illegible]	0.70	1.20	0.54	0.00	0.58
[illegible]	0.30	0.00	0.05	0.00	0.02
TOTAL SERVICIOS	1.45	0.96	1.11	0.79	0.95

Semáforo atm´s

0 - 3.15	
3.16 - 4.20	
4.21 - 5.25	
5.26 - en edelante	

Código de colores

Excelente	Resultados OK dentro de Meta
Bueno	
Alerta	Los resultados No cumplen la Meta
Malo	

Ejemplo[52] de alerta visual en tiempo real:

[52] El ejemplo gráfico está basado en las sucursales de otro país para que no se llegue a determinar la sucursal en base a la cantidad de cajeros y su ubicación geográfica.


Tables
Management
Help
Host
Agencias/Sucursales
Time Span
Last 15 Minutes
Time Scale
Minute
Auto Refresh
Show Dashboard
Export to:
Sucursales
Cajeros Automáticos
Telecomunicaciones
Ofimática
Mensajería


Indisponibilidad de cajeros
Totales País
Indisponibles por estado (Peores 4)
Indisponibles por Causa(Peores 5)
Baja California
Sonora
Chihuahua
Coahuila
Queretaro
DF
Tamaulipas
Nuevo Leon
Durango
Hidalgo
Yucatan
Sinaloa
Zacatecas
San Luis Potosi
Tlaxcala
Campeche
Baja California sur
Aguas Calientes
Nayarit
Guanajuato
Veracruz
Tabasco
Estado de Mexico
Jalisco
Morelos
Puebla
Quintana Roo
Colima
Michoacan
Guerrero
Oaxaca
Chiapas

Comentarios/Conclusiones:

De esta forma, quedaría implementado un control que realmente interesa al área de Comunicaciones, la de Infraestructura y la de Seguridad informática. Permite a las tres áreas trabajar sinérgicamente ante un ROJO en la disponibilidad de alguna de las sucursales/cajeros en momentos críticos.

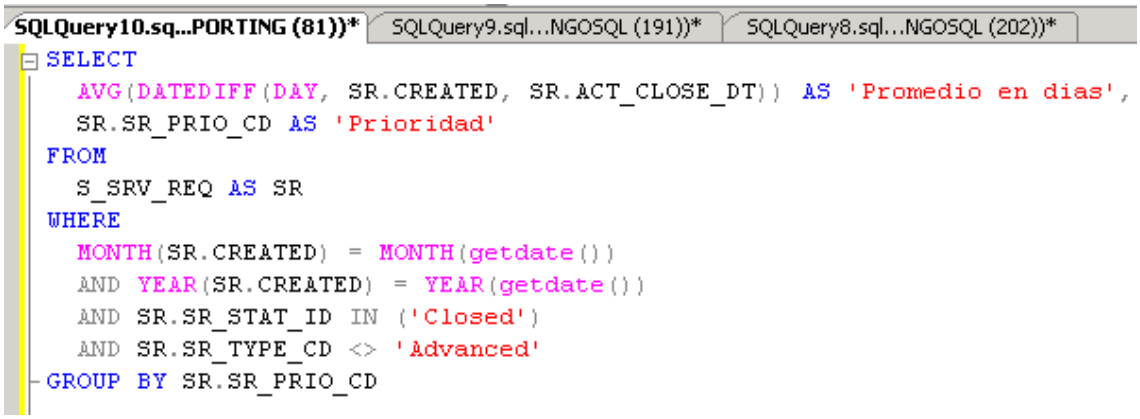
El hecho de marcar un Acuerdo de Nivel de Servicio que esté validado con el resto de áreas internamente y con el directorio, permite trabajar de manera conjunta para brindar un servicio de excelencia a los clientes, sin centrarse en las responsabilidades de cada área, acortando así el GAP (o también llamados *grises*) entre ellas, y pudiendo comprometerse en un objetivo final que interesa al negocio y si bien está basado en temas tecnológicos, la repercusión final y los resúmenes de resultados mensuales interesan directamente a la gerencia general y no solamente a cada gerencia media individualmente.

Métrica aplicada:

Solicitud de Acceso (a aplicaciones / servicios de *software* de la entidad) [53]

Experiencia práctica:

Se implementó un control semi-automatizado que recolectaba datos diariamente de un sistema de gestión de tickets (el sistema es una aplicación de tipo CRM llamado Siebel 7.1 de Oracle; el módulo específico es el *"Service Request – Call Center"*). La consulta SQL que trae la información de la cantidad de días que estuvo abierto un ticket (en promedio) hasta su resolución, agrupada por prioridad era la siguiente:



Esta misma sentencia se lanzó el último día de cada mes, durante la primera mitad del año 2013, para ir obteniendo los resultados siguientes:

Prioridad/Mes	Enero	Febrero	Marzo	Abril	Mayo	Junio
Urgente	2	3	1	8	4	2
Alta	8	11	10	9	9	8
Media	21	20	22	21	25	18
Baja	33	36	29	39	34	38
Programado	128	148	112	94	135	119

Dado que el Acuerdo de Nivel de Servicio pactado internamente en la entidad financiera era de:

[53] La definición teórica de la métrica se encuentra en la página 42, en este mismo trabajo.

Prioridad	Máxima cant. de días seguidos para resolución[54]
Urgente	5
Alta	10
Media	15
Baja	20
Programado	200

Esta medición de tiempos, por priorización, ayudó a determinar que en promedio los requerimientos de nivel Medio y Bajo no llegaban a cumplirse en los tiempos estipulados en el acuerdo de nivel de servicio interno; mientras que los de tipo Urgente y Alta sí lo hacían.

Analizando la causa de incumplimiento del SLA, se encontró que dados los procesos que seguían en el área de Seguridad Informática para los tipos de ticket urgentes o de alta prioridad, los mismos acaparaban casi todos los recursos del área (así también como de otras áreas, por ejemplo, redes o desarrollo); postergando la resolución de los de prioridades más bajas por varios días.

También, se detectó que las solicitudes de requerimiento categorizadas como Urgente/Alta, llevaban por lo general, una presión externa mayor por fuera del proceso interno del área (por ejemplo, correo electrónico de un superior de otro área, o que la solicitud venía por parte de un usuario de alto rango en la compañía, o que el pedido afectaba a algún servicio de negocio que implicaba costos financieros a la compañía, etc.).

Finalmente, el CSO, tomó estos valores, más el promedio de tickets abiertos por mes, con la siguiente consulta SQL ejecutada el último día de cada mes:

[54] Los días de corrido desde la apertura del incidente, no tienen en cuenta fines de semana ni festivos no laborables

SQLQuery10.sq...PORTING (81))* SQLQuery9.sql...NGOSQL (1

```
SELECT
  COUNT(*) AS 'Cantidad de tickets',
  SR.SR_PRIO_CD AS 'Prioridad'
FROM
  S_SRV_REQ AS SR
WHERE
  MONTH(SR.CREATED) = MONTH(getdate())
  AND YEAR(SR.CREATED) = YEAR(getdate())
  AND SR.SR_TYPE_CD <> 'Advanced'
GROUP BY SR.SR_PRIO_CD
```

Y obteniendo los resultados:

Prioridad/Mes	Enero	Febrero	Marzo	Abril	Mayo	Junio
Urgente	13	7	5	15	21	22
Alta	78	68	49	78	72	56
Media	67	59	53	70	80	79
Baja	54	46	39	46	57	38
Programado	11	7	8	9	12	12
TOTAL-->	223	187	154	218	242	207

(205 solicitudes mensuales aproximadamente), más la cantidad de tickets que puede resolver su equipo de trabajo (dado que no es la única tarea que desempeñan); y con esto concluyó que la mejora de los tiempos de resolución para tickets de menor prioridad supondría la contratación de dos personas más en el área, con un *seniority* similar al del equipo de trabajo actual.

Comentarios/Conclusiones:

Cómo se mostraba en el modelo teórico de la definición de esta métrica, esto pudo aportar **visibilidad** al CSO y **números** que puede entender el directorio, y que lo ayude a justificar la contratación de dos personas más en el área; o bien dejar asentado que con los recursos actuales sería preciso re-negociar los acuerdos de nivel de servicio por la imposibilidad de cumplimiento.

Métrica aplicada:

Capacidad de la red para soportar el servicio de HomeBanking [55]

Experiencia práctica:

A simple vista, esta métrica pareciera estar más vinculada al área de Redes/Comunicaciones que de Seguridad Informática, pero como vimos en la definición de la misma y en lo expresado en la comunicación "A" 4609 y la comunicación "A" 5374 [56] del BCRA, el área de Seguridad es responsable de velar por la disponibilidad de los servicios electrónicos prestados a los clientes, en este caso el HomeBanking.

Por ende, dado que la seguridad informática se encarga de asegurar la integridad, disponibilidad y confidencialidad; es preciso prever o solucionar de manera eficiente cualquier problema que surja a nivel de las comunicaciones de la entidad.

Para el trabajo sobre esta métrica se desarrollaron programas (scripts) de lectura de los archivo de *Logging* en el ESB[57] y el SDA[58], que hacían una lectura de forma incremental. La lectura (más allá de que era incremental) se realizó internamente por bloques, para hacer más eficiente el uso de memoria física ya que el Log tenía un tamaño significativamente grande; así es que esta información que se recolectó información daba cuenta de la utilización actual del servicio.

Estos logs contenían información mixta entre los servicios de HomeBanking, Banca Empresa y *Phone Banking*, por lo que en los scripts armados se tuvo que

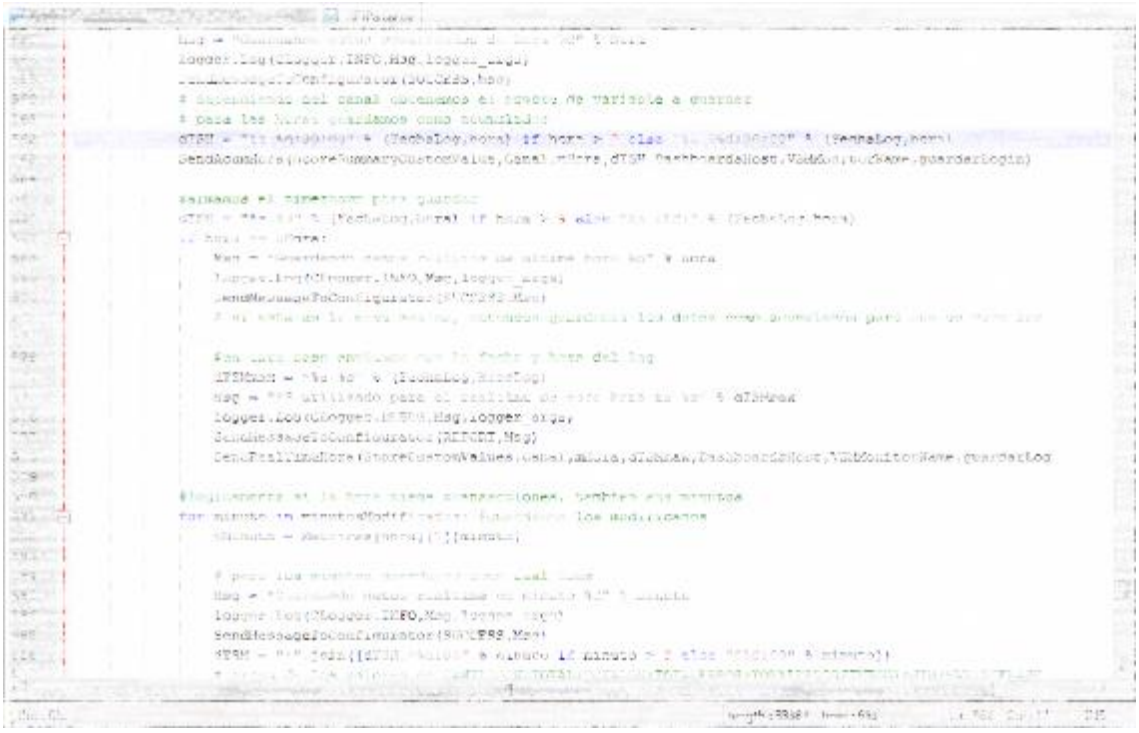
[55] La definición teórica de la métrica se encuentra en la página 55, en este mismo trabajo.
[56] Queda designado el Directorio como responsable primario de los siguientes componentes involucrados en los canales electrónicos: *"**Infraestructura de redes**. Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento y transporte de voz y datos que interconectan e integran los recursos de la infraestructura de tecnología y sistemas.*
***Infraestructura de tecnología y sistemas.** Comprende a todos los recursos informáticos, operativos y de información dispuestos para la administración, operación, mantenimiento, procesamiento y control de los servicios informáticos asociados a los Canales Electrónicos."*
[57] http://www-03.ibm.com/software/products/en/wsesb/
[58] http://publib.boulder.ibm.com/iseries/v5r1/ic2924/books/c0926040.pdf

poner esta diferenciación y para el trabajo de este indicador solamente tuvimos en cuenta lo que ocurría con el servicio electrónico de HomeBanking.

Puntualmente, se desarrolló[59] un módulo en C/C++ con librerías boost [60] (se había descartado el uso de lenguajes interpretados como lo son Python o Perl porque quitaban performance y los logs eran realmente muy grandes) que realizaba la lectura incremental y filtrado de líneas mencionado anteriormente, y además contenía toda la lógica permitiendo contabilizar las transacciones y calcular los valores solicitados.

La arquitectura de este desarrollo implicaba la ejecución del script a modo de *"daemon"* [61] de manera tal que exista al menos un proceso realizando la lectura del archivo log y mantenga en memoria la información de las métricas. Este modulo además se encargaba de la persistencia de estos datos en caso de cualquier inconveniente (esta persistencia se lograba haciendo uso de archivos directamente en el servidor Linux).

[59] Programado por los consultores Esteban Guillardoy y Ezequiel Ruiz, consultores de Barcelona/04 del área de tecnología.
[60] http://www.boost.org/
[61] http://www.techterms.com/definition/daemon



Script 1 - Parte del código del script utilizado

Luego se leían los resultados del *daemon* anterior y que llegaban sin un formato previo, pero podían ser consumidas perfectamente por el área de Seguridad Informática.

Asimismo, se dio la posibilidad de mostrar gráficamente otras métricas que a la entidad le pareció interesante recolectar:

- Cantidad de Transacciones acumuladas por hora (últimas 24 horas)
- Cantidad de Transacciones acumuladas por minuto (últimos 60 minutos)
- Tiempo promedio de Transacciones (últimas 24 horas)
- Tiempo promedio de Transacciones (últimos 60 minutos)
- Transacciones Totales del día
- Transacciones Totales de la Hora Anterior
- Cantidad de *Logins* del día
- Cantidad de *Logins* Acumulados en la Hora Actual

- % de Transacciones finalizadas en OK, ERROR y TIMEOUT para la hora anterior
- % de Transacciones finalizadas en OK, ERROR y TIMEOUT para el día en curso

Haber implementado la solución de esta forma, dio lugar a determinados pros y contras que se tuvieron que validar con el banco y con el directorio para obtener su acuerdo formal y escrito.

Ventajas:

- Se disminuía notablemente la cantidad de información que viajaba por la red desde el servidor Linux al servidor donde se había instalado el producto VISUAL Message Center Thinkserver, ya que solamente se traía el resultado del procesamiento completo de los logs, mientras que haber traído el Log completo para su posterior análisis hubiese sido replicar por completo todo el tráfico de red que ya se tenía para el uso del servicio.
- Al haber implementado el script en C/C++, y no tratarse de un lenguaje interpretado (como Perl o Python), el rendimiento era mucho mayor y se reducían los tiempos de procesamiento del log.

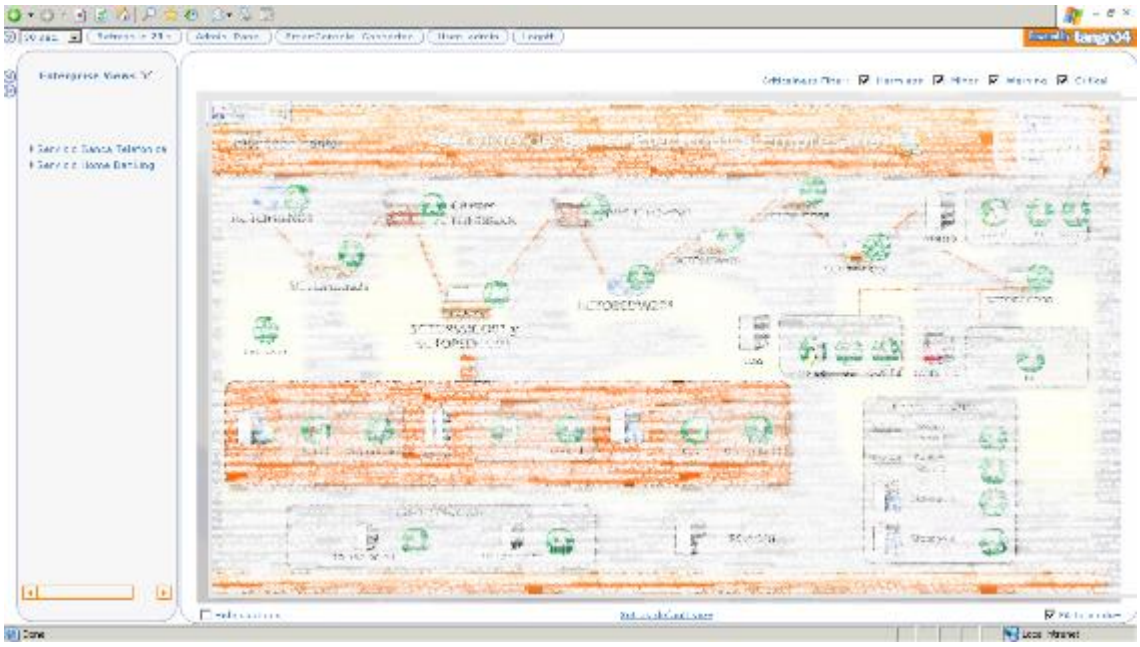
Desventajas:

- Se requería que el script se encuentre en ejecución constante en el servidor Linux (o sea, que se tuvo que crear un nuevo *daemon* en el servidor productivo de HomeBanking que realizaba el procesamiento de datos), y que además hará uso de archivos en el servidor para persistencia de información. Esto, de todas formas, no implicaba utilización exhaustiva de recursos de procesador ni de disco.
- Dadas las librerías que se usaron para el desarrollo del script, fue necesario compilar el programa en cada servidor Linux para asegurar el correcto funcionamiento.

Luego de implementar un recolector de información en cada servidor Linux que procesaba información de HomeBanking, e ir observando la correcta generación de los valores y mediciones sobre el servicio, hubo un trabajo junto al área de Marketing para entender el nuevo proyecto que se pretendía llevar a cabo.

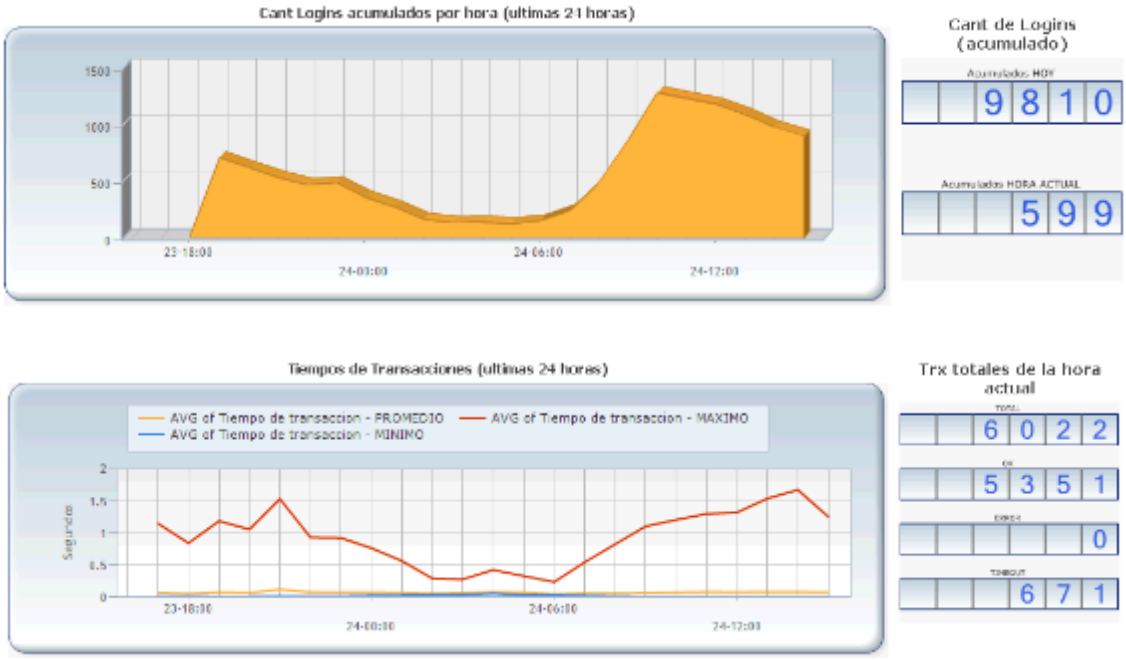
El proyecto pretendía aumentar un 13% la cantidad de usuarios del servicio, mediante publicidad más agresiva, beneficios en el uso del servicio electrónico por sobre el tradicional, promociones y concursos, y una serie de actividades que alentarían a los clientes del banco la utilización del HomeBanking para realizar las actividades que normalmente realizarían de forma presencial en una sucursal física de la entidad.

Se tuvo en cuenta además, un relevamiento de los componentes físicos que intervenían en las comunicaciones del servicio de HomeBanking:



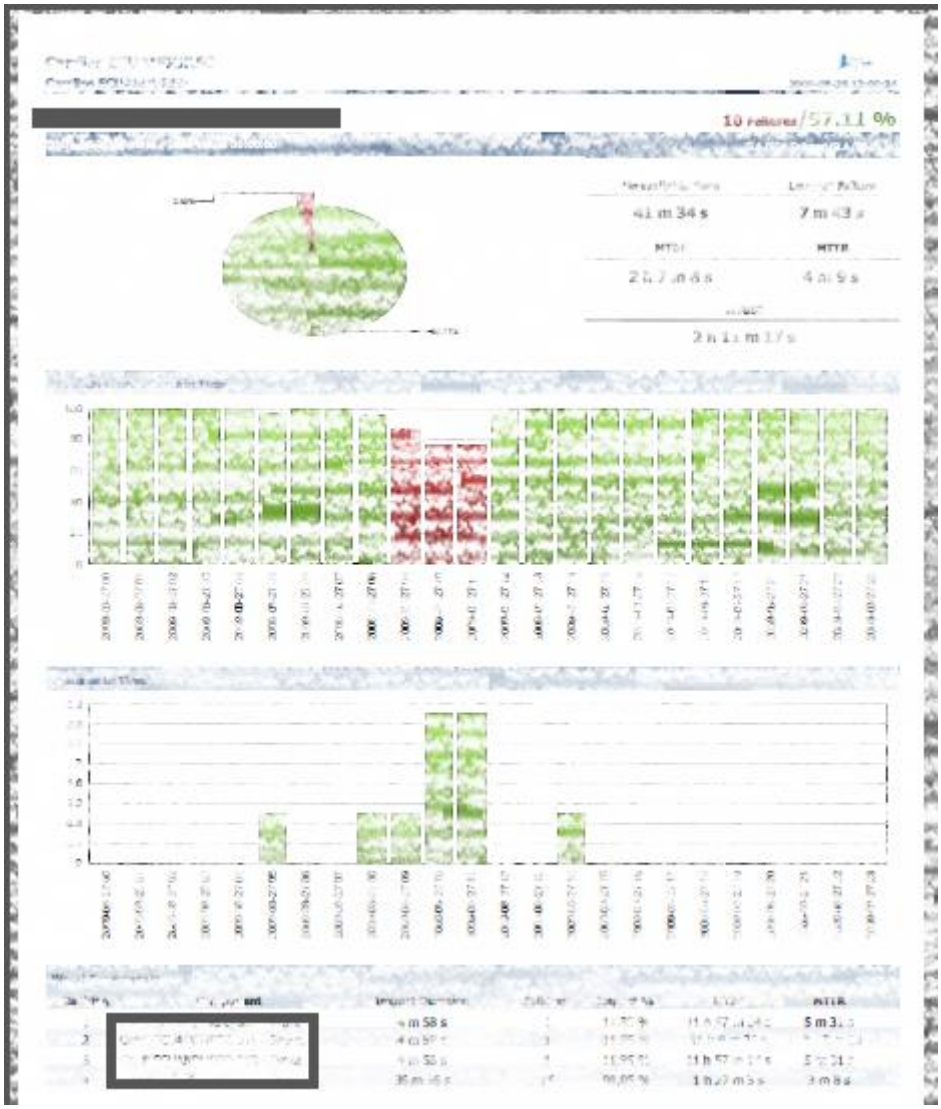
Luego, se analizó la cantidad de usuarios que se conectaban y más precisamente en qué momentos del día se detectaban picos de consumo para modificar ciertas reglas de procesamiento en los equipos y plataformas, dando más prioridad al tráfico de red proveniente del servicio, así como también el tiempo promedio que

llevaba cada transacción en ejecutarse y cuántas terminaban en *TimeOut* por falta de procesamiento a tiempo por parte del sistema de HomeBanking:



Dado que la entidad tenía contratadas líneas de datos con más de un proveedor de servicio de red (en caso de contingencia y por un tema de optimizar el servicio), luego se efectuaron reportes mensuales que expresaban el cumplimiento o no de cada proveedor respecto del Nivel de Servicio Acordado.

Estos reportes se resumían y eran notificados de manera directa a la Gerencia General, para que la misma tome decisiones en ciertos proveedores que hubo que redefinir el contrato de SLA más de una vez en el año por incumplimiento.



Estos reportes se planificaron de manera mensual, para ser ejecutados y exportados a formato PDF a través de la herramienta VISUAL Message center Reports, del proveedor Tango/04.

Luego de unos meses de trabajo, obtención de estas mediciones, análisis conjunto con las distintas áreas, fue posible presentar al directorio un proyecto para el mejorado de los servidores del servicio de HomeBanking, renovación de dispositivos de *networking* y contratación de un proveedor de Internet adicional que proponía mejores condiciones de Nivel de Servicio.

Comentarios/Conclusiones:

Esta métrica impacta de forma directa en el campo de la seguridad informática de la entidad. Esto es así porque la seguridad debe garantizar la disponibilidad de los datos en el momento en que los usuarios precisan utilizarlos; y una deficiente o incorrecta política de redes y comunicaciones en la organización podría llevar involuntariamente a la indisponibilidad de datos críticos al momento de ser necesarios para la toma de decisiones o continuidad del negocio.

Quedó evidenciada la importancia de la investigación previa a realizar una propuesta de mejora al directorio. Contar con mediciones ciertas del servicio, un trabajo interdisciplinario y conjunto entre áreas de la entidad[62], estudios sobre estas mediciones obtenidas y su posibilidad de mejora o no[63], es fundamental para poder presentar alternativas de solución basadas en un trabajo empírico y detallado que estará lo más alineado posible a los requerimientos del negocio y a la realidad de uso por parte de los clientes / usuarios finales.

Indicadores OPERATIVOS (Grupo de trabajo de Seguridad Informática)

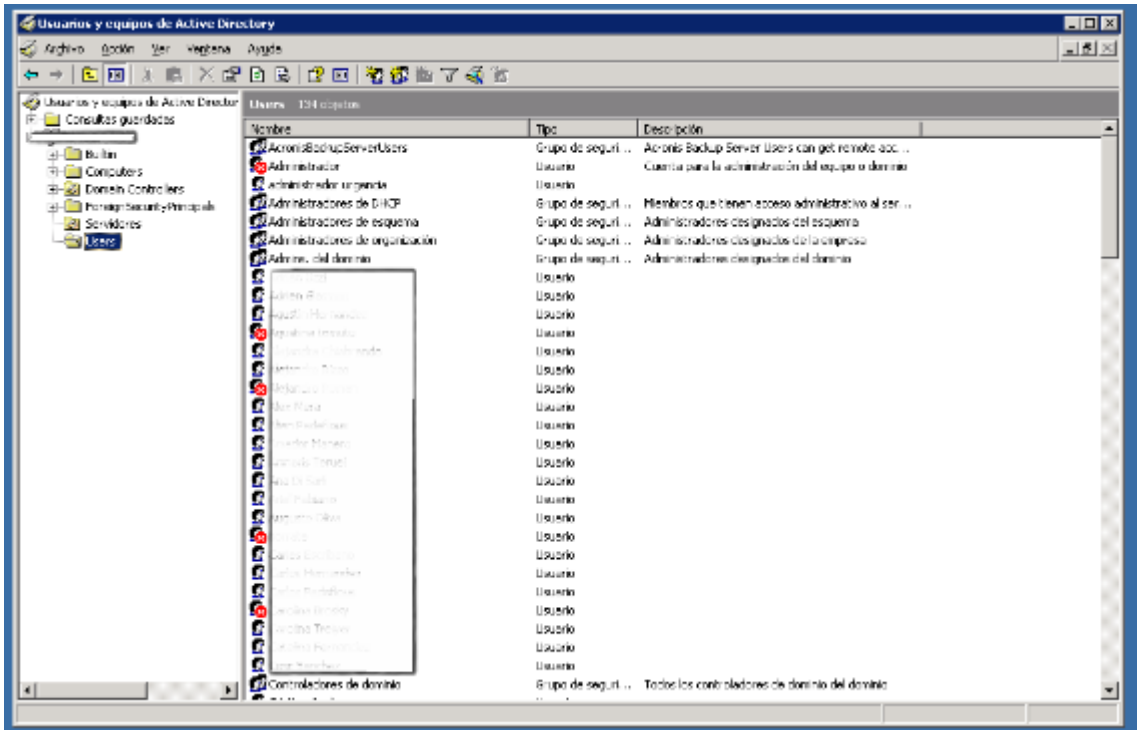
Métrica aplicada:

Cuentas de usuario genéricas / Cuentas inactivas por más de 90 días [64]

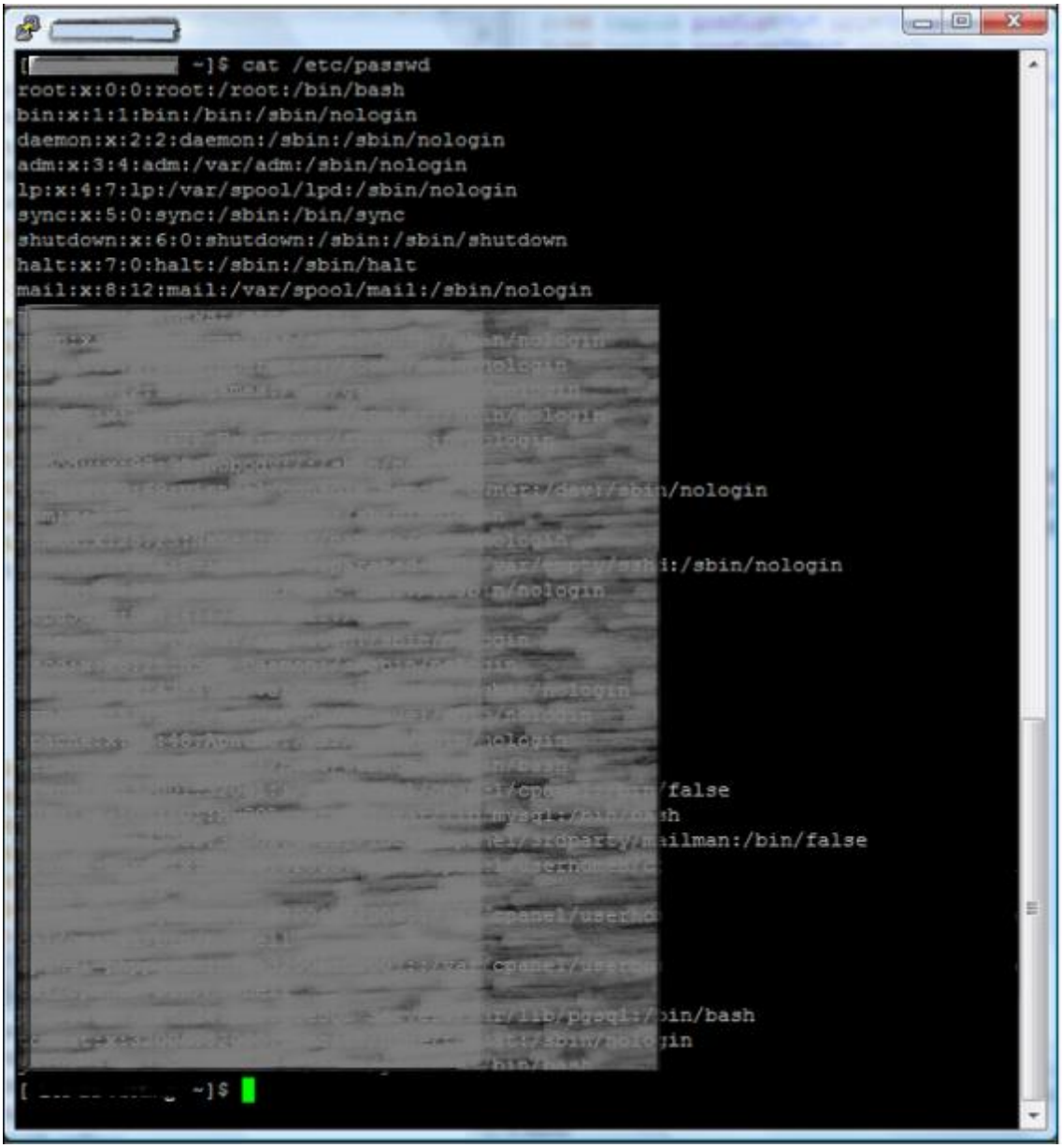
Experiencia práctica:

Esta métrica tuvo en cuenta tres plataformas, para las cuales se trabajó de manera diferenciada. Respecto de las cuentas genéricas se trabajó de forma manual extrayendo del Directorio Activo de Microsoft Windows todos los usuarios registrados,

[62] Cada área aportará donde mayor valor agregado pueda proveer
[63] En ocasiones, por la tecnología en que se basan ciertos aplicativos no es posible efectuar mejora alguna, sino que el único proyecto viable es “mantener” los niveles actuales y evitar su caída o pérdida de rendimiento
[64] La definición teórica de la métrica se encuentra en la página 50, en este mismo trabajo.



En los equipos con sistema operativo Linux, se obtuvo la información del archivo /etc/passwd, donde se encuentran allí todas las cuentas de usuario que vienen por defecto con la instalación más las que se pudieron haber creado por el administrador del equipo con el tiempo.



Luego, en los sistemas operativos OS400, se obtuvo la información mediante la utilización de un agente llamado: “UIN”, el cual pertenece a la empresa Tango/04, y lo que hace a bajo nivel es ejecutar el comando DSPUSRPRF (*Display User Profile*), el cual provee información completa para cada perfil de usuario que hay en el equipo.

Esta información queda contenida en una tabla dentro del mismo sistema operativo llamada: BDHST02X, dentro de la biblioteca B_DETECTOR. La misma

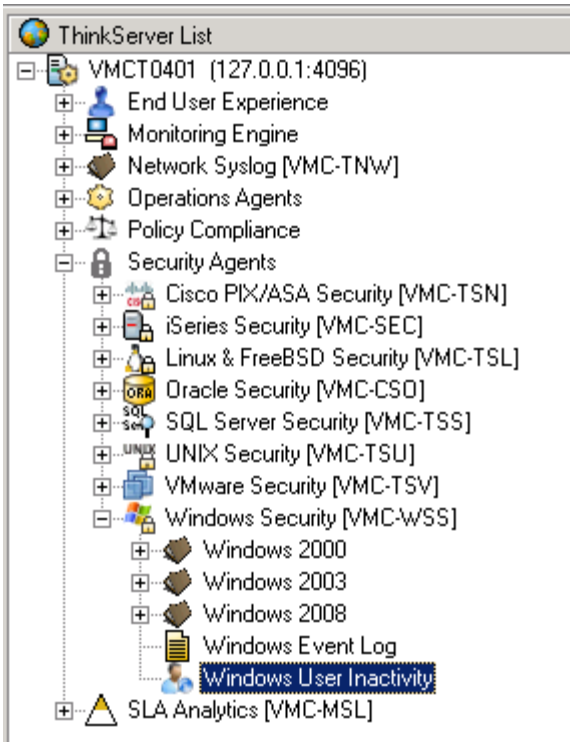
puede ser consumida mediante las herramientas VISUAL Message Center SmartConsole o VISUAL Message Center Reports (también del proveedor Tango/04), directamente con el comando STRSQL en el iSeries, o bien mediante cualquier aplicación de tipo ODBC Query. En nuestro caso, se obtuvieron directamente con el producto Reports de Tango/04, el cual nos dio los listados con la información en formato PDF, seleccionamos como parámetros todos los equipos iSeries, incluyendo todos los perfiles de usuario:

Sistema:	***ALL**
Usuarios Incluidos:	***ALL**
Usuarios Excluidos:	***NONE**

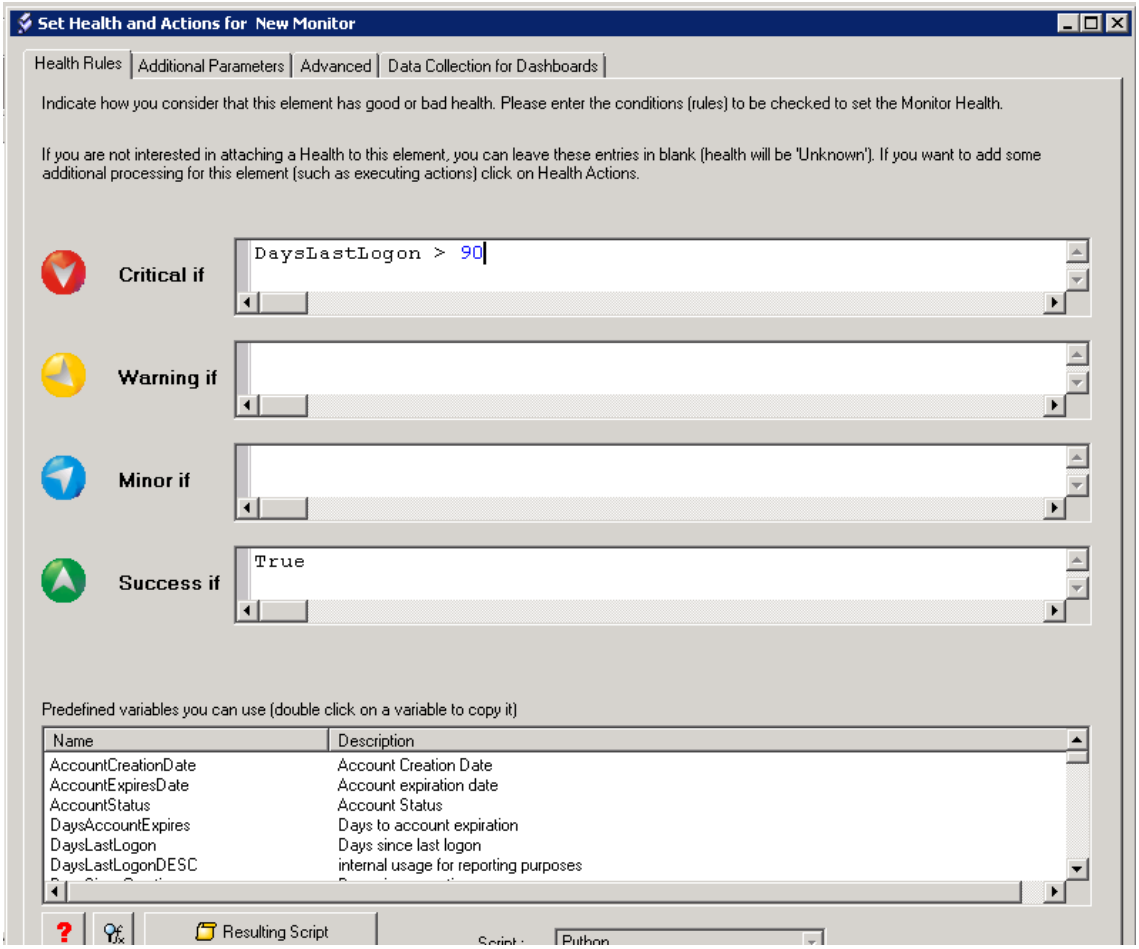
Los listados PDF son sencillos, e incluyen en orden alfabético cada una de las cuentas de usuario creadas y su descripción.

Por último, se solicitó al área de Recursos Humanos la nómina de empleados, cada cuenta que no tuviese una relación directa de uno a uno con un empleado del banco se inhabilitó (no se eliminó directamente puesto que podría haber generado problemas operativos para proyectos activos, o incluso para el correcto funcionamiento de ciertos servicios o aplicaciones); y se dio comunicación general a toda la empresa de esta acción, para que quien notase problemas para ingresar a aplicaciones del banco, o tuviese imposibilidad de realizar sus tareas habituales se comunique con el área de Seguridad Informática y se clarifique la utilización de la cuenta en cuestión.

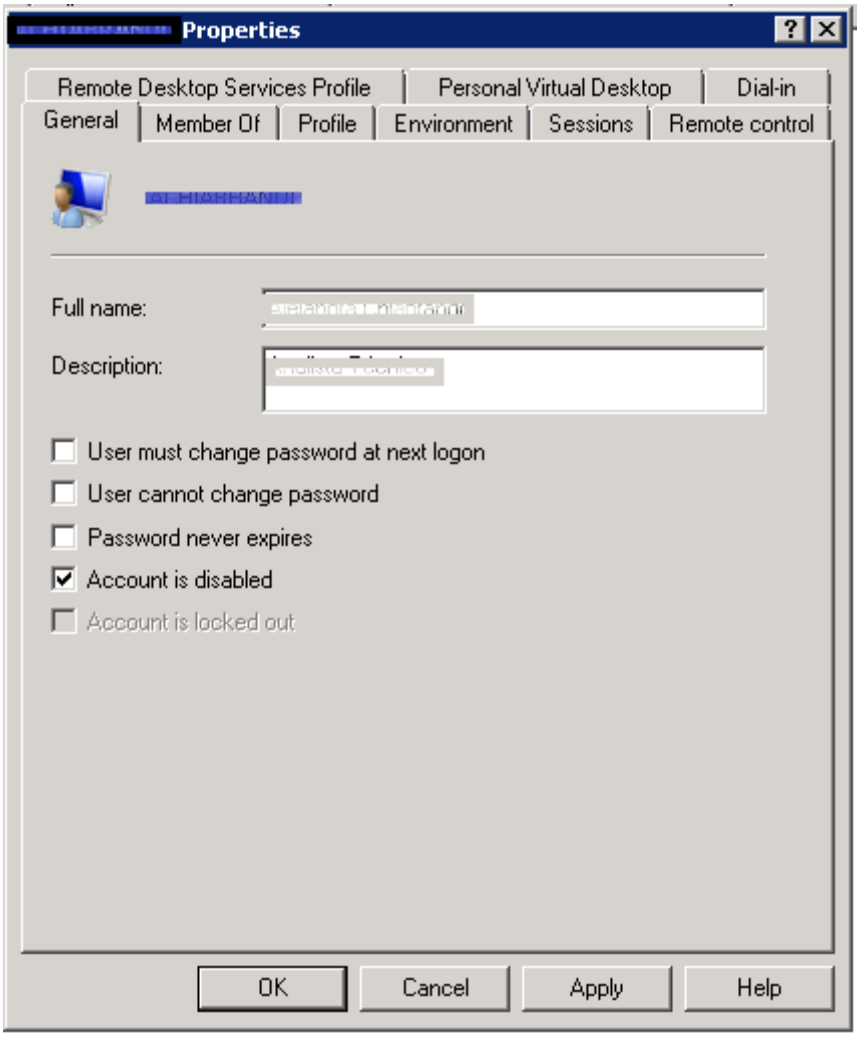
El siguiente trabajo consistió en obtener reportes de inactividad sobre las cuentas, para las mismas tres plataformas, los cuales se obtuvieron mediante reportes automatizados, por lo que fue más sencilla su recolección. Sobre el sistema operativo Microsoft Windows se usó el producto VMC Thinkserver, puntualmente uno de sus agentes de recolección llamado *"User Inactivity"* el cual permite establecer un umbral mínimo de inactividad para que la cuenta en cuestión aparezca en el reporte final.



Ese umbral para criticidad, se configuró a 90 días para que en el reporte luego se pueda especificar que se querían obtener los usuarios en “Rojo”,

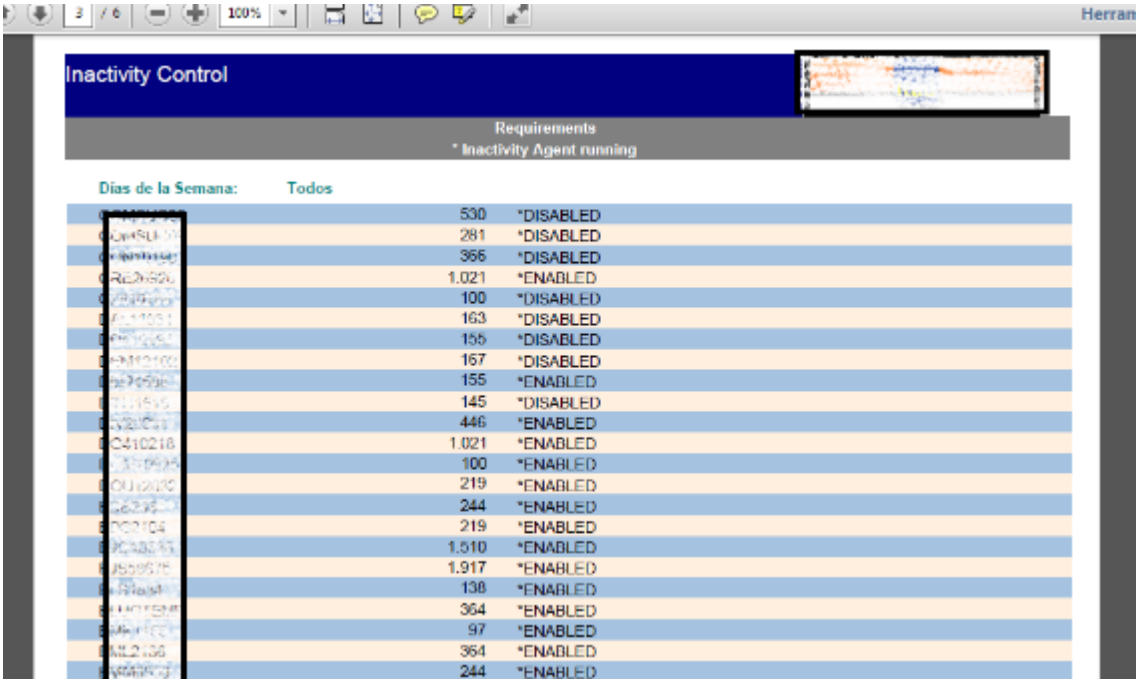


Con el reporte generado en formato PDF de las cuentas, se procedió a ingresar al Directorio Activo de Windows y configurar cada una de esas cuentas como deshabilitada.



En el entorno iSeries, el trabajo consistió en re-utilizar la información obtenida del agente UIN sobre la totalidad de perfiles de usuarios existentes, pero se le puso la condición de que la inactividad de los mismos sea mayor a 90 días.

Y se obtuvo una salida en formato PDF con la lista de usuarios que cumplían la condición,



Inactivity Control

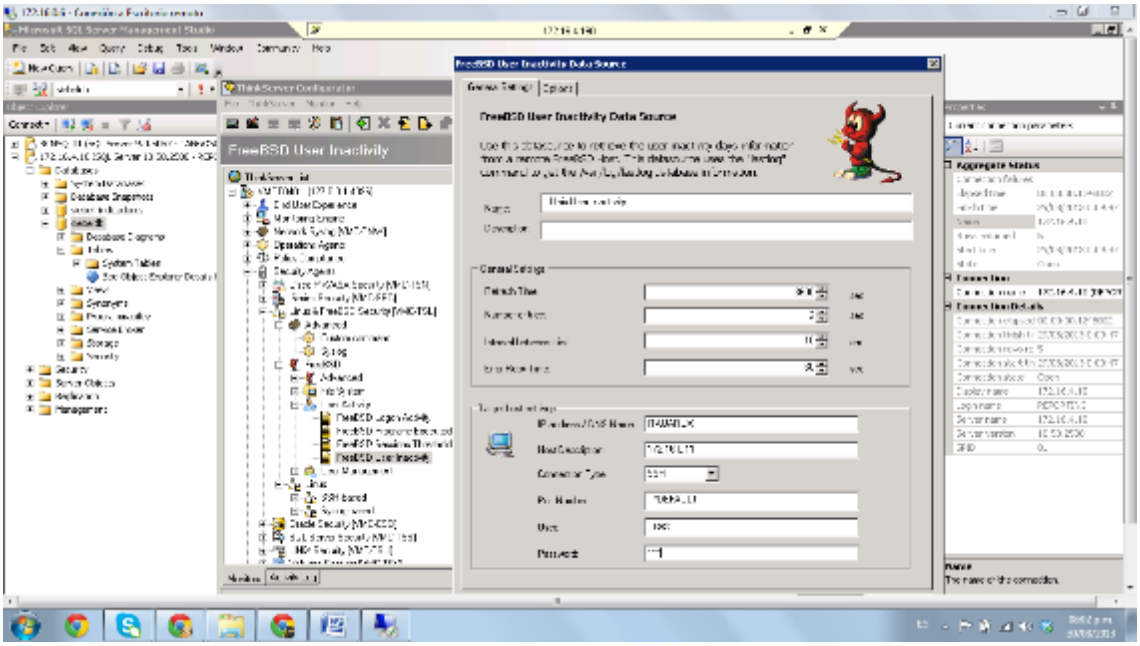
Requirements
* Inactivity Agent running

Días de la Semana: Todos

[redacted]	530	*DISABLED
[redacted]	281	*DISABLED
[redacted]	366	*DISABLED
[redacted]	1.021	*ENABLED
[redacted]	100	*DISABLED
[redacted]	163	*DISABLED
[redacted]	155	*DISABLED
[redacted]	167	*DISABLED
[redacted]	155	*ENABLED
[redacted]	145	*DISABLED
[redacted]	446	*ENABLED
[redacted]	1.021	*ENABLED
[redacted]	100	*ENABLED
[redacted]	219	*ENABLED
[redacted]	244	*ENABLED
[redacted]	219	*ENABLED
[redacted]	1.510	*ENABLED
[redacted]	1.917	*ENABLED
[redacted]	138	*ENABLED
[redacted]	364	*ENABLED
[redacted]	97	*ENABLED
[redacted]	364	*ENABLED
[redacted]	244	*ENABLED

Por último, sobre los OS400 donde se encontraban estas cuentas en tales condiciones, se validaba su estado (*ENABLED/*DISABLED) y se eliminaron las que estaban en estado deshabilitado, y se configuraron en estado deshabilitado las que estaban habilitadas pero no tenían *Login* exitoso hacía más de 90 días.

Para los sistemas Unix, de manera análoga a Windows, se usó un agente del proveedor Tango/04 donde se le configuró una conexión por SSH hacia el equipo en cuestión desde donde se obtuvieron los últimos *Login* exitosos de cada cuenta.



Por debajo, el agente lo que hace es obtener la información del archivo /etc/passwd, el cual contiene información sobre cada cuenta y cada *login* de la misma, y *parseó* esta información para dejarla disponible en un listado.

Luego, en cada cuenta que cumplía la condición de estar inactiva por más de 90 días se procedió a su eliminación manual a través de una terminal interactiva usando el comando “userdel”.

Comentarios/Conclusiones:

Muchos aplicativos antiguos, debían contar con un usuario de servicio que permita *logon* interactivo para funcionar. Esto genera mayor inseguridad por ser un usuario genérico que podría utilizar cualquier persona y realizar actividades de forma prácticamente anónima. El riesgo se acrecienta si además no se establece una política de cambio de contraseña periódica. Por tal motivo, al momento de adquirir un *software* de terceros para cualquiera de las áreas de la entidad, es importante dejar en claro que el área de seguridad informática tiene que realizar un relevamiento de los requisitos y condiciones de seguridad del mismo.

Es considerable notar la cantidad de tiempo que se puede ahorrar al realizar estas tareas con aplicaciones que se encarguen de recolectar esta información de forma automatizada, incluso, en ciertos aplicativos se puede configurar:

- Una alarma que envíe un correo electrónico al detectar la existencia de una cuenta de usuario que exceda los 90 días de inactividad (con información pertinente de la misma como ser: Sistema, Último *Login* exitoso, Nombre de cuenta, Descripción).
- Ejecución de un comando que elimine de forma directa la cuenta (pasándose como variable la salida del punto anterior).
- Ejecución planificada de un reporte mensual que se envíe por correo electrónico un archivo de salida en formato PDF a los responsables de Seguridad Informática indicando qué cuentas se eliminaron con todo su detalle.

Al haber trabajado con la solución de monitorización de seguridad de Tango/04 [65], estas acciones fue posibles automatizarlas, de todas formas, y para cumplimentar con el punto de Gestión de Identidades de la comunicación “A” 4609 del BCRA, si fuese necesario se deberán realizar manualmente, más allá del tiempo que puedan llegar a tomar.

Métrica aplicada:

Acceso de programadores al código fuente del sistema de producción [66]

Experiencia práctica:

Se presentaron dificultades al intentar poner en marcha esta métrica en la entidad, pero por ser considerada importante y tenida en cuenta tanto en las

[65] La empresa Barcelona/04 pertenece al grupo Tango/04, y dependiendo del país puede recibir una denominación o la otra, en este trabajo se las cita con ambos nombres. Puesto que hace unos años se fusionaron, y al día de hoy, los aplicativos y recursos pertenecen indistintamente a una o la otra.
[66] La definición teórica de la métrica se encuentra en la página 48, en este mismo trabajo.

documentaciones de mejores prácticas como en la comunicación “A” 4609 del BCRA, su aplicación se hizo necesaria.

Los problemas enfrentados tenían que ver con:

- Falta de un proceso de Control de cambios (*change management* [67])
- Definición de ambientes de Producción / Homologación / Desarrollo
- Adecuada configuración de seguridad de acceso a activos para cada perfil
- Documentación sobre los procesos generales del mantenimiento de las aplicaciones del banco

A continuación se describe el trabajo realizado para implementar exitosamente esta métrica.

La primera acción fue definir los siguientes conceptos a las áreas intervinientes en el proceso de mantenimiento y soporte de aplicaciones desarrolladas internamente:

- Ambiente de Producción: Entorno operativo de la entidad, el cual se utiliza para llevar adelante el negocio.
- Ambiente de Homologación: Entorno de pruebas (o también llamado pre-producción), que mantiene una infraestructura similar al productivo (en cuanto a la diagramación de sus componentes y versiones de software) y se usa como una etapa anterior a la puesta en producción de cualquier aplicativo.
- Ambiente de Desarrollo: Entorno que es utilizado exclusivamente por las áreas de programación de software de la compañía. Aquí se desarrollan las nuevas versiones de aplicativos y ejecutables, así como la modificación y actualización de versiones existentes que requieran el agregado de una funcionalidad o mantenimiento correctivo de errores.

[67] Proceso que controla con buenas prácticas todos los cambios, incluidos los de emergencia y mantenimiento, relativos a infraestructura y aplicaciones en cualquier entorno productivo de la entidad. http://www.isaca.org/Journal/Past-Issues/2011/Volume-5/Documents/11v5-Auditing-It-Risk-Associated-With-Change-Management-and-Application-Development.pdf

Según la comunicación "A" 4609 del BCRA, en cada cambio realizado al entorno productivo se deben informar mínimamente:

- Aprobación formal de los cambios propuestos,
- Identificación y registro de los cambios realizados,
- Comunicación de detalles de cambios a todas las áreas pertinentes.

Por lo que adicionando ciertos campos que proveían información importante para el banco, y daban mayor seguridad de los cambios a realizar, el posible impacto negativo, y su vuelta atrás en caso de error. Se llegó a la definición del siguiente formulario acordado por los gerentes de las áreas intervinientes.

Campo	Formato de Entrada	Detalle
Número de ticket	9999999999	Número entero para poder dar seguimiento del cambio en un sistema de gestión de cambios (en este caso se utilizó Siebel CRM)
Fecha de Apertura de ticket	AAAA/MM/DD – HH:MM:SS	Fecha en que se solicita el cambio y se abre el ticket en cuestión
Fecha planificada de implementación en pre-producción	AAAA/MM/DD – HH:MM:SS	Fecha en que estaría listo el cambio en la aplicación [68], y se implementaría en ambiente de homologación
Fecha planificada de implementación en Producción	AAAA/MM/DD – HH:MM:SS	Luego de ser aprobado el cambio en pre-producción y dejar un tiempo prudencial de pruebas, se planifica la fecha de pasaje a producción del cambio
Razón		Una explicación del porqué la necesidad del cambio
Riesgos		Cuáles son los riesgos de implementar este cambio (los mismos pueden estar vinculados a errores inherentes de la nueva funcionalidad o a cualquier problema técnico que devengue de la realización de un cambio)
¿Aprobado por el usuario final de la aplicación?	SI / NO	Si no está aprobado por el usuario final, no se llevaría adelante el cambio
¿Quién aprueba?	Apellido, Nombre (correo electrónico)	El o los usuarios finales que estén aprobando el cambio en la aplicación
Responsables de implementación	Apellido, Nombre (correo electrónico)	El personal involucrado en llevar a cabo la implementación práctica del cambio, siguiendo las instrucciones del área de Desarrollo
Responsables de Testing	Apellido, Nombre (correo electrónico)	El personal encargado de realizar las pruebas correspondientes para comprobar que el sistema en general funciona correctamente y que el cambio hecho en la aplicación se comporte de acuerdo a lo esperado

[68] Por un acuerdo entre áreas, las pruebas unitarias y generales que se hiciesen en ambiente de Desarrollo no entraron dentro del alcance de esta métrica, ni dentro del proceso de Control de Cambios definido. Estas pruebas quedarían a cargo del área de Desarrollo.

Notificados	Apellido, Nombre (correo electrónico)	El personal que debe ser notificado al finalizar la implementación, pruebas del cambio y si hubo algún tipo de problema cuál fue y la modalidad de rollback utilizada
Procedimiento de rollback		El área de Desarrollo deberá proveer instrucciones precisas sobre cómo actuar en caso de error para dejar el sistema en el mismo estado que se encontraba anterior al cambio
Requerimientos		El área de Desarrollo deberá proveer los requisitos previos y posteriores a la instalación del cambio para que sean seguidos por el personal de implementación

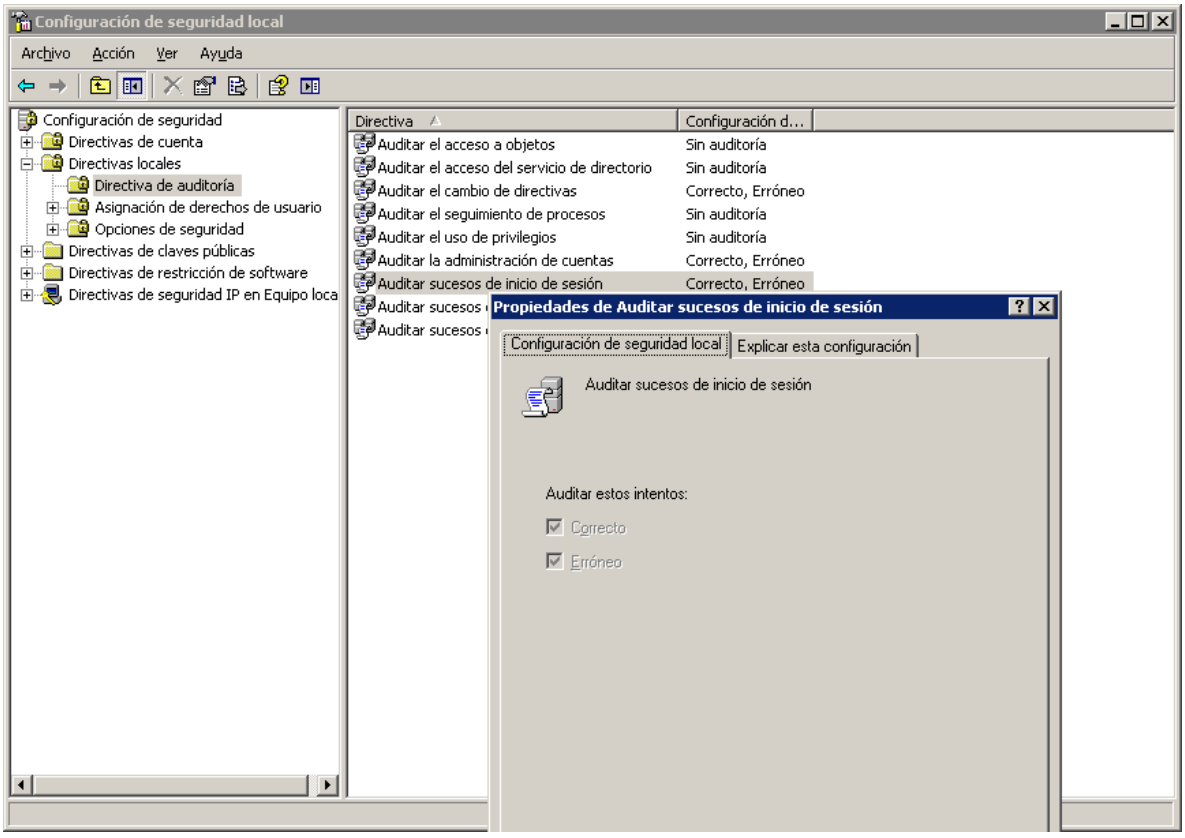
Se encontraron luego excepciones que no podían esperarse a que se cumpla este proceso de manera completa, y se detallaron junto a las diferencias en el tratamiento para enmarcarlas también dentro del proceso de Control de Cambios. Estas excepciones respondían a cambios considerados Urgentes.

De común acuerdo entre todos los intervinientes, se estableció que en casos críticos (donde haya indisponibilidad de la aplicación o una imposibilidad total de operar con algún aplicativo desarrollado *in-house*) no será necesario esperar a que el formulario tenga la aprobación total de todos los involucrados, sino que solamente hará falta la aprobación del usuario final y el responsable del área de Desarrollo. Igualmente, luego de finalizadas las correcciones y acciones tendientes a resolver el problema presentado, el formulario se llena *post-factum* para dejar asentada la información que debe perdurar como mínimo dos años según la normativa del BCRA.

La segunda parte del trabajo, consistió en definir al grupo de programadores, las aplicaciones desarrolladas y los sistemas considerados productivos; de esta forma se armaron controles de *Login* a estos equipos.

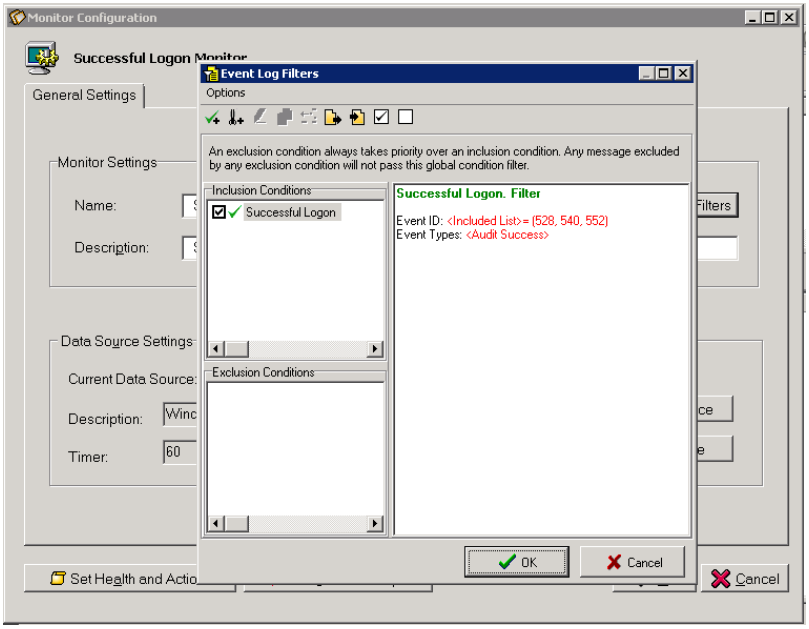
Para controlar los inicios de sesión de cuentas de programadores a los equipos productivos, en los cuales residían las aplicaciones desarrolladas. Se hizo lo siguiente:

- Se configuró en el servidor Windows la auditoría del sistema operativo para que deje constancia en el Log de Eventos de Seguridad los inicios de sesión que se daban en los equipos[69] que contenían las aplicaciones.

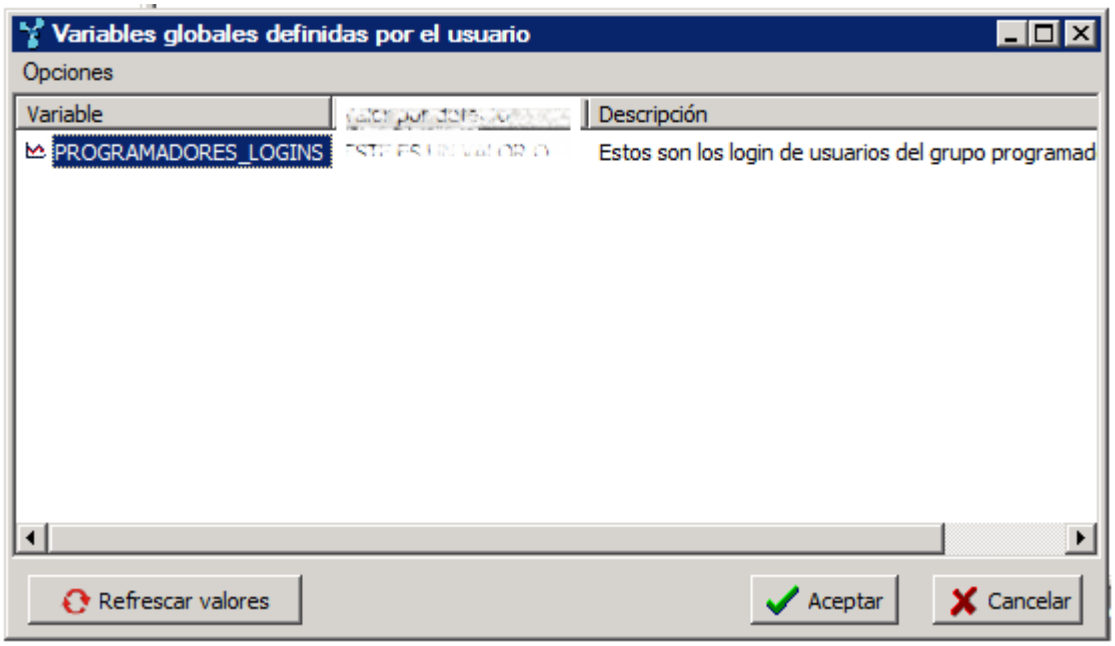


- Se creó un monitor en el producto VISUAL Message Center Thinkserver para que obtuviese todos los eventos de tipo “inicio de sesión” de los Domain Controllers de la red y los guarde en una base de datos.

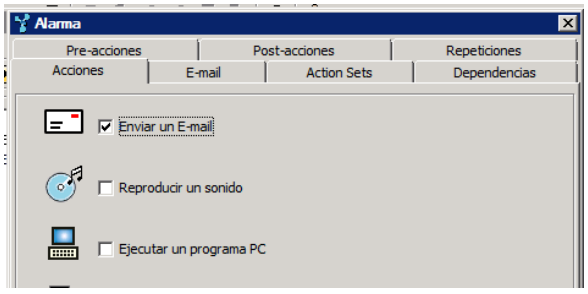
[69] Esto se hizo en los Controladores de Dominio, dado que los inicios de sesión son validados en estos.

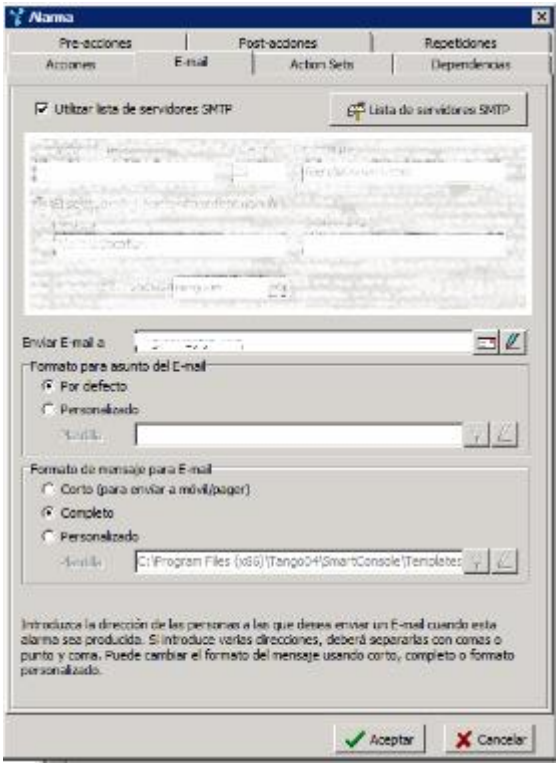


- En el producto VISUAL Message Center SmartConsole (de la empresa Tango/04) se creó una variable global que contenía el nombre de inicio de sesión de cada uno de los programadores.



- Y una alarma para que al llegar un evento de este tipo notifique directamente a los analistas de seguridad





- Finalmente los analistas de Seguridad Informática, cada mes contrastan un reporte que indica los inicios de sesión efectuados por programadores, junto con los formularios de controles de cambio y en caso de detectar que alguno se dio SIN la autorización correspondiente elevan el comentario al gerente de Seguridad Informática, quien analizará el tema junto con el gerente de Desarrollo; y en caso que sea oportuno notificar al directorio o gerencia general.

Comentarios/Conclusiones:

Como corolario final, se llegó a la conclusión que lo principal para poder cumplimentar con este punto es que esté previamente definido y documentado el proceso de gestión de cambios, así como una correcta separación de ambientes (desarrollo, pruebas y producción), y contar con la posibilidad de llevar adelante la monitorización en tiempo real de los cambios producidos en el entorno de producción, y por último un informe periódico que dé cuenta de los cambios

producidos para poder contrastarlo contra las solicitudes de cambio documentadas y autorizadas.

Lamentablemente, no se pudo adjuntar más documentación respaldatoria de la métrica porque la misma contenía gran cantidad de datos específicos de la entidad bancaria, y no se logró un acuerdo con el gerente de seguridad de información ni siquiera si se evitaban ciertos textos. De todas formas, para complementar este control se llevó a cabo una entrevista, donde el CSO [70] describió la importancia de este tipo de métricas.

En la entrevista que se mantuvo se afirmó: *"Nosotros intentamos auditar todo lo que nos pide el Central, y además todo lo que nos solicitan desde Auditoría Interna. El problema es que muchas veces no logramos que se entienda la importancia del porqué pedimos todo esto. Entonces, pareciera una puja entre la velocidad de la operatividad y la seguridad de la información en el banco, cuando realmente es todo lo contrario. Y vas a escuchar en muchos lados que te dicen que el área de seguridad siempre pide un montón de requisitos y que da mil vueltas para algo que debiera ser súper sencillo… pero después nosotros ante la ocurrencia de un incidente de seguridad, si no contamos con toda la info para analizar y hacer en todo caso un informe o pericia, ahí los irresponsables somos nosotros. Y se critica porqué no recolectamos todo lo que haga falta a tiempo."*

Sobre el trabajo realizado comentó: *"Sin ir más lejos, antes que vinieran Uds. a implementar este proyecto al banco, nosotros habíamos intentado hacer un control similar, pero al no haber un proceso de Change Management armado no lo logramos. Ahora, si bien el proceso de cambios no está como debería ser el ideal, por lo menos tenemos un mínimo de cumplimiento para poder armar un ticket en cada cambio que se solicite y guardarlo junto con la información por si nos lo piden del banco central o incluso si algún cambio tira abajo las aplicaciones o un servicio*

[70] CSO → Chief Security Officer, es el encargado de la seguridad de la Información dentro de una entidad

productivo, tenemos los responsables y quiénes debieron haber dado conformidad.".

Métrica aplicada:

Abuso de sitios web restringidos, descargas de software ilegal, control de SPAM [71]

Experiencia práctica:

Para la visualización y seguimiento de estos indicadores se construyó un *dashboard* que contenía los siguientes controles:

- Abuso de sitios web restringidos
    - Filtros para sitios específicos
    - Filtros por contenido HTML
- Cantidad de conexiones abiertas por servidor
- Descargas de software ilegal
    - Top 10 Usuarios MB transferidos (gráfico)
    - Top 10 Usuarios MB transferidos (numérico)
    - Control por tipo de archivo
- Control de SPAM
    - Top 25 cuentas con mayor cantidad de correos entrantes
    - Top 25 cuentas con mayor cantidad de correos salientes

[71] La definición teórica de la métrica se encuentra en la página 37, en este mismo trabajo.

- Abuso de sitios web restringidos
    - Filtros para sitios específicos
    - Filtros por contenido HTML

Sobre el indicador del acceso a sitios web restringidos se trabajó en dos variantes de filtrado. Ambas dentro de un software de seguridad web tipo proxy de la empresa WebSense.

Se identificaron para toda la compañía, sitios permitidos desde cada ordenador (hubo sitios que se agregaron para todos por igual como permitidos), como por ejemplo sitios de actualización de aplicativos con uso permitido:

- http://www.update.microsoft.com/*
- http://get.adobe.com/es/reader/*
- http://liveupdate.symantecliveupdate.com/*

Luego, para cada área se crearon grupos en el aplicativo y dentro de cada grupo se agregaron los empleados que pertenecían a cada una de estas áreas.

Se realizaron entrevistas con cada responsable de área y se llegó a detallar qué sitios y servicios web debían permitirse y cuáles no eran necesarios (siempre basados en la línea de no permitir el ingreso a sitios que no pertenezcan a la

necesidad diaria laboral), y es así que se crearon reglas para permitir el acceso de estos grupos a ciertos sitios y servicios Web[72].

El segundo control dentro de los sitios Web, fue por contenido. En esto el mismo software permite crear un conjunto de reglas para sitios que ya tiene analizados en un motor propio del aplicativo y simplemente se tuvo que poner qué tipos de contenidos no estaban permitidos, sin importar el sitio final de donde viniese, por ejemplo las siguientes categorías quedaron deshabilitadas para su navegación (Drogas, Entretenimiento multimedia, Apuestas, Juegos, entre otras):

Drugs
The parent category that contains the following categories:

- **Abused Drugs:** Sites that promote or provide information about the use of prohibited drugs, except marijuana, or the abuse or unsanctioned use of controlled or regulated drugs; also, paraphernalia associated with such use or abuse.
- **Marijuana:** Sites that provide information about or promote the cultivation, preparation or use of marijuana.
- **Prescribed Medications:** Sites that provide information about approved drugs and their medical use.
- **Supplements and Unregulated Compounds:** Sites that provide information about or promote the sale or use of chemicals not regulated by the FDA (such as naturally occurring compounds).

Entertainment
Sites that provide information about or promote motion pictures, non-news radio and television, books, humor and magazines.

- **MP3 and Audio Download Services:** Sites that support downloading of MP3 or other sound files or that serve as directories of such sites.

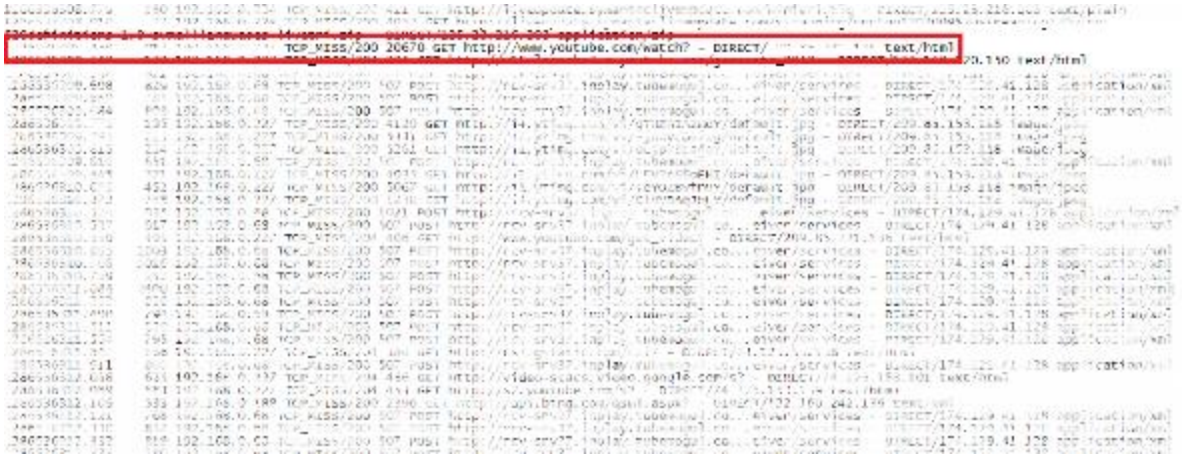
Gambling: Sites that provide information about or promote gambling or support online gambling, involving a risk of losing money.

Games: Sites that provide information about or promote electronic games, video games, computer games, role-playing games, or online games. Includes sweepstakes and giveaways.

De todas formas, el producto cuenta con posibilidad de alertar si alguien intenta entrar a este tipo de sitios, y estas alertas fueron configuradas para avisar por correo electrónico al área de Seguridad Informática. En los logs queda detallado explícitamente el pedido http, y es así que a final de mes se realiza un reporte

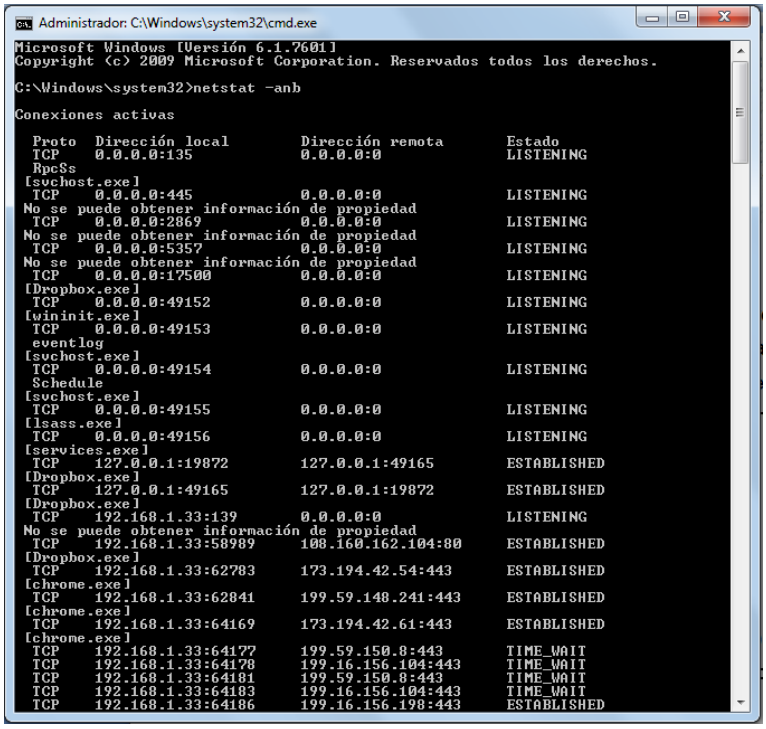
[72] Hubo que dividir las áreas, puesto que por ejemplo el sitio www.youtube.com iba a ser bloqueado para toda la compañía, pero el área de Marketing lo utiliza como una herramienta de trabajo. Esto es solamente por nombrar una de las tantas excepciones que se nos presentaron al mantener entrevistas con cada gerente de área.

agrupado por usuario que permite saber si alguien estuvo intentando acceder a sitios restringidos varias veces:



- Cantidad de conexiones abiertas por servidor

No todos los servidores de la empresa tienen acceso directo a internet, pero en los que sí lo tienen se implementó un *script batch* que cada diez minutos ejecutaba el comando: “netstat –anb > puertos.txt” en línea de comandos, de forma tal que se pueda conocer la cantidad de conexiones abiertas, y el programa ejecutable que la estableció:



En estos servidores, se llevó un análisis detallado de cada uno de los servicios que debieran estar estableciendo conexiones, y luego se creó un monitor en el producto VISUAL Message Center Thinkserver (del agente Universal File Reader) que recorría el archivo llamado puertos.txt y analizaba su contenido para ver si dentro de los procesos aparecía alguno que no estuviese en la lista de permitidos.

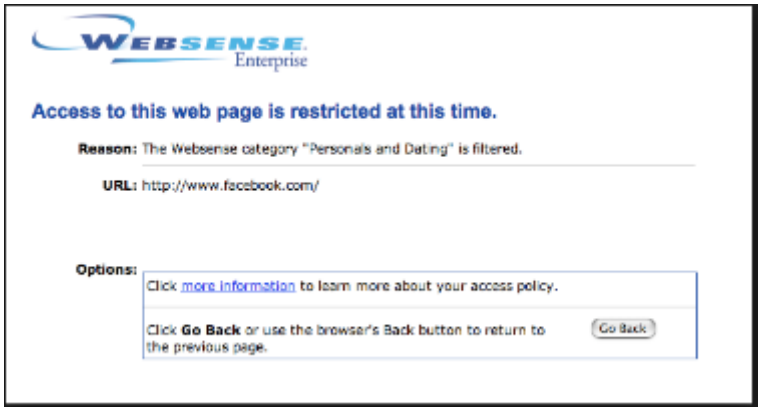
- Descargas de software ilegal
    - Top 10 Usuarios MB transferidos (gráfico)
    - Top 10 Usuarios MB transferidos (numérico)
    - Control por tipo de archivo

La información que provee el *web proxy* es suficiente para obtener los gráficos y disparar alarmas (envío de un correo electrónico a una lista de usuarios definidos en la configuración) ante la excedencia de ciertos umbrales definidos para la transferencia web.

Lo mismo para los filtros configurados para tipos de archivos que podrían ser maliciosos, se definieron los siguientes:

- Exe
- Com
- Ocx
- Bat
- Dll
- Zip
- Rar
- 7z
- Tar
- Tgz
- Taz
- Z
- Gz

En caso de intentar descargar alguno de ellos, se dispara un correo electrónico al área de Seguridad Informática y al usuario que está intentando realizar la acción se le muestra un cartel informativo:



- Control de SPAM
    - Top 25 cuentas con mayor cantidad de correos entrantes
    - Top 25 cuentas con mayor cantidad de correos salientes

En base a la lectura del log del servidor de correos de la empresa, se pusieron contadores que indicaban la cantidad de los correos entrantes y salientes

agrupando según la cuenta destino/origen según la métrica. De esta forma, luego se guardaron en una base de datos y el gráfico es el resultado de la consulta:

```
SELECT Address, MessageCount, Percentage
FROM T4EVENTLOG
WHERE
    YEAR(Timewritten) = YEAR(GetDate())
    AND MONTH(Timewritten) = MONTH(GetDate())
    AND DAY(Timewritten) = DAY(GetDate())
GROUP BY Address
```

En este caso, se mantuvo su visualización en tiempo real, y un reporte mensual pero que en vez de obtener los valores diarios, se modificó la sección de "Condiciones" (Where) para que no tenga en cuenta el día, y a mes pasado se obtenía el del mes anterior: "WHERE YEAR(TimeWritten) = YEAR(GetDate()) AND MONTH(TimeWritten) = MONTH(GetDate()) – 1".

Comentarios/Conclusiones:

El CSO de la compañía ya tenía implementado el *web proxy*, pero fue bien recibida por el CSO la idea de implementar ciertas automatizaciones sobre esta métrica y graficar parte de su operatoria así como enviar alertas por correo electrónico en tiempo real. Todo esto, basado en la facilidad de obtención y el valor agregado de detectar en tiempo real cualquier actividad sospechosa o que pusiese en riesgo la red corporativa, se decidió su implantación casi inmediatamente sin cambios a la propuesta realizada por parte del área de servicios profesionales de Barcelona/04.

Luego hubo cierta dificultad al momento de presentar la utilidad de esta métrica al Directorio, sobre todo porque así como estaba seguía siendo bastante técnica,

entonces se recurrió a comentar los riesgos que traería aparejado cualquier vulnerabilidad que escape a dicho control: “Problemas legales y posibles sanciones económicas por software ilegal; troyanos, virus, spyware, y demás código malicioso que podría infectar la red si pasan la barrera del antivirus ya instalado en cada equipo; y finalmente un breve resumen de lo que era una *botnet* y el riesgo de que uno o varios equipos terminen formando parte activa de una”.

Estos argumentos fueron más que suficientes para que el Directorio quisiera un resumen ejecutivo cada mes sobre la actividad capturada por estos controles en el caso que alguna de las sospechas se confirme como incidente de seguridad (importante recalcar, que sólo se pretendía ver en casos confirmados de un incidente que pudiese ser grave).

Un tema adicional que surgió en el trabajo (y que al principio no se había contemplado) de estos indicadores fue incluir al área de Recursos Humanos en los informes dado que ciertos contenidos de navegación y correos electrónicos de los empleados podría contener información privada y caer así en un problema legal por estar auditando y viendo información propia de un empleado, los controles aquí aplicados cuentan con el aval y autorización por escrito del gerente de Recursos Humanos, quien entendió a la perfección y sabe hasta qué límites alcanza cada control configurado.

Conclusiones

Los sistemas de la información en las entidades bancarias y financieras, han cobrado tanta importancia en la mejora de la producción, que sería impensable no disponer de ellos para el correcto desempeño de las funciones.

En este contexto, el área de seguridad informática cobra un papel clave en la organización, puesto que es el área encargada de gestionar e implementar las políticas, procesos y procedimientos necesarios que aseguren la disponibilidad, integridad y confidencialidad de la información crítica del negocio.

Para una correcta gestión de estas políticas, procesos y procedimientos de seguridad, es preciso desarrollar controles sobre los resultados que surgen de su implementación en la entidad. Estos controles servirán para ajustar y corregir los procesos y proyectos que fuesen necesarios; asimismo el gerente de Seguridad Informática será el responsable primario de que se implementen indicadores de seguridad informática en cada nivel de la organización y ponerla a disposición de la forma correcta al directorio y a las gerencias medias.

Con la información proveniente de las métricas “Incumplimiento de las normativas o leyes vigentes” y “Acceso y disponibilidad de los Cajeros Automáticos (ATMs)” el directorio podrá evaluar y tomar decisiones que mejoren la seguridad informática de la entidad y la calidad de los servicios ofrecidos a sus clientes. Con las conclusiones de analizar las métricas “Solicitud de Acceso (a aplicaciones / servicios de software de la entidad)”, “Capacidad del ancho de banda de la red para *Homebanking*” y “Abuso de sitios web restringidos, descargas de software ilegal, control de SPAM” el CSO puede mejorar los procesos internos del área así cómo las políticas generales de la entidad que involucren otras áreas para mitigar y prevenir ciertos riesgos latentes que siempre están presentes en la entidad.

De la consulta realizada a materiales bibliográficos que tratan sobre métricas e indicadores de seguridad informática, se procesó dicha información y se

comentaron algunas de las métricas que ayudan a gestionar la seguridad informática dentro de una entidad financiera o bancaria de tamaño medio, a distintos niveles en la organización y que por ende, interesan a diferentes estratos de la misma.

Producto de este desarrollo, se eligieron tres de los pilares más importantes de la seguridad informática relativos a cada nivel del negocio, que son:

- Cumplimiento normativo y Marco regulatorio (De negocio - Estratégico)
- Gestión de identidades (Gestión - Táctico)
- Seguridad de la Infraestructura Tecnológica (De la labor diaria - Operativo)

A partir del estudio de los elementos que componen una métrica de seguridad, se definió una plantilla de trabajo utilizada para definir cada indicador clave que contiene los siguientes elementos:

- Nombre de la métrica
- ¿Qué mide?
- ¿Para qué medir las observaciones?
- ¿Cuándo medir las observaciones?
- ¿Quién ve esta métrica?
- ¿Cómo se miden las observaciones?
- Posibles conclusiones a obtener
- Notas adicionales sobre la métrica

Una vez definidas las métricas de seguridad, el trabajo de campo consistió en la investigación y descripción de la implementación empírica de algunas de estas métricas. Y una conclusión sobre su utilidad y la factibilidad real de trabajar con estas métricas en forma práctica. Las mismas, fueron relevadas en entidades financieras de tamaño mediano de Argentina, y permitieron obtener significativas conclusiones.

Se consiguió, además, una conclusión adicional respecto de que las métricas que se plantean tienen en general un público muy específico. Ninguna métrica serviría al 100% si no está bien enfocada al consumidor de la misma. Esto no es un dato menor, dada la imposibilidad encontrada respecto de obtener métricas o indicadores que sirvan para todos los estratos de la compañía.

En esta línea de pensamiento, se comprobó la utilidad de dividir las métricas propuestas en tres grupos, con el fin de optimizar su utilización:

1) El primer grupo servirá al directorio para poder tomar decisiones estratégicas respecto de la seguridad informática o bien respecto de otros proyectos que tengan impacto sobre la misma;
   Cómo ejemplos de este primer tipo de métricas, se citan:
- "Incumplimiento de las normativas o leyes vigentes",
- "Observaciones de auditoría de Seguridad Informática de riesgo alto".

2) El segundo grupo de métricas, serán utilizadas por las gerencias para la priorización de proyectos a emprender, realizar cálculos de tendencias (para anticipar necesidades futuras), etc.
   Como ejemplos de este segundo tipo, se citan:
- "Acceso y disponibilidad de clientes a los Cajeros Automáticos",
- "Abuso de sitios web restringidos, descargas de software ilegal, control de SPAM",
- "Acceso a las instalaciones controladas",
- "Capacidad del ancho de banda de la red para *homebanking*".

3) Y un tercer grupo de métricas, se usarían para mantener el ritmo de trabajo en el equipo de Seguridad Informática. Proveyendo de indicadores operativos para el área, por ejemplo:
- "Solicitud de acceso (a aplicaciones / servicios de *software* de la entidad)",
- "Cuentas de usuario genéricas / Cuentas inactivas por más de 90 días",

- “Seguridad en dispositivos personales”,
- “Acceso de programadores al código fuente del sistema de producción”.

Finalmente, este trabajo confirmó la importancia de incorporar métricas en los distintos niveles de la organización, dado que las mismas proveen información a los sectores operativos, las gerencias medias y a los directivos. Los datos, se consumen a través de indicadores respecto de la seguridad de la organización. Esto ayuda a su vez, a conocer en cierta medida el grado de madurez que posee la entidad respecto de los pilares de seguridad informática mencionados anteriormente y al mismo tiempo cumplimentar con normas y reglamentaciones del Banco Central de la República Argentina (ente regulador de entidades financieras con mayor importancia en el ámbito nacional argentino).

Estas reflexiones permiten responder al enunciado planteado en la hipótesis, demostrando que es posible gestionar aspectos claves de la seguridad informática de la organización con la incorporación de métricas de bajo, medio y alto nivel.

Recomendaciones

El trabajo se centró en tres pilares importantes de la seguridad informática, estos son:

- Cumplimiento normativo y marco regulatorio
- Gestión de identidades
- Seguridad de la Infraestructura Tecnológica

Hay otros pilares de igual importancia que justificarían seguir desarrollando métricas a futuro, como ser:

- Políticas de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Gestión de comunicaciones y operaciones
- Desarrollo y mantenimiento de sistemas
- Gestión de continuidad de negocio

Por tanto, quien deseara continuar en la misma dirección práctica de este trabajo, podría tomar el resto de pilares que quedan pendientes, o bien, explotar aún más alguno de los tres pilares desarrollados aquí.

Al momento de crear una métrica de seguridad informática, será requisito fundamental tener en claro quién, o quiénes, las van a consumir; dada la gran diferencia expuesta en este trabajo sobre una métrica de alto nivel (que será vista por el directorio), y una de nivel más operativo (por ejemplo, para ser consumida por el gerente del área de SI o su equipo de trabajo). De todas formas, habrá métricas que podrían ser calculadas con un detalle más granular para un estrato medio, y luego se estudia, analizan variables y se agrupa para dar como resultado un formato resumido que podría ver un rango más alto de la entidad.

Al momento de presentar un indicador clave sobre un aspecto de la seguridad informática de la entidad al directorio, deberá ser una métrica con la cual, mínimamente, puedan contestar a la pregunta: ¿cómo está la compañía en términos de seguridad informática en ese aspecto?; esta respuesta luego, podría servir para tomar una o más decisiones al respecto.

Si se decidiera presentar una nueva métrica al directorio, será igual de importante (en el caso que aplique) brindarla junto con posibles alternativas de mejora o planes de mitigación de ese riesgo sobre el cual verse el indicador clave. De esta forma, el directorio será capaz de tomar la decisión más conveniente al respecto; y el área de Seguridad Informática cumplirá su rol de asesoría al directorio.

Bibliografía

- ISO/IEC: ISO/IEC 27001, Information technology - Security techniques - Information security management systems – Requirements (Octubre 2005).
- ISO/IEC: ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of practice for Information Security Management (Julio 2007).
- ISO/IEC: ISO/IEC 27004:2009, Information Technology Security Techniques – Information Security Management – Measurement (Diciembre 2009).
- NIST: Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information System and Organizations* (Agosto 2009).
- NIST: Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security* (Julio 2008).
- Andrew Jaquith: Security Metrics – Replacing fear, uncertainty, and doubt. Editorial Addison-Wesley (Marzo 2007).
- Sekar Sethuraman: Framework for Measuring and Reporting Performance of Information Security. ISACA (2008).
- C. Warren Axelrod: Accounting for Value and Uncertainty in Security Metrics. ISACA (2008).
- Corporate Information Security Working Group: Report of the best practices and metrics teams, Revision 100105 (Enero 2005).
- John P. Pironti: Developing Metrics for Effective Information Security Governance. ISACA (2007).
- Suchit Ahuja: Tech Report 2009-21, Integration of COBIT, Balanced Scorecard and SSE-CMM as a strategic Information Security Management (ISM) framework. Center for Education and Research Information Assurance and Security Purdue University - CERIAS (2009).

- Sebastian Sowa, Lampros Tsinas, Roland Gabriel: Business Oriented management of Information Security. Institute for E-Business Security, Ruhr-University of Bochum and Chair of Business Informatics (2007).
- Verne Harnish: Mastering the Rockefeller Habits: What You Must Do to Increase the Value of Your Growing Firm. Gazelles, Inc. (2010).
- Jim Collins: Good To Great - Why some companies make the leap, and others don't. Harper-Collins Publishers (2001).
- B. Maizlitsh y R. Handler, IT Porftfolio Management: Step by Step, John Wiley & Sons, (2005).
- ISO27k Implementers' Forum, www.ISO27001security.com, Dan Geer, Gary Hinson, ISACA, (2009).
- McCabe Cyclomatic Complexity, http://www.klocwork.com/products/documentation/current/McCabe_Cyclomatic_Complexity, KlockWork, (2013),
- Gestión Financiera, http://www.bbv.com.bo/archivos/GesFina4.pdf, Lic. Mba. Ismael Huanaco C., Bolsa Boliviana de Valores S.A., (2013)
- Best Practices to make BYOD simple and secure, http://s3.amazonaws.com/legacy.icmp/additional/byod_best_practices.pdf, Citrix, (2011).
- Network performance and capacity planning: Techniques for an e-business world, http://www.amsoftwareservices.net/KnowledgeBase/IBM%20-%20Network%20Performance%20and%20Capacity%20Planning.pdf, William Nametka, IBM e-Services, (1999).

Anexo I: Gestión de Identidades

¿Qué es la gestión de identidades? [73]

La gestión de identidades (También conocido como *"Access Management"*, *"Identity Management"*, *"ID Management",* "Gestión de Accesos", "Gestión de identidad", "Gestión de Derechos") es un término que se refiere de manera amplia a la administración de identidades individuales dentro de una aplicación, sistema, compañía, red o incluso un país. En lo que respecta a una Infraestructura Tecnológica empresarial, la administración de identidades se trata de establecer y administrar los roles y privilegios de accesos para cada usuario de red individual. Los sistemas de gestión de identidades proveen a los gerentes de TI dentro de las organizaciones con herramientas y tecnologías para controlar los accesos de los usuarios a información crítica dentro de la empresa.

El objetivo fundamental de un sistema de administración de identidades en una arquitectura corporativa es la de poseer una identidad por cada individuo. Pero una vez que la identidad digital se estableció, debe ser mantenida, modificada y monitorizada a través de lo que se llama "ciclo de vida de acceso". Por lo tanto los sistemas de administración de identidades proveen a los administradores herramientas y tecnologías para cambiar el rol de un usuario, seguir sus actividades y forzar la aplicación de políticas con sustento en baselines definidos. Estos sistemas están diseñados para proveer un medio de administración de acceso a usuarios a través de toda la compañía y asegurar el cumplimiento de políticas coporativas como de regulaciones gubernamentales.

La lista de tecnologías que caen dentro de esta categoría incluye herramientas de administración de contraseñas, aplicaciones que fuercen la aplicación de políticas de seguridad, aplicaciones de reportes y monitorización, y repositorios de identidades. Hoy en día, estas tecnologías tienen a ser agrupadas dentro de suites que contienen todas estas herramientas con capacidades adicionales, desde una

[73] http://www.csoonline.com/article/205053/the-abcs-of-identity-management

administración de credenciales empresarial, hasta tarjetas inteligentes (*smart-card*) automatizadas y administración de certificados digitales.

En lo que respecta a la administración de identidades, la frase del momento es "Administración del ciclo de vida de la identidad". El concepto abarca los procesos y tecnologías requeridos para proveer, administrar y sincronizar identificaciones digitales, como también funcionalidades que soporten el cumplimiento de regulaciones gubernamentales. Las tecnologías que caen bajo el rubro de administración del ciclo de vida de identidades incluyen herramientas para la creación, administración de atributos, sincronización de identidades, agregación de funciones y borrado de funciones e identidades.

¿Por qué es importante la gestión de identidades?

La gestión de identidades está intrínsecamente ligada a la seguridad y productividad de toda organización inmersa en comercio electrónico, como es claramente el caso de cualquier entidad financiera o bancaria el día de hoy en Argentina. Las compañías están usando los sistemas de administración de identidades no solo para proteger sus activos digitales, sino para mejorar la productividad del negocio. Las capacidades de los sistemas centrales pueden reducir la complejidad y costo de los procesos esenciales. El control centralizado de acceso también soporta el forzado de aplicación de políticas de seguridad consistentes.

Los sistemas de administración de identidades dan a las organizaciones una forma de controlar el gran número de notebooks no tratadas, PDAs y teléfonos celulares inteligentes alrededor de la empresa. Muchos de estos dispositivos no están en control ni fueron provistos por la compañía, y sin embargo los empleados o externos los usan para acceder a la red de la misma indiscriminadamente. La habilidad de forzar un conjunto de políticas en los dispositivos que se conectan a la red a través de la administración de identidades de usuarios de esos dispositivos móviles se está convirtiendo pronto en una algo que las compañías están obligadas a tener para asegurar la seguridad de activos.

Incluso en nuestro país tenemos el comunicado del Banco Central de la República Argentina, que indica en la sección 6 la obligación de los organismos bancarios o entidades financieras de contar con un sistema de gestión de identidades (nombrado en la comunicación "A" 4609 como política de perfiles y accesos).

¿Cómo funcionan los sistemas de Gestión de identidad?

Un sistema típico de gestión de identidad moderno contiene cuatro elementos básicos:

3) Un directorio con información sobre el personal que usa para individualizar a los distintos usuarios (para simplificarlo sería como un repositorio de identidad);
4) Un conjunto de herramientas para dar de alta, modificar o borrar esa información (aplicaciones para administrar el ciclo de vida de accesos);
5) Un sistema que regula el acceso de usuarios (asegura el forzado de políticas de seguridad y privilegios de acceso);
6) Un sistema de auditoría y reportes (para que el administrador pueda verificar que es lo que realmente está pasando en la organización).

Regular el acceso a usuarios puede involucrar varios métodos de autenticación para verificar la identidad de un usuario, incluir contraseñas, certificados digitales, *tokens* y tarjetas inteligentes. Los *tokens* físicos y tarjetas inteligentes similares en tamaño a las tarjetas de crédito han servido tradicionalmente como un componente de los esquemas de doble autenticación, que combina algo que el usuario sabe (una contraseña) y algo que el usuario tiene (el *token* o la tarjeta) para verificar la identidad de un usuario. Una tarjeta inteligente porta un chip de circuito integrado tipo micro-controlador o equivalente con una memoria interna, o bien una memoria únicamente embebida en un chip. Los *tokens* por *software*, que pueden existir en dispositivos con capacidad de almacenamiento (desde una unidad USB, hasta un teléfono celular, se vienen usando ya desde el 2005 con bastante éxito).

¿Cuál es la terminología utilizada en Gestión de Identidad?

Como siempre, en el campo de la informática los términos varían constantemente para nombrar mismas cosas, la gestión de identidad no es la excepción, pero ciertos términos son clave en el tema y vale la pena conocerlos para luego poder leer el resto del trabajo:

1) Gestión de Acceso

   Nunca veremos escrito Gestión de Identidad sin el término gestión de acceso al lado. De hecho, gran cantidad de proveedores de software y analistas están combinando ambos términos en un único concepto: Gestión de identidad y acceso (también lo veremos como IAM por sus siglas en inglés *Identity and Access Management*[74]). Se refiere al proceso y tecnologías usadas para controlar y monitorear el acceso a la red. Las funcionalidades de administración de acceso, como la autenticación, autorización, confianza y auditoría de seguridad, son parte integrante de los mejores sistemas de gestión de Identidad.

2) Credencial

   Un identificador utilizado por el usuario para ganar acceso a una red. Es la contraseña del usuario, certificado en una infraestructura de clave pública (PKI[75]) o información biométrica (huella digital, escaneo de la retina).

3) Desproveer usuarios

   Es el proceso de remover una identidad del repositorio de identidades y terminar así con todos los privilegios de acceso que pudiese tener.

4) Identidad digital

[74] http://www.sans.org/reading_room/whitepapers/services/identity-access-management-solution_1640
[75] http://www.tech-faq.com/pki-certificate.html

Es la Identidad en sí misma, incluye una descripción del usuario y los privilegios de acceso correspondientes. (Ya sea una persona física, o bien una *notebook*, teléfono celular, o cualquier otro dispositivo que pueda tener una identidad digital).

5) Derechos

   El conjunto de atributos que especifican los derechos de acceso y privilegios de una identidad digital autenticada en la red.

6) Gestión del ciclo de vida de la identidad digital

   Esta es una frase o concepto que está siendo utilizado en la actualidad para referirse al conjunto entero de procesos y tecnologías que se pueden utilizar para el mantenimiento y actualización de identidades digitales. La gestión del ciclo de vida de una identidad incluye la sincronización de identidad, provisionar identidades digitales, des provisionar identidades digitales, y la administración continua de sus atributos, credenciales y permisos de acceso.

7) Sincronización de identidades

   Es el proceso que asegura que la misma identidad digital que puede estar contenida en dos o más almacenes (o repositorios) de identidades esté completamente sincronizada de manera que estos dos repositorios contengan la misma información exacta sobre cada identidad digital. (En definitiva, es el proceso que asegura la consistencia de la información).

8) Restablecer contraseña

   En el contexto de la gestión de identidades, es una funcionalidad del sistema administrador que permite a los usuarios re-establecer su propia contraseña, reduciendo así el trabajo de los administradores y las llamadas al soporte interno de la compañía. Por lo general, el usuario puede blanquear su contraseña accediendo al sistema mediante un navegador. La

aplicación le pregunta al usuario una palabra secreta, o una serie de preguntas que solamente conocería aquel para verificar la identidad del usuario en cuestión.

9) Proveer

   El proceso de crear identidades, definir sus privilegios de acceso y agregarlas al repositorio de identidades.

10) Principal de Seguridad

   Una identidad digital con una o más credenciales que pueden ser autenticadas y autorizadas para interactuar con la red de la compañía.

Anexo II: Cumplimiento Regulatorio y Marco Normativo

¿Qué es el Cumplimiento Regulatorio?

Según el diccionario de la Real Academia Española[76] se entiende por **cumplimiento** a la: *"Acción y efecto de cumplir o cumplirse."*, si indagamos un poco más y buscamos la palabra **cumplir** encontraremos que es la acción de: *"Ejecutar, llevar a efecto. Cumplir un deber, una orden, un encargo, un deseo, una promesa."* [77].

En el idioma inglés, la palabra que se usa para nombrar al cumplimiento de normas y leyes es ***compliance***, la cual significa "conforme a una regla, la cual podría ser una especificación, política, estándar o ley" [78].

Más allá de la diferencia entre el concepto que engloba la palabra *compliance*, respecto del término español cumplimiento, ambos dos apuntan a lo mismo cuando se refiere al cumplimiento de regulaciones, o sea, se apunta a que una empresa tenga las herramientas y procesos necesarios para que todo el personal conozca las regulaciones legales que rigen a la compañía (cada país y tipo de negocio tendrá las suyas propias más las internas de la organización) y realizar su mayor esfuerzo por cumplimentar con cada una de ellas de la mejor forma posible.

¿Por qué es importante el cumplimiento de las regulaciones?

Quizá la historia más conocida dentro del mundo informático, contable y legal, fue la que ocurrió con Enron en el año 2001[79], un caso emblemático puesto que durante 6 años seguidos mostraban sus libros contables con ganancias extraordinarias, y finalmente todo fue un engaño, los números estaban en su mayoría falseados y tuvo que declarar la banca rota el 2 de diciembre del 2001.

[76] http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=cumplimiento
[77] http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=cumplir
[78] http://en.wikipedia.org/wiki/Regulatory_compliance
[79] http://en.wikipedia.org/wiki/Enron

Fue por ello que Enron se tornó en el acto de fraude y corrupción más conocido de Estados Unidos de América.

Fue en ese año que surgió la necesidad explícita de contar con un contexto regulatorio para las empresas que pudiera garantizar tanto a los empleados como a los inversionistas la veracidad de la información y libros contables que maneje una compañía, la respuesta fue brindada por dos congresistas de Estados Unidos (el senador Paul Sarbanes y Michael Oxley) en el año 2002, se llamó el Acta Sarbanes-Oxley[80], en ese acta está declarada la responsabilidad personal que llevará la alta dirección corporativa respecto de la veracidad de los reportes que haga la compañía sobre el estado financiero.

¿Qué se debería medir respecto de *Compliance*?

Las entidades bancarias deben cumplir con normativas internas como externas, por ende tienen un grupo de auditores (ya sean propios o tercerizados) que trabajan para ellos y ayudan a revisar que se esté dando cumplimiento a las distintas políticas que los regulan; y adicionalmente habrá auditores que no pertenecen a la compañía ni trabajan para la misma (por ejemplo auditores del Banco Central de la República Argentina) y que verifican que se estén llevando a cabo los controles adecuados y que los valores sean los esperados.

Entonces es necesario tener métricas sobre los siguientes puntos:

- Monitorización de eventos e incidentes de Seguridad Informática
- Cuantificación de horas insumidas (para cumplir con auditorías y para suministrar la información solicitada por los auditores)
- Estado de las Observaciones de Auditoría (con su correspondiente nivel de Riesgo)
- Proyectos en curso o finalizados durante el período en cuestión (ya sean para resolver alguna observación o para mejorar los controles vigentes)

[80] http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

Metodología de Trabajo

1) Definir los distintos niveles a los que puedan darse los incidentes (Perímetro de red, red interna, aplicaciones: ¿cuáles?, etc.)
2) Definir todas las plataformas y entornos para los cuales se posean usuarios administradores en custodia bajo sobre
3) Declarar las horas que se insumen para brindar información para auditoría, por lo que sería conveniente tener en claro los distintos orígenes de pedido de información para que el informe sea más provechoso, por ejemplo auditoría interna, auditores externos para certificar ISO 27001, auditoría externa por parte del proveedor xxxxx, etc.
4) Detallar las observaciones que se hayan hecho en períodos anteriores pero que serán trabajadas durante el período en cuestión, teniendo en cuenta su riesgo siendo lo más común diferenciarlas en “Muy Alto, Alto, Moderado o Bajo”
5) Detallar los proyectos que estén activos durante el período analizado
6) Seleccionar los gráficos y tablas a utilizar para mostrar la información obtenida a partir de la implementación de los puntos anteriores

Ejemplo práctico resumido

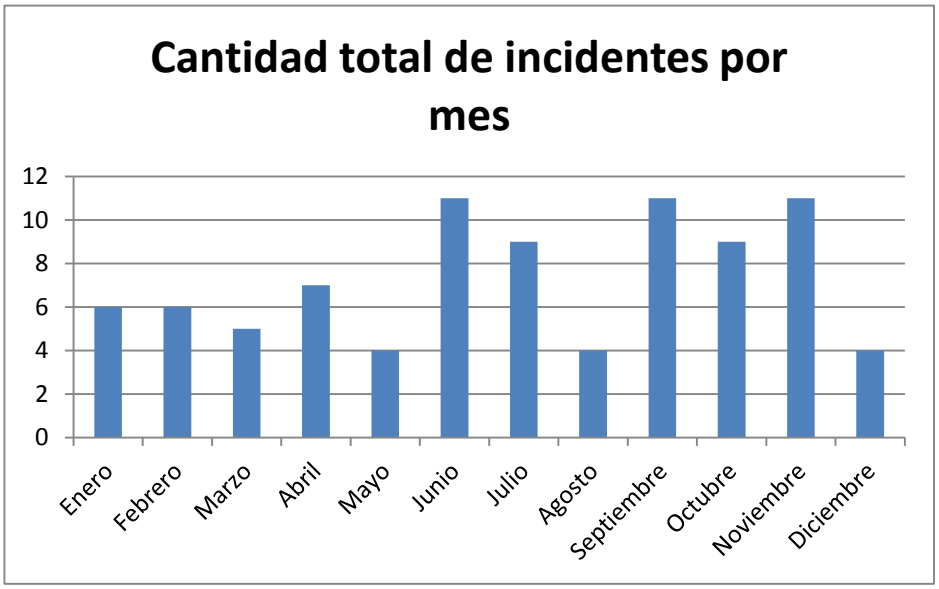
1) Definición de niveles de incidentes:
    a. Perímetro
    b. Red interna
    c. Servidores de la red interna
    d. Aplicaciones
        i. SIEBEL
        ii. SWIFT
        iii. MEP
        iv. SIOPEL
        v. Productos de Monitorización Tango/04
    e. Datos
        i. MS SQL Server – Base de datos SIEBEL

ii. MS SQL Server - Bases de datos de Tango/04
iii. Sybase – Bases de datos SIOPEL
iv. Archivos del servidor de Contabilidad y Finanzas
v. Archivos de Log SWIFT
vi. Archivos de Log MEP

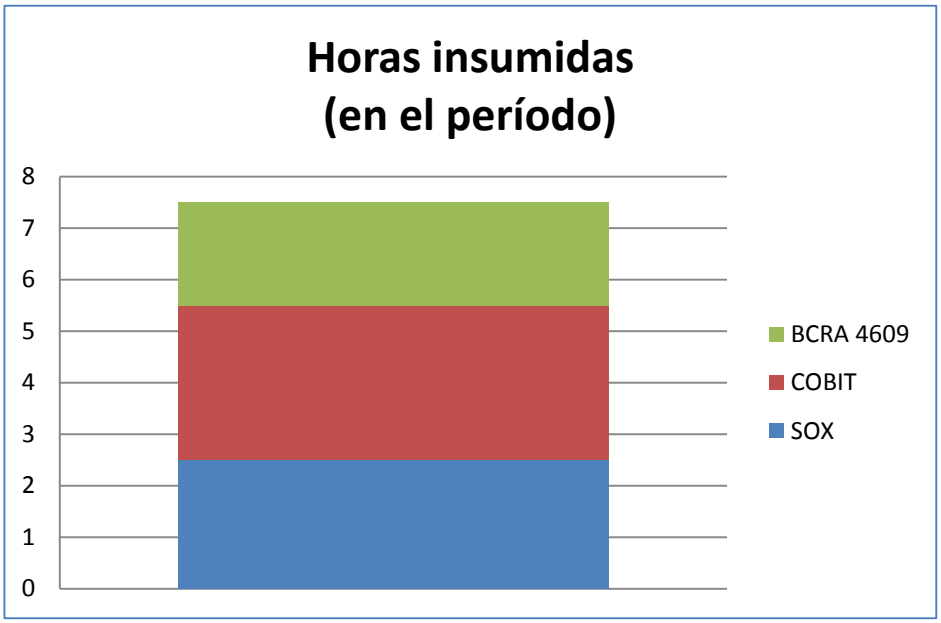
2) Entornos/Plataformas que poseen usuarios bajo sobre:
   a. Mainframe
   b. System i
   c. MS Windows
   d. Solaris
   e. Bases de datos
      i. SIEBEL
      ii. Tango/04
      iii. SIOPEL
   f. Aplicaciones
      i. SIEBEL
      ii. SWIFT
      iii. MEP
      iv. SIOPEL
      v. Productos de Monitorización Tango/04
3) Quienes pueden solicitar información al área de Seguridad Informática durante este período serán:
   a. Directorio corporativo
   b. Auditoría interna
   c. Auditores externos – Ayuda certificación SOX
4) Detalle de las Observaciones y estado:
   a. (Alto) MS Windows - Auditar la actividad de administradores de dominio productivo
   b. (Alto) System i – Eliminar los perfiles de usuarios que ya no están trabajando para la empresa

c. (Muy Alto) Firewall – Cambiar contraseñas de usuarios administradores
d. (Moderado) Auditoría MS SQL Server 2008 – Hay ciertos faltantes en las auditorías de SQL Server 2008, se deben establecer los controles para las nuevas bases de datos

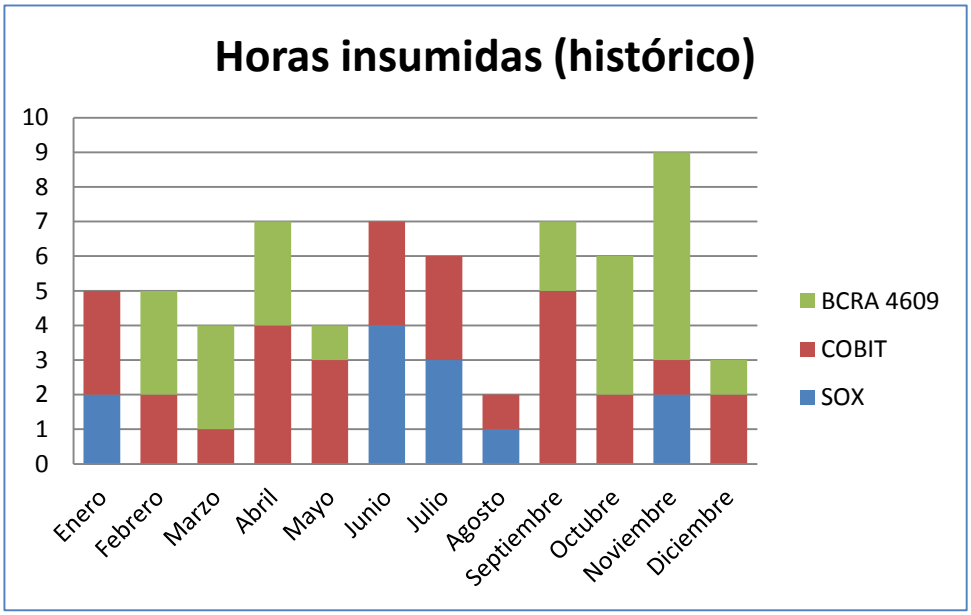
5) Proyectos activos:
   a. Migración del Active Directory corporativo de Windows 2000 a Windows 2008 R2 – En curso *(pruebas iniciales)*
   b. Monitorización en tiempo real de intentos de inicio de sesión fallidos a servidores críticos – En curso
   c. Configuración de herramientas para obtener reportes mensuales de bloqueo de transacciones en System i – Próximo a iniciarse durante el período analizado
6) Selección de gráficos o tablas para cada métrica elegida:
   a. Cantidad total de incidentes



   b. Cantidad de horas invertidas (Solicitud de información para auditorías)



c. Igual a punto a, pero histórico por mes



d. Detalle de las Observaciones Pendientes con Riesgo Muy Alto

Detalle Observaciones Pendientes (Riesgo muy alto) - Febrero 2012	
Descripción	**Estado**
La documentación de la compañía que posee la gerencia media en sus dispositivos móviles no posee encripción ni está regulada bajo	En Curso

ninguna política.	
En la auditoría externa realizada por el BCRA se detectaron más de 15 cuentas de dominio creadas para proveedores externos que actualmente están activas y estos últimos ya no prestan servicios a la empresa.	No iniciado

e. TOP 10 – Detalle Observaciones Pendientes Riesgo Alto

Proyectos del período Febrero 2012	
Descripción	**Estado**
	En Curso
	En Curso
	No iniciado

f. Proyectos del área de Seguridad Informática relativos al tema

Proyectos del período Febrero 2012	
Descripción	**Estado**
Migración del Active Directory corporativo de Windows 2000 a Windows 2008 R2	En Curso
Monitorización en tiempo real de intentos de inicio de sesión fallidos a servidores críticos	En Curso
Configuración de herramientas para obtener reportes mensuales de bloqueo de transacciones en System i	No iniciado

Obtención de Conclusiones

Incidentes del mes

Las métricas de esta categoría se refieren a incidentes de Seguridad Informática detectados en el período de análisis. Puntualmente es importante detectar a qué nivel se dio el incidente, si fue a nivel de Red, algún Aplicativo bancario, ataques al

Perímetro de red, si hubo fraude o cambios sin autorización en datos críticos de la entidad, etc.

Es importante mantener un registro de la cantidad de tickets que se abren para los incidentes de seguridad informática detectados, pero es también importante conocer el nivel al que se dieron, puesto que no es lo mismo detectar varios intentos de acceso a información crítica del banco desde el exterior del perímetro de red, que desde la propia LAN. Ambos dos pueden llegar a ser críticos para la compañía, pero uno interno podría ser más comprometedor o bien, un simple "falso positivo" si es que faltaba definir correctamente los permisos sobre ciertos recursos de red para un usuario.

Además, en ambos dos casos del ejemplo se tomarán medidas completamente distintas, puesto que una de ellas será revisada a nivel de la configuración del Firewall de la red, y la otra podría revisarse a nivel de políticas de acceso del dominio para ese usuario para acceder al recurso en cuestión.

Solicitudes de usuario bajo sobre

La utilización de usuarios administradores, o bien, con ciertos privilegios elevados para ciertos sistemas operativos (Mainframe, Windows, Linux, Solaris, AS/400, etc.), bases de datos (Oracle, MS SQL Server, PostgreSQL, etc.), o aplicaciones bancarias (SWIFT, MEP, Mesa de dinero, etc.) tiene que estar debidamente controlada.

Todas las normas de control y auditoría tienen apartados especiales donde comentan la importancia de mantener el uso de cuentas de tipo administrador bajo supervisión del área de Seguridad informática de la compañía, es preciso por ende tener las mismas bajo sobre para que no sean de público conocimiento y para controlar su uso al máximo.

Si se requirió el uso de una cuenta con privilegios administrativos para cualquier entorno es preciso que se documento, y a la vez es importante analizar la cantidad de veces que se usó y vincularla a una explicación racional, puesto que podría ser

normal en una etapa inicial en un proyecto que se comienza a implementar en la entidad tener gran cantidad de uso de cuentas administrativas para la instalación de software o para el mantenimiento de equipos.

Sea cual fuera el motivo, el equipo de trabajo de seguridad informática no puede permanecer ajeno a la apertura de los sobres que contienen la información de inicio de sesión de estas cuentas de administradores o altos privilegios.

Solicitudes de Información

Durante los procesos de auditoría internos o externos, es normal que los auditores soliciten información al área de seguridad informática. Los analistas de seguridad están prácticamente obligados a brindarla y en la forma que la soliciten los auditores para su mejor compresión y con los contenidos indicados.

Si bien hay pedidos que salen casi automáticamente por su simplicidad de cálculo u obtención, hay ciertos otros que son totalmente manuales y llevan mucho tiempo, es por ello que es muy importante declarar la cantidad de horas que se insumieron durante estas labores, para poder llevar un control respecto de la conveniencia o no de automatizar ciertos controles o reportes, y además para entender cuánto tiempo insumen estas actividades al área de seguridad informática.

Adicionalmente, si cada año o período la información solicitada es algo que se pueda prever, sería ideal utilizar los tiempos ociosos o con menor carga laboral de los analistas de seguridad para ir preparando los informes que seguramente serán solicitados por los auditores, para ir balanceando la carga y que no quede toda incurrida en un período corto donde se satura el área y se deben dejar de lado la realización de otras tareas competentes a la misma.

Observaciones

Al finalizar el análisis de los auditores, se obtiene un reporte o informe que contiene todas las observaciones realizadas por los mismos. Es fundamental hacer un seguimiento de las mismas, ya sea por el riesgo inherente sobre los

activos informáticos que puede existir, como para alertar al directorio de los riesgos que existen y las posibles acciones para controlarlo, eliminarlo, compartirlo o bien aceptarlo.

Se diferenciarán las observaciones Resueltas de las que aún están pendientes. De esta forma se podrían poner los proyectos y las tareas que se fueron cumpliendo relacionadas a cada una de estas observaciones para poder dar una priorización a ellas, seguramente basándose en los costos y recursos del área, pero principalmente teniendo en cuenta el “Riesgo”.

Anexo III: Seguridad de la Infraestructura Tecnológica[81]

La Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"[82]. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Tipos de Desastres

No será la primera vez que se mencione en este trabajo, que cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este concepto vale, también, para el edificio en el que nos encontramos. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos. Para ejemplificar esto: valdrá de poco tener en cuenta aquí, en Entre Ríos, técnicas de seguridad ante terremotos; pero sí será de máxima utilidad en Los Ángeles, EE.UU.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

1) Desastres naturales, incendios accidentales tormentas e inundaciones.
2) Amenazas ocasionadas por el hombre.
3) Disturbios, sabotajes internos y externos deliberados.

Basta recurrir al sentido común para darse cuenta que, cerrar una puerta con llave o cortar la electricidad en ciertas áreas de una institución son técnicas válidas en cualquier entorno productivo para causar un problema operativo grave al negocio.

[81] http://www.segu-info.com.ar/fisica/seguridadfisica.htm

[82] *HUERTA, Antonio Villélón. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License v.10 o Later. 2 de Octubre de 2000.* http://www.kriptopolis.org

A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

- Incendios
- Inundaciones
- Condiciones Climatológicas
- Señales de Radar
- Instalaciones Eléctricas
- Ergometría

Acciones Hostiles

- Robo

  Las computadoras son posesiones valiosas de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero.

  Es frecuente que los operadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina.

  La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora.

  El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro

- Fraude

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

- Sabotaje

El peligro más temido en los centros de procesamiento de datos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos.

Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

Control de Accesos

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

- Utilización de Guardias
- Utilización de Detectores de Metales

- Utilización de Sistemas Biométricos
- Verificación Automática de Firmas (VAF) [83]
- Seguridad con Animales
- Protección Electrónica

Notas finales

Evaluar y controlar permanentemente la seguridad física del edificio es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

Las distintas alternativas estudiadas son suficientes para conocer en todo momento el estado del medio en el que nos desempeñamos; y así tomar decisiones sobre la base de la información brindada por los medios de control adecuados.

Estas decisiones pueden variar desde el conocimiento de la áreas que recorren ciertas personas hasta la extremo de evacuar el edificio en caso de accidentes.

[83] Mientras es posible para un falsificador producir una buena copia visual o facsímil, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo la firma genuina con exactitud. La VAF, usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada. El equipamiento de colección de firmas es inherentemente de bajo costo y robusto. Esencialmente, consta de un bloque de metal (o algún otro material con propiedades acústicas similares) y una computadora barata.

Anexo IV: Comunicación “A” 4609 (Banco Central de la Rep. Argentina)

<< Impresión aparte>>

Anexo V: Sistema MEP (Medio Electrónico de Pagos)

Según informa el Banco Central de la República Argentina[84]:

SISTEMA NACIONAL DE PAGOS - MEDIO ELECTRÓNICO DE PAGOS (MEP)

El MEP fue desarrollado y es operado por el BCRA, las entidades financieras y las Cámaras Electrónicas de Compensación (C.E.C.), habiéndose iniciado su funcionamiento en 1997.

Permite que las instituciones autorizadas a operar realicen transferencias en tiempo real (Real-time Gross Settlement Systems – Sistema de liquidaciones brutas en tiempo real) a través de las cuentas corrientes que tienen registradas en el BCRA, a lo largo de un ciclo operacional prolongado y dispongan de información en tiempo real acerca de los saldos disponibles en cada una de sus cuentas.

La seguridad de las transacciones se logra con los rigurosos procedimientos que deben seguir las entidades para enviar los pagos que canalizan por este medio. Para ello se definen distintos niveles de operación:

- Carga de Operaciones
- Autorización
- Consultor

El operador de carga ingresa las operaciones que el autorizador verifica y autoriza. Esa autorización deja en firme el débito en la cuenta de la entidad ordenante y el crédito en la cuenta de la entidad beneficiaria, pasando en ese momento a ser **IRREVOCABLES**.

Las transacciones que, entre otras, pueden ejecutar las entidades financieras y las cámaras compensadoras electrónicas son las siguientes:

- Transacciones interbancarias: liquidación de fondos de transacciones con títulos-valores, mercado de dinero, etc.
- Transacciones iniciadas por los clientes: transferencias del mismo o distinto titular; transferencias por pago de sueldos

[84] Fuente oficial BCRA: http://www.bcra.gov.ar/pdfs/snp/SNP0035.pdf

- Transferencias transfronterizas: principalmente entre cuentas MEP y cuentas en dólares que las entidades financieras y el BCRA mantienen en Nueva York
- Cancelación de operaciones referidas a los Convenios de Pago y Crédito Reciproco suscriptos por el BCRA.
- Liquidación de los saldos netos del proceso de compensación
- Liquidación de pases activos en el BCRA, es decir, de contratos de recompra contra títulos del gobierno en moneda extranjera.
- Operaciones con las cuentas de garantías
- Pagos Judiciales

Las entidades emisoras de transferencias MEP que actúen por cuenta de sus clientes, deben informar los detalles del pago (clave bancaria uniforme –CBU- nombre de la cuenta, número de CUIL-CUIT O CDI optativo para operaciones gravadas y obligatorio para operaciones no gravadas y en el caso de no disponer de CBU: sucursal de la entidad acreedora, tipo y número cuenta.) con el objetivo de permitir una correcta aplicación de los fondos.

Existen un sistema alternativo denominado “Plan de Contingencia” utilizado en los casos de un funcionamiento inadecuado de los enlaces de comunicación entre el BCRA y las entidades miembro, permitiendo de esta forma evitar un corte en la cadena transaccional.

Actualmente el BCRA no aplica comisiones a las entidades miembros por los servicios que brinda a través del MEP como una manera de promover la utilización del sistema, la que creció con el transcurso del tiempo en forma sostenida, juntamente con la bancarización de operaciones.

El BCRA se encuentra en proceso de implementación de un sistema transaccional que moderniza la tecnología que soporta este sistema haciéndolo mas amigable para su operación, pero con las mismas características de seguridad que posee el sistema actual.

Anexo VI: Método de Evaluación C.A.M.E.L.

Por sus siglas en inglés: Capital, Asset, Management, Earning and Liquidity.[85]

El método de evaluación de CAMEL, consiste en medir y analizar cinco parámetros fundamentales: Capital, Activos, Manejo Corporativo, Ingresos y Liquidez.

Dicha evaluación es utilizada principalmente en el sector financiero para hacer mediciones de riesgo corporativo.

Fue un método adoptado por los entes reguladores de la Banca Norteamericana, con el fin de evaluar la solidez financiera y gerencial de las principales entidades comerciales de los Estados Unidos. CAMEL hace la revisión y calificación de cinco áreas de desempeño financiero y gerencial: Idoneidad de Capital, Idoneidad de Activos, Manejo Gerencial, Estado de Utilidades, y Liquidez Administrativa.

Generalmente para llevar a cabo una evaluación tipo CAMEL se requiere la siguiente información: (1) estados financieros; (2) presupuestos y proyecciones de flujo de efectivo; (3) tablas de amortización de cartera; (4) fuentes de financiamiento; (5) información relativa a la junta de directores; (6) operaciones/patrones de personal; e (7) información macro-económica.

Los estados financieros constituyen la base del análisis cuantitativo que realiza CAMEL. Se precisa que las empresas presenten estados financieros debidamente auditados, correspondientes a los últimos tres años, así como estados interinos para el último período de 12 meses. Los demás materiales requeridos proporcionan información de planificación y muestran la evolución que ha tenido la institución. Estos documentos demuestran a los analistas de CAMEL el nivel y estructura de las operaciones de préstamo.

Calificación Otorgada por CAMEL

Basándose en los resultados de los estados financieros debidamente ajustados, y las entrevistas con el personal ejecutivo y operativo de las empresas CAMEL asigna una calificación comprendida del uno al cinco, para cada uno de los 21 índices identificados

[85] Esta primer parte está copiada íntegramente del artículo publicado en: http://www.gestiopolis.com/recursos/experto/catsexp/pagans/eco/14/CAMEL.htm

por CAMEL, los cuales se sopesan concordantemente. A continuación se presenta una definición para cada área y la gama de criterios que determinan cada calificación:

Idoneidad de Capital.

El objetivo que persigue el análisis de la idoneidad de capital es el de medir la solvencia financiera de una empresa o institución financiera, mediante la determinación de si los riesgos en los que ha incurrido están adecuadamente equilibrados con el capital y reservas necesarios para absorber posibles pérdidas.

Un índice es el apalancamiento que ilustra la relación que existe entre los activos de la IMF y sus riesgos y su equidad. Otro índice, la capacidad para captar equidad constituye una evaluación cualitativa de la capacidad que posea la IMF para responder ante la necesidad de reponer o incrementar su equidad en cualquier momento dado. Un tercer índice, la idoneidad de reservas constituye una medida cuantitativa de las reservas que posea la empresa para confrontar pérdidas de cartera y la medida en que la institución pueda absorber posibles pérdidas de cartera.

Calidad de los Activos.

El análisis que se hace sobre la calidad de los activos se divide en tres componentes: calidad de la cartera, sistema de clasificación de cartera, y activos fijos. La calidad de cartera incluye dos índices cuantitativos: cartera en riesgo, que determina el monto de cartera vencida más allá de 30 días; y política de sanciones/anulaciones, que determina cuáles son las anulaciones y sanciones introducidas por la empresa basándose en criterios CAMEL. El sistema de clasificación de cartera conlleva la revisión de las tablas de amortización de cartera y la evaluación de las políticas que tiene la institución con respecto a la evaluación de riesgos de cartera.

Bajo los activos fijos, un índice constituye la productividad de los activos a largo plazo, que evalúan las políticas de la empresa con respecto a inversiones en bienes fijos. ***El otro índice tiene que ver con la infraestructura institucional, que se evalúa para determinar si es que cumple con las necesidades tanto del personal como de los clientes.***

Administración Gerencial.

Son cinco los índices comprendidos en este aspecto del análisis: administración, recursos humanos, procesos, controles y auditoría; sistema de tecnología informática; y planificación estratégica y presupuestos. Administración se centra en torno a cuán bien funciona el directorio o junta directiva de la institución, incluyendo la diversidad de su destreza técnica, su independencia de la gerencia, y su capacidad de adoptar decisiones de manera flexible y efectiva. El segundo índice, recursos humanos evalúa si es que el departamento de recursos humanos proporciona una guía clara y presta el apoyo indispensable para el personal operativo, incluyendo contratación y capacitación de nuevo personal, sistemas de incentivos para el personal, y sistema de evaluación de desempeño. El tercer índice, procesos, controles y auditoría se centra en torno al grado al que la empresa ha formalizado sus procesos claves y la eficacia con la que controla sus riesgos abarcando toda la organización, según se deduce por su ambiente de control y la calidad de su auditoría interna y externa. El cuarto índice, sistema de tecnología informática evalúa los sistemas de información computarizada y si es que están funcionando eficaz y eficientemente, si se generan informes para fines gerenciales de manera oportuna y exacta. Estos análisis revisan el ambiente tecnológico de la información, así como la magnitud y calidad de los controles específicos introducidos en la tecnología de informática. El quinto índice, planificación estratégica y elaboración de presupuestos indaga el hecho de si la institución lleva a cabo un proceso comprehensivo y participativo para generar proyecciones financieras en el corto y largo plazo, y si es que el plan es actualizado de acuerdo a las necesidades, y empleado dentro del proceso de tomar decisiones.

Utilidades.

CAMEL elige tres índices cuantitativos y uno cualitativo para medir el rendimiento de la empresa créditos ajustados sobre equidad, eficiencia operativa, réditos ajustados sobre activos, y la política aplicada a la tasa de interés. Rédito ajustado sobre equidad (ROE) mide la capacidad que tiene la institución de mantener e incrementar su valor neto a través de las utilidades que le genera sus operaciones. Eficiencia Operativa determina la eficiencia que ha alcanzado la institución y guía su progreso hacia lograr una estructura de costos que se acerca al nivel logrado por instituciones financieras formales. Réditos ajustados sobre activos (ROA) mide cuán bien han sido utilizados los activos de la empresa o la capacidad institucional para generar utilidades sobre una base de activos

definida. Los analistas CAMEL también estudian la política aplicada a tasas de interés que ha adoptado la empresa o institución financiera a fin de evaluar el grado al que la administración analiza e introduce ajustes a las tasas de interés de la institución con relación a préstamos micro-empresariales (y depósitos, de aplicar), basándose en el costo de los fondos, metas de utilidad, y ambiente macro-económico.

Manejo de Liquidez.

La quinta área que evalúa CAMEL tiene que ver con la capacidad que tiene la institución para manejar las disminuciones en las fuentes de fondos e incrementos en activos, así como para cubrir gastos a un costo razonable. Los índices en este aspecto se basan en estructura de pasivos, disponibilidad de fondos para satisfacer la demanda de crédito, proyecciones de efectivo, y productividad de otros activos corrientes. Bajo estructura de pasivos, los analistas de CAMEL revisan la composición de los pasivos de la institución, incluyendo su tendencia, tasa de interés, condiciones de pago y sensibilidad a los cambios que se dan en el ambiente macro-económico. Los tipos de garantías que precisan las facilidades de crédito, fuentes de crédito de que dispone y la medida en que se analiza de buena forma la diversificación de recursos. Este índice también se centran en torno a la relación se mantiene con la banca en términos de apalancamiento logrado sobre la base de garantías, nivel de credibilidad que maneja la institución con respecto al sector bancario, y la facilidad con la que la institución puede obtener fondos cuando lo precisa.

Adicionalmente, según el trabajo realizado por Malave y Morillo[86] en el año 2006, se nota la importancia del control y auditoría de los sistemas de información tanto en el capítulo ACTIVOS como en el de MANAGEMENT.

Según indican los autores en su trabajo:

> 2.4 EFICIENCIA DE LA GERENCIA.
>
> Son cinco los índices comprendidos en este aspecto del análisis: administración, recursos humanos, procesos, controles y auditoria; sistema de tecnología informática; y planificación estratégica y presupuestos.

[86] Aplicación del método CAMEL a mi Casa Entidad de Ahorro y Préstamo. C.A.: http://ri.biblioteca.udo.edu.ve/bitstream/123456789/485/1/TESIS-658.151_M212_01.pdf

Administración se centra en torno a cuán bien funciona el directorio o junta directiva de la institución, incluyendo la diversidad de su destreza técnica, su independencia de la gerencia, y su capacidad de adoptar decisiones de manera flexible y efectiva. El segundo índice, recursos humanos evalúa si es que el departamento de recursos humanos proporciona una guía clara y presta el apoyo indispensable para el personal operativo, incluyendo contratación y capacitación de nuevo personal, sistemas de incentivos para el personal, y sistema de evaluación de desempeño. El tercer índice, procesos, controles y auditoria se centra en torno al grado al que la empresa ha formalizado sus procesos claves y la eficacia con la que controla sus riesgos abarcando toda la organización, según se deduce por su ambiente de control y la calidad de su auditoría interna y externa. El cuarto índice, sistema de tecnología informática evalúa los sistemas de información computarizada y si es que están funcionando eficaz y eficientemente, si se generan informes para fines gerenciales de manera oportuna y exacta. Estos análisis revisan el ambiente tecnológico de la información, así como la magnitud y calidad de los controles específicos introducidos en la tecnología de informática. El quinto índice, planificación estratégica y elaboración de presupuestos indaga el hecho de si la institución lleva a cabo un proceso comprehensivo y participativo para generar proyecciones financieras en el corto y largo plazo, y si es que el plan es actualizado de acuerdo a las necesidades, y empleado dentro del proceso de tomar decisiones.

En el área de calificación de la eficiencia administrativa se toman variables tales como:

- Nivel y calidad de respaldo de las directivas y de la gerencia a las actividades desarrolladas por el ente.
- Habilidad de directivas y administradores para tomar decisiones, planear y responder ante cambios y riesgos imprevistos, así como para desarrollar oportunamente nuevos productos o planes de negocios.
- ***Políticas internas adecuadas para identificar y controlar las operaciones de riesgo.***

- Oportunidad en el manejo de la información e implantación de sistemas de control de riesgos, de acuerdo al tamaño de la organización y a las actividades desarrolladas.
- ***Cumplimiento de leyes, normas y reglamentos.***
- ***Respuesta oportuna a recomendaciones presentadas por auditores o autoridades externas.***
- Concentración de autoridad en pocas manos.

Normalmente se consideran en ésta área, riesgos inherentes a las actividades crediticias, de mercado, operacionales, de imagen, legales y de liquidez, dependiendo de la naturaleza y alcance de las actividades desarrolladas por el ente.

CALIFICACIÓN DE EFICIENCIA DE LA GERENCIA

CALIFICACIÓN UNO (1)
Excelente desempeño en la administración por parte de la junta directiva y la gerencia, teniendo un manejo óptimo del riesgo, en coherencia con el tamaño, complejidad y perfil de riesgo de la entidad. Todos los riesgos significativos han sido identificados, medidos y controlados.
CALIFICACIÓN DOS (2)
Buen desempeño en la administración por parte de la junta directiva y la gerencia, teniendo un manejo bueno del riesgo según el tamaño, complejidad y perfil de riesgo de la entidad. Aunque pueden existir debilidades, éstas no comprometen a la institución y están siendo atendidas de manera satisfactoria.
CALIFICACIÓN TRES (3)
La junta directiva y la gerencia necesitan mejorar las prácticas del manejo del riesgo ya que no son del todo satisfactorias, tomando en cuenta el tamaño y perfil de riesgo de la entidad. Esta calificación denota el incumplimiento de una o más medidas de supervisión formal o informal.
CALIFICACIÓN CUATRO (4)
La administración es deficiente y, por lo tanto, es inadecuado el desempeño en el manejo del riesgo si se tiene en cuenta la naturaleza, tamaño y perfil de la institución. Se han encontrado problemas serios y la exposición al riesgo es alta, por lo que se debe considerar la posibilidad de reemplazar o reforzar la junta directiva.
CALIFICACIÓN CINCO (5)
Es señal de incompetencia en el manejo de la entidad. Las prácticas de administración del riesgo son deficientes y la inadecuada identificación, monitoreo y control de los riesgos comprometen la viabilidad de la institución.

Debe fortalecerse o sustituirse la administración.

Anexo VII: Comunicación “A” 5374 (Banco Central de la Rep. Argentina)

<< Impresión aparte >>