5 de agosto de 2010
SSOI-0176-2010

Máster
Sandra Valerín Martínez, Directora
DIRECCIÓN DESARROLLO HUMANO ORGANIZACIONAL

Estimada señora:

En cumplimiento al procedimiento denominado "Presentación y Publicación de Informes de Fin de Gestión", me permito adjuntar el respectivo informe de gestión del suscrito como Jefe del Subproceso de Seguridad Operativa Informática en el periodo Julio 2003 – Julio 2010 (hasta el pasado 30 de julio de 2010).

El Subproceso de Seguridad Operativa Informática cuenta con siete funcionarios, cuyos puestos se distribuyen de la siguiente manera: cinco Profesionales en Procesamiento Electrónico de Datos 2 y, un Profesional Procesamiento Electrónico de Datos 1 y el Jefe del Subproceso.

El Manual de Puestos de la Dirección de Tecnología de Información, que contiene el detalle funciones de los puestos indicados, fue aprobado según oficio N° GGC-1731-2007 del 5 de octubre de 2007, de acuerdo con el Reglamento de Clasificación y Valoración de Puestos del Banco Popular, Capítulo 3, artículo 6, aprobado en Junta Directiva Nacional según sesión 4367 del 02 de febrero 2006.

Atentamente,

BANCO POPULAR Y DE DESARROLLO COMUNAL
SUBPROCESO SEGURIDAD DE INFORMATICA TDI
B. C. R.

Lic. Daniels Hidalgo Jiménez, Jefe
SUBPROCESO SEGURIDAD OPERATIVA INFORMÁTICA

- Dirección de Tecnología
- Proceso de Control Operativo
- Subproceso Banca Fácil
- Daniels Hidalgo Jiménez
- Archivo

Ant

Antecedentes

El Subproceso de Seguridad Operativa Informática fue creado en el año 2003 su objetivo es el siguiente:

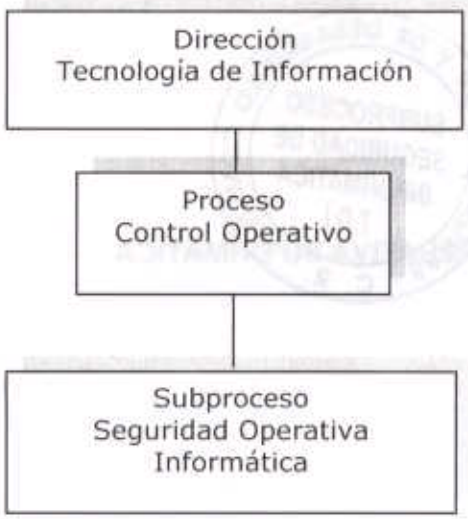
Objetivo:

Planear, coordinar y administrar los servicios de Seguridad de la Información en la organización con el fin de garantizar una seguridad razonable en todas las operaciones realizadas, a través del establecimientos de procesos, normas, reglas, políticas y estándares que aseguren una adecuada protección de los recursos informáticos.

Objetivos específicos

- Asegurar la confidencialidad, integridad y disponibilidad de la información
- Velar por la seguridad física y lógica de los activos de la Institución.
- Desarrollar y establecer políticas sobre seguridad y control interno para proteger los recursos informáticos del Banco Popular.
- Minimizar los riesgos que se generan en el ámbito informático.
- Difundir la importancia y conceptos de la Seguridad Informática a los miembros de la organización.
- Garantizar que se cumplan los objetivos del Plan Anual Operativo.

Estructura Funcional



Actividades

El área de Seguridad Operativa debe cumplir las siguientes actividades u objetivos de control, de manera que el adecuado cumplimiento de éstos asegure al Macro Proceso de Tecnología de Información el alcance de los objetivos propuestos, en apego a las normativas internas y externas y leyes vigentes.

Los siguientes objetivos de control pertenecen al modelo COBIT, el cual contiene las mejores prácticas en Tecnología de Información. Cada uno de ellos debe ser interpretado y aplicado en concordancia con la función de cada Subproceso para lograr un cumplimiento total a nivel del Macro Proceso de Tecnología de Información:

1.4 Definir la organización y sus relaciones

1.4.6 Responsabilidad de la Seguridad Lógica y Física

Se deberá asignar formalmente la responsabilidad de la seguridad lógica y fisica de los activos de información de la organización a un encargado de seguridad de la información. Como mínimo, la responsabilidad del encargado de seguridad deberá establecerse a todos los niveles de la organización para manejar los problemas generales de seguridad en la organización. En caso necesario, deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles específicos con el fin de resolver los problemas de seguridad relacionados con ellos.

1.6 Comunicar la dirección y objetivos de la gerencia

1.6.8 Política de Seguridad y Estructura del Control Interno

La dirección deberia asumir plena responsabilidad por el desarrollo y mantenimiento de una política estructural que establezca el enfoque general de la organización respecto de la seguridad y el control interno para establecer y mejorar la protección de los recursos de tecnología informática. La política debería cumplir con los objetivos generales del negocio y estar orientada a minimización de los riesgos mediante medidas preventivas, identificación oportuna de las irregularidades, limitación de las pérdidas y restauración oportuna. Las medidas deberían estar basadas en análisis de costo-beneficio y deberían ser priorizadas. Además, la dirección debería asegurar que esta política de seguridad y de control interno de alto nivel especifica el propósito y los objetivos, la estructura de administración, el alcance dentro de la organización, la definición y asignación de responsabilidades por la implementación a todos los niveles, y la definición de penalidades y acciones disciplinarias asociadas con el incumplimiento de las políticas de seguridad y control interno. Deberían definirse criterios para la re-evaluación periódica de la estructura para sustentar la responsabilidad por el cambio de los requerimientos organizacionales, ambientales y técnicos.

1.6.11 Comunicación de Conciencia de Seguridad en TI

Un programa de concientización sobre seguridad en TI, deberá comunicar las políticas de seguridad en TI a cada uno de los usuarios de tecnología y asegurar un completo entendimiento sobre la importancia de la seguridad en tecnología de información. Deberá transmitir el mensaje de que la seguridad en TI beneficiará a la organización, a todos sus

empleados y que todos son responsables de ella. El programa de concientización de seguridad, deberá contar con el soporte y representar la perspectiva de la alta gerencia.

1.10 Administrar proyectos

1.10.9 Planeación de Métodos de Aseguramiento

Las tareas de aseguramiento deberán ser definidas durante la fase de planeación del marco de referencia de administración de proyectos. Las tareas de aseguramiento deberán apoyar la acreditación de sistemas nuevos o modificados y garantizar que los controles internos y los dispositivos de seguridad cumplan con los requerimientos necesarios.

2.1 Identificar soluciones de automatización

2.1.9 Controles de Seguridad Económicos

Se debería asegurar que los costos y beneficios de la seguridad se examinan cuidadosamente en términos monetarios y no monetarios para garantizar que los costos de los controles no exceden los beneficios. La decisión requiere una aprobación formal de la gerencia. Deberían identificarse todos los requerimientos de seguridad en la fase de requerimientos del proyecto y ser justificados, acordados y documentados como parte del caso general del negocio para un sistema de información. Deberían definirse los requerimientos de seguridad para administrar la continuidad del negocio para asegurar que la activación, recupero y restauración de los procesos planeados están sustentados por la solución propuesta.

2.3 Adquirir y mantener la arquitectura tecnológica

2.3.3 Seguridad de Software del Sistema

Se deberá asegurar que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo. Deberá ponerse gran atención a la instalación y mantenimiento de los parámetros del software del sistema.

3.2 Administrar servicios con terceros

3.2.3 Contratos con terceros

Se deben definir procedimientos específicos para asegurar que un contrato formal sea definido y acordado para cada relación de servicio con un proveedor.

3.2.8 Monitoreo

Deberá establecerse un proceso continuo de monitoreo sobre la prestación de servicio de terceros, con el fin de asegurar el cumplimiento de los acuerdos del contrato.

3.5 Garantizar la seguridad de sistemas

3.5.1 Administrar Medidas de Seguridad

La seguridad en Tecnología de Información deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye:

* traducir información sobre evaluación de riesgos a los planes de seguridad de tecnología.
* implementar el plan de seguridad de tecnología de información.
* actualizar el plan de seguridad de tecnología de información para reflejar cambios en la configuración de tecnología.
* evaluar el impacto de solicitudes de cambio en la seguridad de tecnología de información.
* monitorear la implementación del plan de seguridad de tecnología de información.
* alinear los procedimientos de seguridad de tecnología de información a otras políticas y procedimientos.

3.5.2 Identificación, Autenticación y Acceso

El acceso lógico a, y el uso de los recursos de computación, de la función de servicios informáticos debería estar restringida mediante la implementación de una adecuada identificación, mecanismos de autenticación y autorización, vinculación de usuarios y recursos con reglas de acceso. Tales mecanismos deberían prevenir que personal no autorizado, conexiones por discado y otras puertas de entrada al sistema (red) accedan a los recursos de computación y minimizar la necesidad de que los usuarios autorizados utilicen "sign-ons" múltiples. También debería haber vigentes procedimientos que mantengan efectivos los mecanismos de autenticación y acceso (Ej.: cambios regulares de passwords).

3.5.3 Seguridad de Acceso a Datos en Línea

En un ambiente de tecnología de información en línea, se deberá implementar procedimientos acordes con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos.

3.5.4 Administración de Cuentas de Usuario

Se debería establecer procedimientos para asegurar una acción oportuna en relación al pedido, establecimiento, emisión, suspensión y cierre de cuentas de usuarios. Debería incluirse un procedimiento formal de aprobación que describa los datos o el propietario del sistema que concede los privilegios de acceso. La seguridad de acceso de terceros debería estar definida contractualmente y considerar los requerimientos de administración y de no divulgación. Los arreglos de tercerización deberían considerar en el contrato entre las partes los riesgos, controles de seguridad y procedimientos para los sistemas de información y redes.

3.5.5 Revisión Gerencial de Cuentas de Usuario

Se debería tener instalado un proceso de control para revisar y confirmar periódicamente los derechos de acceso. Debería realizarse periódicamente la comparación de los recursos con las responsabilidades asignadas para ayudar a reducir el riesgo de errores, fraudes, abusos o alteraciones no autorizadas.

3.5.6 Control de Usuarios sobre Cuentas de Usuario

Los usuarios deberán controlar en forma sistemática la actividad de su(s) propia(s) cuenta(s). También se deberán establecer mecanismos de información para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.

3.5.7 Vigilancia de Seguridad

Se debería asegurar que se registra toda la actividad de seguridad y que cualquier indicación de una inminente violación a la seguridad se notifica inmediatamente a todos a quienes les pueda concernir, interna y externamente, y se actúa en consecuencia.

3.5.8 Clasificación de Datos

Se debería implementar procedimientos para asegurar que todos los datos son clasificados por el propietario de los datos en términos de sensitividad mediante una decisión formal y explícita de acuerdo con el esquema de clasificación de datos. Aún los datos que "no necesitan protección" deberían requerir una decisión formal para ser designados de esta manera. Los propietarios deberían determinar la disposición y uso compartido de los datos, como asimismo, si los programas y archivos deben ser mantenidos, archivados o dados de baja y cuándo. Debería mantenerse una evidencia de la aprobación del propietario y de la disposición de los datos. Deberían definirse políticas que consideren reclasificar la información, según la sensitividad cambiante de la misma. El esquema de clasificación debería incluir criterios para administrar intercambios de información entre organizaciones, considerando tanto la seguridad como el cumplimiento de la legislación relevante.

3.5.9 Identificación Central y Manejo del Acceso Correctamente

Deben existir controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control global de acceso.

3.5.10 Reportes de Violación y de Actividades de Seguridad

Se deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas. El acceso lógico a la información sobre el registro de recursos de cómputo (seguridad y otros registros) deberá otorgarse tomando como base el principio de menor privilegio (necesidad de saber).

3.5.11 Manejo de Incidentes

Se deberá implementar la capacidad de manejar incidentes de seguridad computacional, dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras. Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.

3.5.12 Reacreditación

Se deberá asegurar que se lleve a cabo periódicamente una reacreditación de seguridad por ejemplo, a través de equipos de personal técnico "tigre" con el fin de conservar al día el nivel de seguridad aprobado formalmente y la aceptación del riesgo residual.

3.5.15 No negación

La política organizacional debería asegurar que, cuando sea apropiado, las transacciones no puedan ser denegadas por ninguna parte, y que existan controles implementados para proveer "no-repudio" del origen o recepción, prueba del envío y recepción de transacciones. Esto puede ser implementado mediante firmas digitales, registro de

horarios y terceras partes confiables, con políticas adecuadas que tienen en cuenta la legislación relevante.

3.5.16 Sendero Seguro

Las políticas organizacionales deberán asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros (trusted paths). La información sensitiva incluye: información sobre administración de seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas. Para lograr esto, se pueden establecer canales confiables mediante el encriptamiento entre usuarios, entre usuarios y sistemas y entre sistemas.

3.5.17 Protección de funciones de seguridad

Todo el hardware y software relacionado con seguridad debe encontrarse permanentemente protegido contra intromisiones para proteger su integridad y contra divulgación de sus claves secretas. Adicionalmente, la organización deberá mantener discreción sobre el diseño de su seguridad, pero no basar la seguridad en mantener el diseño como secreto.

3.5.18 Administración de Llaves Criptográficas

Se debería definir e implementar procedimientos y protocolos a utilizar para la generación, cambio, revocación, destrucción, distribución, certificación, almacenaje, ingreso, uso y archivo de claves criptográficas para asegurar la protección de las claves contra modificación y divulgación no autorizada. Si una clave se ve comprometida, la gerencia debería asegurar que esta información se propaga a todas las partes interesadas mediante el uso de Listas de Revocación de Certificados o mecanismos similares.

3.5.19 Prevención, Detección y Corrección de Software "Malicioso"

En relación al software malicioso, tales como los virus de computador o "caballos troyanos", se debería establecer una estructura adecuada de medidas de control para prevención, detección y corrección, respuesta a la ocurrencia y emisión de informes. Se deberían asegurar que se establecen procedimientos en toda la organización para proteger los sistemas y tecnología de la información de los virus de computación. Los procedimientos deberían incorporar protección contra virus, detección, respuesta a la ocurrencia y elaboración de informes.

3.5.20 Arquitectura de Fire Walls y conexión a redes públicas

Si existe conexión con Internet u otras redes públicas en la organización. Se deberá contar con sistemas Fire Wall adecuados para proteger en contra de negación de servicios y cualquier acceso no autorizado a los recursos internos; deberá controlar en ambos sentidos cualquier flujo de administración de infraestructura y de aplicaciones y deberá proteger en contra de negación o ataques de servicio.

3.7 Educar y capacitar a usuarios

3.7.3 Entrenamiento sobre Principios y Conciencia de Seguridad

Todo el personal debe ser entrenado y educado en los principios de seguridad de sistemas, incluyendo actualizaciones periódicas con un enfoque especial en toma de conciencia sobre seguridad y manejo de incidentes. La dirección superior debería proveer un programa de educación y entrenamiento que incluya: conducta ética de la función de servicios informáticos, prácticas de seguridad para proteger contra el daño producido por

fallas que afecten la disponibilidad, confidencialidad, integridad y desempeño de las tareas de una manera segura.

3.10 Administrar problemas e incidentes

3.10.4 Autorizaciones de Acceso de Emergencia y Temporarias

Las autorizaciones de acceso de emergencia y temporarias deberían documentarse en formularios estándar y mantenerse archivadas, estar aprobadas por los gerentes apropiados, ser comunicadas con seguridad a la función de seguridad y automáticamente terminadas luego de un período predeterminado.

3.11 Administrar la información

3.11.27 Protección de Mensajes Sensitivos

Con respecto a la transmisión de datos a través de Internet u otra red pública, la Gerencia deberá definir e implementar procedimientos y protocolos para ser utilizados para el aseguramiento de la integridad, confidencialidad y "no negación" de mensajes sensitivos.

3.11.28 Autenticación e Integridad

Definir las políticas para que previo a alguna acción sobre información originada fuera de la Organización que se reciba via teléfono, correo de voz, documentos (en papel), fax o correo electrónico, se deberá verificar adecuadamente la autenticidad e integridad de dicha información.

3.12 Administrar las instalaciones

3.12.1 Seguridad Física

Deberían establecerse medidas apropiadas de seguridad física y control de accesos para las instalaciones de tecnología informática, incluyendo la utilización fuera del sitio de dispositivos informáticos en conformidad con la política general de seguridad. La seguridad física y los controles de acceso deberían considerar no sólo el área que contiene el hardware del sistema, sino también dependencias en que se aloja el cableado utilizado para conectar elementos del sistema, servicios de soporte (tales como energía eléctrica), backup de medios y cualquier otro elemento requerido para operación del sistema. El acceso debería ser restringido a los individuos que han sido autorizados para tener dicho acceso. Cuando los recursos de tecnología informática están localizados en áreas públicas, los mismos deberán estar adecuadamente protegidos para prevenir o disuadir pérdidas o daños por robo o vandalismo.

3.13 Administrar la operación

3.13.8 Operaciones Remotas

Para las operaciones remotas, deberán existir procedimientos específicos que aseguren que la conexión y desconexión de los enlaces con la(s) instalación(es) remota(s) sean identificadas e implementadas.

4.1 Monitorear el proceso

4.1.2 Evaluación de Desempeño

Los servicios a ser proporcionados por la función de servicios de información deberán ser medidos (indicadores clave de desempeño y/o factores críticos de éxito) y comparados con los niveles objetivo. Las evaluaciones a la función de servicios de información deberán ser desarrolladas en forma continua.

4.1.4 Reportes Gerenciales

Deberían proveerse informes gerenciales para la revisión por la alta dirección del progreso de la organización hacia los objetivos identificados. Los informes de estado deberían incluir el grado de logro de los objetivos planeados, de obtención de sub-productos, el logro de objetivos de desempeño y de mitigación de riesgos. Luego de la revisión, debería iniciarse y controlarse la acción gerencial adecuada.

4.2 Evaluar lo adecuado del control interno

4.2.1 Monitoreo de Control Interno

Se debería monitorear la efectividad de los controles internos en el curso normal de las operaciones mediante actividades de gerenciamiento y supervisión, comparaciones, reconciliaciones y otras acciones de rutina. Los desvíos deberían originar análisis y acción correctiva. Además, los desvíos deberían ser comunicados al individuo responsable por la función y también, como mínimo, a un nivel de gerencia por sobre ese individuo. Los desvíos serios deberían ser reportados a la dirección.

4.2.2 Operación Oportuna de Controles Internos

La confiabilidad en los controles internos requiere que los controles operen rápidamente para resaltar errores e inconsistencias y que éstos sean corregidos antes de que impacten a la producción y a la prestación de servicios. La información relacionada con los errores, inconsistencias y excepciones deberá ser conservada y reportada sistemáticamente a la Gerencia.

4.2.4 Seguridad de Operación y Aseguramiento de Control Interno

Deberá establecerse el aseguramiento de la seguridad operativa y del control interno y repetirlo periódicamente, mediante auto-evaluación o auditoria independiente para examinar si la seguridad y los controles internos están operando de acuerdo con los requerimientos de seguridad y control interno establecidos o implícitos. Las actividades permanentes de monitoreo de la gerencia deberían tratar de detectar las vulnerabilidades y los problemas de seguridad.

En forma general se presenta un desglose de las actividades que el Subproceso de Seguridad Operativa Informática debe realizar en cada una de las plataformas y que concuerdan con los objetivos de control y las normativas adoptadas:

- ✓ Administración de la seguridad de las diferentes plataformas.
- ✓ Revisión y actualización continua de las políticas, normativas y procedimientos de seguridad de la información.

- ✓ Monitoreo y seguimiento a intentos de acceso no autorizado.
- ✓ Control y monitoreo del cumplimiento de las normas, procedimientos y políticas de seguridad de la información.
- ✓ Monitoreo a nivel de seguridad de la información de:
  - Sistemas Operativos.
  - Aplicativos
  - Equipos de comunicación
  - Seguridad perimetral
  - Logs de eventos generados por cualquier tipo de tecnología que administre información de la organización
- ✓ Realizar el análisis de riesgos del Macro Proceso de Tecnología de Información.
- ✓ Asesorar a otras áreas todo lo concerniente a seguridad de la información en la adquisición de nuevas herramientas de software y hardware.
- ✓ **Cumplimiento de normativa vigente:**
  Los funcionarios son responsables de cumplir y dar cumplimiento a todas las políticas, así como las normas de control interno emitidas tanto por la Dirección de TDI como por el Banco Popular, como las normas externas de entes regulatorios.

Adicionalmente, se deberá realizar cualquier otra función que sea asignada por el Proceso o la Dirección.

Resultados de la Gestión

De facto:

- Actividades o funciones de gestión del área:
  - Se da ejecución y atención a las labores administrativas correspondientes como:
    - Generación, administración y control del presupuesto
    - Administración y control de contratos
    - Desarrollo de Planes Anuales de trabajo.
    - Proceso de Actualización de infraestructura, Herramientas, procesos y procedimientos ene le tiempo
      - Dentro de estos procesos de actualización podemos nombrar entre ellos:
        - Cambio de Infraestructura física, a saber, servidores y telecomunicaciones
        - Migración ISA 2000 a ISA 2004 sobre W2003
        - Migración Exchange a W2003
        - Migración Antivirus de versión 7,8, 9, 10 y ahora a 11
        - Migración de AD a Windows 2003

- Mejoramiento, limpieza y ordenamiento del DNS
- Mejoramiento del WINS
- Mejoramiento y ordenamiento del DHCP

- Generación de Informes de labores mensuales y trimestrales:
  - Se elaboran los informes mensuales y trimestrales debidos, llenando la información dentro de la intranet institucional y a la vez generando un informe de ingreso hacia la Jefatura inmediata.
- Plan de Capacitación
  - Se ha procedido a esquematizar la continua capacitación y actualización de conocimientos en materia de Seguridad Informática del área, de acuerdo a los roles y funciones de los funcionarios, garantizando un adecuado aprendizaje y contingencia de conocimiento.
- Autoevaluaciones de Control Interny Riesgo Operativo
  - Se ha logrado cumplir con las metas establecidas en cuanto el cumplimiento de metas y plazos establecidos para obtener la ejecución de las autoevaluaciones, según lo establecido por la Unidad Técnica de Evaluación de la Gestión y la Auditoria Interna, ambos con resultados positivos y mostrando avances en cada uno de ellos
- Generación de Informes técnicos
  - Se elaboran informes periódicos y bajo solicitud de las diferentes plataformas que aministra el área de Seguridad Informática, a saber, Antivirus, AntiSPAM, Internet, Active Directory, Correo Electrónico, Microsoft, Vulnerabilidades, Firewalls, Detectores de Intrusos, etc.
- Mantenimiento y Monitoreo de plataformas seguridad
  - Se procede a un monitoreo constante y periódico de las plataformas que amistar el área, a saber, Antivirus, AntiSPAM, Internet, Active Directory, Correo Electrónico, Microsoft, Vulnerabilidades, Firewalls, Detectores de Intrusos, DNS, WINS, DHCP, etc.

Periodo: 2003 – 2008
Modelaje del área:

- Definición, establecimiento y consolidación del Subproceso.
  - Área de Apoyo y soporte para todas las funciones de aseguramiento desde el punto de vista de la información, aspectos como Hardware, Software, documentación y Datos. Se realizaron actividades como:
    - Selección del Personal para el área
    - Contratación de personal para el área
    - Definición de labores y ámbito de trabajo
    - Establecimiento de funciones y roles.
    - Capacitación Especializada
    - Definición del modelo del subproceso de Seguridad Informática
    - Definición de Planes de Acción
- Desarrollo y Aprobación del Reglamento de Seguridad Informática del Conglomerado Banco Popular.
  - Se refiere a parte del Marco documental y legal sobre el cual se basa la Seguridad de la información y su proceder dentro del conglomerado, el cual incluye apartados de:
    - Artículo 1. Fundamento
    - Artículo 2. Régimen Jurídico

- Artículo 3. Órgano contralor
- Artículo 4. Ámbito de regulación o control
- Artículo 5. Desarrollo, modificación, aprobación e implementación de nuevas políticas
- Artículo 6. Del uso del correo electrónico
- Artículo 7. Del acceso y uso de Internet
- Artículo 8. Del uso de antivirus
- Artículo 9. Del uso de dispositivos tipo módem.
- Artículo 10. De la definición y uso de contraseñas
- Artículo 11. Del uso de los recursos de información
- Artículo 12. De las infracciones a este Reglamento
- Artículo 13. Regulación a las empresas que ofrezcan servicios informáticos de cualquier naturaleza.
- Artículo 14. Sanciones a Directores e integrantes de Junta de Crédito Local
- Artículo 15. Vigencia del Reglamento

- Desarrollo y Aprobación del Manual de Políticas de Seguridad Informática del Conglomerado Banco Popular.
  - Se refiere a parte del Marco documental y legal sobre el cual se basa la Seguridad de la información y su proceder dentro del conglomerado. El mismo incluye los siguientes ámbitos:
    - POLITICA DE SEGURIDAD
    - ORGANIZACION DE LA SEGURIDAD
    - CLASIFICACIÓN y CONTROL DE ACTIVOS
    - SEGURIDAD DEL PERSONAL
    - SEGURIDAD FÍSICA y AMBIENTAL
    - COMUNICACIONES Y OPERACIONES
    - CONTROL DE ACCESOS
    - DESARROLLO Y MANTENIMIENTO DE SISTEMAS
    - ADMINISTRACIÓN DE LA CONTINUIDAD DE LOS NEGOCIOS
    - CUMPLIMIENTO
- Desarrollo y Aprobación de Políticas de Seguridad Informáticas
  - Establecimiento del Marco documental en el cual se basa la Seguridad de la información y su proceder. Adicional al Reglamento y al manual, se procedió a desarrollar, gestionar y aprobar 25 políticas de Seguridad Informática.
- Establecimiento de procedimientos de Seguridad Informática
  - Coordinación de procesos para el Mejoramiento de la infraestructura tecnológica y por ende su proceso de aseguramiento desde el punto de vista de seguridad de la información
- Normativa de desarrollo de proyectos
  - Se han desarrollado y aprobado las normas o requerimientos mínimos desde el punto de vista de seguridad de la información para:
    - Desarrollo o adquisición de infraestructura
    - Desarrollo o adquisición de sistemas o herramientas
    - Modificación de sistemas
    - Clausula de Confidencialidad para contratos de Tecnología de Información
    - Clausula de Seguridad de la Información en los contratos de nuevos empleados del banco
- Proceso de Análisis de Riesgos Interno

- Se logró ejecutar un proceso de contratación de una empresa externa con experiencia en seguridad informática para hacer una valoración de temas de seguridad en las diferentes plataformas del Banco, obteniendo de ella insumos para un mejor direccionamiento de acciones y funciones del área.

- Proceso de Escaneo de vulnerabilidades externo
  Se ha logrado realizar un proceso de escaneo externo de vulnerabilidades, desde afuera hacia todas las direcciones expuestas a redes públicas del banco, con resultados positivos.
- Proceso de concientización y culturización de empelados
  - Participación mensual en el desarrollo de artículos relacionados con temas de seguridad informática, tanto en el periódico Mi Banco, correos masivos y la Intranet Institucional
  - Concientizar al personal del Banco sobre la importancia de la Seguridad informática y la existencia de Riesgos y sus consecuencias.
  - Desarrollo y participación de los programas de inducción realizados por áreas de Desarrollo Humano.
- Control de Acceso Físico
  - Se han establecido en coordinación del Subproceso de Seguridad Bancaria:
    - Dispositivos de control de acceso a las diferentes áreas de Tecnología de Información
    - Dispositivos de control de acceso biométrico a áreas sensibles o criticas de Tecnología de Información
    - Procedimientos y lineamientos de ingreso y salida del Edificio de Tecnología de Información.
    - Gestión y desarrollo de un área dentro de la Intranet Institucional para el control de acceso de personas ajenas al Edificio de Tecnología de Información.
- Gestión y establecimiento de un área independiente físicamente para equipos de seguridad informática
  - Localización y adecuación física de un área específica dentro del Edificio de TDI para elementos de Seguridad Informática, logrando el cumplimento de regulaciones externas e internas y buenas prácticas.

Plataforma:

- Adquisición e implementación de herramientas de seguridad
  - Se ha gestionado y dotado al Banco de Herramientas por medio de las cuales se logra contar con una mejor seguridad de la información y los recursos del banco, así como el monitoreo de las plataformas. Algunos ejemplos son:
    - Escaneo de vulnerabilidades
    - Escaneo de elementos de Telecomunicaciones
    - Filtrado de Contenido
    - Gestión de AD
    - Implementación del sistema Antivirus y antiSPAM
    - Implementación de Firewalls
    - Implementación de IPS (Sistema Preventor de Intrusos)
    - Implementación Certificados SSL
- Filtrado de contenido de acceso a internet
  - Implementación de Herramientas por medio de las cuales se regula, registra y controla el acceso y uso de Internet, logrando reducción del gasto y un uso

controlado de los recursos del Banco, por medio de la categorización de sitios para establecer rangos de accesos y el filtrado del acceso.

- Eliminación de Cuentas Genéricas
  - Se ha logrado reducir a cero la cantidad de Cuentas genéricas del sistema de directorio del Banco, logrando así una reducción notable en riesgo y un aumento en lo referente al establecimiento de pistas de auditoría.
- Segregación de computadoras por unidad organizacional
  - Se ha logrado esquematizar una estructura jerárquica dentro del sistema de directorio (Active Directory) con el fin de organizar las unidades organizacionales y poder contar con flexibilidad de monitoreo, reportes y aplicación de políticas de seguridad y uso.
- Establecimiento de políticas de AD
  - Gracias al ordenamiento realizado sobre la estructura del Active Directory, en su organización de Unidades Organizacionales, ha permitido establecer políticas de seguridad focalizadas y orientadas a Servidores, Computadoras, Usuarios, Grupos de usuarios, Administradores
- Establecimiento y aplicación de políticas donde los usuarios no son administradores
  - Se ha logrado en un 100% de que los usuarios no sean usuarios administradores de sus equipos, logrando
    - Mayor estandarización en la configuración del as computadoras
    - Reducción de casos para soporte en relación a que el usuario no puede alterar o aplicar cambios dentro de la computadora.
    - Control de Software que se instala en las computadoras y así no infringir leyes de propiedad intelectual, así como llevar el debido control e inventario.
    - Control de Hardware que se instala en las computadoras.
    - Mejora en los proceso de aplicación de otras políticas de Active Directory
    - Centralización en áreas de control especializadas en relación a las funciones de administración del cambio y la configuración de las computadoras.
    - Facilidad de aplicación de estándares de configuraron.
- Separación de roles de funcionarios en accesos a Servidores
  - Se ha logrado en un 100% de que los usuarios administradores de servidores solo tengan acceso a los servidores correspondientes según sus labores, logrando una separación de funciones, roles, accesos y responsabilidades
- Endurecimiento de la Política de contraseñas
  - Se ha logrado y conforme se ha necesitado incrementar el nivel de Seguridad y complejidad del como las contraseñas son creadas y se ha logrado establecer un esquema de cambio de contraseña obligatorio cada 30 días de uso de la misma.
- Reducción de Cuentas Administrador de Dominio
  - Se ha logrado reducir el alto riesgo de contar con "n" cuentas tipo Administrador de Dominio a solamente 3 cuentas (2 de ellas administradas por el área de Seguridad Informática y una de ellas almacenadas en Caja fuerte)
- Establecimiento de Estructura de Seguridad de servicios por Internet
  - Se han establecido los mecanismos e infraestructura de Seguridad Informática que garantizara un nivel adecuado de confiabilidad, confidencialidad, integridad y disponibilidad de los servicios por Internet hacia nuestros clientes, procediendo a etapas como: Definición de la Infraestructura, Proceso de

contratación, Procesos de Implementación, Procesos de Monitoreo, Aseguramiento de los servicios.

- Ordenamiento del Sistema de Antivirus
  - Desarrollo y puesta en marcha de un nuevo esquema de sistema de antivirus y antiSPAM de forma tal que se hace una distribución de la listas de firmas de código malicioso de manera tal que reduce el uso de la red de telecomunicaciones.
- Control de correo SPAM, interno y externo
  - Implementación de Herramientas por medio de las cuales se regula, registra y controla el acceso y uso del correo electrónico, logrnado rrducción del gasto, un uso controlado de los recursos del Banco y la protección de los activos del Banco contra malware (Virus, troyanos, etc.)
- Separación de ambientes de envío de correo (Normal y masivo)
  - Se ha concluido la implementación de una plataforma por medio de la cual se obtiene separar el ambiente de envio y recepción de correo normal de los funcionarios del banco del ambiente de envío de correo masivo del banco, logrando así el hecho de que las direcciones IP y dominios del correo normal del banco no se vean afectados pro restricciones establecidas a nivel de otras instituciones por políticas de correo SPAM.
- Separación de ambientes de laboratorio - Producción
  - Se ha definido las políticas y diseño necesarios para lograr una separación de os ambientes de producción y desarrollo/pruebas. El ambiente de desarrollo/pruebas está en proceso de implementación por parte del área de Soporte Técnico, el mismo ya es utilizable y operable bajo ciertas limitaciones.
- Establecimiento de la Red Corporativa
  - Coordinación del proceso de presupuesto, compra, pruebas e implementación de equipos y servicios necesarios para la integración de las redes de telecomunicaciones y servicios de las sociedades anónimas y el banco. Se ha logrado la integración total de la Popular Pensiones y está planteada la integración de Popular Valores y Fondos de Inversión, facilitando la integración de de la infraestructura y servicios brindados por el Banco y las Sociedades Anónimas en un ente común.
- Control de dispositivos USB (Sociedad Popular Pensiones)
  - Se han logrado establecer las políticas necesarias por medio las cuales se controla el uso de dispositivos tipo USB, en una primera etapa se ha implementado para Popular Pensiones, en al cual se encuentra en periodo de prueba, más que todo para valorar la reacción y uso por parte del personal.
- Gestión y establecimiento de un área independiente físicamente para equipos de seguridad informática
  - Localización y adecuación física de un área específica dentro del Edificio de TDI para elementos de Seguridad Informática, logrando el cumplimento de regulaciones externas e internas y buenas prácticas.
- Infraestructura de llave Publica PKI
  - Se ha logrado implementar los elementos de software y hardware necesarios para una infraestructura de llave publica par clientes del sitio Web transaccional del Banco. Esta infraestructura aun no esta en uso por parte del banco.
- Participación en proyectos
  - Se refiere a la intervención oportuna del área de Seguridad Informática en el desarrollo de proyectos informáticos, contribuyendo a una clara y objetiva definición de elementos de Seguridad de la información. Algunos ejemplos:

"Midleware" Corporativo, Cajas y plataforma, CORE SYSTEM, Débitos y créditos directos, Migraciones Sistemas Operativos, Telecomunicaciones, Ley de Legitimación de Capitales, Conectividad, SINPE, Débitos y Créditos, Web Banking, Consolidación de servidores, Laboratorio de Pruebas (Soporte Técnico), Oficialía de cumplimiento, Conexión de Popular Pensiones al BCCR, Software de Pedidos de Chequeras, Proyecto DHCP, Mejoramiento de Redes, BUC, etc.

- Desarrollo y consolidación de un único esquema de periodos de licencias de herramientas de seguridad
  - Se ha gestionado el contar con un único proceso licitatorio el cual cubre las licencias de todas las herramientas de seguridad, logrando una economía procesal importante.

Periodo: 2009

I Trimestre.

- Continuidad del Negocio: Se ha logrado dejar instalado y configurado a nivel de sistema Operativo la plataforma que soportaría la infraestructura Microsoft para un caso de contingencia en el área de sitio Alterno del Banco
- CORE System: Se ha logrado definir el plan y el cronograma de trabajo del sub-proyecto de seguridad informática en relación al proceso de implementación del CORE System.
- Proyecto PKI Interno: Se ha utilizado con éxito la infraestructura de OKI Interno para su I etapa de Correo Electrónico a nivel de un plan Piloto para los funcionarios del área de Seguridad Informática.
- Mantenimiento y Monitoreo: Se ha ampliado la cobertura de seguridad informática sobre la infraestructura Microsoft y Redes, con herramientas de monitoreo y generación periódica de reportes

II Trimestre.

- Continuidad del Negocio:
  - Se ha logrado documentar (Versión borrador) de los procesos necesarios a nivel de sistema Operativo la plataforma que soportaría la infraestructura Microsoft para un caso de contingencia en el área de sitio Alterno del Banco
- CORE System:
  - Se ha dado cumplimiento al plan y el cronograma de trabajo del sub-proyecto de seguridad informática en relación al proceso de implementación del CORE System.
  - Se ha iniciado con la implementación de un pequeño laboratorio de ambiente SOALRIS – ORACLE con el fin de auto-capacitación en materia de seguridad informática de plataformas SOALRIS- ORACLE.
- Proyecto PKI Interno:
  - Se ha utilizado con éxito la infraestructura de PKI Interno para su I etapa de Correo Electrónico a nivel de un plan Piloto para los funcionarios del área de Seguridad Informática.
  - Se está a la espera de la documentación por parte del área de RRHH..
- Mantenimiento y Monitoreo:

- Se ha dado cobertura de seguridad informática sobre la infraestructura Microsoft y Redes, con herramientas de monitoreo y generación periódica de reportes, principalmente en el tema de Antivirus.
- Se ha logrado contener la infección por el virus CONFICKER.

III Trimestre.

- Continuidad del Negocio:
  - Se ha logrado documentar (Versión final) los procesos necesarios a nivel de sistema Operativo la plataforma que soportaría la infraestructura Microsoft para un caso de contingencia en el área de sitio Alterno del Banco
- CORE System:
  - Se ha dado cumplimiento al plan y el cronograma de trabajo del sub-proyecto de seguridad informática en relación al proceso de implementación del CORE System.
- Proyecto Firma Digital Nacional:
  - Se ha logrado implementar el proceso de emisión de Firma Digital Nacional,
- Mantenimiento y Monitoreo:
  - Se ha dado cobertura de seguridad informática sobre la infraestructura Microsoft y Redes, con herramientas de monitoreo y generación periódica de reportes, principalmente en el tema de Antivirus.

IV Trimestre.

- CORE System:
  - Se ha dado cumplimiento al plan y el cronograma de trabajo del sub-proyecto de seguridad informática en relación al proceso de implementación del CORE System.
- Proyecto PKI Interno:
  - Se está en proceso de Capacitación del área de RRHH.
- Mantenimiento y Monitoreo:
  - Se ha dado cobertura de seguridad informática sobre la infraestructura Microsoft y Redes, con herramientas de monitoreo y generación periódica de reportes, principalmente en el tema de Antivirus.
- Restricción de SW no autorizado.
  - Se ha logrado implementar y aplicar controles automáticos para la ejecución de SW no autorizado.
- Incremento en instalación de sistema antivirus
  - Se ha logrado un nivel de actualización de l aversión del sistema antivirus de un 70%
- Redes inalámbrica seguras.
  - Se ha iniciado con el proceso de implementación de infraestructura para poder brindar una red inalámbrica segura.
- Sistema de Comunicación Unificad Segura
  - Se ha iniciado un plan piloto de uso de una infraestructura de comunicación unificada en forma asegurada.

Periodo: 2010

I Trimestre.

- Continuidad del Negocio: Se ha logrado probar la instalación y configuración a nivel de sistema Operativo (AD y DNS) de la plataforma que soportaría la infraestructura Microsoft para un caso de contingencia en el área de sitio Alterno del Banco
- Proyecto PKI Interno: Se ha avanzado en el proceso de capacitación del área de RRHH para lo referente a la infraestructura de PKI Interno
- Mantenimiento y Monitoreo: Se ha mantenido la cobertura de seguridad informática sobre la infraestructura Microsoft y Redes, con herramientas de monitoreo y generación periódica de reportes
- Malware: Se ha logrado un 99% de cobertura de la versión 5 del sistema antivirus a la plataforma cubierta por instalación de antivirus.
- OCS: Se ha logrado una implementación exitosa y funcional del Plan piloto para al menos 50 funcionarios en el manejo de una herramienta de comunicación unificada.
- Correo Electrónico: Se ha una implementación exitosa y funcional del Plan piloto para al menso 25 funcionarios en lo referente a Acceso al correo electrónico vía móvil.

II Trimestre.

- Continuidad del Negocio: Se ha coordinado esfuerzos para llevar a cabo la segunda prueba del sitio remoto.
- Proyecto PKI Interno: Se ha finalizado en el proceso de capacitación del área de RRHH para lo referente a la infraestructura de PKI Interno
- Mantenimiento y Monitoreo: Se ha mantenido la cobertura de seguridad informática sobre la infraestructura Microsoft y Redes, con herramientas de monitoreo y generación periódica de reportes
- Malware: Se ha logrado un 100% de cobertura de la versión 5 del sistema antivirus a la plataforma cubierta por instalación de antivirus.
  Se ha iniciado la migración a la versión 6 del sistema antivirus a la plataforma, teniendo hasta es te momento un 60% de cobertura.

Avance el Plan Anual Operativo (PAO) 2010

Se ha logrado con el cumplimiento del 100% de lo planteado como metas para el I y II trimestre para el Subproceso de Seguridad Operativa informática. Se ha completado con el registro tanto en SIPRE como en avance de PAO en la Intranet.

Avance el BSC y BDP's 2010

Se ha realizado la entrega y cumplimiento de lo estipulado como metas tanto en BDP's, como en BSC para el Subproceso de Seguridad Operativa informática.

Inventario de activos

Con el fin de mantener un control sobre los activos asignados al Subproceso durante los últimos años se ha venido efectuando en forma semestral aproximadamente un inventario de activos por funcionario según los equipos que le han sido asignados a cada uno de ellos.

Informes de labores mensuales y trimestrales

Los informes mensuales correspondientes a los meses de enero a junio de este período fueron elaborados por el suscrito. Asimismo, el informe correspondiente al primer y segundo trimestre de este año también quedó confeccionado y se encuentran en la intranet de TI.

Plan de Capacitación:

El Plan de Capacitación actualizado para el Subproceso de Seguridad Informática fue elaborado. Con respecto a este asunto se debe retomar efectuar las solicitudes de inscripción que correspondan según las necesidades que se identifican para cada funcionario del Subproceso.

Autoevaluación de Control Interno

En cumplimiento al **inciso c** del artículo 17 de la Ley General de Control Interno, se aplicó el cuestionario de control interno según lo solicitado por la Unidad Técnica de Evaluación de la Gestión. El resultado obtenido fue "nivel excelente".

Evaluación de Riesgo Operativo

Por su parte en cuanto a la última Evaluación de Riesgo Operativo aplicada por la Auditoría Interna para el año 2007, se obtuvo que el nivel de exposición al riesgo se disminuyó, ubicándose en un 3% "Excelente".

Autoevaluación del Modelo de Riesgo Operativo

Durante la gestión a mi cargo como coordinador del Subproceso de Seguridad Operativa informática, las Autoevaluaciones del Modelo de Riesgo implementado por la Dirección de TI que han sido aplicadas han mostrado resultados positivos de la gestión realizada.

Recomendaciones de la Contraloría General de la República u otros entes externos

Al momento del retiro del puesto de Coordinador de este subproceso no se tiene ninguna recomendación pendiente o incumplida.

Recomendaciones de Auditoría Interna

A mi salida del área como coordinador del Subproceso de Seguridad Operativa informática se tienen en proceso de cumplimiento, mas no a destiempo, 2 recomendaciones que están siendo atendidas.

Asuntos restantes:

1. **Desarrollo de Carteles:** Se tiene en proceso de desarrollo de cartel los siguientes temas:
    a. Consultoría para elaboración de Plan Integral de Seguridad Informática.
    b. Contratación de empresa para escaneos externos.
    c. Contratación de Consultoría - Tutoría de Seguridad Oracle-Sun

2. **Cambio de Versión de Antivirus:** Debe continuarse con el proceso de migración de la versión 5 a la versión 6, falta aproximadamente un 40% o menso del parque computacional.

3. **Participación en proceso de Mejora:** Actualmente el área participa en forma activa (en temas de Seguridad y de infraestructura Red Micorosft) en los siguientes temas:
   a. Teletrabajo, liderado por RRHH.
   b. PKI Interno.
   c. Contingencia, liderado por Proceso Gerencial de Continuidad del Negocio.
   d. Implementación UAG (Unified Access Gateway)
   e. Implementación OCS (Office Comunnicator Server)

4. **Participación en Proyecto CORE:** El subproceso de Seguridad Informática tiene una amplia y estrecha participación ene l proyecto CORE, bajo los siguientes puntos o temas:
   a. Sub-proyecto de Seguridad Informática: Se ha participado en forma conjunta con Personal del Proyecto CORE, en el cronograma y plan (ya definido todo su alcance) de este sub-proyecto. El mismo está a la espera del momento correcto para su ejecución dentro de todo el plan del Proyecto CORE.
   b. Esquema único de Autenticación para el CORE (Canal Web Banking) : Se ha procedido junto con personal del CORE, de TEMENOS y empresa proveedoras a la definición del modelo que supliría las necesidades del Baco en temas de Autenticación de Clientes par su canal de Web Banking. El mismo ya ha sido entregado a TEMENOS para su valoración. Se está a la espera de respuesta por parte de TEMENOS para proceder a tomar decisiones del curso que debería llevarse.