ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"APLICACIÓN DE LA METODOLOGÍA SOX IT (COBIT) A SISTEMAS DE SEGURIDAD PARA BASE DE DATOS, APLICATIVOS Y SISTEMAS OPERATIVOS"

TESIS DE GRADO

Previa a la obtención del Título de:

MAGÍSTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

Presentado por:

GLADYS MARIA VILLEGAS RUGEL

Guayaquil - Ecuador

2012

AGRADECIMIENTO

Primeramente agradezco a Dios, por darme las bendiciones necesarias para culminar esta etapa de mi vida académica.

A mi padre, por su esfuerzo y dedicación para darme los recursos necesarios durante toda mi vida académica.

A mi esposo, por darme su apoyo incondicional durante la realización de esta tesis.

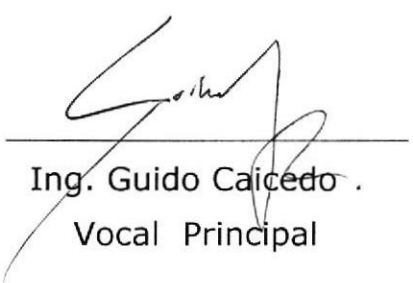
A todos los profesores que aportaron con sus conocimientos durante esta promoción del MSIG.

DEDICATORIA

La culminación de este trabajo es muy importante para mí y a la vez muy especial. Es importante porque refleja el logro de haber alcanzado un nivel más en mi vida académica y es muy especial porque desde el inicio de este trabajo he estado junto a mi esposo, quien me ha enseñado que no hay obstáculos que impidan alcanzar nuestras metas y también porque durante esta tesis han estado junto a mí, los seres que me enseñaron que uno puede ser responsable ante cualquier cambio que nos ponga la vida, como el hecho de ser madre. Por tal motivo este trabajo se lo dedico a mi esposo e hijos.

TRIBUNAL DE GRADUACIÓN

Ing. Lenin Freire
Director de Tesis



Ing. Guido Caicedo .
Vocal Principal

Ing. Fabricio Echeverría
Vocal Suplente

POL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

(Art. 12 del Reglamento de Graduación de la ESPOL)

GLADYS MARIA VILLEGAS RUGEL

ÍNDICE GENERAL

Contenido

INDICE DE FIGURAS

INDICE DE TABLAS

Introducción

Debido a la dependencia de la Tecnología de la información que tienen las empresas a través de los procesos y transacciones más relevantes, se ha creado la necesidad de implementar buenas prácticas que ayuden asegurar el activo más importante de los negocios "La información".

Inicialmente las empresas trabajaban por tener los mejores equipos y software de seguridad que puedan existir en el mercado pero hoy en día esa visión está cambiando debido a que las empresas están preocupándose por implementar metodologías de mejora y control de procesos que ayuden a identificar actividades de control que mitigan los riesgos existentes y proyectan los riesgos futuros.

Cobit ha sido el marco de referencia más utilizado por las empresas, a partir de este se han creado algunas metodologías de evaluación de procesos de TI.

Cobit es un marco referencial que cubre todos los alcances que se pueden presentar en una ambiente que está totalmente dependiente de las Tecnologías de Información. Adicionalmente Cobit es el complemento de la Ley Sox, un motivo más porque se

ha vuelto en el marco referencial más implementado por grandes empresas.

Capítulo 1: Definiciones

1.1 Objetivos de la tesis.

El objetivo principal de esta tesis es determinar los elementos que se aplican al implementar la metodología SOX IT (COBIT) en los diferentes procesos del área de Tecnología de la Información (TI), a través de un procedimiento de desarrollo de la metodología que optimice los recursos en la ejecución de una auditoria de sistemas.

Además se desea convertir esta tesis en un manual de consulta que permita al lector entender como implementar la metodología SOX IT (COBIT) como herramienta que ayuda a identificar y administrar los riesgos asociados con la tecnología de información.

A continuación se detallan los objetivos específicos:

- Conocer los conceptos que se aplican en la metodología SOX IT (Cobit).
- Identificar de actividades de control en los procesos de seguridad de TI que se encuentren alineados a los objetivos del negocio.
- Identificar los riesgos latentes en los sistemas de seguridad de bases de datos, aplicativos y sistemas de operación.
- Determinar las actividades de control que mitigan los

riesgos identificados en los diferentes sistemas de seguridad.

- Mostrar la coherencia que existe entre los objetivos de los controles y los objetivos del negocio.
- Exponer los pasos que intervienen en la implementación de la metodología SOX IT (Cobit)
- Exponer la aplicación de la metodología SOX IT (Cobit) mediante un caso de estudio.

1.2 Alcance de la tesis

El alcance de esta tesis está orientado a entregar una documentación ordenada que ayudará a identificar los riesgos y controles que se encuentran involucrados dentro del proceso de seguridad de cualquier empresa.

La visión de la autora es que esta tesis se convierta en un manual importante para la identificación de actividades de control que mitiguen riesgos dentro del proceso de seguridad de TI para finalmente aplicar la metodología SOX IT, por lo que el alcance de esta tesis involucra lo siguiente:

- Revisión de la definición de los elementos que forman parte de la metodología SOX IT.
- Identificación de los riesgos que limitan el cumplimiento de

los objetivos del negocio.

- Planteamiento de actividades de control que ayuden a mitigar los riesgos identificados.
- Identificación de las evidencias que satisfacen la evaluación de la actividad de control.
- Identificación de responsables de la ejecución de la actividad de control.
- Elaboración de documentos y matrices que intervienen en el desarrollo de una auditoría de sistemas.
- Adecuación de la documentación que interviene en la metodología SOX IT de tal manera que abarque la información necesaria para evaluar el área de TI, optimizando el tiempo.

1.3 Solución del problema

La problemática encontrada en la implementación de la metodología SOX IT es el exceso de tiempo que demanda llenar la documentación que incluye la metodología, debido a esto en muchas ocasiones los auditores no relevan ni analizan información importante que puede contribuir a hallazgos de debilidades en el área de TI.

En esta tesis se ha planteado una mejora a la metodología SOX IT

donde se ha seleccionado y modificado las matrices de tal manera que solamente incluyan información necesaria y trascendental para concluir con el objetivo de la auditoría dentro de un tiempo que es considerable para que el auditor realice su trabajo de campo.

Dejando así, este trabajo de tesis como una referencia para las personas que quieran hacer una auditoría de manera objetiva y concisa utilizando una metodología basada en el marco referencial COBIT.

1.4 La Ley de Sarbanes-Oxley

La Ley de Sarbanes – Oxley fue creada en Julio del 2002, después de los múltiples fraudes, corrupción administrativa, conflictos de interés, negligencia y la mala práctica de algunos profesionales y ejecutivos que conociendo los códigos de éticas y políticas, sucumbieron a la mala acción de ganar dinero de manera deshonesta, que a través de empresas y organizaciones engañaron a socios, empleados y grupo de interés entre ellos sus clientes y proveedores.

La ley Sarbanes-Oxley contiene **conjunto de medidas** que tienden a asegurar la efectividad de los controles internos sobre reportes e informes financieros:

- **Sección 302**: El "CEO" (Chief Executive Officier) y "CFO" (Chief Financial Officier) preparará una certificación que acompañará el informe de auditoría para certificar "la razonabilidad de los estados financieros y sus notas, y que los mismos representan las operaciones y la condición financiera de la empresa." Una violación de esta sección tiene que existir el conocimiento y la intención para que resulte en una obligación.[1]
- **Sección 404** "La SEC (Securities and Exchange Commission) obligará a las empresas cotizadas a incluir en la memoria anual un informe de control interno que deberá ser auditado".[1]

Claramente esta ley deja previsto que los auditores externos deben enfocarse en lo siguiente:

- El proceso de evaluación seguido por la gerencia para emitir su certificación.
- La efectividad y eficacia de los controles internos que se ejecutan sobre la información financiera. La evaluación de estos controles deben ser de manera independientes por un auditor financiero.

La Ley SOX sigue una secuencia lógica establecida por una serie

de actividades que alinean a la gerencia y a los auditores a encontrar una conclusión. El inicio de este proceso considera un análisis del contenido de los estados financieros de la compañía. Después se identifican sus balances.

La aplicación de este marco regulatorio hace que los proceso IT tomen mayor importancia dentro del control interno de una organización. El proceso IT es el soporte informático de los otros procesos de negocio, por tal motivo debe brindar la seguridad para las aplicaciones que lo soportan. [1]

Aunque la Ley SOX no especifica un alcance preciso a las áreas de riesgos que deben considerarse para los controles generales de la Tecnología de la información, COBIT (Control Objetives Information Technology) ha sido la solución para la mayoría de las compañías quienes han tomado los dominios de este marco referencial quedando a criterio de ella los subdominios que se consideraran para su alcance. Por ejemplo, la metodología que hace referencia con Plan de continuidad del negocio, no se incluye en SOX, pero la mayoría de las empresas han tomado este sub dominio de COBIT y lo están incluyendo en el alcance de la evaluación de control interno para mitigar riesgos.

Las compañías en algunas ocasiones ven el proceso de evaluación de controles y mitigación de riesgos como un trámite burocrático, al implementar la Ley Sarbanes-Oxley (SOX), sin embargo, cada vez es más utilizada por las gerencias para asegurar sus procesos. [1]

En la actualidad el proceso de evaluación y mitigación de riesgos se considera un pilar fundamental en las empresas, se debe destacar que la existencia de un proceso de evaluación de control tradicional o frecuente tiende a generar "acostumbramiento" hasta llegar a perder su eficiencia, cuando el objetivo es que este sea proactivo para detectar deficiencias de control para asegurar a la compañía integridad en sus estados financieros.

1.5 Marco de trabajo: Cobit

El marco de control recomendado por el PCAOB (Public Company Acounting Oversight Board) para el cumplimiento de la ley SOX es COSO (Committee of Sponsoring Organizations of the Treadway Commission) el mismo que se encarga del control de reportes financieros y operativos sin considerar los aspectos de tecnología de la información, debido a esto muchas empresas en

el mundo han identificado al marco de control COBIT (Control Objetives for Information and Related Technology) para definir los lineamientos de control para el área de Tecnología de la información. [2]

En mayo 2007, se publicó la versión 4.1 de COBIT, el mismo que fue creado por la Asociación para la Auditoría y Control de Sistemas de Información, ISACA (Information System Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información, ITGI (The IT Governance Institute). Proporciona un estándar cual es un marco referencial que reúne las mejores prácticas en la seguridad de la información. [3]

COBIT es un conjunto de mejores prácticas para la seguridad de la información que ayudan a la alta dirección, ejecutivos y administradores a incrementar el valor de las tecnologías de la Información y a reducir los riesgos del negocio. [3]

COBIT es un marco referencial que ayuda a asegurar que las Tecnologías de la Información se encuentren alineadas a los objetivos del negocio, su recursos sean administrados de manera eficientes y seguros, y para administrar los riesgos del negocio de

manera apropiada. Este marco de trabajo comprende un conjunto de dominios y procesos, y presenta las actividades o tareas a realizar en una estructura manejable y lógica. [3]

Existen algunas razones para aplicar un marco de trabajo para el control del Gobierno de TI en las organizaciones, sin importar su actividad o tamaño, debido a que se está incrementando la preocupación de la alta gerencia por el impacto significativo que la información puede tener en los objetivos de una empresa.

En la actualidad, la alta gerencia o dirección de una organización espera que la Tecnología de la Información contribuyan al éxito del negocio y pueda obtenerse una ventaja competitiva de su buen uso.

En toda organización, el éxito viene dado por su identificación y administración de riesgos así como también la utilización eficiente y eficaz de los recursos de TI.

Las organizaciones necesitan implementar un marco de referencia de gobierno y de control para la Tecnología de Información con el objetivo de responder de manera eficiente a los requerimientos del negocio. [4]

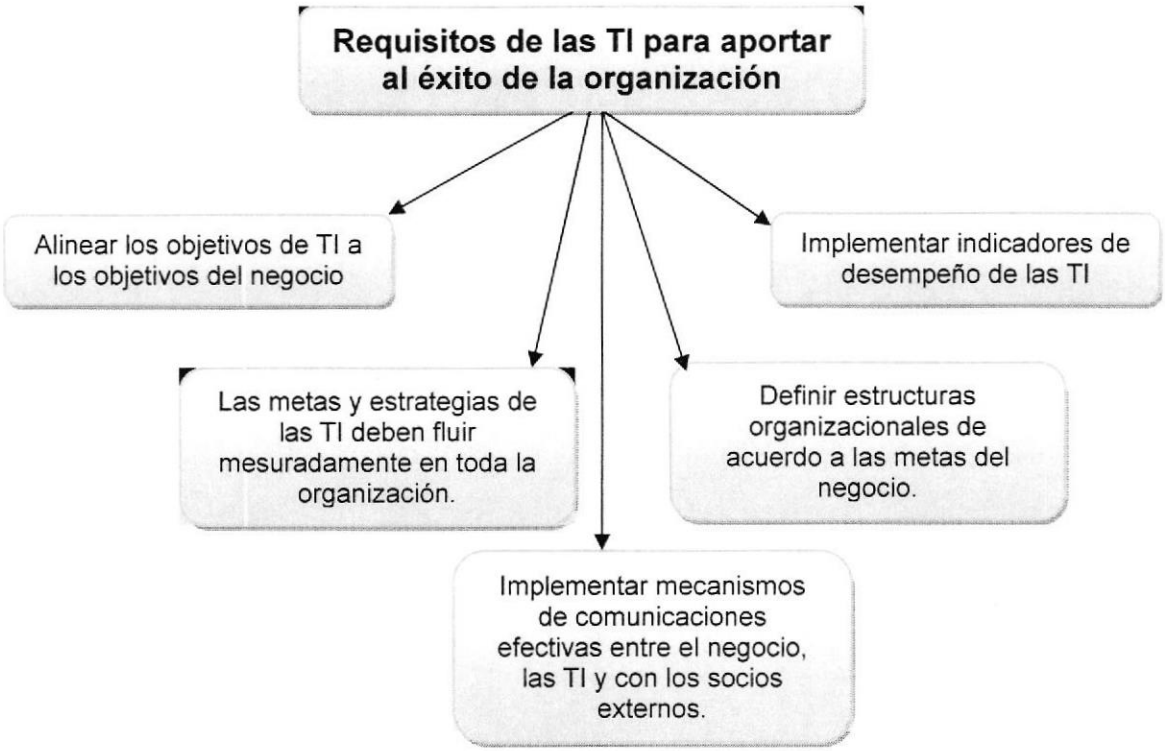


Figura (1.1): Requisitos de las TI

La necesidad de cumplir con los nuevos de requerimientos regulatorios ha llevado a implementar en las organizaciones un marco de trabajo de control que en conjunto con el gobierno de TI se ajustan a las mejores prácticas. Las mejores prácticas se han convertido importantes debido a algunos factores, tales como: [4]

- Las TI se encuentran embebidas en la mayoría de los procesos organizacionales.

- Preocupación del gobierno de TI por el aumento del nivel de gastos en las TI.
- Directivos del negocio que exigen un mayor retorno de la inversión de las TI.
- El proceso de selección para los proveedores de servicio y administración del Outsourcing y niveles de acuerdos de servicios.
- Aumento de vulnerabilidades en las TI.
- La exigencia de las entidades regulatorias locales y del exterior.
- Optimizar y minimizar los costes a través de una perspectiva estandarizada y probada en lugar de una perspectiva individualista y no probada.

COBIT clasifica las actividades de TI dentro de sus cuatro dominios. Los dominios de COBIT son: [5]

- Planear y Organizar
- Adquirir e Implementar
- Entregar y Dar Soporte
- Monitorear y Evaluar

El marco de trabajo COBIT facilita un modelo de procesos de referencia y el mismo lenguaje para todos involucrados en las tareas de la organización, con el objetivo de visualizar y administrar las actividades de TI. [5]

La implementación de un modelo y un lenguaje común para cada uno de los procesos del negocio involucrados en TI es uno de los pasos iníciales más importantes hacia un buen gobierno.

COBIT también ofrece un marco de trabajo para medir y monitorear el desempeño y cumplimiento de las Tecnología de la información, y adicionalmente define actividades e identifica los riesgos que necesitan ser administrados, promueve la robustez de los procesos y definición de responsabilidades.

1.6 Relaciones Cobit-SOX

Es necesario identificar los objetivos de control de Cobit que tienen relación con SOX y que a su vez estén relacionados con mantener la integridad y confidencialidad de la información, para poder dar cumplimiento a la ley Sarbanes – Oxley y cubrir los aspectos tecnológicos de las empresas. [6]

Los aspectos tecnológicos más importantes a controlar en toda empresa son: Seguridad, Control de cambios y Control de Operación.

La primera gran diferencia es que COSO está enfocado a toda la organización, mientras que COBIT se centra en el entorno IT. La segunda es que COBIT contempla de forma específica la seguridad de la información como uno de sus objetivos, cosa que COSO no hace. Y la tercera, que el modelo de control interno que presenta COBIT es más completo, dentro de su ámbito, que el de COSO, ya que contempla políticas, procedimientos y estructuras organizativas además de procesos para definir el modelo de control interno. [6]

1.7 Descripciones de dominios Cobit

PLANEAR Y ORGANIZAR. El alcance de este dominio es identificar si los objetivos de TI están alineados con los objetivos del negocio. Este dominio delinea todo lo que corresponde a nivel estratégico, tal como políticas, procedimientos, funciones, organigramas del área de TI. [7]

ADQUIRIR E IMPLEMENTAR. Este dominio considera que las soluciones de TI sean estas desarrolladas en la empresa o adquiridas por terceros, ayuden a los procesos del negocio. En este dominio se considera todas las etapas del desarrollo de soluciones de TI, desde que se tiene la idea o requerimiento hasta que la utiliza al usuario final. [7]

ENTREGAR Y DAR SOPORTE. El alcance de este dominio considera todo el trabajo operativo que se realiza a nivel de TI tal como soporte a los usuarios, aplicaciones e infraestructura. [7]

MONITOREAR Y EVALUAR. En este último dominio se considera la evaluación del funcionamiento de los procesos de TI, es decir si todo está funcionando tal como se lo consideró desde el inicio de la idea. Además evalúa si todo esta correcto bajo el marco regulatorio. [7]

Capítulo 2: ¿Cómo lo empleo? Desarrollo de la metodología

2.1 Identificación y documentación de sistemas relevantes a Estados Financieros.

Después que se han identificado las cuentas significativas a través de una evaluación del proceso financiero, ahora deben ser identificados los procesos y transacciones relevantes, con los que se realizará la identificación de sistemas / aplicaciones de información relacionadas. La identificación de los sistemas y procesos relevantes son determinados por los dueños del proceso ya que son ellos quienes manejan diariamente tales procesos. [8]

Para la identificación de estos sistemas es importante realizar un análisis exhaustivo y detallado de los procesos tomando en cuenta cuales son los aplicativos que intervienen en las transacciones de estos procesos. [8]

Una vez que se haya realizado el análisis y se determine el conjunto de sistemas de alcance, se debe guardar esta información en algún documento debido a que en los posteriores análisis será de mucha importancia.

2.2 Identificación de controles en los sistemas de información relevantes.

El PCAOB (Public Company Accounting Oversight Board), es una autoridad regulatoria que se encarga de emitir estándares de auditoría para dar cumplimiento a los lineamientos establecidos por la ley SOX. Dentro de estos estándares se encuentra el estándar no.2 de auditoría, el cual fue aprobado por la SEC (Securities and Exchange Commission) en el 2004, en donde establece los lineamientos que debe de seguir el auditor en la revisión del control interno aplicable en la preparación de la información financiera, y en el párrafo No.50 nos menciona los controles generales de cómputo que deben evaluarse, los cuales son: [8]

- Desarrollo y cambio de programas.
- Operación de computadora.

- Acceso a programas y datos.

Los controles generales de cómputo nos ayudan a que la información generada por los sistemas y que es utilizada en el proceso de negocio para la emisión de los estados financieros, cuenten con integridad y confidencialidad entendiéndose por estos términos, lo siguiente:

- Integridad: garantizar la exactitud de la información frente a la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- Confidencialidad: característica o atributo de la información por el que la misma sólo puede ser revelada a las personas autorizadas en tiempo y forma determinados.

Estos controles aplican a todos los sistemas de información, y al ser estos controles un soporte para la generación de la información financiera, entran en el ámbito de la gestión de la evaluación del control interno en virtud de la Sección 404 de SOX. Como resultado de la mejora continua, reducir costos e integrar a las pequeñas empresas, el PCAOB, en el año 2006 emitió el estándar No.5 de auditoría, observándose que para los lineamientos establecidos para la evaluación de controles generales de cómputo, éste no presenta cambios.

2.3 Identificación de los procesos de control en los sistemas de información críticos.

Los procesos de control que se deben evaluar en una organización están identificados de acuerdo al impacto que tienen estos dentro de los objetivos o metas de la empresa. [8]

En algunas organizaciones se evalúa el proceso estratégico, proceso de control de cambios, proceso operativo y proceso de seguridades, siendo el último el proceso más importante debido a los fraudes identificados por vulnerabilidades en los sistemas o procesos de una organización.

Los procesos de control de seguridades en los sistemas críticos son:

- Procesos de seguridad de aplicativos.
- Procesos de seguridad de base de datos.
- Procesos de seguridad de sistemas operativo.

2.4 Descripción del proceso de seguridad.

El proceso de seguridad se encarga de describir el cumplimiento

efectivo de las políticas y procedimientos de seguridad en una organización. Este tipo de auditoría debe realizarse con conocimientos previos de los distintos riesgos y controles aplicables a una organización, no tiene sentido auditar todos los controles recomendados si estos no son aplicables a la organización, debido a que no existe un riesgo en ese sentido, o porque el coste de la implementación de dichos controles se ha considerado superior al coste resultante de la materialización de una amenaza (impacto) o del propio activo.

2.4.1 Seguridad de Aplicativos

Los aspectos de seguridades que se analizan en los aplicativos son integridad, disponibilidad y confidencialidad. Los aplicativos que son analizados en base a sus seguridades incluyen desde los aplicativos desarrollados en casa hasta los que son proveídos por outsoursing. A los aplicativos desarrollados en casa se analiza cada una de las etapas de desarrollo de software, es decir incluyendo el requerimiento del sistema hasta el monitoreo del sistema en producción. En cuanto a los aplicativos proveídos por

outsoursing se analiza la documentación y pruebas realizadas.

2.4.2 Seguridad de Base de Datos

Las bases de datos son la parte más crítica de toda empresa debido a que en ella se guarda la información del negocio. La seguridad que se analiza en las bases de datos abarca la infraestructura en la cual se ejecuta el motor de bases de datos, datos antiguos, datos operacionales extractores de datos, bodega de datos, metadatos, herramienta de consulta y extracción de información.

2.4.3 Seguridad de Sistemas Operativo.

El análisis que se realiza para la seguridad de los sistemas operativos está dividido en dos partes: seguridad interna y seguridad externa.

Dentro de la seguridad externa se revisa la seguridad física y seguridad de administración. Mientras que en la seguridad interna se revisa seguridad del procesador, seguridad de memoria y seguridad de los archivos.

2.5 Determinación de sistemas de información, áreas que soportan la tecnología y proceso asociado.

El análisis respectivo para saber cuáles son los sistemas de información que deben auditarse se lo realiza mediante la matriz de "Determinación de Sistemas Relevantes".

El objetivo de la determinación de la matriz sistemas de información relevantes, con las áreas que soportan dicha tecnología y sus procesos asociados, es crear un inventario de los sistemas de información relevantes a los estados financieros, que asocie a qué dirección pertenece el sistema y declare la nomenclatura del proceso en el cual está incluido el sistema, incluyendo la prioridad de los sistemas para el desarrollo del negocio, para el llenado se debe considerar lo siguiente: [8]

MATRIZ: Determinación de Sistemas relevantes, áreas que soportan la tecnología y procesos asociados									
Sistema de información relevante	Dirección Responsable					Proceso Asociado			
	Dirección Informática	Dirección de Finanzas	Dirección de Proyectos y Procesos	Dirección de Sistemas	Dirección Técnica	CC (Control de Cambios)	CCAP (Control de Cambios Aplicativos)	SE (Seguridades)	OP (Operaciones)
Integrex		1					CCAP-SIS-01	SE-SIS-01	OP-SIS-01
Evolution				3			CCAP-SIS-02	SE-SIS-01	OP-SIS-01
Charging system			2		2	CC-TEC-01		SE-TEC-01	OP-TEC-01

NOMENCLATURA	
1	Muy importante
2	Medio importante
3	Poco importante

Tabla (2.1): Esquema de la Matriz de Determinación de Sistemas relevantes, áreas que soportan la tecnología y procesos asociados.

2.6 Alcance del objetivo de control para el proceso de seguridad.

Para el análisis de esta tesis se ha seleccionado 8 de los objetivos de control del dominio de Entrega y Soporte (DS) de los procesos:

- (DS5) Garantizar la seguridad de los sistemas.
- (DS12) Administración del ambiente físico.

Los objetivos de control para los procesos de seguridad de aplicativos, bases de datos y sistemas operativos son los mismos, la diferencia es la forma de aplicarlos.

A continuación se detallan los objetivos de control aplicables a los procesos de seguridad de aplicativos, bases de datos y sistemas operativos. [9]

Objetivo: DS5.1 Administración de la seguridad de TI.

"Asegurar que se definen y establecen las directrices para salvaguardar la integridad de la información que contienen los sistemas".

Alcance para el objetivo de control: En busca del cumplimiento del objetivo de control se recomienda considerar las siguientes prácticas:

- Definir los lineamientos para la seguridad de TI, considerando los siguientes aspectos:
    - Alcances y objetivos para la función de administración de seguridad.
    - Responsabilidad.
    - Directrices.
- La estrategia de seguridad debe estar ligada con los planes de negocio de la organización. Para lo anterior, la dirección responsable de esta estrategia debe mantenerse al tanto de los planes de la organización para corroborar que éstos no afectan la estrategia de seguridad o en su caso, realizar los cambios necesarios.
- Administrar los cambios y revisiones realizados periódicamente a las estrategias, estándares y políticas que aseguren el apego al negocio.
- Los requerimientos de seguridad, objetivos, políticas, estándares y procesos deben ser consistentes con leyes y

regulaciones aplicables así como con acuerdos legales, contractuales y niveles de servicio. [9]

Objetivo: DS5.2 Plan de seguridad.

"Garantizar que el Plan de Seguridad satisface los requerimientos del negocio, cubriendo los riesgos internos o externos a los cuales el negocio está expuesto, así como, crear conciencia a todos los usuarios de que existe y se debe aplicar el Plan de Seguridad."

Alcance para el objetivo de control: En busca del cumplimiento del objetivo de control, considerar la siguiente práctica:

- El Plan de seguridad de TI puede incluir:
    - Políticas y estándares de seguridad.
    - Procedimientos implementados para hacer cumplir efectivamente las políticas y estándares previamente definidos.
    - Roles y responsabilidades de los involucrados.
    - Requerimientos para la contratación de proveedores.
    - Conciencia y formación sobre seguridad.
    - Aplicación práctica del plan de seguridad.
    - Revisiones periódicas al Plan de Seguridad.

- La versión actualizada del Plan de seguridad de TI debe ser comunicada a los interesados y a los usuarios.[9]

Objetivo: DS5.3 Administración de la Identidad.

"Asegurar que los usuarios internos, externos y temporales que tienen accesos a los sistemas de TI son identificados y autenticados antes de realizar cualquier transacción que contenga información sensitiva para el negocio."

Alcance para el objetivo de control: En busca del cumplimiento del objetivo de control, considerar la siguiente práctica:

- Establecer y comunicar políticas y procedimientos para la identificación, autenticación y autorización de accesos para todos los usuarios que necesiten consultar, manipular, registrar, validar la información sensitiva del negocio contenida en los sistemas.
- Asegurarse que la definición y autorización de roles considere los siguientes criterios:
    - Sensibilidad de la información y aplicaciones involucradas (clasificación de datos).

- Políticas de protección de la información y difusión (legal, regulatorio, políticas internas y requerimientos contractuales).
- Roles y responsabilidades definidas dentro de la empresa.
- La necesidad de tener accesos de acuerdo a las funciones realizadas.

- Definir e implementar procesos para identificar nuevos usuarios y registrar sus accesos, además de aprobarlos y mantener sus derechos de accesos.
- Asegurar que se notifique a tiempo los reportes de cambio de puesto (por ejemplo, personal que entra, personal que sale y personal que cambia de puesto o área). Otorgar, revocar y adaptar los accesos de usuarios de acuerdo a los cambios de puesto o roles.[9]

Objetivo: DS5.4 Administración de las cuentas de usuario.

"Asegurar la administración y revisión periódica de la requisición, establecimiento, uso, suspensión y cierre de las cuentas de usuarios internos y externos y de los privilegios que se tienen asociados a dichas cuentas."

Alcance para el objetivo de control: En busca del cumplimiento del objetivo de control se recomienda considerar las siguientes prácticas:

- Asegurar que los procedimientos de control de accesos incluyan la requisición, establecimiento, uso, suspensión y cierre de cuentas de usuario, así como que estas acciones deben requerir una aprobación formal.
- Las reglas de contraseña deben ser establecidas en la organización considerando los siguientes criterios:
    - El sistema solicita el cambio obligatorio del contraseña del usuario, la primera vez que éste ingresa.
    - El sistema debe obligar a un cambio periódico de contraseña.
    - El sistema debe bloquear la cuenta del usuario después de un número de intentos fallidos.
    - La sesión del usuario debe expirar en un tiempo determinado.
    - Los usuarios temporales no deben tener acceso después de la fecha de expiración establecida.

- Terceras partes no deben ser provista de un nombre de usuario y contraseña hasta que hayan firmado un acuerdo de no-revelación. Además debe brindarse acceso a las políticas de seguridad de la organización, así como confirmar que están en el entendido de sus obligaciones.
- Que los derechos de acceso sean revisados periódicamente para confirmar que están como fueron otorgados en su origen, y que corresponden a las necesidades de la organización y a las funciones que los usuarios desempeñan en ésta. [9]

Objetivo: DS5.5 Pruebas de Seguridad, Vigilancia y Monitoreo.

"Garantizar que la información proporcionada por los logs de seguridad de los sistemas contengan lo necesario para detectar con oportunidad intentos de violación al sistema, así como que estos logs sean monitoreados para asegurar que cualquier evento que pueda causar daño a la seguridad del sistema sea reportado. Por otra parte se deben realizar pruebas a la seguridad implementada en los sistemas, con la finalidad de confirmar que cumplen con su objetivo o si se requieren cambios, sean identificados para evitar vulnerabilidades."

Alcance para el objetivo de control: En busca del cumplimiento del objetivo de control se recomienda considerarlas siguientes prácticas:

- Implementar monitoreo, pruebas y revisión para:
    - La organización debe contar con procedimientos manuales o automáticos que le permitan descubrir brechas de seguridad así como reportarlas a todos los involucrados internos o externos, los hallazgos deben ser evaluados, escalados e investigados.
    - Contar con procedimientos para determinar si una acción tomada para resolver una brecha de seguridad es efectiva.
- Realizar pruebas regularmente para garantizar que la seguridad es efectiva considerando:
    - Verificar que los procesos de administración de identidad son efectivos.
    - Verificar que la administración de cuentas de usuario es efectiva.
    - Garantizar que la configuración de la seguridad en los sistemas relevantes está definida y cumplen con los lineamientos de seguridad de la información.

- Garantizar que los controles y configuración de seguridad de la red estén configurados y cumplen con los lineamientos de seguridad de la información.
- Garantizar que los procesos de monitoreo de la seguridad trabajan de acuerdo a como fueron definidos.[9]

Objetivo: DS5.6 Definición de Incidentes de Seguridad.

"Asegurar que se tiene un concepto de incidente de seguridad estándar para toda la organización y que esté documentado considerando características y nivel de impacto para ser atendido apropiadamente."

Alcance para el objetivo de control: En busca del cumplimiento del objetivo de control se recomienda considerar las siguientes prácticas:

- Documentar qué debe ser considerado como incidente de seguridad, cuáles son las características que presenta un incidente de seguridad, así como los niveles de impacto que tiene de tal modo que sea posible dar una respuesta acorde a cada tipo de incidente.

- Los incidentes de seguridad reportados deben ser revisados con el fin de minimizar el daño, así como encontrar y eliminar la causa raíz de la brecha de seguridad.
- La gerencia / administración debe ser informada de todos los incidentes.
- Definir lineamientos para proteger la información confidencial relacionada con los incidentes de seguridad.[9]

Objetivo: DS12.2 Medidas de Seguridad Física.

"Garantizar que se cuenta con las medidas de seguridad física en las instalaciones y activos de TI para protegerlos contra robo, temperatura, fuego, humo, agua, vandalismo, cortes de energía, químicos o explosivos."

Alcance para el objetivo de control: En busca del cumplimiento del objetivo de control se recomienda considerar las siguientes prácticas:

- Definir e implementar políticas de seguridad física y medidas de control de accesos físicos para los sitios de TI (todo lugar donde se encuentren equipos que contengan los sistemas de alcance SOX).

- Revisar regularmente las políticas para asegurar que se mantienen actualizadas.
- Periódicamente probar y documentar las medidas preventivas, detectables y correctivas de seguridad física para verificar su diseño, implementación y efectividad.
- El diseño de las medidas de seguridad deben tomar en cuenta aspectos como: sistemas de alarma, protección de cableado, corriente regulada, piso falso, detectores de humo y fuego, termómetros.
- Definir procesos para que todo cambio de lugar físico de los equipos que contienen los sistemas significativos, se realicen con autorización de la persona que corresponda. [9]

Objetivo: DS12.3 Acceso Físico

"Asegurar que toda persona (interno o externo) que entre en las instalaciones de TI y tenga contacto con los activos de TI es identificada plenamente."

Alcance para el objetivo de control: En busca del cumplimiento del objetivo de control se recomienda considerar las siguientes prácticas:

- Definir e implementar una política de acceso a las instalaciones de TI. Esta política debe incluir responsabilidades de los empleados respecto a la vigilancia de los visitantes.
- Definir procesos para el monitoreo de todas las entradas a los sitios de TI.
- La política de acceso debe solicitar que los visitantes sean escoltados en todo momento por algún miembro del equipo de operaciones de TI, quien debe portar su identificación permanentemente.
- Requerimientos de acceso formal deben ser completados y autorizados por el administrador / responsable del sitio de TI. Los requerimientos deben ser guardados para tener un historial. [9]

2.6.1 Objetivos de control para el proceso de seguridad de aplicativos

Los objetivos de control para el proceso de seguridad de aplicativos son alineados a las diferentes aplicaciones que existen en una organización y además a su entorno, es decir servidores de aplicaciones y el espacio físico donde estos se encuentran.

Dentro de los aplicativos evaluados pueden constar aplicaciones desarrolladas fuera de la organización, es decir proveído por externos.

2.6.2 Objetivos de control para el proceso de seguridad de Base de datos.

Los objetivos de control para el proceso de seguridad de bases de datos son aplicables a las bases de datos q poseen la información más importante de la empresa sin importar en que motor de base de datos están ejecutándose.

Adicionalmente, los objetivos de control para este proceso también se enfocan en el servidor y ubicación física donde esta ejecutándose la base de datos.

2.6.3 Objetivos de control para el proceso de seguridad de sistemas operativos.

Los objetivos de control para el proceso de seguridad de sistemas operativos son aplicables a los diferentes Sistemas Operativos que ejecutan los aplicativos y bases de datos más importantes y de mayor impacto dentro de la organización.

Cabe recalcar que los objetivos de control para este proceso

también evalúan los servidores y su ubicación física donde se encuentran implementados estos sistemas operativos.

2.7 Identificación de los riesgos para el proceso de seguridad.

Los riesgos se han identificado de acuerdo al impacto generado sobre los objetivos de control anteriormente descritos.

A continuación el listado de los riesgos para el proceso de seguridad: [10]

- **Riesgo (R1):** Que la organización no establezca las estrategias, estándares y políticas para administrar la seguridad de TI (protección de datos y activos de información), las cuales deben estar alineadas con las necesidades y dinámica del negocio. [10]

- **Riesgo (R2):** Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.[10]

- **Riesgo (R3):** Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.[10]

- **Riesgo (R4):** Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios. [10]

- **Riesgo (R5):** Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.[10]

- **Riesgo (R6):** Que no exista un plan de definición, revisión y análisis de los incidentes para el descubrimiento de brechas de seguridad y ataques informáticos de tal manera que esto impida encontrar la causa raíz de éstos y minimizar los daños ocasionados a la organización. [10]

- **Riesgo (R7):** Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo. [10]

- **Riesgo (R8):** Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI. [10]

Capítulo 3: Documentación de Procesos SOX IT (Cobit)

3.1 Documentación de procesos de aplicaciones para soporte del negocio.

La documentación de los procesos para las aplicaciones que se encuentran involucradas en la metodología SOX IT debe considerar en su diseño controles que regulen los procesos de seguridades, los cuales también deben estar orientados a cumplir los objetivos de control del marco de referencia COBIT.

Para la documentación de los procesos de seguridades que incluyen los aplicativos y los sistemas críticos para el negocio se debe considerar las seguridades lógicas y físicas de los sistemas, administración de cuentas de usuarios, mecanismos de seguridad en el intercambio de la información y vigilancia física a los equipos. [11]

Cabe mencionar que antes de desarrollar la documentación de las aplicaciones que soportan los movimientos críticos del negocio se debe identificar si existen controles de manejo simultáneo para

documentar en un solo procesos, por ejemplo, si tenemos un control que mitigue algún riesgo en el proceso de seguridad de aplicativos y el mismo control se lo mantiene para el proceso de seguridad de base de datos, solamente se lo debe detallar en uno de los procesos y en el otro proceso hacer referencia al control existente. Para el caso que se presenten controles que no se puedan englobar y generalizar para ambos procesos, entonces se debe detallar en cada proceso las particularidades y diferencias para dicha aplicación. [11]

3.2 Descripción del proceso y flujograma

La descripción del proceso es el documento que detalla las secuencias de las actividades de un proceso desde como inicia hasta que termina siendo el objetivo principal la entrega de una mejor descripción del mismo el cual ayudará a un mejor entendimiento por parte de la persona que lo auditará. [11]

En este documento se debe explicar claramente y cronológicamente la actividad con sus respectivos responsables de ejecución, revisión y aprobación en caso que lo hubiere; además se deben describir los tiempos.

El documento deber ser creado por las personas que ejecutan las actividades, las responsabilidades dentro de las actividades deben ser específicas, si existe alguna política o procedimiento al que se hace referencia se debe especificar su código, nombre y ruta donde se lo encuentra. [11]

El flujograma es una herramienta de esquematización y análisis que representa la secuencia de pasos para alcanzar un resultado especifico. Además de la secuencia de actividades, el flujograma muestra lo que se realiza en cada etapa, los materiales o servicios que entran y salen del proceso, las decisiones que se toman y las personas involucradas.

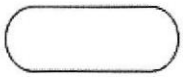
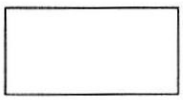
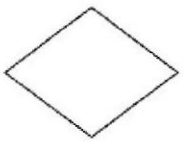
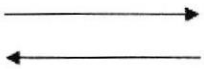
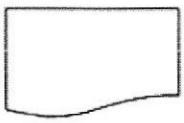
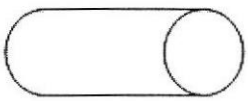
Nombre Símbolo	Descripción	Símbolo
Terminador	Representa el inicio o fin de un diagrama de flujo	
Proceso	Representa una actividad o proceso.	
Decisión	Representa la bifurcación de un proceso	
Flecha	Representa el camino que une los elementos del diagrama	
Documento	Representa documentos en el soporte papel	
Base de Datos	Representa información en soporte digital	

Figura (3.1): Simbología de Diagramas de Flujo

3.3 Documentación de la Matriz de riesgo

La matriz de riesgos y controles reúnen y clasifican los riesgos y controles de cada proceso, siendo el objetivo principal facilitar la identificación y administración de los mismos y de esta forma no equivocarse al momento de detallar las actividades de control con actividades operativas. [11]

Esta matriz se la utiliza al momento de evaluar lo controles en las áreas respectivas, a través de esta matriz podemos evaluar que el control mitiga el riesgo que atenta contra el objetivo de control debido a que permite analizar individualmente el riesgo estándar y el control. [11]

EMPRESA: *POLICOM*		***DIRECCION RESPONSABLE:***	*SISTEMAS*	***PROCESO:***	*SAP-SIS-01 PROCESO DE SEGURIDAD DE APLICATIVOS DE SISTEMAS*	***FECHA ULTIMA DE ACTUALIZACION:*** *Enero/2011* ***FECHA ULTIMA DE EJECUCION:*** *Noviembre/ 2011*
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**

Tabla (3.1): Esquema de la Matriz de Riesgo

3.4 Documentación de los objetivos de control Vs riesgos

La matriz que detalla los objetivos de control Vs riesgos, facilita identificar que objetivos de control está cubriendo los riesgos existente en el proceso. [11]

Se asocia a través del nivel del riesgo es decir A (Riesgo Alto), M (Riesgo Medio) y B (Riesgo Bajo).

Existen excepciones para el cumplimiento de los objetivos de control por motivo que estos no aplican al proceso para esto se

debe explicar en la parte inferior del documento la razón del porque no es aplicable.

EMPRESA:	*POLICOM*	***DIRECCION RESPONSABLE:***	*SISTEMAS*	***PROCESO:***	*SAP-SIS-01 PROCESO DE SEGURIDAD DE APLICATIVOS DE SISTEMAS*	***FECHA ULTIMA DE ACTUALIZACION:*** *Enero/2011* ***FECHA ULTIMA DE EJECUCION:*** *Noviembre/ 2011*
Objetivos de Control / Riesgos	**R1**		**R2**		**R3**	
OBJETIVO 1			B			
OBJETIVO 2	M					
OBJETIVO 3					A	

Tabla (3.2): Matriz de Objetivos de Control Vs. Riesgos

Capítulo 4: Caso de estudio: Ejemplo con sus resultados

4.1 Descripción de caso de estudio.

La empresa Policom, es una empresa de telecomunicaciones que cotiza en las bolsas de valores de Estados unidos.

El objetivo del negocio es vender servicios de comunicaciones tanto de voz como de datos y a través de un buen servicio tecnológico poder posicionarse en el mercado con planes que se encuentran acorde a la necesidad de los usuarios.

Policom está formada por un comité ejecutivo y contiene 3000 empleados distribuidos en las siguientes áreas.

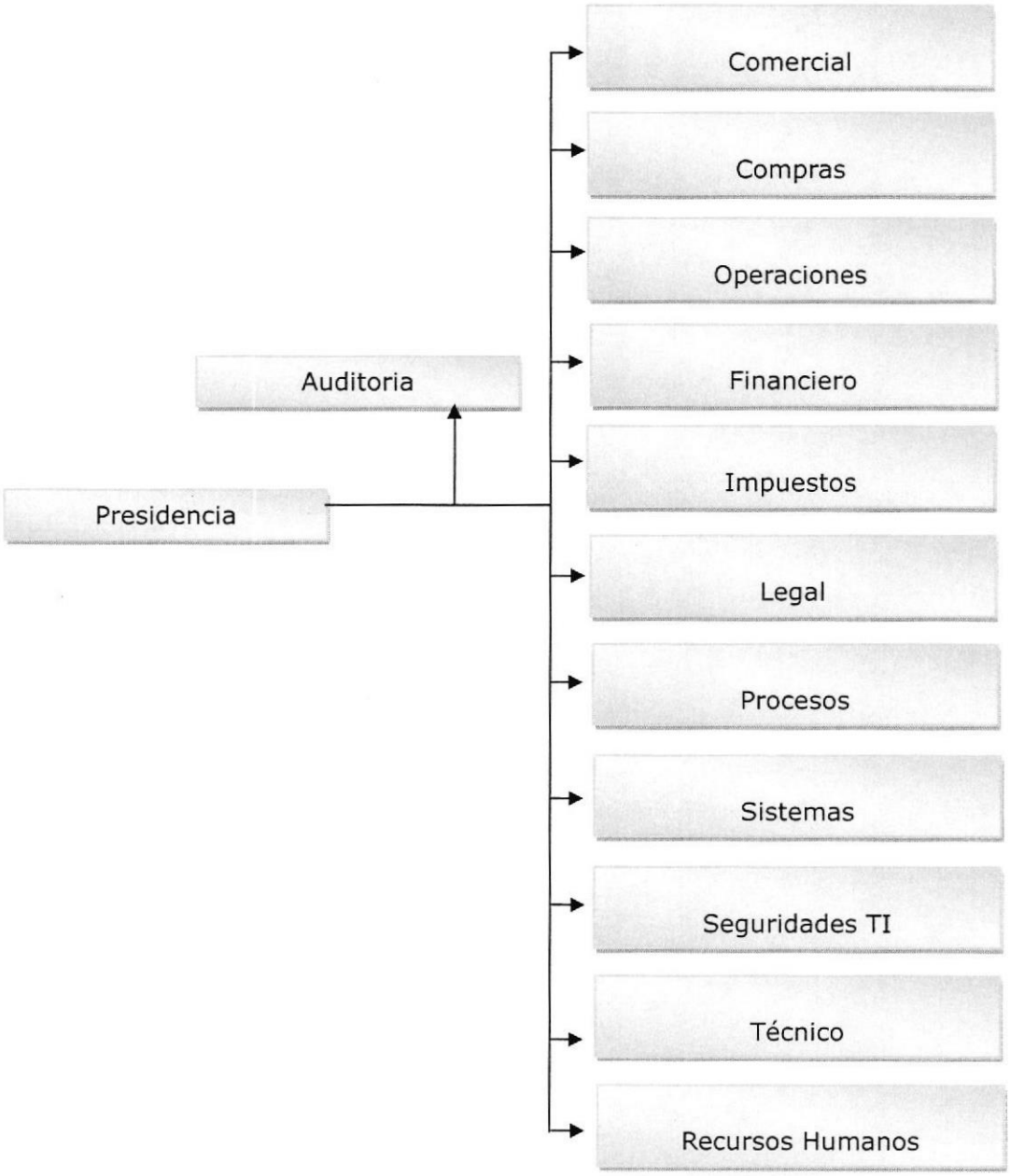


Figura (4.1): Organigrama de la empresa Policom

La empresa ha documentado algunos de los procesos que realizan las diferentes áreas y se han creado algunas políticas en las

diferentes áreas.

La empresa maneja un sistema integrado denominado *Integrex* dónde se almacenan las transacciones del área Comercial, Financiera, Impuestos, Compras y operaciones.

Integrex tiene una interfaz que se comunica con las transacciones de los usuarios que utilizan el servicio de voz y datos, debido a que estas son registradas en los servidores del área Técnica.

- El área Comercial tiene como objetivo cumplir la meta de ventas que son trazadas antes de iniciar un ciclo (cada tres meses). Esta área utiliza el módulo Ventas del sistema Integrex y Cognos (Aplicativo de cubos de información).
- El área de Compras es responsable de comprar servicios o productos que son usados internamente en la empresa y también para ser proveídos a los clientes de Policom. Esta área utiliza el módulo Compras del sistema Integrex y Cognos (Aplicativo de cubos de información).
- El área Financiera se encarga de registrar contablemente las transacciones que se dan diariamente en la empresa. Utiliza los módulos de cuentas por cobrar, cuentas por pagar y contabilidad Integrex.
- El área de Impuestos se encarga de calcular las obligaciones

de impuestos tanto para los clientes como para la misma empresa. Esta área utiliza el módulo Impuesto del sistema Integrex y adicionalmente los aplicativos proporcionados por el ente regulador de impuestos.

- El área de Legal se encarga de gestionar todos los procesos contractuales que implican el negocio.
- El área de Operaciones se encarga de ingresar al sistema las solicitudes de servicios.
- El área de Recursos Humanos se dedica a reclutar y gestionar la capacitación al personal de la empresa. Esta área maneja el módulo Recursos Humanos del sistema Integrex.
- El área de Seguridades es responsable de la seguridad que existe en los aplicativos y equipos. Para manejar las seguridades de los aplicativos y equipos tienen acceso a ellos como Administradores.
- El área Técnica se encarga de administrar el servicio de comunicación de voz y datos que se les brinda a los clientes. Para esto se trabaja con equipos especiales que tienen sus propios sistemas operativos y aplicativos. El mantenimiento o administración de algunos equipos está dada por personal

externo a la empresa.

- El área de Sistemas se encarga de dar soporte a las aplicaciones que utilizan las diferentes áreas de la empresa. Algunos aplicativos son desarrolladas in house otros son proveídos por externos.
- El área de Auditoría se encarga de ejecutar revisiones en los procesos contables y operativos.

4.2 Identificación Procesos de Seguridad

Los Procesos de Seguridad que se ejecutan bajo la metodología SOX IT vienen dado por los aplicativos, bases de datos y sistemas operativos que intervienen en los procesos críticos del negocio.

Inicialmente se identifican cuáles son los procesos que impactan el objetivo del negocio y se seleccionan los aplicativos, bases de datos y sistemas operativos que forman parte de estos procesos.

Para el ejercicio que se está analizando en esta tesis, a la empresa Policom se ha identificado los siguientes procesos críticos:

- Proceso Ventas de productos
- Proceso de Generación de servicio de voz
- Proceso de Generación de servicio de datos

Adicionalmente pueden existir otros procesos que también son importantes pero la premisa para seleccionar los procesos con los que se inicia una revisión bajo la metodología SOX IT (Cobit) es que se escoge los procesos críticos que donde llegue a fallar uno de ellos se paraliza el negocio.

Es importante recalcar que no se recomienda inicializar con más de 4 procesos debido a que esto afecta el alcance de la auditoría y dificulta la aplicación de la metodología la cual debe ser bien detallada y específica.

Si los procesos identificados están documentados se procede evaluar el proceso en el área que se ejecuta.

En caso de que no se encuentre documentado, el auditor tiene que levantar el proceso y documentarlo, esta documentación formará parte de los papeles de trabajo del auditor más no del área auditada.

A través de la evaluación de los procesos se identifican los aplicativos que son utilizados en el desarrollo de las actividades que están involucradas en los procesos.

PROCESOS DEL NEGOCIO	SISTEMAS
Proceso de Ventas de productos	Integrex – Modulo de Ventas
Proceso de generación de servicios de voz	MSC
	HLR
	Charging Gateway
	SDP
Procesos de generación de servicio de datos	MSC
	SGSN
	SDP
	Charging Gateway

Tabla (4.1). Identificación de Sistemas de procesos críticos del negocio.

Una vez identificados los sistemas, se procede a completar la matriz "**Determinación de Sistemas relevantes, áreas que soportan la tecnología y procesos asociados**", como se muestra en la tabla 4.2.

En la tabla 4.2, se puede observar que se han listado los sistemas relevantes que intervienen en los procesos críticos del negocio, además se ha asociado la dirección responsable de cada proceso, esto quiere decir que se ha referenciado al aplicativo con el área que es dueña o responsable del aplicativo o plataforma crítica para el negocio.

En la tabla 4.2 también detallamos los procesos de seguridades que estamos utilizando bajo la metodología SOX IT (Cobit), hemos utilizado la siguiente nomenclatura:

Este código está dividido en tres partes. La primera significa el tipo de procesos de seguridad que estamos utilizando, es decir SAP (Proceso de Seguridad de Aplicativos), SDB (Procesos de Seguridad de Bases de datos), SSO (Proceso de Seguridad de Bases de datos).

La segunda parte de este código describe el área responsable del proceso de seguridades que se va a evaluar. Para el ejemplo de este ejercicio tenemos las áreas SIS (Área de Sistemas) y TEC (Área Técnica).

La tercera parte de este código describe la secuencia del proceso o número identificador del proceso.

MATRIZ: Determinación de Sistemas relevantes, áreas que soportan la tecnología y procesos asociados								
Sistema relevante	Dirección Responsable					Proceso Asociado		
	Dirección Seguridades	Dirección de Comercial	Dirección de Proyectos y Procesos	Dirección de Sistemas	Dirección Técnica	Seguridades Aplicativos (SAP)	Seguridades Bases de Datos (SBD)	Seguridades Sistemas Operativos (SSO)
Integrex		1				SAP-SIS-01	SBD-SIS-01	SSO-SIS-01
MSC					2		SBD-TEC-01	SSO-TEC-01
Charging Gateway					1			SSO-TEC-01
HLR					1			SSO-TEC-01
SDP					2		SBD-TEC-01	SSO-TEC-01
SGSN					3			SSO-TEC-01

NOMENCLATURA	
1	Muy importante
2	Medio importante
3	Poco importante

Tabla (4.2) MATRIZ: Determinación de Sistemas relevantes, áreas que soportan la tecnología y procesos asociados

4.3 Identificación Objetivos de control para procesos de seguridad de aplicativos, bases de dato y sistemas operativos.

Los objetivos de control son los mismos para todos los procesos de seguridades, la diferencia es la aplicación. Pueden existir casos que un objetivo de control no aplique para uno o dos procesos ó también puede existir el caso que aplique para los tres. Adicionalmente la relación que existe entre el objetivo de control y el proceso es medido a través de la criticidad de esta relación en los objetivos del negocio, donde se representa A = Criticidad Alta,

M = Criticidad Media y B = Criticidad Baja.

A continuación se detallan los objetivos de control y se señala para cual proceso aplica.

OBJETIVO DE CONTROL	PROCESOS		
	SAP	SBD	SSO
DS5.1 Administración de la seguridad de TI.	M	M	M
DS5.2 Plan de seguridad.	M	B	B
DS5.3 Administración de la Identidad.	A	A	A
DS5.4 Administración de las cuentas de usuario.	A	A	A
DS5.5 Pruebas de Seguridad, Vigilancia y Monitoreo.	A	M	M
DS12.2 Medidas de Seguridad Física.	M	A	A
DS12.3 Acceso Físico	B	M	M

Tabla (4.3): Identificación de Objetivos de Control

4.4 Identificación riesgos para el proceso de seguridad de aplicativos, bases de dato y sistemas operativos.

Una vez identificados los objetivos de control procedemos a referenciar los riesgos que se mencionaron en el Capítulo 2 de esta tesis.

Cabe señalar que se puede existir el caso que mas es un objetivo de control se encuentren expuestos al mismo riesgo, también

puede existir el caso que el auditor encuentre necesario añadir un riesgo adicional a los que señalamos en la metodología SOX IT (Cobit).

OBJETIVO DE CONTROL	RIESGO
DS5.1 Administración de la seguridad de TI.	R1: Que la organización no establezca las estrategias, estándares y políticas para administrar la seguridad de TI (protección de datos y activos de información), las cuales deben estar alineadas con las necesidades y dinámica del negocio.
DS5.2 Plan de seguridad.	R2: Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.
DS5.3 Administración de la Identidad.	R3: Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.
DS5.4 Administración de las cuentas de usuario.	R4: Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.
DS5.5 Pruebas de Seguridad, Vigilancia y Monitoreo.	R5: Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.
DS12.2 Medidas de Seguridad Física.	R7: Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.
DS12.3 Acceso Físico	R8: Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.

Tabla (4.4): Identificación de Riesgos

4.1. Identificación actividades de control para el proceso de seguridad de aplicativos, bases de dato y sistemas operativos.

Se procede a identificar cuáles son las actividades de control que mitigan los riesgos a los que está expuesto cada objetivo de control.

OBJETIVO DE CONTROL	RIESGO	Actividades de Control
DS5.1 Administración de la seguridad de TI.	R1	• Documentar las políticas de seguridades que indiquen el personal responsable de la ejecución de configuraciones de los aplicativos, Bases de datos o sistemas operativos.
DS5.2 Plan de seguridad.	R2	• Documentar de manera formal un Plan de seguridad que contenga procedimientos que aseguren que los aplicativos, bases de datos y sistemas operativos no son vulnerables. • Establecer un periodo de revisión de la ejecución del Plan de Seguridad. • Establecer un periodo de la actualización del Plan se Seguridad.
DS5.3 Administración de la Identidad.	R3	• Configurar los sistemas para que pidan usuario y clave en cada acceso. • Configurar mecanismo de clave segura y cambio de clave cada cierto tiempo.
DS5.4 Administración de las cuentas de usuario.	R4	• Comunicarse con Recursos Humanos a través de alguna aplicación o correo electrónico para conocer que usuario ya no pertenece a la empresa o está suspendido temporalmente. • Realizar revisiones periódicas que validen usuarios inexistentes o cambios de áreas.
DS5.5 Pruebas de Seguridad, Vigilancia y Monitoreo.	R5	• Almacenar los log de seguridad siempre en lugares seguros. • Revisar los logs generados periódicamente. • Realizar respaldo de los logs
DS12.2 Medidas de Seguridad Física.	R7	• Establecer políticas de acceso para el acceso al Centro de cómputo. • Implementar alarmas contra incendio o robo. • Realizar mantenimiento periódico a los equipos de refrigeración del Centro de Cómputo.
DS12.3 Acceso Físico	R8	• Establecer políticas de acceso para el acceso al Centro de cómputo. • Implementar cámaras de seguridad que ayuden a identificar quien ingresa a los centros de cómputo.

Tabla (4.5): Identificación de actividades de control.

4.6 Documentación del proceso de seguridad de aplicativos, bases de dato y sistemas operativos.

La documentación que detalla el Proceso, es desarrollada por los dueños de los procesos, es decir por las áreas que ejecutan las actividades a evaluar. Esta documentación del proceso viene adjunta con un diagrama de flujo para que ayude al auditor al

momento de hacer la evaluación de los controles en los procesos. En muchas ocasiones este diagrama de flujo no es secuencial para todo el proceso debido a que en las áreas tecnológicas se ejecutan varias actividades que no son consecutivas una de otras. Para esta tesis se ha desarrollado la documentación del proceso de seguridades de aplicativos la cual esta adjunto en el ANEXO 1.

Continuando con la documentación que generan las evaluaciones a los procesos bajo la Metodología SOX IT (COBIT) detallamos las matrices de riesgo para los procesos de proceso de Seguridad de Aplicativos, Seguridad de bases de datos y Seguridad de Sistemas Operativos que están bajo el control del área de sistemas. Y para el área técnica las matrices de riesgos para los controles del Proceso de Seguridad de bases de datos y aplicativos.

Cabe recalcar que los objetivos de control y riesgos para estos procesos son los mismos, la diferencia es la aplicabilidad. Adicionalmente existirán las mismas actividades de control que se ejecutan para más de un proceso, en este caso solamente se detallará la actividad de control en un proceso y en los otros se hace referencia a través del código del control y del proceso.

EMPRESA:	POLICOM	**DIRECCION RESPONSABLE:**	SISTEMAS	**PROCESO:**	SAP-SIS-01 PROCESO DE SEGURIDAD DE APLICATIVOS DE SISTEMAS	**FECHA ULTIMA DE ACTUALIZACION:** Enero/2011 **FECHA ULTIMA DE EJECUCION:** Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R1-C1	Que la organización no establezca las estrategias, estándares y políticas para administrar la seguridad de TI (protección de datos y activos de información), las cuales deben estar alineadas con las necesidades y dinámica del negocio.	El Gerente de Sistemas Documenta las políticas de seguridades que indiquen quien es el personal responsable de la ejecución de configuraciones de los aplicativos, Bases de datos o sistemas operativos.	El documento donde se detalla la política de seguridades de Sistemas.	Semestralmente	Gerente de Sistemas	Dirección de Sistemas
R2-C1	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	El Gerente de Sistemas documenta de manera formal un Plan de seguridad que contenga procedimientos que aseguren que los aplicativos, bases de datos y sistemas operativos no son vulnerables.	Documento que contiene el Plan de Seguridad.	Anualmente	Gerente de Sistemas	Director de Sistemas
R2-C2	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	El Gerente de Sistemas revisa que el Plan de Seguridad se encuentre ejecutando.	Configuraciones de seguridad en los equipos, correos con solicitudes de acceso.	Trimestralmente	Gerente de Seguridad	Dirección de Seguridad
R2-C3	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	El Gerente de Sistemas revisa la bitácora de cambios del Plan de seguridad para saber que se está actualizando.	Bitácora de Actualización del Plan de Seguridad	Semestralmente	Gerente de Sistemas	Dirección de Sistemas
R3-C1	Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.	El Ingeniero de sistemas Configura los sistemas para que pidan usuario y clave en cada acceso.	Configuración de seguridades del sistema Integrex	Eventual	Ingeniero de Sistemas	Gerente de Sistemas
R3-C2	Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.	El ingeniero de sistemas debe configurar mecanismo de clave segura y cambio de clave cada cierto tiempo.	Configuración de seguridades del sistema Integrex Pantallas ingresando un nueva clave.	Eventual	Ingeniero de Sistemas	Gerente de Sistemas

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	SISTEMAS	PROCESO:	SAP-SIS-01 PROCESO DE SEGURIDAD DE APLICATIVOS DE SISTEMAS	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R4-C1	Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.	El Ingeniero de Sistemas recibe correos por parte de Recursos Humanos indicando que usuarios dejaron de pertenecer a la empresa o está suspendido temporalmente y que se encuentran habilitados para acceder al sistema Integrex.	Correos enviados por Recursos Humanos indicando personal cesante o suspendido	Eventual	Asistente de RH	Gerencia de RH
R4-C2	Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.	Realizar revisiones periódicas que validen usuarios inexistentes o cambios de áreas en los usuarios que acceden al sistema Integrex.	Correos reportando el estado de los usuarios en el sistema Integrex enviados por el Ingeniero de sistemas a sus superiores	Mensualmente	Ingeniero de Sistemas	Gerente de Sistemas
R5-C1	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero de Sistemas almacena los log de seguridad en cintas y dentro de una caja fuerte	Bitácora de cintas que almacena los logs. Cintas que contienen logs	Eventual	Ingeniero en Sistemas	Gerente de Sistemas
R5-C2	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero de Sistemas mensualmente valida si los logs del sistema Integrex se están guardando correctamente y luego envía un correo al Gerente con alguna novedad encontrada. La validación se la realiza a través de una re ejecución de la cinta.	Correo enviado al Gerente indicando novedades encontrada en la ejecución de las cintas.	Mensualmente	Ingeniero de Sistemas	Gerente de Sistemas
R5-C3	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero de Sistemas revisa que se generen los respaldos de Logs de acceso al sistema Integrex y envía novedad encontrada a su superior.	Correo que indica que el log de acceso al sistema Integrex se está respaldando	diariamente	Ingeniero de Sistemas	Gerente de Sistemas

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	SISTEMAS	PROCESO:	SAP-SIS-01 PROCESO DE SEGURIDAD DE APLICATIVOS DE SISTEMAS	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R7-C1	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	El Gerente de Sistemas documenta las políticas de acceso al Centro de Computo.	Documentación de las políticas de acceso al centro de cómputo.	Anualmente	Gerente de Sistemas	Dirección de Sistemas
R7-C2	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	El jefe de seguridad física debe implementar alarmas contra incendio o robo en las instalaciones del centro de cómputo	Contrato de instalación de alarmas de seguridad.	Semestralmente	Jefe de Seguridad Física	Gerencia de Seguridad
R7-C3	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	El Ingeniero de Sistemas de solicitar al proveedor de mantenimiento de refrigeración que ejecuta una revisión y mantenimiento a los equipos del centro de cómputo.	Contrato de mantenimiento de equipos de refrigeración ubicados en el área del centro de cómputo.	Semestralmente	Ingeniero en Sistemas	Gerente de Sistemas
R8-C1	Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.	El Gerente de Sistemas elabora un documento que contiene las políticas de accesos al centro de cómputo	Documento de Políticas de acceso al centro de cómputo.	Anualmente	Gerente de Sistemas	Dirección de Sistemas
R8-C2	Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.	El Jefe de Seguridad física instala las cámaras de seguridad dentro del centro de cómputo.	Videos tomados por las cámaras de seguridad y guardados en un medio de almacenamiento.	Trimestralmente	Jefe de Seguridad física	Gerente de Seguridad

Tabla (4.6): Matriz de riesgo del Proceso de Seguridad de Aplicativos de Sistemas

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	SISTEMAS	PROCESO:	SBD-SIS-01 PROCESO DE SEGURIDAD EN BASES DE DATOS EN SISTEMAS	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R1-C1	Que la organización no establezca las estrategias, estándares y políticas para administrar la seguridad de TI (protección de datos y activos de información), las cuales deben estar alineadas con las necesidades y dinámica del negocio.	SAP-SIS-01 R1-C1	SAP-SIS-01 R1-C1	SAP-SIS-01 R1-C1	SAP-SIS-01 R1-C1	SAP-SIS-01 R1-C1
R2-C1	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	SAP-SIS-01 R2-C1	SAP-SIS-01 R2-C1	SAP-SIS-01 R2-C1	SAP-SIS-01 R2-C1	SAP-SIS-01 R2-C1
R2-C2	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	SAP-SIS-01 R2-C2	SAP-SIS-01 R2-C2	SAP-SIS-01 R2-C2	SAP-SIS-01 R2-C2	SAP-SIS-01 R2-C2
R2-C3	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	SAP-SIS-01 R2-C3.	SAP-SIS-01 R2-C3	SAP-SIS-01 R2-C3	SAP-SIS-01 R2-C3	SAP-SIS-01 R2-C3
R3-C1	Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.	El Ingeniero de sistemas Configura Las opciones de seguridad de las bases de datos para que pidan usuario y clave en cada acceso.	Configuración de seguridades del las bases de datos del sistema Integrex	Eventual	Ingeniero de Sistemas	Gerente de Sistemas
R3-C2	Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.	El Ingeniero de sistemas debe configurar mecanismo de clave segura y cambio de clave cada cierto tiempo en las bases de datos del sistema Integrex.	Configuración de seguridades de las bases de datos del sistema Integrex Pantallas ingresando un nueva clave.	Eventual	Ingeniero de Sistemas	Gerente de Sistemas

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	SISTEMAS	PROCESO:	SBD-SIS-01 PROCESO DE SEGURIDAD EN BASES DE DATOS EN SISTEMAS	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R4-C1	Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.	El Ingeniero de Sistemas recibe correos por parte de Recursos Humanos indicando que usuarios dejaron de pertenecer a la empresa o está suspendido temporalmente y que tienen acceso a las bases de datos del sistema Integrex.	Correos enviados por Recursos Humanos indicando personal cesante o suspendido. Usuarios configurados en las bases de datos	Eventual	Asistente de RH	Gerencia de RH
R4-C2	Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.	Realizar revisiones periódicas en las configuraciones de las bases de datos del sistema Integrex, que validen usuarios inexistentes o cambios de áreas.	Correos reportando el estado de los usuarios en la bases de datos del sistema Integrex enviados por el Ingeniero de sistemas a sus superiores	Mensualmente	Ingeniero de Sistemas	Gerente de Sistemas
R5-C1	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero de Sistemas almacena los log de seguridad de las bases de datos del sistema Integrex en cintas y dentro de una caja fuerte	Bitácora de cintas que almacena los logs de las bases de datos del sistema Integrex. Cintas que contienen logs de las bases de datos del sistema Integrex	Eventual	Ingeniero en Sistemas	Gerente de Sistemas
R5-C2	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero de Sistemas mensualmente valida si los logs de las bases de datos del sistema Integrex se están guardando correctamente y luego envía un correo al Gerente con alguna novedad encontrada. La validación se la ejecuta a través de una re ejecución de las cintas.	Correo enviado al Gerente indicando novedades encontrada en la ejecución de las cintas.	Mensualmente	Ingeniero de Sistemas	Gerente de Sistemas
R5-C3	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero de Sistemas revisa que se generen los respaldos de Logs de las bases de datos del sistema Integrex y envía novedad encontrada a su superior.	Correo que indica que el log de las bases de datos del sistema Integrex se está generando correctamente.	diariamente	Ingeniero de Sistemas	Gerente de Sistemas

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	SISTEMAS	PROCESO:	SBD-SIS-01 PROCESO DE SEGURIDAD EN BASES DE DATOS EN SISTEMAS	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R7-C1	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	SAP-SIS-01 R7-C1	SAP-SIS-01 R7-C1	SAP-SIS-01 R7-C1	SAP-SIS-01 R7-C1	SAP-SIS-01 R7-C1
R7-C2	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	SAP-SIS-01 R7-C2	SAP-SIS-01 R7-C2	SAP-SIS-01 R7-C2	SAP-SIS-01 R7-C2	SAP-SIS-01 R7-C2
R7-C3	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	SAP-SIS-01 R7-C3	SAP-SIS-01 R7-C3	SAP-SIS-01 R7-C3	SAP-SIS-01 R7-C3	SAP-SIS-01 R7-C3
R8-C1	Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.	SAP-SIS-01 R8-C1	SAP-SIS-01 R8-C1	SAP-SIS-01 R8-C1	SAP-SIS-01 R8-C1	SAP-SIS-01 R8-C1
R8-C2	Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.	SAP-SIS-01 R8-C2	SAP-SIS-01 R8-C2	SAP-SIS-01 R8-C2	SAP-SIS-01 R8-C2	SAP-SIS-01 R8-C2

Tabla (4.7): Matriz de riesgo del Proceso de Seguridad de Bases de Datos de Sistemas.

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	SISTEMAS	PROCESO:	SSO-SIS-01 PROCESO DE SEGURIDAD EN SISTEMAS OPERATIVOS DE SISTEMAS	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R1-C1	Que la organización no establezca las estrategias, estándares y políticas para administrar la seguridad de TI (protección de datos y activos de información), las cuales deben estar alineadas con las necesidades y dinámica del negocio.	SAP-SIS-01 R1-C1	SAP-SIS-01 R1-C1	SAP-SIS-01 R1-C1	SAP-SIS-01 R1-C1	SAP-SIS-01 R1-C1
R2-C1	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	SAP-SIS-01 R2-C1	SAP-SIS-01 R2-C1	SAP-SIS-01 R2-C1	SAP-SIS-01 R2-C1	SAP-SIS-01 R2-C1
R2-C2	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	SAP-SIS-01 R2-C2	SAP-SIS-01 R2-C2	SAP-SIS-01 R2-C2	SAP-SIS-01 R2-C2	SAP-SIS-01 R2-C2
R2-C3	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	SAP-SIS-01 R2-C3.	SAP-SIS-01 R2-C3.	SAP-SIS-01 R2-C3.	SAP-SIS-01 R2-C3.	SAP-SIS-01 R2-C3.
R3-C1	Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.	El Ingeniero de sistemas Configura las opciones de seguridad del sistema operativo donde se ejecuta el sistema Integrex para que pidan usuario y clave en cada acceso.	Configuración de seguridades de sistema operativo del sistema Integrex	Eventual	Ingeniero de Sistemas	Gerente de Sistemas
R3-C2	Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.	El Ingeniero de sistemas debe configurar mecanismo de clave segura y cambio de clave cada cierto tiempo en el sistema operativo donde se ejecuta el sistema Integrex.	Configuración de seguridades del sistema operativo donde se ejecuta el sistema Integrex Pantallas ingresando un nueva clave.	Eventual	Ingeniero de Sistemas	Gerente de Sistemas

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	SISTEMAS	PROCESO:	SSO-SIS-01 PROCESO DE SEGURIDAD EN SISTEMAS OPERATIVOS DE SISTEMAS	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R4-C1	Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.	El Ingeniero de Sistemas recibe correos por parte de Recursos Humanos indicando que usuarios dejaron de pertenecer a la empresa o está suspendido temporalmente y que tienen acceso al sistema operativo del sistema Integrex.	Correos enviados por Recursos Humanos indicando personal cesante o suspendido. Usuarios configurados en el sistema operativo donde se ejecuta el sistema Integrex.	Eventual	Asistente de RH	Gerencia de RH
R4-C2	Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.	Realizar revisiones periódicas que validen usuarios inexistentes o cambios de áreas dentro de las configuraciones del sistema operativo del sistema Integrex	Correos reportando el estado de los usuarios en el sistema operativo del sistema Integrex enviados por el Ingeniero de sistemas a sus superiores	Mensualmente	Ingeniero de Sistemas	Gerente de Sistemas
R5-C1	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero de Sistemas almacena los log de seguridad del sistema operativo del sistema operativo Integrex en cintas y dentro de una caja fuerte	Bitácora de cintas que almacena los logs del sistema operativo del sistema Integrex. Cintas que contienen logs del sistema operativo del sistema Integrex	Eventual	Ingeniero en Sistemas	Gerente de Sistemas
R5-C2	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero de Sistemas mensualmente valida si los logs del sistema operativo del sistema Integrex se están guardando correctamente y luego envía un correo al Gerente con alguna novedad encontrada. La validación se la ejecuta a través de una re ejecución de las cintas.	Correo enviado al Gerente indicando novedades encontrada en la ejecución de las cintas.	Mensualmente	Ingeniero de Sistemas	Gerente de Sistemas
R5-C3	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero de Sistemas revisa que se generen los respaldos de Logs del sistema operativo del sistema Integrex y envía novedad encontrada a su superior.	Correo que indica que el log del sistema operativo del sistema Integrex se está generando correctamente.	diariamente	Ingeniero de Sistemas	Gerente de Sistemas

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	SISTEMAS	PROCESO:	SSO-SIS-01 PROCESO DE SEGURIDAD EN SISTEMAS OPERATIVOS DE SISTEMAS	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R7-C1	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	SAP-SIS-01 R7-C1	SAP-SIS-01 R7-C1	SAP-SIS-01 R7-C1	SAP-SIS-01 R7-C1	SAP-SIS-01 R7-C1
R7-C2	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	SAP-SIS-01 R7-C2	SAP-SIS-01 R7-C2	SAP-SIS-01 R7-C2	SAP-SIS-01 R7-C2	SAP-SIS-01 R7-C2
R7-C3	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	SAP-SIS-01 R7-C3	SAP-SIS-01 R7-C3	SAP-SIS-01 R7-C3	SAP-SIS-01 R7-C3	SAP-SIS-01 R7-C3
R8-C1	Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.	SAP-SIS-01 R8-C1	SAP-SIS-01 R8-C1	SAP-SIS-01 R8-C1	SAP-SIS-01 R8-C1	SAP-SIS-01 R8-C1
R8-C2	Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.	SAP-SIS-01 R8-C2	SAP-SIS-01 R8-C2	SAP-SIS-01 R8-C2	SAP-SIS-01 R8-C2	SAP-SIS-01 R8-C2

Tabla (4.8): Matriz de Riesgo del Proceso de Seguridad de Sistemas Operativos de Sistemas

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	TECNICA	PROCESO:	SBD-TEC-01 PROCESO DE SEGURIDAD DE BASES DE DATOS DEL AREA TECNICA	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R1-C1	Que la organización no establezca las estrategias, estándares y políticas para administrar la seguridad de TI (protección de datos y activos de información), las cuales deben estar alineadas con las necesidades y dinámica del negocio.	El Gerente Técnico Documenta las políticas de seguridades que indiquen quien es el personal responsable de la ejecución de configuraciones de los aplicativos, Bases de datos o sistemas operativos.	El documento donde se detalla la política de Seguridades Tecnica.	Semestralmente	Gerente Técnico	Director Técnico
R2-C1	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	El Gerente técnico documenta de manera formal un Plan de seguridad que contenga procedimientos que aseguren que los aplicativos, bases de datos y sistemas operativos no son vulnerables.	Documento que contiene el Plan de Seguridad.	Anualmente	Gerente Técnico	Director Técnico
R2-C2	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	El Gerente Técnico revisa que el Plan de Seguridad se encuentre ejecutando.	Configuraciones de seguridad en los equipos y correos con solicitudes de acceso.	Trimestralmente	Gerente Técnico	Director Técnico
R2-C3	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	El Gerente Técnico revisa la bitácora de cambios del Plan de seguridad para saber que se está actualizando.	Bitácora de Actualización del Plan de Seguridad	Semestralmente	Gerente Técnico	Director Técnico
R3-C1	Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.	El Ingeniero técnico Configura la base de datos del MSC y SDP para que pidan usuario y clave en cada acceso.	Configuración de seguridades de las bases de datos del MSC y SDP	Eventual	Ingeniero Técnico	Gerente Técnico
R3-C2	Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.	El ingeniero técnico debe configurar mecanismo de clave segura y cambio de clave cada cierto tiempo para el acceso a las bases de datos del MSC y SDP.	Configuración de seguridades de las bases de datos del MSC y SDP Pantallas ingresando un nueva clave.	Eventual	Ingeniero Técnico	Gerente Técnico

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	TECNICA	PROCESO:	SBD-TEC-01 PROCESO DE SEGURIDAD DE BASES DE DATOS DEL AREA TECNICA	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R4-C1	Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.	El Ingeniero Técnico recibe correos por parte de Recursos Humanos indicando que usuarios dejaron de pertenecer a la empresa o está suspendido temporalmente y que se encuentran habilitados para acceder a las bases de datos del MSC y SDP.	Correos enviados por Recursos Humanos indicando personal cesante o suspendido	Eventual	Asistente de RH	Gerencia de RH
R4-C2	Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.	Realizar revisiones periódicas que validen usuarios inexistentes o cambios de áreas que se encuentren habilitados para el acceso a las bases de datos MSC y SDP.	Correos reportando el estado de los usuarios de las bases de datos del MSC y SDP enviados por el Ingeniero de sistemas a sus superiores	Mensualmente	Ingeniero Técnico	Gerente Técnico
R5-C1	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero Técnico almacena los log de seguridad de las bases de datos del MSC y SDP en cintas y dentro de una caja fuerte	Bitácora de cintas que almacena los logs de las bases de datos del MSC y SDP. Cintas que contienen logs de los MSC y SDP	Eventual	Ingeniero Técnico	Gerente Técnico
R5-C2	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero Técnico verifica si los logs de las bases de datos del MSC y SDP se están guardando correctamente y luego envía un correo al Gerente con alguna novedad encontrada. La validación se la realiza a través de una re ejecución de la cinta.	Correo enviado al Gerente indicando novedades encontrada en la ejecución de las cintas.	Mensualmente	Ingeniero Técnico	Gerente Técnico

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	TECNICA	PROCESO:	SBD-TEC-01 PROCESO DE SEGURIDAD DE BASES DE DATOS DEL AREA TECNICA	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/ 2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R5-C3	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero de Sistemas revisa que se generen los respaldos de Logs de acceso a las bases de datos del MSC y SDP y envía novedad encontrada a su superior.	Correo que indica que el log de acceso a la bases de datos del MSC y SDP se está respaldando	Diariamente	Ingeniero Técnico	Gerente Técnico
R7-C1	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	El Gerente Técnico documenta las políticas de acceso al cuarto de equipos del área técnica.	Documentación de las políticas de acceso al cuarto de equipos.	Anualmente	Gerente Técnico	Director de Sistemas
R7-C2	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	El jefe de seguridad física debe implementar alarmas contra incendio o robo en las instalaciones del cuarto de equipos	Contrato de instalación de alarmas de seguridad.	Semestralmente	Jefe de Seguridad Física	Gerencia de Seguridad
R7-C3	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	El Ingeniero de Sistemas de solicitar al proveedor de mantenimiento de refrigeración que ejecuta una revisión y mantenimiento a los equipos del área técnica.	Contrato de mantenimiento de equipos de refrigeración que se encuentran enfriando el cuarto de equipos del área técnica	Semestralmente	Ingeniero Técnico	Gerente Técnico
R8-C1	Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.	El Gerente Técnico elabora un documento que contiene las políticas de accesos cuarto de equipos del área técnica	Documento de Políticas de acceso al cuarto de equipos del área técnica.	Anualmente	Gerente Técnico	Director Técnico
R8-C2	Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.	El Jefe de Seguridad física instala las cámaras de seguridad dentro cuarto de los equipos del área técnica.	Videos tomados por las cámaras de seguridad y guardados en un medio de almacenamiento.	Trimestralmente	Jefe de Seguridad física	Gerente de Seguridad

Tabla (4.9): Matriz de Riesgos del Proceso de Seguridad de Bases de datos del área técnica

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	TECNICA	PROCESO:	SSO-TEC-01 PROCESO DE SEGURIDAD DE SISTEMAS OPERATIVOS DEL AREA TECNICA	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R1-C1	Que la organización no establezca las estrategias, estándares y políticas para administrar la seguridad de TI (protección de datos y activos de información), las cuales deben estar alineadas con las necesidades y dinámica del negocio.	SBD-TEC-01 R1-C1	SBD-TEC-01 R1-C1	SBD-TEC-01 R1-C1	SBD-TEC-01 R1-C1	SBD-TEC-01 R1-C1
R2-C1	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	SBD-TEC-01 R2-C1	SBD-TEC-01 R2-C1	SBD-TEC-01 R2-C1	SBD-TEC-01 R2-C1	SBD-TEC-01 R2-C1
R2-C2	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	SBD-TEC-01 R2-C2	SBD-TEC-01 R2-C2	SBD-TEC-01 R2-C2	SBD-TEC-01 R2-C2	SBD-TEC-01 R2-C2
R2-C3	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	SBD-TEC-01 R2-C3	SBD-TEC-01 R2-C3	SBD-TEC-01 R2-C3	SBD-TEC-01 R2-C3	SBD-TEC-01 R2-C3
R3-C1	Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.	El Ingeniero técnico Configura el sistema operativo del MSC, HLR, SGSN, Charging gateway y SDP para que pidan usuario y clave en cada acceso.	Configuración de seguridades de las bases de datos del MSC, SGSN, HLR, SDP y Charging	Eventual	Ingeniero Técnico	Gerente Técnico
R3-C2	Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.	El ingeniero técnico debe configurar mecanismo de clave segura y cambio de clave cada cierto tiempo para el acceso al sistema operativo del MSC, HLR, SGSN, Charging y SDP.	Configuración de seguridades del sistema operativo del MSC, HLR, SGSN, Charging y SDP. Pantallas ingresando un nueva clave.	Eventual	Ingeniero Técnico	Gerente Técnico

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	TECNICA	PROCESO:	SSO-TEC-01 PROCESO DE SEGURIDAD DE SISTEMAS OPERATIVOS DEL AREA TECNICA	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R4-C1	Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.	El Ingeniero Técnico recibe correos por parte de Recursos Humanos indicando que usuarios dejaron de pertenecer a la empresa o está suspendido temporalmente y que se encuentran habilitados para acceder al sistema operativo del MSC, HLR, SGSN, Charging y SDP.	Correos enviados por Recursos Humanos indicando personal cesante o suspendido	Eventual	Asistente de RH	Gerencia de RH
R4-C2	Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.	Realizar revisiones periódicas que validen usuarios inexistentes o cambios de áreas que se encuentren habilitados para el acceso al sistema operativo del MSC, HLR, SGSN, Charging y SDP.	Correos reportando el estado de los usuarios de los sistemas operativos del MSC, HLR, SGSN, Charging y SDP. enviados por el Ingeniero de sistemas a sus superiores	Mensualmente	Ingeniero Técnico	Gerente Técnico
R5-C1	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero Técnico almacena los log de seguridad de los sistemas operativos del MSC, HLR, SGSN, Charging y SDP, en cintas y dentro de una caja fuerte	Bitácora de cintas que almacena los logs del sistema operativo del MSC, HLR, SGSN, Charging y SDP. Cintas que contienen logs del MSC, HLR, SGSN, Charging y SDP.	Eventual	Ingeniero Técnico	Gerente Técnico
R5-C2	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero Técnico valida si los logs de los sistemas operativos del MSC, HLR, SGSN, Charging y SDP, se están guardando correctamente y luego envía un correo al Gerente con alguna novedad encontrada. La validación se la realiza a través de una re ejecución de la cinta.	Correo enviado al Gerente indicando novedades encontrada en la ejecución de las cintas.	Mensualmente	Ingeniero Técnico	Gerente Técnico
R5-C3	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	El Ingeniero de Sistemas revisa que se generen los respaldos de Logs de acceso de los sistemas operativos del MSC, HLR, SGSN, Charging y SDP, y envía novedad encontrada a su superior.	Correo que indica que el log de acceso al sistema operativo del MSC, HLR, SGSN, Charging y SDP se está respaldando	Diariamente	Ingeniero Técnico	Gerente Técnico

EMPRESA:	POLICOM	DIRECCION RESPONSABLE:	TECNICA	PROCESO:	SSO-TEC-01 PROCESO DE SEGURIDAD DE SISTEMAS OPERATIVOS DEL AREA TECNICA	FECHA ULTIMA DE ACTUALIZACION: Enero/2011 FECHA ULTIMA DE EJECUCION: Noviembre/2011
REF	**RIESGO**	**ACTIVIDAD DE CONTROL**	**EVIDENCIA**	**FRECUENCIA**	**RESPONSABLE DE EJECUCION**	**RESPONSABLE DE AUTORIZACION**
R7-C1	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	SBD-TEC-01 R7-C1	SBD-TEC-01 R7-C1	SBD-TEC-01 R7-C1	SBD-TEC-01 R7-C1	SBD-TEC-01 R7-C1
R7-C2	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	SBD-TEC-01 R7-C2	SBD-TEC-01 R7-C2	SBD-TEC-01 R7-C2	SBD-TEC-01 R7-C2	SBD-TEC-01 R7-C2
R7-C3	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	SBD-TEC-01 R7-C3	SBD-TEC-01 R7-C3	SBD-TEC-01 R7-C3	SBD-TEC-01 R7-C3	SBD-TEC-01 R7-C3
R8-C1	Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.	SBD-TEC-01 R8-C1	SBD-TEC-01 R8-C1	SBD-TEC-01 R8-C1	SBD-TEC-01 R8-C1	SBD-TEC-01 R8-C1
R8-C2	Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.	SBD-TEC-01 R8-C2	SBD-TEC-01 R8-C2	SBD-TEC-01 R8-C2	SBD-TEC-01 R8-C2	SBD-TEC-01 R8-C2

Tabla (4.10): Matriz de riesgo del proceso de Seguridad de Sistemas Operativos del área técnica

Finalmente se documenta los riesgos que amenazan nuestros objetivos de control con la finalidad de identificar que riesgos tenemos cubiertos y asegurar que el objetivos de control se puede cumplir exitosamente.

La matriz de Objetivo de Control Vs Riesgos es documentada para cada proceso, es decir para el ejemplo utilizado en esta tesis elaboraremos 5 Matrices de riesgos.

Para el ejemplo que hemos venido haciendo en esta tesis, la matrices de objetivos de control Vs Riesgos son idénticas, por ese caso solamente se elaboraremos una matriz y ya que lo único que se diferencia del resto serían las cabeceras porque cambiaría el nombre del proceso.

Nombre: Policom	**Area:** Sistemas	**Proceso:**	SAP-SIS-01 Proceso de Seguridades de Aplicativos de Sistemas		**Fecha de Actualización:** Enero 2011		**Fecha de Ejecución:** Noviembre 2011	
	R1	**R2**	**R3**	**R4**	**R5**	**R6**	**R7**	**R8**
OBJETIVO	Que la organización no establezca las estrategias, estándares y políticas para administrar la seguridad de TI (protección de datos y activos de información), las cuales deben estar alineadas con las necesidades y dinámica del negocio	Que no se ejecuten los lineamientos establecidos en el Plan de Seguridad, y que éstos no sean comunicados a todos los interesados.	Que la organización no cuente con los procedimientos y medios para establecer la identificación y autenticación de usuarios tanto internos como externos para otorgarle acceso a los sistemas de TI.	Que no se administren y revisen periódicamente las cuentas de usuarios internos y externos, ocasionando que no se detecten oportunamente los cambios no autorizados en los derechos de acceso de los usuarios.	Que los archivos de logs no sean monitoreados y no brinden los rastros suficientes para descubrir brechas de seguridad ni reconocer patrones de ataque.	Que no exista un plan de definición, revisión y análisis de los incidentes para el descubrimiento de brechas de seguridad y ataques informáticos de tal manera que esto impida encontrar la causa raíz de éstos y minimizar los daños ocasionados a la organización.	Que las instalaciones no cuenten con medidas de seguridad para prevenir accesos de personal no autorizado, daños físicos por dolo o descuido a los recursos de TI y robo de equipo.	Que personal y visitantes que hayan accedido, no puedan ser identificados y rastreados poniendo en riesgo el acceso al equipo y a la información de TI.
DS5 Asegurar la seguridad de los sistemas								
DS5.1 Administración de la seguridad de TI.	B							
DS5.2 Plan de seguridad.		M						
DS5.3 Administración de la Identidad.			M					
DS5.4 Administración de las cuentas de usuario.				A				
DS5.5 Pruebas de Seguridad, Vigilancia y Monitoreo.					A			
DS12 Administración de las Instalaciones								
DS12.2 Medidas de Seguridad Física.							M	
12.3 Acceso Físico								M
Observaciones:								
El Riesgo 6 (R6) no se ha considerado porque este riesgo lo evalúa el área de Seguridades de TI en sus procesos el cual no es el alcance de esta tesis.								

Tabla (4.11): Matriz de Objetivos de control Vs Riesgo del proceso de Seguridad de Aplicativos de Sistemas

CONCLUSIONES y RECOMENDACIONES

Como experiencia personal, he trabajado con metodologías de auditoría de sistemas que tienen un proceso de desarrollo burocrático, donde el auditor pierde el enfoque o el objetivo de la auditoría ya que se preocupa en llenar documentos que no aportan en identificar las debilidades y deficiencias de controles existentes en los procesos de una empresa, la metodología propuesta en esta tesis ha mejorado el proceso de desarrollo de una auditoría de sistemas, por la experiencia obtenida en el desarrollo de esta metodología se concluye y recomienda lo siguiente:

- La Metodología de auditoría debe desarrollarse a través de un proceso que no involucre mal gastar el tiempo en documentar hallazgos que no servirán para identificar las deficiencias y ausencias de controles. Al llevar esta metodología de manera ordenada y concisa ayuda a determinar los riesgos que impactan al negocio identificar las actividades de control que los mitigan.

- Los documentos, tales como las matrices que se utilizan para documentar el desarrollo de la auditoria de sistemas deben mantener la misma estructura para todos los procesos y contener información relevante al procesos y hallazgos encontrados, para que esta documentación pueda servir como referencia en auditorias posteriores.

- La Metodología SOX IT (Cobit) cubre todos los aspectos de seguridad que deben considerarse para poder asegurar que la infraestructura y procesos de la Tecnología de Información que estamos utilizando en nuestras empresas protegidos de la vulnerabilidad de ataques informáticos.

- La implementación de la metodología SOX IT (Cobit) nos ayuda a encontrar que procesos no están completos o no se están ejecutando como está documentado.

- La implementación de la metodología SOX IT (Cobit) ayuda al personal de TI a identificar cuáles son sus responsabilidades y como aplicar controles que ayuden a proteger sus recursos.

- Antes de implementar la metodología SOX IT (Cobit) se debe conocer muy bien el objetivo del negocio y como funciona este para poder identificar cuáles son los procesos que necesitan aplicar controles.

- Al seleccionar los procesos auditables se debe asegurar que son procesos que si dejan de funcionar se paraliza el negocio.

- De todos los procesos que tiene el marco de referencia COBIT 4.1, se debe seleccionar solamente los procesos más importantes y aplicables al negocio, es un grave error querer seleccionar todos los procesos y todos los dominios.

- Los procesos del negocio a los cuales se les aplicará la metodología SOX IT (Cobit) no deben ser mas de 4 procesos, y estos deben representar el objetivo del negocio.

- Cuando se identifique las actividades de control se debe tener en cuenta que estas deben representar un control más no una tarea operativa.

GLOSARIO

Término	Descripción
SAP	Proceso de Seguridades aplicativo
SBD	Procesos de Seguridades bases de datos
SSO	Proceso de Seguridades Sistemas Operativos
SAP-SIS-01	Proceso de seguridades de aplicativos del área de sistemas de la empresa.
SBD-SIS-01	Proceso de seguridades de bases de datos del área de sistemas de la empresa
SBD-TEC-01	Procesos de seguridades de bases de datos del área técnica de la empresa
SSO-SIS-01	Procesos de seguridades de los sistemas operativos del área de sistemas de la empresa
SSO-TEC-01	Procesos de seguridades de los sistemas operativos del área técnica de la empresa.
R1- C2	Segunda actividad de control para el riesgo 1.
R7- C1	Primer actividad de control para el riesgo 7
DS	Delivery and Support, Dominio de COBIT
MSC	Mobile Switching Center
HLR	Home Location Register
SDP	Service Delivery Platform
SGSN	Serving GPRS Support Node

REFERENCIAS

[1] LEY SARBANES-OXLEY. Extraído el 2 Noviembre de 2011 desde http://www.interamericanusa.com/articulos/Leyes/Ley-Sar-Oxley.htm

[2] Tommie Singleton. 2007. *The COSO Model: How IT Auditors Can Use It to Evaluate the Effectiveness of Internal Controls* , ISACA

[3] Espiñeira, Sheldon y Asociados. 2008. *El Gobierno de TI: La práctica en tiempo de crisis.* PRICEWATERHOUSECOOPERS.

[4] IT GOVERNANCE INSTITUTE. 2008. *Alineando COBIT 4.1, ITIL V.3 E ISO/IEC 27002 en Beneficio del Negocio.* ISACA, ITGI.

[5] Mario Piattini Velthuis, Emilio del Peso Navarro, Mar del Peso Ruiz. *2008. Auditoría de tecnologías y sistemas de información.* RA-MA

[6] Gary A Bannister. 2006. *Using COBIT for Sarbanes and Oxley* . IT GOVERNANCE INSTITUTE

[7] Information Systems Audit and Control Foundation. 2007. *COBIT 4.1 (Control Objetives for Information and related technology).* IT Governence Institute

[8] Colegio de contadores Públicos de Nicaragua. SEMINARIO COBIT 4.1. *Extraído el 15 Junio de 2011 desde* http://www.ccpn.org.ni/descargas.html

[9] Information Systems Audit and Control Foundation. 1998. *COBIT: Directrices de Auditoría.* IT Governence Institute.

[10] Information Systems Audit and Control Foundation. 2000. *COBIT: Audit Guidelines.* IT Governence Institute.

[11] Jorge Arteaga. *2008. Guía para la documentación de controles generales de tecnologías de información.* AMERICA MOVIL

ANEXOS I

Proceso de Seguridad de Aplicativos de Sistemas

El Gerente de Sistemas es responsable de decidir quiénes ejecutaran configuraciones en los aplicativos, bases de datos o sistema operativo, esto es documentado y revisado cada semestre para considerar algún cambio pertinente. La documentación es amplia y detallada. Y además es desarrollada en conjunto con los jefes de cada departamento.

Adicionalmente el Gerente de Sistema tiene la responsabilidad de elaborar un plan de seguridad que considere todos los lineamientos que ayuden a cautelar los programas y equipos administrados por el área de Sistemas. Este documento es revisado anualmente para considerar algún cambio pertinente, este documento es desarrollado por el Gerente de Sistemas con ayuda de los jefes de cada departamento. Para saber si este plan se está ejecutando, el Gerente de Sistemas revisa trimestralmente y aleatoriamente las tareas debieron haberse ejecutado de acuerdo al cronograma acordado dentro del Plan de Seguridad. Como parte del proceso, el Gerente de Sistemas se revisa semestralmente la bitácora de cambios que se han efectuado en el Plan de Seguridad.

El Oficial de Seguridad de la Información configura el ingreso al Sistema Integrex de la empresa para que pidan usuario y clave, esto se lo realiza por la creación de cada usuario sin excepción. Adicionalmente el Ingeniero de Oficial de seguridad de Sistemas configura los mecanismos de seguridad tales como clave segura y cambio de clave cada cierto tiempo, esto se lo hace al mismo tiempo que se crea el nuevo usuario.

Para la eliminación de usuarios o actualización de perfiles, el Oficial de Seguridad de la Información recibe correos con novedades de egreso o cambio de los Jefes o Gerentes de las áreas solicitantes.

Los logs de seguridad del sistema Integrex son almacenados en cintas y luego estas cintas son almacenadas en cajas fuertes, cada que se procede a sacar una cinta que este llena se detalla en una bitácora, fecha desde y fecha hasta la información que contiene la cinta, este proceso es ejecutado por el Ingeniero en Sistemas. Cada mes se evalúa y se re ejecuta la información que poseen las cintas para validar si esta información es válida. La generación de los logs de accesos son ejecutados automáticamente por el sistema y le llega una notificación al Ingeniero de sistemas responsable de esta actividad, donde indica que se ejecuto el respaldo del log sin ninguna novedad.

El Gerente de Sistemas documenta las políticas de acceso al centro de computo, este documento contiene el detalle de lo que debe hacer cualquier persona sea autorizada o no autorizada y que desee ingresar al centro de computo, anualmente se revisa esta política para revisar si esto amerita alguna actualización. Esta revisión la ejecuta el Gerente de Sistemas en conjunto con el departamento de Infraestructura.

El jefe de seguridad física es responsable en implementar mecanismos de seguridad que ayuden a precautelar las seguridades en las ubicaciones físicas donde se encuentra ubicado el centro de computo tales como alarmas de acceso no autorizado, alarmas contra incendio, alarmas contra inundaciones, cámaras de vigilancia, etc. Además el Jefe de seguridad física es el encargado de la instalación de las cámaras de seguridad dentro del centro de cómputo, el Jefe de Seguridad Física envía al Jefe de Sistemas el reporte mensual del funcionamiento de los equipos de seguridad en el Centro de cómputo.

El Ingeniero de Sistemas se encarga de contactar al proveedor de mantenimiento de los equipos de refrigeración del centro de cómputo para que elaboren un mantenimiento preventivo cada semestre, luego se envía reporte de mantenimiento de los equipos

de refrigeración al Jefe de Sistemas.

Diagrama de Flujos del Proceso de Seguridad de Aplicativos del Sistema

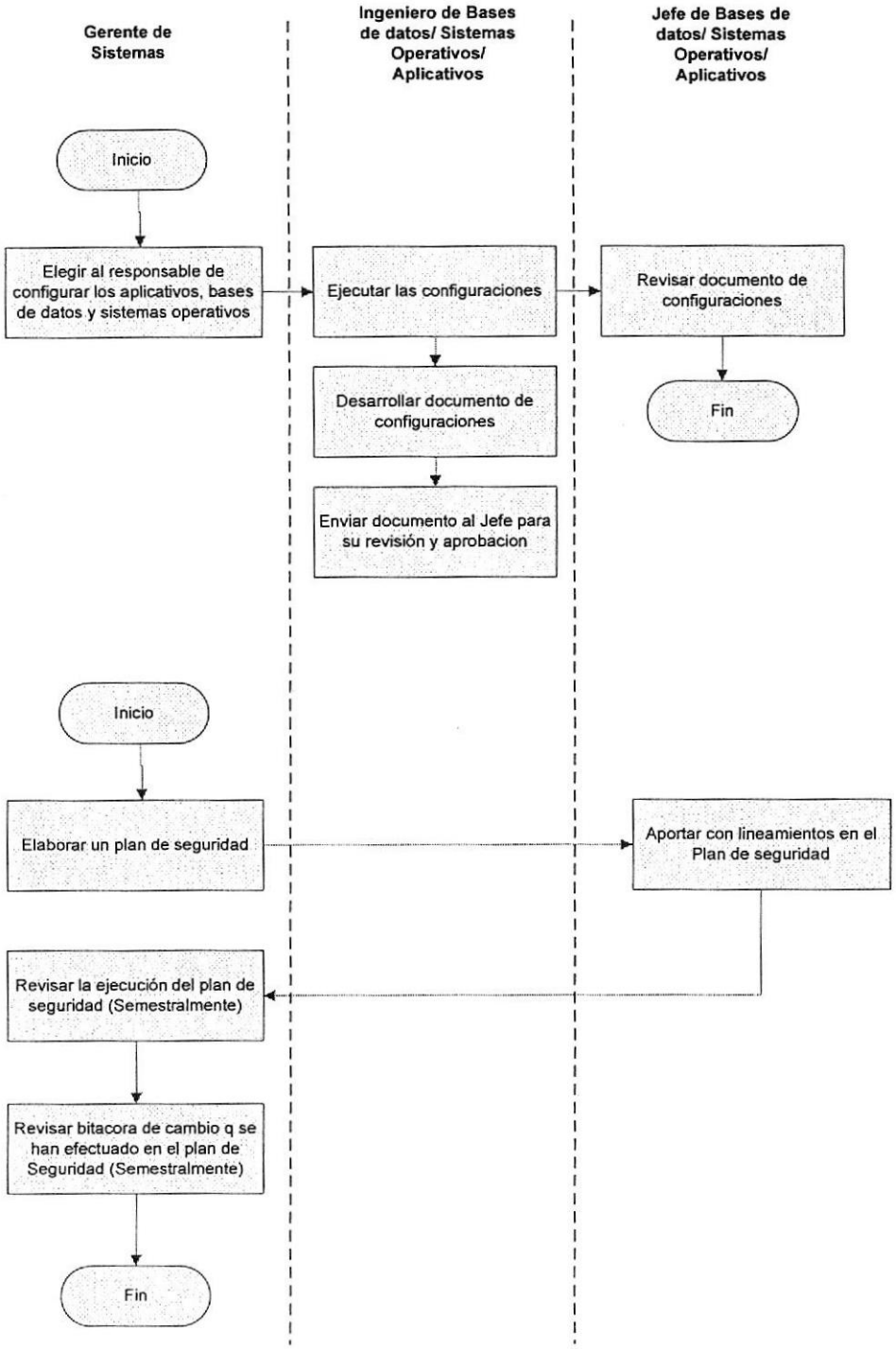


Figura (Anexo.1): Diagramas de Flujo del proceso de Seguridad de Aplicativos I

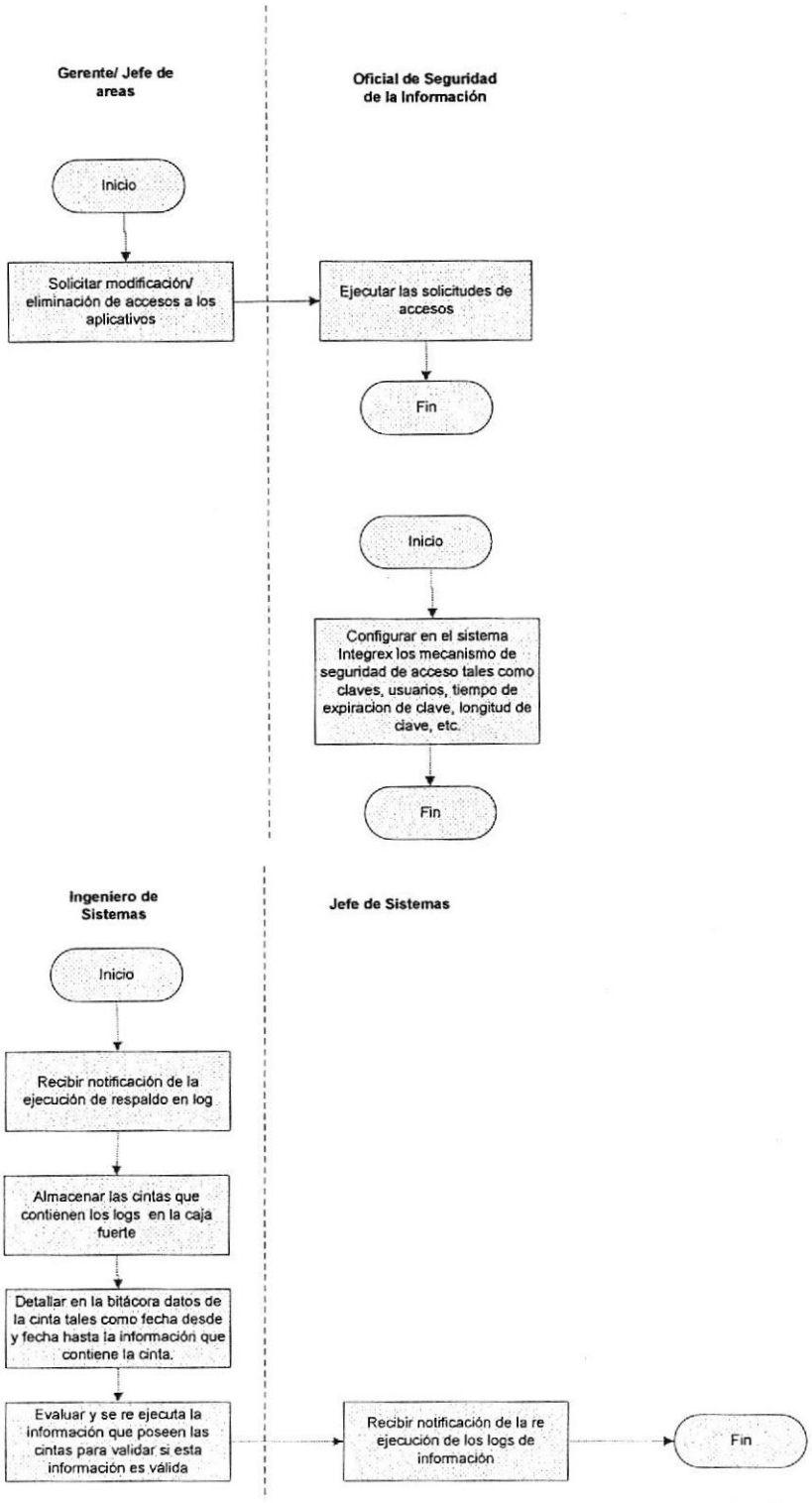


Figura (Anexo.1): Diagramas de Flujo del proceso de Seguridad de Aplicativos II

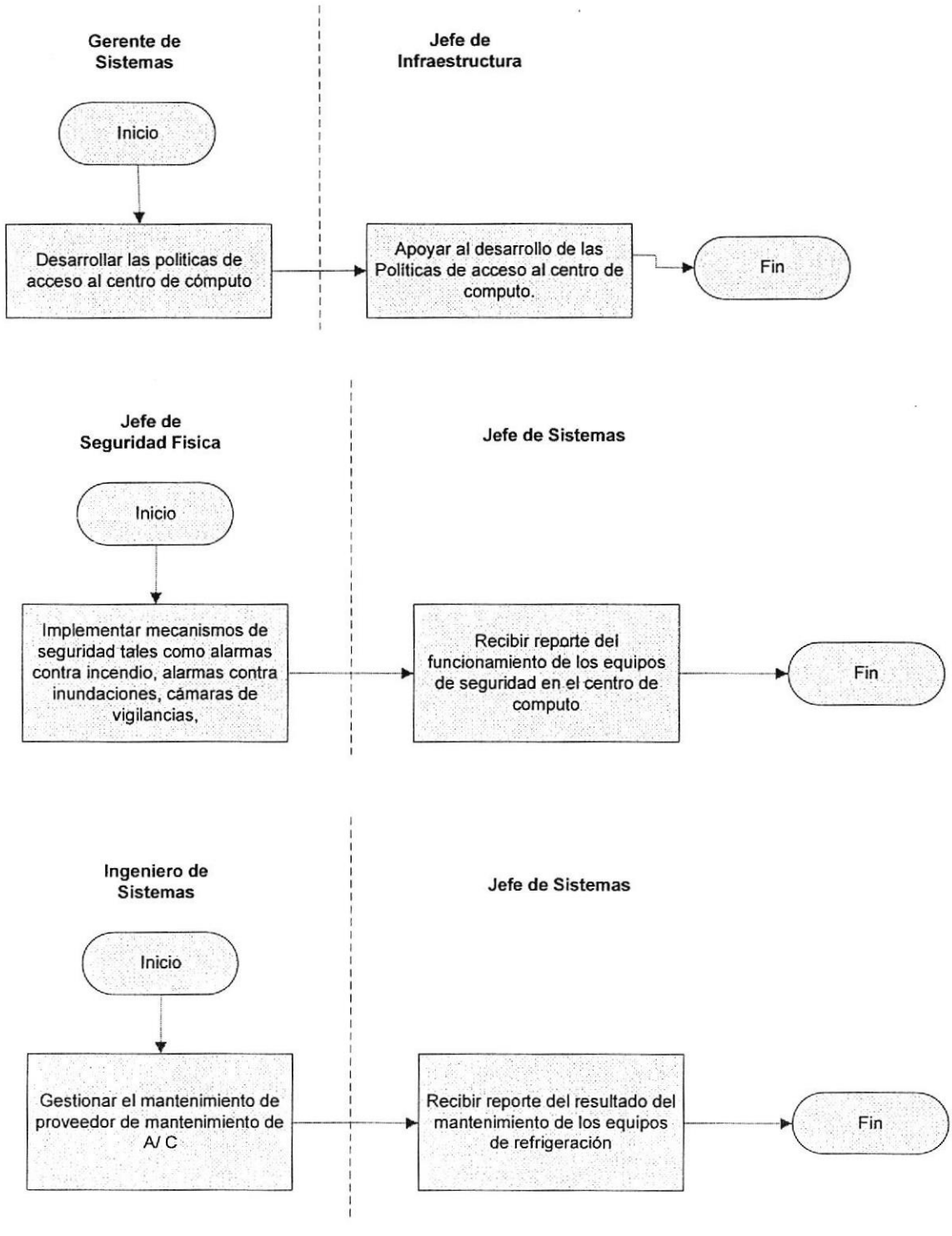


Figura (Anexo.1): Diagramas de Flujo del proceso de Seguridad de Aplicativos III