ISSN 1560-795X

BCC

REVISTA DEL BANCO CENTRAL DE CUBA

2019/Año 22. N° 2

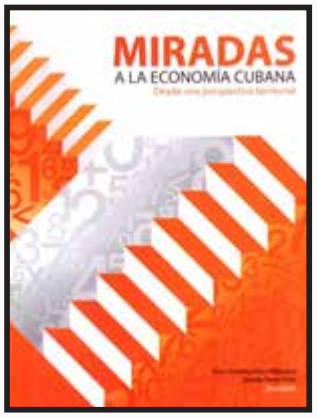
OCTUBRE 13 TRABAJADOR Bancario

Nuevas adquisiciones

DECRETO-LEY Nº 304 "DE LA CONTRATACIÓN ECONÓMICA"
Ministerio de Justicia

Se aborda uno de los temas fundamentales del Derecho Constitucional y la Ciencia Política, con especial referencia a las particularidades de su proceso de formación en Cuba.

MIRADAS A LA ECONOMÍA CUBANA: DESDE UNA PERSPECTIVA TERRITORIAL
Omar Everleny Pérez Villanueva y Ricardo Torres Pérez



Se concentra en el análisis de la dimensión territorial de los procesos de reforma económica y cambio social, con el propósito de contribuir a avanzar en las políticas de desentralización de las facultades y los recursos hacia los territorios.

MIRADAS A LA ECONOMÍA CUBANA
Omar Everleny Pérez Villanueva, Pavel Vidal Alejandro, Armando Nova González y Luisa Iñiguez Rojas

Libro ameno y oportuno que establece un diálogo inteligente y argumentado sobre temas económicos mediante herramientas analíticas actuales. Reflexiona sobre el entorno económico y social cubano.

MIRADAS A LA ECONOMÍA CUBANA: EL PROCESO DE ACTUALIZACIÓN
Pavel Vidal Alejandro y Omar Everleny Pérez Villanueva

En esta serie los autores analizan las principales ausencias y desafíos, a partir de sus propias miradas a los problemas fundamentales de la economía y a las políticas económicas y sociales para enfrentarlos.

BCC
REVISTA DEL BANCO CENTRAL DE CUBA
2019/Año 22. Nº 2




SUMARIO

Edición y corrección: Carmen Alling García. caridad.carmen@bc.gob.cu
Diseño: Ariel Rodríguez Pérez. graphik.cu@gmail.com
Encuéntrenos en Internet: www.bc.gob.cu.
Publicación a cargo de la Dirección de Información y Comunicación Institucional (DICI)

Homenaje a los bancarios

Lic. CARMEN ALLÍNG GARCÍA*

Con motivo del "Día del Trabajador Bancario", fueron diversas las actividades protagonizadas por los trabajadores del Sistema Bancario Nacional (SBN), quienes festejaron y rememoraron el 13 de octubre de 1960, fecha en que el Gobierno cubano promulgó la Ley Nº 891, que implementó la nacionalización de la banca cubana.

Esta celebración tuvo una connotación especial, teniendo en cuenta que el 26 de noviembre se conmemora el 60 Aniversario del nombramiento de Ernesto Che Guevara como presidente del Banco Nacional de Cuba, paradigma a seguir de la joven generación.

Otras razones para esta festividad fue la conmemoración del XX Aniversario de la creación del Banco Exterior de Cuba, el XXV de CADECA S. A. y del XXXV del Banco Financiero Internacional.

Entre las actividades realizadas, tuvo lugar el significativo acto de reconocimiento a 150 trabajadores de las oficinas centrales de las instituciones financieras del sistema, quienes recibieron los sellos por los 25 y hasta 55 años de labor, en representación de los bancarios del país.

Fue presidido por Irma Martínez Castrillón, ministra presidente del Banco Central de Cuba (BCC); Dulce María Iglesias Suárez, secretaria general del Sindicato Nacional de Trabajadores de la Administración Pública; Yaisel Osvaldo Pieter Terry, miembro del Comité Central del PCC y del Consejo Nacional de la CTC; Nicolás Valladares, miembro del Ejecutivo Nacional de la Asociación de Economista y Contadores de Cuba; presidentes de las instituciones financieras; miembros del Consejo de Dirección del BCC, y dirigentes de las organizaciones políticas y de masas.

La actividad contó con la reconocida cantante Annié Garcés, quien nos deleitó con sus magistrales interpretaciones.

La secretaria general del Sindicato Nacional de la Administración Pública se dirigió a los trabajadores del Sistema Bancario Nacional para felicitarlos en su día, y recibió un ramo de flores de la ministra presidente del BCC, en representación de todos los bancarios del SBN.

En la ceremonia, Martínez Castrillón entregó los sellos a los trabajadores de 45, 50 y 55 años de labor, quienes representan un ejemplo de lealtad y consagración al sector.

Se otorgaron los sellos por 45 años de labor a Lázaro Luis Hernández Polledo (BNC), Marta Reme-

dios Gascón Fernández (BICSA) y Abelardo Mulet Santos (BanMet); por 50 a María Isabel Mejías Monzón, Deysi Hildelisa de la Rosa Martínez y Aurora Encarnación Abascal Gómez (BANDEC), y por 55 a Pedro González González (BPA).

Asimismo, los presidentes de las instituciones financieras entregaron las distinciones por años de servicios a trabajadores que cumplieron de 25 a 40 años de labor en el SBN.

29 trabajadores de la capital, en representación de los 122 que ostentan esta categoría en el SBN, recibieron el diploma por 40 años de servicio, entregado por Irma Martínez Castrillón, Dulce María Iglesias y Yaisel Osvaldo Pieter Terry, en nombre del Sindicato Nacional de los Trabajadores de la Administración Pública.

También se debe destacar el merecido reconocimiento a Benigno Regueira Ortega, jubilado del sector, quien por más de cuatro décadas trabajó entregando lo mejor de sí al sistema bancario cubano.

Inició sus labores en 1975 en el Banco Nacional de Cuba. Posteriormente pasó a trabajar al BCC en 1997, donde ocupó distintas responsabilidades, y finalmente, fue nombrado director adjunto de la Vicepresidencia de Macroeconomía, cargo que ejerció hasta 2019, cuando se jubiló a la edad de 88 años.

Por estas razones, la ministra presidente del Banco Central de Cuba le hizo entrega del reconocimiento por su consagración a la vida laboral.

Igualmente, se reconoció el trabajo de los colectivos laborales destacados en 2019, por cada una de las instituciones financieras con representación en la red bancaria nacional. De esta forma, los directores provinciales de las instituciones recibieron los diplomas: por BANDEC, la Dirección Provincial de Las Tunas; por BPA, la Dirección Provincial de Cienfuegos, y por las Casas de Cambio, la Dirección Provincial de Matanzas.

En las palabras de clausura, Irma Martínez Castrillón destacó el papel que ha jugado la banca

Fue Premio Nacional de Economía en el año 2000, y Premio Provincial de Economía en 2007.

En su trayectoria se resalt ó su activa participación en la lucha revolucionaria antes de 1959, así como los cargos que ocupó en diferentes instituciones y las misiones fuera del país.

revolucionaria cubana desde sus inicios, así como también valoró las transformaciones que aún se están realizando en el sistema bancario para su perfeccionamiento.

Finalmente, expresó sus felicitaciones a todos los trabajadores del sector bancario.

*** Editora de la Revista BCC**

Los bancarios a la vanguardia

DISCURSO DE IRMA MARTÍNEZ CASTRILLÓN, MINISTRA PRESIDENTE DEL BCC, EN EL ACTO CENTRAL POR EL "DÍA DEL TRABAJADOR BANCARIO"

Estimados trabajadores e invitados:

No se puede hablar de la banca revolucionaria cubana sin hacer un viaje a nuestras raíces; es por ello que se vuelve imprescindible, entre tantos eventos que distinguen al sector:

- Recordar el 26 de noviembre como una fecha histórica, pues en 1959 el Consejo de Ministros del Gobierno Revolucionario acordó designar a Ernesto Che Guevara como primer Presidente revolucionario del Banco Nacional de Cuba. Esta designación fue una decisión estratégica que procuraba rescatar la confianza del pueblo en esa institución, valiéndose de la firmeza de su carácter y su convicción de defender los intereses de Cuba y su Revolución, cualidades que le permitieron implementar los cambios radicales, sin los cuales el banco no habría podido cumplir su verdadera función de dirección del crédito y apoyo al programa de industrialización del país.
- El 13 de octubre de 1960 se nacionaliza la banca privada y se designa al Banco Nacional de Cuba como banco del Estado. Comienza en ese momento un capítulo de cambios trascendentales, donde la economía y los recursos financieros constituían un arma esencial que la contrarrevolución intentaba utilizar para desencadenar ataques contra Cuba.
- Desde ese momento, el banco fue depositario de un importante papel en la transformación económica de la nación. Varias etapas de transformaciones hasta que en 1997 se crean y fortalecen otras instituciones financieras. Surge así el Banco Central de Cuba, encargado entonces de dotar a la isla de una institución que concentrara sus fuerzas en la ejecución de las funciones básicas inherentes a una banca central independiente, convirtiéndose en la autoridad rectora del sistema bancario. El trabajo del sistema en su conjunto ha coadyuvado al desarrollo de la economía, mantener la independencia y preservar las conquistas de nuestro sistema político y económico.
- Cuba, a pesar de su condición de país agredido, ha logrado constituir un sistema bancario sólido, que siempre ha estado al servicio del pueblo cubano, actuando en un entorno adverso, debido al efecto negativo del bloqueo económico, comercial y financiero ejercido por el Gobierno de Estados Unidos desde inicios de la Revolución, y que hasta la fecha ha continuado recrudeciéndose con un marcado carácter intencional en la esfera bancaria y financiera, ocasionando serias dificultades que impiden el adecuado funcionamiento del sector y de las operaciones bancarias y comerciales del país. Ha sido y continúa siendo una política festinada y perversa, que trata de rendirnos y de que dejemos a un lado los principios que siempre hemos defendido de soberanía, independencia y solidaridad con nuestros pueblos hermanos de América Latina, con especial énfasis en la hermana República Bolivariana de Venezuela.

Compañeras y compañeros, hoy el sistema bancario continúa implementando transformaciones para su perfeccionamiento, incluida la actividad de las entidades financieras no bancarias para incentivar la economía y propiciar el desarrollo empresarial, que aseguren el capital de trabajo y permitan establecer esquemas de encadenamientos productivos, dando prioridad a la exportación de bienes y servicios y a las producciones para el turismo; potenciando las

medidas de control que garanticen la seguridad de las operaciones.

Ante el llamado del Presidente de la República de Cuba Miguel Díaz-Canel Bermúdez a "Pensar como País", sin amedrentarnos por las dificultades existentes, la banca se inserta en los programas de informatización de la sociedad, de gobierno electrónico; en la implementación de la política bancaria, y en el desarrollo de nuevos productos y servicios asociados al uso de la tarjeta magnética como medio de pago, no solo vinculada a la utilización de los cajeros automáticos, sino a otros canales de pago que garantizan la agilidad y la seguridad en las operaciones bancarias, al reducir los trámites presenciales en las sucursales, al hacer un mayor uso de la banca móvil, la banca virtual, la telebanca y la multibanca, Transfermóvil y ENZONA.

Como servidores públicos, trabajamos para implementar la eficiencia y la cultura del detalle como prácticas de vida, que favorezcan despojarnos de la inercia, la indolencia, las trabas, la burocracia, la falta de sensibilidad e inquietudes revolucionarias, las chapucerías y de las demoras en las respuestas y la acción.

Las buenas prácticas deben reflejarse en la prestación de los servicios bancarios, en las medidas dirigidas a fomentar la educación financiera de la población y asegurar mayores prestaciones que contribuyan al mejoramiento del nivel de vida.

Todas estas transformaciones no hubieran sido posible sin la presencia del capital más valioso con que cuenta cualquier institución: el humano y su compromiso incondicional, su alto sentido de la responsabilidad, y amor a la institución y a su trabajo. Tampoco serían posibles sin una adecuada gestión del capital intelectual y la atención y compromiso de los jóvenes que se nutren de la experiencia de generaciones anteriores de bancarios y del intercambio continuo con las universidades y centros de investigación, haciéndolos partícipes de la batalla económica.

Como expresara nuestro Presidente Miguel Díaz-Canel en el discurso pronunciado en la clausura del VIII Congreso de la ANEC, el 14 de junio del presente año, y cito: "No está en nuestras manos decretar el fin del bloqueo, obstáculo fundamental al desarrollo del país. La actual administración estadounidense es abiertamente hostil al país y se ha propuesto asfixiar la economía con particular saña. (…) Debemos concentrarnos, por tanto, en lo que sí depende de todos nosotros: la inteligencia, la creatividad y el esfuerzo. (…) La batalla económica consiste, por tanto, en generar una actitud más proactiva, inteligente y concreta de los dirigentes, convocados a impulsar, no trabando ni demorando, soluciones seguras y específicas" (…).

Al cumplirse en este año el 151 Aniversario del inicio de las luchas por la independencia –proceso único e irreversible iniciado por Carlos Manuel de Céspedes el 10 de octubre de 1868 en La Demajagua, y continuado por héroes y mártires de la Patria– y el 500 Aniversario de la fundación de la ciudad de San Cristóbal de La Habana, aprovechamos la especial ocasión para homenajear a 150 trabajadores de las oficinas centrales de las instituciones financieras, que cumplen de 25 a 55 años de servicios ininterrumpidos en el sistema bancario.

Reitero las felicitaciones a todos los trabajadores del sector y, en especial, a aquellos que hoy reciben este merecido reconocimiento. Como bien dice nuestro Presidente, nos esperan días intensos y desafiantes, pero nadie va a quitarnos la alegría y la confianza en el futuro.

¡Hasta la Victoria Siempre!

¡Patria o Muerte!

¡Venceremos!

Banco Financiero Internacional S.A. arriba a su XXXV Aniversario

Lic. FRANCISCO RODRÍGUEZ ACOSTA*

El 5 de noviembre de 1984 se inauguró el Banco Financiero Internacional S. A. (BFI).

Esta institución bancaria de objeto comercial se constituyó al amparo del Decreto-Ley Nº 84 de 1984, que autorizaba el establecimiento de bancos cubanos no estatales de nacionalidad cubana en el territorio nacional, obteniendo por ello la correspondiente licencia por el Banco Nacional de Cuba (BNC), en calidad de autoridad bancaria, y sus operaciones estarían vinculadas fundamentalmente con las relaciones monetario-crediticias internacionales, lo que le faculta realizar las operaciones propias de un banco comercial.

Se fundó con 12 empleados, y actualmente cuenta con alrededor de 830 trabajadores y 29 sucursales localizadas en las más importantes ciudades del país, en principales polos turísticos y de desarrollo económico, incluyendo la Zona Especial de Desarrollo del Mariel.

Mediante la Resolución Nº 29/2019 del Banco Central de Cuba (BCC) se emitió nueva licencia al BFI, al amparo del Decreto-Ley Nº 362 de 2018.

En estos 35 años, el BFI ha devenido banco líder del Sistema Bancario Nacional en todos los segmentos, servicios y productos que ofrece, con alto nivel de informatización e integración en los sistemas de pagos, en cumplimiento de su misión de impulsar el éxito de sus clientes con soluciones financieras, asesoramiento y servicios bancarios de alta calidad, generando valor para la institución y continuar apoyando el desarrollo sostenido del país.

El fortalecimiento de su solidez se apoya en los valores sostenidos y demostrados por los directivos y trabajadores, teniendo como premisas y bases que sus resultados se sustentan en el éxito de los clientes, donde el empeño y contribuciones del colectivo crean valor para ellos y mejoran las capacidades del banco, aplicando la mejora continua y necesaria para así elevar la calidad y eficiencia de la institución, con apertura e iniciativa, integridad y el trabajo en equipo.

* Vicepresidente Ejecutivo del BFI

Procedimiento para la realización de pruebas de seguridad automatizadas a las aplicaciones web

Ing. EILEÉN LLANO CASTRO E ING. ARIEL MARTÍNEZ MONTIEL*

(TRABAJO QUE RECIBIÓ MENCIÓN EN EL EVENTO CIENTÍFICO DEL SISTEMA BANCARIO NACIONAL "RAÚL LEÓN TORRAS" 2018, CELEBRADO EN LA HABANA)

1. PROYECTO DE SEGURIDAD DE APLICACIONES WEB ABIERTAS (OWASP)

El proyecto abierto de seguridad de aplicaciones web abiertas (OWASP, por sus siglas en inglés) es una comunidad abierta para facultar a las organizaciones a desarrollar, adquirir y mantener aplicaciones que pueden ser confiables. Los proyectos del OWASP cubren muchos aspectos de la seguridad en aplicaciones, desarrollando documentos, herramientas, entornos de formación, guías prácticas, listados de comprobación y otros materiales para ayudar a las organizaciones a mejorar la capacidad de producir código seguro.

1.1. OWASP Top 10

OWASP Top 10 constituye un estudio realizado por este proyecto para actualizar cada cierto tiempo los riesgos más críticos que afectan a las organizaciones. El objetivo principal del Top 10 es educar a los desarrolladores, diseñadores, arquitectos, gerentes y organizaciones sobre las consecuencias de las vulnerabilidades de seguridad más importantes en aplicaciones web. El Top 10 provee técnicas básicas sobre cómo protegerse en estas áreas de alto riesgo, y también orienta sobre los pasos a seguir.

La Figura 1 muestra los riesgos más comunes en las aplicaciones web definidos en la versión Top 10

de 2017, última versión publicada, haciendo una comparación con los definidos en la primera versión del Top 10 publicada en 2013.

A1:2017 – Inyección. Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios, o acceda a los datos sin la debida autorización.

A2:2017 – Pérdida de autenticación. Las funciones de la aplicación relacionadas con la autenticación y la gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer a usuarios y contraseñas, *token* de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).

A3:2017 – Exposición a datos sensibles. Muchas aplicaciones web y *APIs* no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.

A4:2017 – Entidades externas XML (XXE). Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, así como también para escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).

A5:2017 – Pérdida de control de acceso. Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, y para ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etcétera.

A6:2017 – Configuración de seguridad incorrecta. La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, *ad hoc* o por omisión (o directamente por la falta de configuración). Son ejemplos: *buckets* abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, *frameworks,* dependencias y componentes desactualizados, etcétera.

A7:2017 – Secuencia de comandos en sitios cruzados (XSS). Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario, utilizando una API que ejecuta *JavaScript* en el navegador. Permiten ejecutar comandos en el navegador de la víctima, y el atacante puede secuestrar una sesión, modificar *(defacement)* los sitios web o redireccionar al usuario hacia un sitio malicioso.

A8:2017 – Deserialización insegura. Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos, que pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.

A9:2017 – Uso de componentes con vulnerabilidades conocidas. Los componentes como bibliotecas, *frameworks* y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos.

A10:2017 – Registro y monitoreo insuficientes. El registro y el monitoreo insuficientes, junto a la falta de respuesta ante incidentes, permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros y no por procesos internos.

1.2. El Proyecto Estándar de Verificación de Seguridad de la Aplicación OWASP (ASVS)

El Proyecto Estándar de Verificación de Seguridad de la Aplicación OWASP (ASVS) es un esfuerzo comunitario por establecer un marco de referencia para los requisitos de seguridad, controles funcionales y no funcionales necesarios al diseñar, desarrollar y testear aplicaciones web modernas. Define tres niveles de verificación de seguridad, incrementando la profundidad con cada nivel.

- ASVS Nivel 1 (L1) se encuentra dirigido a todo tipo de software.
- ASVS Nivel 2 (L2) es para aplicaciones que contienen datos sensibles, que requieren protección.
- ASVS Nivel 3 (L3) es para las aplicaciones más críticas –aplicaciones que realizan transacciones de alto valor y requieren el más alto nivel de confianza.

Cada nivel ASVS contiene una lista de requerimientos de seguridad o controles. También cada uno de estos requisitos puede también corresponderse con funcionalidades específicas de seguridad

y capacidades que deben construirse por los desarrolladores de *software*. Se recomienda el Nivel 1 para toda aplicación, y el Nivel 3 para aquellos casos en que se podría poner en peligro la seguridad humana, o cuando una violación a la aplicación podría impactar seriamente y por completo a la organización.

Los requisitos definidos se agrupan en las siguientes temáticas: arquitectura, diseño y modelado de amenazas (V1), autenticación (V2), gestión de sesiones (V3), control de acceso (V4), manejo de entrada de datos maliciosos (V5), criptografía en el almacenamiento (V7), gestión y registro de errores (V8), protección de datos (V9), comunicaciones (V10), configuración de seguridad HTTP (V11), controles maliciosos (V13), lógica de negocio (V15), archivos y recursos (V16), móvil (V17), servicios web (V18), configuración (V19).

A juicio de los autores del presente trabajo, el sector bancario puede beneficiarse de la adopción del Proyecto Estándar de Verificación de Seguridad de la Aplicación OWASP (ASVS), eligiendo, según las características de la aplicación web desarrollada en la institución, la verificación de los requisitos establecidos para el Nivel 1 (L1), y refinar únicamente lo que se requiere para cada nivel de riesgo de la aplicación en un dominio específico. Es importante destacar que, aunque una gran mayoría de los requisitos establecidos en el Nivel 1 se puede verificar con herramientas automatizadas, el proyecto recomienda que no se utilice solamente la automatización, pues algunos controles se verifican aplicando la lista de chequeo definida.

1.3. Guía de Pruebas OWASP (OTG) 4.0

La Guía de Pruebas OWASP (OTG) ha sido desarrollada como proyecto durante muchos años, teniendo como objetivo ayudar a las personas a entender qué, por qué, cuándo, dónde y cómo de las pruebas de las aplicaciones web. Esta guía está estructurada con los siguientes aspectos: prerrequisitos de las pruebas de aplicaciones web y su alcance, los principios exitosos de pruebas y las técnicas de pruebas, el marco de pruebas de OWASP y sus técnicas y tareas en relación con las distintas fases del ciclo de vida del desarrollo de aplicaciones. Además, explica cómo comprobar vulnerabilidades específicas mediante inspección de código y pruebas de penetración.

1.3.1. Pruebas de seguridad de aplicaciones web a partir de OTG

Esta sección describe en la metodología OWASP las pruebas de seguridad sugeridas para las aplicaciones web y explica cómo evaluar para encontrar vulnerabilidades dentro de la aplicación, debido a las deficiencias de los controles de seguridad identificados durante el desarrollo de la aplicación. El proceso implica un análisis activo de la aplicación en busca de deficiencias, fallas técnicas o vulnerabilidades. Cualquier problema de seguridad que se encuentre, OWASP propone que sea presentado al propietario del sistema, junto con una evaluación del impacto y propuesta de mitigación o solución técnica.

El objetivo de este proyecto es recoger todas las técnicas de pruebas posibles, explicar estas técnicas y mantener la guía actualizada. El método de pruebas de seguridad de aplicaciones web OWASP se basa en el enfoque de Caja Negra.

El evaluador no sabe nada o tiene muy poca información sobre la aplicación a probar.

La prueba se divide en dos fases:

- *Fase 1. Modo pasivo:*

  En el modo pasivo, el evaluador intenta comprender la lógica de la aplicación y juega con la aplicación. Se pueden utilizar herramientas para la recopilación de información. Por ejemplo, un *proxy* HTTP puede ser utilizado para observar todas las solicitudes y respuestas HTTP. Al final de esta fase, el evaluador debe comprender todos los puntos de acceso (puertas) de la aplicación (por ejemplo, encabezados HTTP, parámetros y *cookies*). La sección Recolección en el documento Guía de Pruebas de OWASP explica cómo realizar una prueba de modo pasivo.

- *Fase 2. Modo activo:*

  En esta fase, el evaluador empieza a probar, utilizando la metodología. El conjunto de pruebas activas se divide en 11 categorías para un total de 91 controles:

  - Recopilación de información.
  - Pruebas de gestión de configuración e implementación.
  - Pruebas de gestión de identidad.
  - Pruebas de autenticación.
  - Pruebas de autorización.
  - Pruebas de gestión de sesión.
  - Pruebas de validación de ingreso.
  - Manejo de errores.
  - Criptografía.
  - Pruebas de lógica del negocio.
  - Pruebas del punto de vista del cliente.

La metodología recomienda utilizar una herramienta como interceptor del *prozy*, por ejemplo, OWASP *Zed Attack Proxy* (OWASP ZAP).

2. PROCEDIMIENTO DEFINIDO PARA REALIZAR PRUEBAS DE SEGURIDAD EN EL SECTOR BANCARIO

Para desarrollar el siguiente trabajo, se decidió utilizar las herramientas representadas con la última actualización de vulnerabilidades publicadas, el *Acunetix* WVS 10.0 y el *Zed Attack Proxy* 2.6.0 (ZAP), para verificar los mecanismos de protección cons-

truidos ante respuesta a una penetración impropia en los sistemas utilizados en el Banco Popular de Ahorro (BPA). El *Acunetix* permite verificar muchas de las vulnerabilidades definidas en el Top 10 y es muy fácil de aplicar. El *Zed Attack Proxy* 2.6.0 es la herramienta predefinida por OWASP para realizar las pruebas de seguridad.

Se recomienda aplicar las pruebas en el siguiente orden:

- Verificación de los aspectos definidos en el Proyecto Estándar de Verificación de Seguridad de la Aplicación OWASP (ASVS). Esta lista de chequeo se recomienda aplicarla desde el inicio del desarrollo del software para que el desarrollador de la aplicación o el analista tengan en cuenta los aspectos recomendados que debe tener el software en el sector bancario, de acuerdo con la experiencia de expertos internaciones y la complejidad del software que se realiza.
- Aplicación de la herramienta Acunetix. En el Anexo 2 se especifica el manual de usuario del uso de la herramienta. Se recomienda realizar la prueba de seguridad y documentar los resultados a partir del reporte especificado por el propio Acunetix. Una vez que se corrijan las no conformidades, se recomienda realizar las pruebas de regresión para verificar si en el proceso de corrección no se introdujeron nuevas no conformidades. Esas pruebas pueden realizarse también con el Acunetix.
- Aplicación de la Guía de Pruebas OWASP (OTG) 4.0 con las técnicas y herramientas especificadas a continuación:

Utilizar la herramienta *Zed Attack Proxy* 2.6.0 (ZAP), una de las más potentes del programa *OWASP,* que tiene las principales características:

- Totalmente gratuita y de código abierto.
- Multiplataforma.
- Fácil de instalar, dependiendo únicamente de Java 1.7 o superior.
- Posibilidad de comprobar todas las peticiones y respuestas entre cliente y servidor.
- Puede ayudar a encontrar automáticamente vulnerabilidades de seguridad en las aplicaciones web. Es también una herramienta para la realización de pruebas de seguridad de forma manual.
- Posibilidad de asignar un sistema de prioridades.
    - (Puede ejecutarse en 4 modos: seguro, protegido, estándar y ataque, y en dependencia del modo seleccionado, se realizan las pruebas deseadas).

Utilizar el FoxyProxy 4.5.6 como *proxy* de intercepción, que es un *plugin* de *Firefox* que facilita el intercambio de proxys en el navegador. El *FoxyProxy* se recomienda utilizar para el estudio de las peticiones y respuestas HTTP, resultando necesario interceptar el flujo de mensajes que se establecen entre el navegador y la aplicación web, pues hacer estas configuraciones manuales es un proceso bastante engorroso.

Utilizar los *plugin* de *Firefox HttpRequester* 2.2, que permite manipular peticiones HTTP directamente en el navegador y el *Wappalyzer* para identificar cuáles son las tecnologías utilizadas en la creación de las aplicaciones web, mostrándolas de forma transparente. De este modo, podemos ver si las aplicaciones utilizan algún CMS, *framework*, API, etcétera.

2.1. Políticas a seguir para la realización de las pruebas de seguridad automatizadas

Para realizar las pruebas de seguridad, se definen las siguientes políticas o medidas de seguridad:

- Montar un entorno de prueba para hacer las pruebas de seguridad automatizadas.
- Utilizar las herramientas que permiten realizar las pruebas de seguridad automatizadas por los especialistas de seguridad informática o desarrollador del *software*, con previa autorización por escrito del jefe del Departamento de Protección, Seguridad y Defensa, y del jefe del Departamento de Informática.
- Una vez realizada la prueba de seguridad, se deben documentar los resultados como prueba de la revisión realizada y de las no conformidades detectadas.
- Realizar pruebas de regresión de la aplicación para comprobar que las no conformidades identificadas fueron eliminadas y no fueron introducidas otras en el proceso de corrección de las mismas.
- Dar seguimiento de no conformidades hasta erradicarlas.
- Instalar solamente la aplicación de verificación de seguridad cuando se ejecuten las pruebas al software.

3. RESULTADOS OBTENIDOS, UNA VEZ REALIZADAS LAS PRUEBAS

Las pruebas de seguridad definidas fueron aplicadas a uno de los sistemas utilizados en las entidades del BPA. Por motivos de seguridad, no se menciona su nombre. Esta aplicación se encontraba desarrollada al 100% y en uso, por lo que no se pudo aplicar la lista de chequeo definida en el Proyecto Estándar de Verificación de Seguridad de la Aplicación OWASP (ASVS).

Con el *Acunetix* fueron identificadas 84 vulnerabilidades, y 80 se definieron como válidas, agrupadas en categorías: 57 altas, 10 medias, 7 bajas y 6 de información.

Se identificaron vulnerabilidades que permitirían:

- Realizar posibles ataques de inyección SQL.
- Existencia de formularios en páginas con redirección, lo que podría permitir a un atacante obtener información de los mismos.

- Realizar ataques de denegación de servicios, obtención de la información de las *cookies*, obtención de información del servidor web, errores que muestran información sensible, formularios sin protección ante ataques cruzados, contraseñas enviadas en texto plano y acceso a archivos de configuración del servidor.

Problemas de seguridad identificados:

- Se encontraron problemas con las secciones que permitió burlar los mecanismos de autenticación.
- Mediante Inyección SQL, el *Acunetix* permitió cambiar datos importantes como las contraseñas de los usuarios, lo cual impidió acceder a la aplicación.
- La prueba eliminó los datos de una tabla de la base de datos, utilizando funcionalidades del propio *Acunetix*.

Una vez corregidas las no conformidades encontradas mediante la herramienta *Acunetix Web Vulnerability Scanner*, se aplicaron las técnicas mencionadas anteriormente, especificadas en la Guía de Pruebas *OWASP (OTG) 4.0*, con la herramienta *Zed Attack Proxy (ZAP)*. En estas pruebas se detectaron algunas vulnerabilidades, lo cual demuestra que, una vez terminado un proceso de pruebas, no significa que el *software* esté libre de defectos, sino que la aplicación es más segura, una vez revisada.

A continuación, se muestran las vulnerabilidades halladas:

- Divulgación de error de aplicación, de clasificación media. Esta vulnerabilidad identifica la existencia de un mensaje de error o advertencia que puede divulgar información confidencial, como la ubicación del archivo que produjo la excepción no controlada. Esta información puede usarse para lanzar ataques adicionales contra la aplicación web.
- El encabezado *X Frame Options* no está configurado, de clasificación media. Encabezado *X-Frame-Options* no estaba incluido en la respuesta HTTP para proteger contra los ataques de '*ClickJacking*'.
- *Cookie* sin bandera *HTTPOnly,* de clasificación baja. Fue configurada una *cookie* sin el indicador *HttpOnly*, lo que significa que se podría acceder a la *cookie* mediante *JavaScript*. Si se puede ejecutar un *script* malicioso en esta página, entonces se podrá acceder a la *cookie* y se podrá transmitir a otro sitio. Si se trata de una *cookie* de sesión, puede ser posible el secuestro de la sesión.
- Contraseña autocompletada en el navegador, de clasificación baja. El atributo AUTOCOMPLETE no estaba deshabilitado en un elemento HTML FORM/INPUT que contenía entrada de tipo de contraseña. Las contraseñas podrían almacenarse en navegadores y recuperarse.
- Navegador web Protección XSS no habilitada, de clasificación baja. En el navegador web, la protección XSS no estaba habilitada, o estaba desactivada por la configuración del encabezado de respuesta *HTTP 'X-XSS*-Protección' en el servidor web.
- El encabezado *Anti-MIME -Sniffing*-X-*Content-Type-Options* no se configuró en '*nosniff*', de cla-

sificación baja. Esto permitía a las versiones anteriores de *Internet Explorer* y *Chrome* realizar el rastreo de MIME en el cuerpo de la respuesta, lo que puede causar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado.

CONCLUSIONES

- Fue definido un procedimiento para la realización de pruebas de seguridad automatizadas para aplicaciones web, que incluye: riesgos más críticos que afectan a las mismas, manual de uso de las herramientas, políticas de seguridad o medidas para la realización de este tipo de actividad. También se demostró la efectividad del uso de la herramienta *Acunetix* y Zed Attack Proxy en este tipo de pruebas.
- Se verificaron los mecanismos de protección construidos ante respuesta a penetraciones impropias de la aplicación X que está en uso en el Banco Popular de Ahorro, lo cual permitió conocer vulnerabilidades existentes en la misma e inmediatamente proyectarse en la corrección de las no conformidades encontradas.
- En el ámbito bancario se aplicaron algunas técnicas para realizar pruebas de seguridad definidas en los documentos "Guía de Pruebas OWASP (OTG) 4.0" y el "Estándar de Verificación de Seguridad en Aplicaciones (ASVS) 3.0.1", para contribuir a mejorar las prácticas de realización de este tipo de pruebas en el sector.
- La realización de nuevas pruebas de seguridad a una aplicación probada anteriormente con la herramienta *Acunetix Web Vulnerability Scanner* demostró que, para encontrar la mayor cantidad de defectos en el software, es importante aplicar variadas técnicas de prueba, ya que, aunque se encontraron vulnerabilidades de menor impacto con el ZAP, se demuestra que la aplicación aún era vulnerable.
- Se obtuvo un procedimiento genérico que permite realizar pruebas de seguridad automatizadas en cualquier aplicación web.

RECOMENDACIONES

Se recomienda examinar la lista de chequeo definida en el MIP del Banco Popular de Ahorro para la revisión de las aplicaciones, con el propósito de incorporar algunos aspectos definidos en el "Estándar de Verificación de Seguridad en Aplicaciones (ASVS) 3.0.1", los cuales pueden ser muy útiles para evaluar niveles de seguridad de un *software* por temáticas definidas.

Se recomienda incorporar en el MIP del BPA el uso del *Zed Attack Proxy* (ZAP) como otra herramienta posible de utilizar para las pruebas de seguridad en las aplicaciones web.

Bibliografía

- Barrio, J. F. (2010). La calidad de las aplicaciones.
- DSA (2013). DSA Distribuidora de productos antivirus. https://dsav.net/wp-content/uploads/2013/02/Acunetix-WVS- castellano.pdf
- IEEE (1990). Standard Glossary of Software Engineering Terminology.
- IEEE (1997). Standard Glossary of Software Engineering Terminology. 1997.
- Lineamientos de la Política Económica y Social del Partido y la Revolución para el periodo 2016-2021. Julio de 2017. Cuba.
- OWASP (2014). Guía de Pruebas OWASP (OTG) 4.0. The OWASP Foundation.
- OWASP (2016). OWASP Top 10 Proactive Controls 2016, 10 Critical Security Areas That Web Developers Must Be Aware Of. Open Web Application Security Project (OWASP).
- OWASP Top 10 (2017). Los diez riesgos más críticos en aplicaciones web.
- Pressman, R. S. (2002). Ingeniería del software, un enfoque práctico.

*** Especialista en Seguridad Informática y Especialista en Ciencias Informáticas de la Dirección Provincial del BPA de Sancti Spíritus, respectivamente**

Sistema para el registro y control del estado de las tarjetas magnéticas y pines

Lic. ROBHIL BARCIA SARDIÑAS e Ing. MÓNICA SÁNCHEZ ROCA*

(TRABAJO QUE RECIBIÓ MENCIÓN EN EL EVENTO CIENTÍFICO DEL SISTEMA BANCARIO NACIONAL "RAÚL LEÓN TORRAS" 2018, CELEBRADO EN LA HABANA)

El presente trabajo propone una solución a la problemática del control del estado de las tarjetas magnéticas por parte de todas las entidades que intervienen en el ciclo de vida de las mismas, desde su impresión en REDSA hasta que son entregadas al cliente o destruidas.

Para el análisis se toma como punto de partida el papel que desempeñan las instituciones financieras cubanas en el proceso de implementación de los Lineamientos de la Política Económica y Social del Partido y la Revolución, y de actualización del modelo económico, haciendo énfasis en lo relacionado con el proceso de informatización de la sociedad cubana.

Además del registro y control de las tarjetas magnéticas, el sistema informático propuesto emitirá los reportes necesarios para cada una de las entidades que intervienen en el proceso, desde REDSA hasta la sucursal.

Para la implementación del sistema se utilizó *SQL Server 2012*, *Visual Studio 2013*, utilizando el *framework ASP.NET MVC* y *Bootstrap 3.0*.

En el XV Aniversario del Palacio Central de Computación, celebrado el 7 de marzo de 2006, Fidel expresó: "*La informática se convertirá en una poderosísima fuerza científica, económica e incluso política del país…*". Tal afirmación toma vigencia cada vez más a partir de la estrategia de informatización de la sociedad cubana. En todas las esferas de la sociedad se han dado pasos sólidos en este sentido; ejemplo de esto son los proyectos de la Red Cuba. A estos proyectos tributan varias instituciones del país, entre las pertenecientes al sistema bancario.

En la actualización de los Lineamientos de la Política Económica y Social del Partido aprobada en el 7mo Congreso del PCC en abril 2016, y respaldada por la Asamblea Nacional del Poder Popular en julio del mismo año, se hace referencia en el Lineamiento Nº 108 a la importancia de "*…Avanzar gradualmente, según lo permitan las posibilidades económicas, en el proceso de informatización de la sociedad, el desarrollo de la infraestructura de telecomunicaciones y la industria de aplicaciones y servicios informáticos…*".

El Banco de Crédito y Comercio (BANDEC) está desempeñando un papel protagónico en el proceso de informatización de la sociedad, presentando sus nuevos servicios de banca electrónica, asociados al uso de las tarjetas magnéticas débito RED y las tarjetas Multibanca. La prestación de estos servicios con calidad constituye un reto, debido a que intervienen varias entidades en el proceso, y no existe una herramienta eficaz para el registro y control de cada uno de los estados por los que pasa la tarjeta, para brindar una información oportuna y veraz al cliente.

Actualmente, el proceso de registro y control de las tarjetas magnéticas presenta los siguientes inconvenientes:

- La sucursal no conoce el estado de la tarjeta para informar del mismo al cliente.
- El registro de la custodia de las tarjetas y pines se lleva de forma manual, lo que ocasiona demora y errores en el servicio.
- Ante una reclamación de las sucursales, la sucursal de medios de pagos electrónicos no tiene información exacta del momento del proceso en que se encuentra la tarjeta.

Teniendo en cuenta estos aspectos, el **problema** a resolver en este trabajo se centra en la necesidad de registrar y controlar el estado de las tarjetas magnéticas y pines de una manera veraz y eficaz durante todo el proceso.

Por todo lo anterior, el **objetivo** es desarrollar un sistema informático para el registro y control de las tarjetas magnéticas.

Para lograr cumplir este objetivo, se realizaron las siguientes tareas:

1. Estudio del Manual de Instrucciones y Procedimientos (MIP).
2. Análisis de todos los estados por los que transita la tarjeta magnética, desde su personalización hasta que la misma se entrega al cliente o se destruye en la sucursal.
3. Revisión de los antecedentes a este trabajo.
4. Diseño de la base de datos y el sistema propuesto.
5. Implementación del sistema propuesto.
6. Elaboración del manual de usuario.

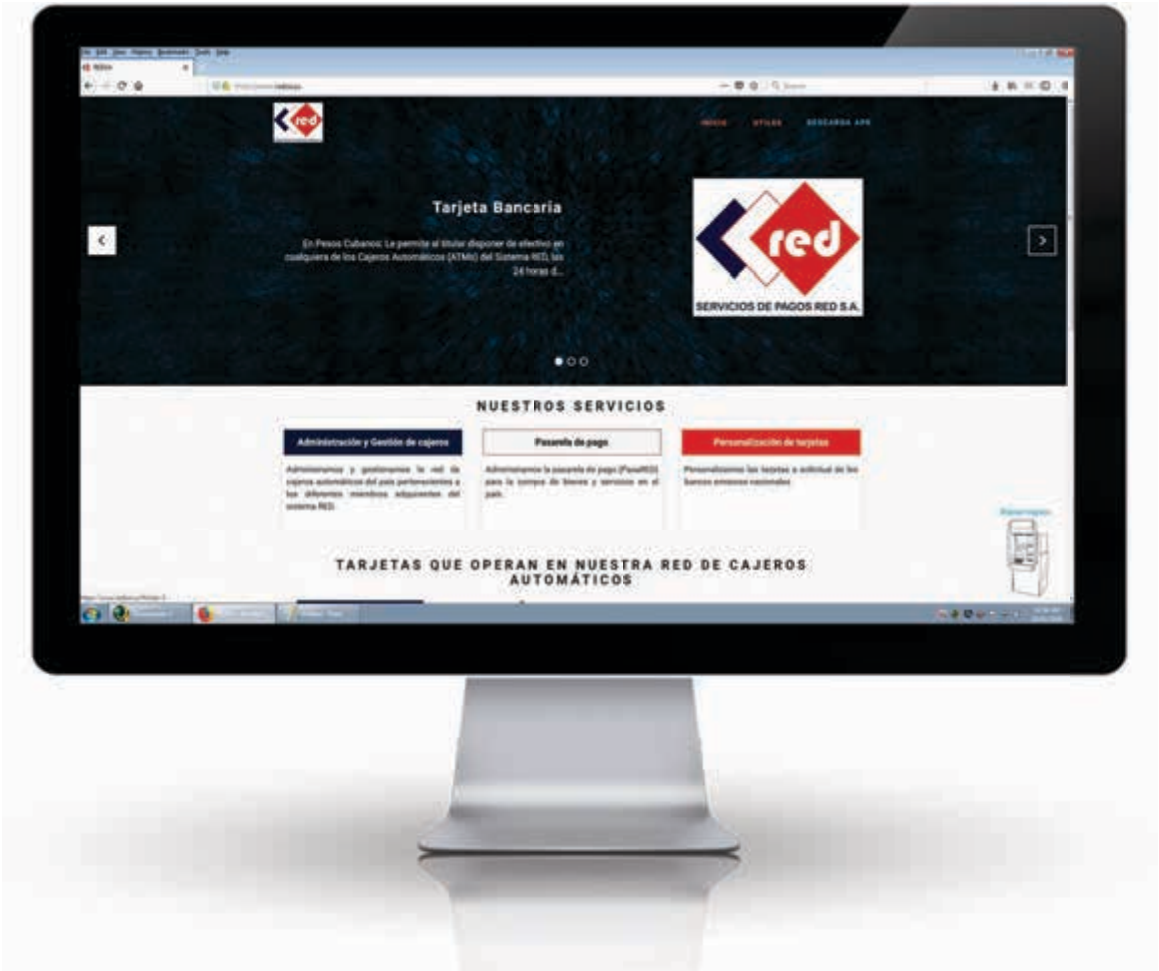
ANÁLISIS DE LA SITUACIÓN ACTUAL

A partir de 1995, en el Sistema Bancario Nacional (SBN) comienza una serie de transformaciones. En esa etapa fue significativa la introducción de equipamiento y sistemas informáticos en toda la red de sucursales. Esos fueron los primeros pasos para conseguir que nuestras instituciones financieras se caracterizaran por el alto grado de informatización de los servicios que actualmente brindan a sus clientes.

Las instituciones del SBN, específicamente el Banco de Crédito y Comercio, están comprometidas con el proceso de informatización de la sociedad cubana, participando activamente en proyectos que tributan a su desarrollo.

La introducción de una red de cajeros automáticos (ATM) y terminales de puntos de venta (POS) ha propiciado la masividad en el uso de las tarjetas magnéticas. Además de este instrumento de pago, se ha extendido el empleo de las tarjetas Multibanca, que conjuntamente con las tarjetas débito RED son necesarias para ser beneficiario de las bondades de los nuevos servicios desarrollados de los canales de pago, los cuales se introducen en nuestra institución y en el sistema bancario, en general. Estos canales de pago son las diferentes vías electrónicas que permiten al cliente efectuar consultas y operaciones de pago (por prestación de servicios, pago de impuestos, ejecución de transferencias, etc.) desde sus cuentas asociadas a tarjetas magnéticas, sin necesidad de personarse en la sucursal bancaria. Entre ellos se encuentran:

- Banca Telefónica (BANTEL).
- Virtual BANDEC (Banca Remota para personas jurídicas y TCP).



- Kiosco (Banca Remota para particulares).
- Banca Móvil (Transfermóvil).
- Pasarela de Pagos.

Para lograr la excelencia a la que se aspira en la prestación de todos estos novedosos servicios, es necesario erradicar o minimizar las deficiencias que hoy se presentan, relacionadas con el proceso de registro y control del estado de las tarjetas magnéticas.

Este proceso que comienza con la personalización de las tarjetas y la orden a REDSA para la impresión de las mismas, y culmina con la entrega de la tarjeta al cliente, presenta algunas deficiencias que provocan errores y demora en las respuestas a los clientes, titulares de cuentas asociadas a tarjetas magnéticas. Algunos de los inconvenientes del proceso se describen a continuación:

- La sucursal tiene confirmación de la personalización de la tarjeta, pero no conoce el estado de la tarjeta en cada momento, para poder informarlo al cliente cuando lo solicita.
- Los registros de la custodia de las tarjetas y pines se llevan de forma manual, por lo que la búsqueda se hace muy engorrosa y lenta, debido al volumen de tarjetas existentes, lo cual provoca demora en el servicio y una mayor probabilidad de respuesta errónea al cliente.
- Ante una reclamación de las sucursales, la sucursal de medios de pagos electrónicos no tiene información exacta del momento del proceso en que se encuentra la tarjeta.

Por todo lo anterior y a solicitud de la Dirección de las Tecnologías de la Informática, Comunicaciones y Procedimientos de la Oficina Central de BANDEC, se decide realizar este trabajo.

Primeramente, se consultan los grupos 216 y 218 del MIP, que tratan los temas relacionados con las tarjetas débito RED y los canales de pago, respectivamente. Luego se hace un análisis de todos los estados por los que transitan las tarjetas magnéticas, desde su personalización hasta que la misma se entrega al cliente o se destruye en la sucursal.

Como referencia se toma el trabajo titulado "Control automatizado integral de gestión de tarjetas de bandas magnéticas", realizado en 2015 por el Lic. Cástulo Esteban Daudinot Chaveco, de la Sucursal 8351 del BANDEC en Santiago de Cuba. En esta presentación se hace un análisis detallado de la problemática planteada, y se propone como solución una herramienta para el control automatizado de las tarjetas magnéticas y pines por parte de la sucursal.

Teniendo en cuenta estos antecedentes, se diseña un sistema que permita la actualización de los estados de las tarjetas magnéticas y pines oportunamente, por cada una de las partes que intervienen en esta modificación, lo que permitirá conocer en cada momento la situación real de las tarjetas y pines, y actuar con más eficacia ante algún problema o reclamación de los clientes.

DESCRIPCIÓN DE LA SOLUCIÓN PROPUESTA

El sistema informático propuesto se ha desarrollado con *SQL Server 2012*, *Visual Studio 2013*, utilizando el *framework ASP.NET MVC* y *Bootstrap 3.0*. Esta tecnología de programación se aplica siguiendo las líneas de trabajo de la Oficina Central.

Está diseñado para todas las entidades que intervienen en el ciclo de vida de las tarjetas magnéticas RED, comenzando por la orden de impresión a REDSA, a partir de la personalización de las tarjetas en la sucursal de medios de pago electrónicos.

Asimismo, por ser imprescindibles las tarjetas multibanca para utilizar los canales de pago, se diseñó un módulo para su entrega de forma promocional.

Para la autenticación, se utiliza el mismo servicio web instalado en las sucursales para el Virtual BANDEC, en el cual se creó un método para validar el nivel de acceso del usuario que va a acceder al sistema, el que se hace contra la base de datos Sabic, utilizando las mismas credenciales ya creadas en este sistema. Además, se valida que la dirección IP, desde donde se está accediendo al sitio, esté en la misma subred del servicio web, para garantizar que los usuarios solo puedan acceder al sitio desde la sucursal a la que pertenecen.

Principales operaciones con tarjetas y pines

Las sucursales de BANDEC podrán conocer en cada momento el estado de las tarjetas y pines, teniendo la posibilidad de dar seguimiento a la situación de las mismas, al tener también la información de la valija en que recibirán las tarjetas, pines y la fecha en que estas fueron conformadas. También tendrán opciones para todas las operaciones con tarjetas magnéticas y pines, como la *Entrega individual* y la *Entrega a entidades,* las cuales irán cambiando los estados en que se encuentran.

Los estados por los que transitan las tarjetas y pines son:

Estado	Descripción
00	Ordenada la impresión a REDSA
01	Impresión realizada en REDSA
02	Enviada para la sucursal
03	Recibida valija
04	En custodia de la sucursal
05	Entregada al cliente
06	Entregadas a una entidad
07	Recibida de la entidad
10	Destruida
11	Tarjeta no recibida en valija

Mediante esta opción se haría la entrega de las tarjetas multibanca, solicitando el número de tarjeta Red del cliente y verificando que este no posea una multibanca. De esta forma, se le entregaría la multibanca al cliente, quedando asociado a la tarjeta red.

Reportes del sistema

Se han implementado varios reportes, y aún se trabaja para incluir otros de acuerdo con las necesidades de todas las áreas que intervienen en el proceso.

CONCLUSIONES

- Con la identificación de los inconvenientes presentes para el registro y control del estado de las tarjetas magnéticas y pines, se pudo diseñar un sistema que involucra a todos los actores del proceso.
- El sistema propuesto constituye una herramienta eficaz para conocer el estado de las tarjetas y pines en cada momento.
- La generalización del sistema propuesto a toda la red de sucursales de BANDEC redundará en una mejora en la prestación de los servicios asociados al uso de las tarjetas magnéticas.

RECOMENDACIONES

- Definir con REDSA lo relacionado con la conformación de valijas.
- Continuar trabajando en la implementación de reportes y consultas necesarias para los usuarios del sistema.
- Poner a prueba el sistema propuesto, para su posterior generalización.

* Administrador de Red, DAPRO, y Jefa del Departamento DRAPO, Cienfuegos, respectivamente

Propuesta del Modelo de supervisión y seguimiento de los financiamientos para clientes TCP Y OFGNE

Lic. MARÍA ELENA BORJAS ROMERO*

La política bancaria está dirigida a financiar las actividades por cuenta propia y otras formas de gestión, lo que demanda modificaciones a las disposiciones, instrucciones y nuevos diseños que cumplan con los lineamientos 37, 38, 77, 195 y 196 aprobados en el III Pleno del Comité Central del PCC, y respaldados por la Asamblea Nacional del Poder Popular en 2017.

Las instrucciones establecidas tienen como objetivo fundamental implantar los procedimientos generales que se aplicarán a los financiamientos que el Banco de Crédito y Comercio (BANDEC) apruebe a los trabajadores por cuenta propia (TCP), así como también a otras formas de gestión no estatal (OFGNE), que necesitan acceder a los recursos financieros, incluyendo una correcta supervisión a los mismos. Para ello se requiere un documento que recoja de forma factible la información necesaria, para que el trabajador bancario que da seguimiento al crédito realice la verificación.

Este trabajo propone un modelo abarcador, con elementos descriptivos del cliente y su negocio, como parte de los procesos de debida diligencia y de la evaluación del riesgo, con la comprobación visual del negocio o actividad comercial del cliente.

El trabajador bancario que hace la verificación supervisa la actividad comercial o negocio con los datos registrados por la institución financiera, relacionados con las actividades comercial y crediticia asociadas a este cliente, previstas desde las primeras visitas y entrevistas, así como en los términos y condiciones de los préstamos, análisis de riesgo, análisis financiero, garantías, entre otros, lo cual facilita el resumen integrador asentado en este modelo, contactando *in situ* un resumen visual y analítico de fácil aplicación para el que realiza la comprobación.

Esta investigación propone un modelo abarcador con elementos descriptivos del cliente y su negocio, como parte de los procesos de debida diligencia y de la evaluación del riesgo mediante la comprobación visual del negocio o de la actividad comercial del cliente, con el propósito de contribuir a desarrollar la recuperación y supervisión de los financiamientos otorgados.

Problema real. Deficiente control y recuperación de los créditos otorgados a TCP y OFGNE por parte del banco.

Problema científico. ¿Cómo contribuir al control, supervisión y recuperación de créditos otorgados a TCP y OFGNE por parte del banco?

Objetivo. Proponer el diseño de un modelo que permita la supervisión y el seguimiento de los financiamientos para TCP y OFGNE.

Objetivos específicos:

- Integrar sobre la base de un enfoque sistémico de debida diligencia, evaluación de los riesgos, situación financiera y de seguimiento del crédito con la actividad comercial propuesta, para mitigar una posible actividad ilícita.
- Sistematizar la legislación vigente que sustenta el trabajo.
- Analizar el resultado de la aplicación del modelo utilizado en esta investigación.
- Proponer un modelo que permita la supervisión y el seguimiento de los financiamientos para clientes TCP y OFGNE por parte de los gestores de negocio, supervisores y órganos colegiados del banco.
- Validar la aplicación de la propuesta.

Métodos:

Teóricos

- Análisis y síntesis. Permitirá determinar las partes del modelo propuesto y establecer relaciones entre ellas.
- Histórico lógico. Servirá para estudiar la existencia de modelos de este tipo, y sobre esta base elaborar una nueva propuesta superior.

Empíricos

- Encuestas.

Los métodos mencionados anteriormente permitirán obtener información para elaborar la propuesta y resolver el problema científico.

Población. Está conformada por 32 créditos a TCP y 6 gestores de negocios del BANDEC.

Muestra. Está compuesta por 12 créditos y 3 gestores del BANDEC.

El presente trabajo consta de tres epígrafes. En el primero se presenta una fundamentación sobre la base legal que sustenta el diseño de este modelo; en el segundo se analizan los métodos empíricos aplicados para recopilar la información necesaria acerca del objeto de investigación, y en el último se presenta la propuesta de un modelo que permita la supervisión y el seguimiento de los financiamientos para clientes TCP y OFGNE.

EPÍGRAFE 1
Fundamentación legal

Para dar cumplimiento a los objetivos de trabajo de 2018, en la Estrategia para la prevención y enfrentamiento a los presuntos hechos delictivos y manifestaciones de corrupción en el Banco de Crédito y Comercio, se plantea fortalecer las acciones dirigidas al enfrentamiento de los hechos y a la recuperación de los daños económicos, mediante la actuación inmediata, según corresponda, con la detección temprana de los hechos. Por eso se requiere una correcta supervisión y seguimiento de las relaciones comerciales que se establecen entre el banco y el cliente.

El Decreto Ley Nº 317 de 2014 y la Resolución Nº 51/13 del BCC establecen que la debida diligencia está orientada a prevenir y detectar las operaciones que se realicen para dar apariencia de legitimidad a cualquier activo, relacionadas con el lavado de dinero, sus delitos determinantes, el financiamiento al terrorismo y a la proliferación de armas y otros de similar gravedad. Para ello se debe tener en cuenta:

- Las prácticas y procesos establecidos para prevenir el uso indebido de los servicios bancarios intencionalmente o no.
- Las obligaciones de todos los que intervienen en la tramitación de operaciones financieras.
- Identificar y verificar la información del cliente y del beneficiario final, ya sean personas naturales o jurídicas.
- Monitorear las cuentas.
- Custodiar los registros sobre la identificación de clientes y transacciones, etcétera.
- Utilizar documentos, datos o información confiable de fuentes independientes.
- Realizar la debida diligencia continua de la relación comercial y examinar las transacciones llevadas a cabo a lo largo de esa relación.
- Asegurar conocimiento que tiene la institución financiera sobre el cliente y su actividad comercial.
- Determinar el perfil de riesgo, incluyendo la fuente u origen de los fondos, cuando sea necesario.
- Entender y cuando corresponda obtener información sobre el propósito que se pretende dar a la relación comercial.

Importancia del proceso de la debida diligencia

- Es la herramienta principal de trabajo del banco.
- Permite el conocimiento real del cliente.
- Corroborar la correspondencia entre lo que se conoce y la naturaleza de las operaciones realizadas.
- Realizar la debida diligencia continua de la relación comercial y examinar las transacciones llevadas a cabo a lo largo de esa relación.

Como parte de la base legal para el proceso de supervisión y seguimiento de los financiamientos para clientes TCP y OFGNE y para el ejercicio del trabajo por cuenta propia, se dictó: El Decreto-Ley Nº 289/2011 define los principios y procedimientos generales que regulan los créditos y otros servicios bancarios para las personas naturales. Para dar a conocer el alcance de esta ley y su ampliación en la Gaceta Oficial extraordinaria Nº 35 de 2018, hacemos referencia a lo legislado en sus artículos, según las interrogantes más comunes, como sigue:

¿A quiénes están dirigidos estos créditos? En el Capítulo I, Artículo 3, se establece que pueden acceder al crédito las personas naturales autorizadas a ejercer el trabajo por cuenta propia y otras formas de gestión no estatal.

¿Qué se puede financiar? En su Capítulo II sobre la concesión de los créditos, en el Artículo 8, se plantea que los créditos se otorgarán para financiar la compra de bienes, insumos y equipos, y para cualquier otro fin que contribuya al adecuado funcionamiento de la actividad.

¿Qué voy a depositar en mi cuenta bancaria fiscal? En el Capítulo IV. *Otros servicios bancarios*, Artículo 17, plantea las personas naturales autorizadas a ejercer el trabajo por cuenta propia… y las personas naturales autorizadas a ejercer otras formas de gestión no estatal, titulares de cuentas corrientes, depositan en ellas solamente los fondos obtenidos por las actividades autorizadas.

¿Está legislada la obligación de operar una cuenta bancaria? La Gaceta Oficial Nº 35 Extraordinaria del 10 de julio 2018, en su Decreto-Ley Nº 355, Artículo 18, establece la obligatoriedad de operar cuentas corrientes por estos sectores, planteando que las personas naturales autorizadas a ejercer el trabajo por cuenta propia y otras formas de gestión no estatal están obligadas a operar una cuenta corriente en una institución bancaria, a los efectos del control de las obligaciones tributarias, según los términos, límites, alcance y condiciones que disponga el ministro de Finanzas y Precios.

¿Están autorizados a ejercer el trabajo por cuenta propia los extranjeros? El Decreto-Ley Nº 356, Capítulo 2, Artículo 2, delimita que están autorizados a ejercer el trabajo por cuenta propia los ciudadanos cubanos y extranjeros residentes permanentes en Cuba, mayores de 17 años de edad, que cumplan los requisitos establecidos en la ley. La autorización para el ejercicio es personal e intransferible.

¿Pueden los jóvenes ejercer el trabajo por cuenta propia? Lo establecido en la Ley Nº 356 ampara la incorporación de manera excepcional de los jóvenes de quince (15) y dieciséis (16) años de edad al trabajo por cuenta propia, así como las condiciones que deben garantizarse a los jóvenes de diecisiete (17) y dieciocho (18) años de edad.

Otras obligaciones precisan que las personas naturales pueden ejercer el trabajo por cuenta propia de manera individual o como trabajador contratado por otro TCP, que está obligado a inscribirse en el Registro de Contribuyentes de la Oficina Nacional de Administración Tributaria y a afiliarse al Régimen Especial de Seguridad Social.

A su vez, los organismos rectores, incluido el BCC, tienen una función metodológica y de control, para lo cual se debe:

- Identificar y analizar los riesgos y vulnerabilidades de mayor relevancia.
- Indicar las acciones de control correspondientes.
- Informar al órgano correspondiente los indicios de operaciones sospechosas que se detecte en el control de las finanzas que ingresan al país y del pago por las entidades estatales relacionadas con el ejercicio del trabajo por cuenta propia.
- La entidad garante queda responsabilizada, al igual que el banco, de chequear el buen cumplimiento de las obligaciones del deudor.

Además de los elementos que define el Manual de Instrucciones y Procedimientos para la confección del Modelo de Supervisión a Financiamientos de TCP-OFGNE, se tuvieron en cuenta los siguientes aspectos:

- Importancia de la debida diligencia oportuna.
- Inconsistencia en el uso de los financiamientos.
- Insuficiente recuperación de los créditos otorgados en el sector que nos ocupa.
- Experiencias acumuladas de auditorías, del área comercial, ONAT, etcétera.
- Información contenida en el Modelo 114-130B "Conozca a su cliente-TCP".
- Términos y condiciones fijados en el Contrato de Financiamiento firmado con el cliente.
- Documentos archivados en el expediente de crédito correspondiente.
- Comprobación visual del negocio o de la actividad comercial del cliente.

EPÍGRAFE 2
Análisis de los métodos e instrumentos utilizados

Para realizar este trabajo, se utilizaron entrevistas como métodos empíricos, las cuales fueron aplicadas a gestores y directivos del sistema bancario.

Encuesta

La encuesta aplicada (ver Anexo 1) muestra los siguientes datos:

Los encuestados plantean que no existe un modelo que integre los datos de las personas naturales con los datos de los financiamientos, que permita un óptimo seguimiento por parte del personal bancario que necesita comprobar cómo se emplean esos financiamientos. Por eso se puede decir que este planteamiento argumenta la propuesta dada.

También expresan que este modelo recoge en síntesis los elementos necesarios referidos en las legislaciones vigentes y en los manuales del banco, que les permite una adecuada orientación como supervisores, al contar con los datos personales, la situación crediticia, financiera, legal y de riesgo, más los análisis realizados en el Comité de Crédito, lo cual facilita una visión sistémica de la relación comercial establecida entre el financiado y el prestamista.

Los entrevistados consideran incluir en el Manual de Instrucciones y Procedimientos el empleo de este Modelo de supervisión y seguimiento de los financiamientos a clientes TCP-OGFNE, y confirman su utilidad como herramienta en los procesos de la debida diligencia en el Banco de Crédito y Comercio.

Además, piensan que no están lo suficientemente preparados para supervisar los financiamientos sin una guía que recoja los elementos a verificar, tales como:

- Situación legal del cliente.
- Elementos del financiamiento en cuestión.
- Análisis de riesgo.
- Análisis financiero.
- Asentar los datos de la comprobación visual.

Diagnóstico general

El estudio de aplicación de los métodos facilitó llegar al siguiente diagnóstico general.

- No existe un modelo que integre los datos de las personas naturales con los datos de los financiamientos otorgados.
- Falta de información para efectuar el seguimiento a los financiamientos otorgados por parte de los supervisores.
- Necesidad de una guía de supervisión que contribuya a verificar *in situ* los financiamientos, integrando debida diligencia, análisis de riesgos, situación financiera y acuerdos del Comité de Crédito.
- Incluir en el Manual de Instrucciones y Procedimientos un modelo integrador para el proceso de supervisión y seguimiento de los créditos otorgados por el banco.
- Preparar el sistema *Sabic.Nef* para que permita obtener esta información mediante un reporte, lo cual facilita una visión rápida del cliente y su historial financiero, crediticio y legal para dar el seguimiento oportuno en su localidad y en otros niveles.

EPÍGRAFE 3.

Propuesta del Modelo de Supervisión a Financiamiento del Trabajador por Cuenta Propia u OFGNE, que a continuación se muestra.

Supervisión a Financiamiento del TCP u OFGNE

Sucursal: (1)_____ Día_(2)_ Mes_(2)_ Año_(2)_

Relación de números de cuentas: (3)_____

Fiscal o de operaciones:		
Créditos:		
Otras:		

Nombres y apellidos: (4) _____ Edad__

Carné de Identidad: (5) _____ Serie: (6)_____

Nacionalidad: Cubana (7)_____Extranjera (7) _____ País (8)_____

Dirección de residencia: (9)_____

Teléfono fijo, móvil: (10)_____

Nº de Licencia del TCP o de Asociación: (11)_____

Inscripción en el Registro de Contribuyentes (Código NIT): (12)_____

Monto de la última declaración a la ONAT si corresponde: (13) _____

Inscripción en el Régimen Especial de Seguridad Social: (14) Sí __ No __
Situación legal del cliente: (15)_____

Dirección del local donde realiza su actividad: (16) _____

Teléfonos del local: (17)_____

Tipo de licencia: (18) _____

Existencia física de los inventarios y medios financiados:(19)

Sí _____No _____Parcialmente_____

Detallar:_____

Principales productos y/o servicios que produce y/o vende: (20)_____
_____

Principales proveedores y clientes: (21) _____

Importe mensual de pagos a trabajadores contratados: (22)_____

Objeto del crédito: (23) _____

Cumple con los términos y condiciones establecidos en el contrato de financiamiento: (24)

Sí ___No____ Parcialmente_____

Detallar:_____

Calificación de la situación financiera: (25)

Muy buena__ Satisfactoria __Buena ___Regular __Insatisfactoria___

Detallar:_____

Validez y calidad de las garantías: (26)

Muy efectivas __ Efectivas___ Poco efectivas___ No efectivas___

Detallar:_____

Comportamiento de los pagos: (27)

Muy Bueno__ Bueno __ Regular ____Insatisfactorio____

Probabilidad de incumplimiento del deudor: (28)

Mínima ___Baja __ Media ___Medio alta ___Alta ___Muy alta___

Clasificación de riesgo: (29) Mínimo __Bajo__ Medio __Medio-Alto__

Alto__ Alto-Irrecuperable__ Irrecuperable___

Utilización del financiamiento: (30)

Para otros fines_____ Fin aprobado_____

Detallar:_____

Causas que provoquen el deterioro financiero: (31)
_____

Renegociación: (32) _____ Reestructuración____

Detallar:_____

Acciones tomadas por los funcionarios de la sucursal: (33)
_____

_____ _____
Firma del cliente Funcionario que realiza la verificación

Fecha: (34) _____

Objetivos:

Detectar y prevenir dificultades financieras del cliente, conocer las características del negocio y la utilización del financiamiento, y corroborar las informaciones de nuestros clientes mediante las relaciones entre ellos y el banco. Asimismo, es aplicable también por los órganos colegiados de la sucursal, con el fin de informar al órgano correspondiente los indicios de operaciones sospechosas que se detecten en el control de las finanzas que ingresan al país.

Cumplimentación:

1. Sucursal donde se abre la cuenta.
2. Día, mes y año en que se cumplimenta el modelo.
3. Números de cuentas que serán supervisadas.
4. Nombres y apellidos del titular de la cuenta.
5. Carné de Identidad.
6. Nº de serie.
7. Nacionalidad: Definir si son ciudadanos cubanos o extranjeros residentes permanentes, según la ley.
8. País de origen en caso de extranjero.
9. Dirección particular del titular.
10. Teléfonos particulares del titular.
11. Número de la licencia como TCP.
12. Código de inscripción tributaria coincide con el CI.
13. Importe de los ingresos declarados en la ONAT, según corresponda (régimen simplificado o general).
14. Para conocer si está aportando la Seguridad Social a la ONAT.
15. Referir si el cliente está o tiene pendiente algún proceso penal, o se encuentra fuera del país; financiamientos en proceso de cobro judicial o en otras instituciones financieras.
16. Dirección particular del negocio o actividad.
17. Teléfonos del negocio o actividad.
18. Tipo de licencia referirse también a la actividad real del negocio.
19. Se refiere a si tiene medios financiados, da la oportunidad de detallar.
20. Se refiere a principales productos y servicios; da la oportunidad de detallar.
21. Referir si los clientes y proveedores son entidades jurídicas y/o naturales.
22. Importe aproximado del pago a los trabajadores, según contrato.
23. Objeto del financiamiento.
24. Se marca Sí o No en dependencia de si cumple con los términos de los financiamientos, da la oportunidad de detallar.
25. Para conocer en qué rango se encuentran los ingresos y en qué periodo de tiempo. Puede referirse a las causas que provoquen el deterioro financiero, da la oportunidad de detallar. Mip 238-85.
26. Referirse si está vigente la garantía y su calidad.
27. Para conocer si tiene plazos vencidos del financiamiento y el número de plazos pendientes.
28. Clasificación de riesgo de los activos crediticios de los TCP y OFGNE, de acuerdo con la situación del financiamiento.
29. Clasificación según lo establecido, puede ser:
    MÍNIMA: Probabilidad de incumplimiento: 0%.
    BAJA: Probabilidad de incumplimiento: 1-10%
    MEDIA: deudores cuyo flujo de fondos proyectado es insuficiente para cumplir con el cronograma de pagos pactado, o el análisis de la información demuestre deficiencias importantes que comprometen la solvencia del deudor. Probabilidad de incumplimiento: 11-20%.
    MEDIO ALTA: Presentan atrasos en los pagos. Probabilidad de incumplimiento: 21-30%.

ALTA: Difícil situación financiera, obliga a reestructurar. Probabilidad de incumplimiento: 31-50%.

30. Referirse si se usaron los financiamientos para el fin aprobado, da la oportunidad de detallar.
31. Referirse a las causas reales que provocaron el deterioro de los ingresos, de la operatividad de la cuenta o del negocio como tal.
32. Referir si el crédito está renegociado o reestructurado, da la oportunidad de detallar.
33. Las acciones definidas por el gestor, las del Comité de Crédito, sean de seguimiento, de ejecución de garantía, u otro que el analizador desee dejar constancia.
34. Fecha de la verificación al cliente.

Custodia:

- El modelo se archivará en el expediente, según corresponda con la relación establecida entre banco y cliente.

Conservación:

- Se conservará por la vigencia de la relación comercial entre el banco y el cliente TCP-OFGNE.

CONCLUSIONES

- El empleo de este modelo facilita la supervisión, control y recuperación de los financiamientos otorgados a clientes TCP-OFGNE.
- Emplear este modelo en los procesos de actualización de la debida diligencia.

RECOMENDACIONES

- Emplear este modelo por parte del banco, con el fin de ejercer supervisión a la relación comercial entre el TCP-OFGNE y nuestra institución.
- Incluir en el Manual de Instrucciones y Procedimientos un modelo integrador para el proceso de supervisión, control y seguimiento de los créditos otorgados por el banco.
- Implementar en el sistema *Sabic.Nef* la emisión de un reporte basado en los principios de este modelo, que facilita una visión rápida del cliente, su historial financiero, crediticio y legal, para dar el seguimiento oportuno en su localidad y a otros niveles.

Anexo. Encuesta a trabajador bancario

Estimado trabajador:

Con el objetivo de elaborar un modelo de supervisión que pueda emplear para el seguimiento, recuperación y control de los financiamientos otorgados, nos dirigimos a usted para conocer sus criterios y sugerencias sobre este tema, por lo que le pedimos su colaboración.

1. ¿Considera necesario un modelo actualizado, donde se integren todos los elementos referidos en el Manual de Instrucciones, que rigen el proceso de seguimiento y supervisión a los financiamientos, con el fin de sentirse más orientado, de acuerdo con sus necesidades de verificación y control?

   Sí _____ No _____

2. En la tabla siguiente marque con una cruz, según su criterio, cómo se reflejan las siguientes cualidades en los modelos existentes de seguimiento y supervisión de financiamientos:

	B	M	R
Cuentan con información suficiente para supervisar la utilización del financiamiento.			
Presenta un adecuado nivel de integración los datos que permiten verificar los créditos otorgados a TCP y OFGNE.			

3. ¿Necesita una guía o modelo actualizado, donde se integre todos los elementos referidos en el Manual de Instrucciones que rigen el proceso de verificación, con el fin de sentirse más orientado para supervisar los financiamientos?

   Sí _____ No _____

4. En la tabla que aparece a continuación, marque con una cruz, según su criterio, con qué elementos debe contar para verificar correctamente los financiamientos.

Elementos a verificar	**Sí**	**No**
Datos personales y del negocio		
Comportamiento de los pagos		
Si tiene plazos vencidos		
Presenta el cliente algún proceso penal o se encuentra fuera del país, financiamientos en proceso de cobro judicial o en otras instituciones financieras.		
Vigencia de la garantía y su calidad		

Bibliografía

- *El Decreto-Ley Nº 289 de 2011.*
- *Gaceta Oficial Nº 35 Extraordinaria de 10 de julio de 2018.*
- *Manual de Instrucciones y Procedimientos para la confección del Modelo de supervisión a financiamientos de TCP-OFGNE.*
- *Gaceta Oficial Nº 004 Extraordinaria de 21 de febrero de 2013.*
- *Circular Nº 1/2014 del BCC.*
- *Instrucción Nº 7/2011. Indicaciones a las entidades estatales para la contratación de los productos y servicios de los trabajadores por cuenta propia.*
- *Instrucción Nº 04/2016. BCC-Superintendente.*
- *Resolución Nº 60/11.*

*** Oficial de Cumplimiento de la Sucursal de BANDEC 7001 Maceo. Cacocúm, Holguín**

Pruebas de software: valoración de un procedimiento aplicado en Desoft Guantánamo

MSc. LOURDES AINTZANE DELGADO CORRONS,
Ing. ARLETHY BETANCOURT MATOS
e Ing. LIAN LISETTE HURTADO LINARES*

El objetivo de este trabajo es presentar un procedimiento para la realización de pruebas de *software*, detallado a continuación, que establece el proceder en la gestión de la calidad parcial de los productos desarrollados en la División Territorial Guantánamo. Este proceder puede ser utilizado en el sistema bancario o, al menos, extraer las ventajas, desventajas, buenas prácticas, entre otros aspectos.

En la actualidad, el proceso de desarrollo de *software* se ha vuelto controversial. Por tal motivo, es necesario un proceso que guíe a sus desarrolladores. En estos momentos existen diversas metodologías que permiten guiar el proceso de pruebas, pero en ocasiones no se ajustan a las características de las entidades o son muy complejas, entre otros factores. En el presente artículo se pretende valorar un procedimiento propuesto por Desoft Guantánamo y analizar la posibilidad de replicarlo en entidades bancarias. Además, es interés dar a conocer elementos de calidad del *software* que, en ocasiones, son poco conocidos en el sistema bancario, o la operatividad de trabajo no permite darles el espacio que requieren.

La metodología que seguía la empresa *Desoft* proporcionaba una guía de actividades y flujos de trabajo que organizaba el proceso de desarrollo de *software* en esta institución. Para manejar el enorme esfuerzo necesario para ejecutar un proyecto con esta metodología, es necesario dividirlo en iteraciones. Cada iteración del proceso (entregable realizado) toma como entrada el producto resultado de la iteración anterior y genera como salida un producto incrementado, que deberá ir verificando y validando cada iteración con el área de calidad y el cliente. Este proceso no se aplica a todas las divisiones; está centralizado por regiones (Occidente, Centro y Oriente), lo cual imposibilita medir el avance de la calidad en cada etapa del proyecto.

Por lo antes expuesto, surgió la necesidad de crear un procedimiento para realizar pruebas parciales en las diferentes iteraciones de desarrollo de *software*, con el fin de limar aquellas asperezas que puedan llegar a manos del usuario final, una vez terminado el producto solicitado.

En la industria del *software*, la construcción de sistemas va encaminada a productos cada vez más grandes y complejos. Con mucha frecuencia se hace necesario producirlos en un breve perio-

do de tiempo, bajo las especificaciones de los clientes. El mundo de la comercialización y de los negocios se vuelve cada día más competitivo y exige mayor calidad en el proceso de desarrollo y control de la ejecución de los proyectos de *software*. Es imprescindible el uso de las más modernas tecnologías de la informática para garantizar una mayor efectividad en los procesos de desarrollo de *software*.

Estas situaciones, aparejadas a la metodología de desarrollo implementada en las divisiones territoriales de la Empresa de Aplicaciones Informáticas, conllevaron implementar un mecanismo para controlar el avance con calidad de los proyectos en cada iteración, lo cual propicia que el producto llegue con un mínimo de errores a manos del usuario final. Esto es interesante, ya que, a partir de un método ágil, se logra crear un procedimiento para cubrir aquellas etapas que quedaban con menos atención.

Caracterización de la División Territorial Guantánamo

La Empresa de Aplicaciones Informáticas (Desoft) tiene un objeto enfocado a la informatización de la sociedad cubana, para ello se dedica fundamentalmente al desarrollo, comercialización, despliegue y soporte de *software*, aunque también trabaja líneas como: servicios de movilidad, la formación, la seguridad informática, entre otras. Está estructurada en divisiones territoriales y una Oficina Central en la capital, por lo que los especialistas y técnicos que en ella laboran se encuentran distribuidos por todo el país. En la División Territorial Guantánamo el grupo de desarrollo cuenta con 15 integrantes. La duración promedio de cada proyecto es de nueve meses, y cada equipo de desarrollo está integrado por tres especialistas cuando más. Las pruebas de aceptación se realizan al finalizar cada proyecto, según plantea la Metodología de Desarrollo de *Desoft* en su versión vigente 3.0. El grupo de calidad a nivel nacional se encuentra en la División Territorial Santi Spíritus, y solo revisa los proyectos que posean las características para formar parte de la cartera de productos de la empresa a nivel nacional. En tanto, los demás productos quedan a la merced del criterio de los clientes que, en muchas ocasiones, no saben expresar lo que quieren y firman las actas de aceptación sin analizar.

Procedimiento de pruebas

La realización de las pruebas no funcionales cumple un papel importante a la hora de comprobar la calidad de un producto de *software*, partiendo de la premisa de que, cuanto más se pruebe el producto y mientras más grande sea la gama de los tipos de prueba, más se logra un acercamiento a la calidad deseada. El presente documento sirve de guía para la revisión de la calidad de un producto; está confeccionado siguiendo las normas establecidas en la metodología para el desarrollo de un producto de *software* en la empresa *Desoft*. En él se detallan las etapas, los roles con sus responsabilidades, las herramientas y artefactos involucrados en cada etapa, los tipos de pruebas a realizar y el flujo de las no conformidades, una vez detectadas.

Alcance

Es aplicable a todas las áreas de desarrollo de las subdirecciones de Informatización y centros territoriales de servicios informáticos de las divisiones territoriales. A este procedimiento estarán sujetas las aplicaciones informáticas que constituyan desarrollo a la medida, así como aquellas que puedan o no formar parte de la cartera de productos. También es ajustable a entidades con características de infraestructura semejante, y que poseen equipos de desarrollo pequeños como muchos bancos e instituciones financieras.

Objetivo

- Definir los pasos a seguir y requisitos a cumplir para la revisión parcial de sistemas informáticos.
- Lograr que los productos se entreguen con niveles consistentes de calidad que cumplan con las expectativas de los clientes.
- Validar la funcionalidad de los módulos, sistemas e interfaces definidas dentro del alcance del proyecto.

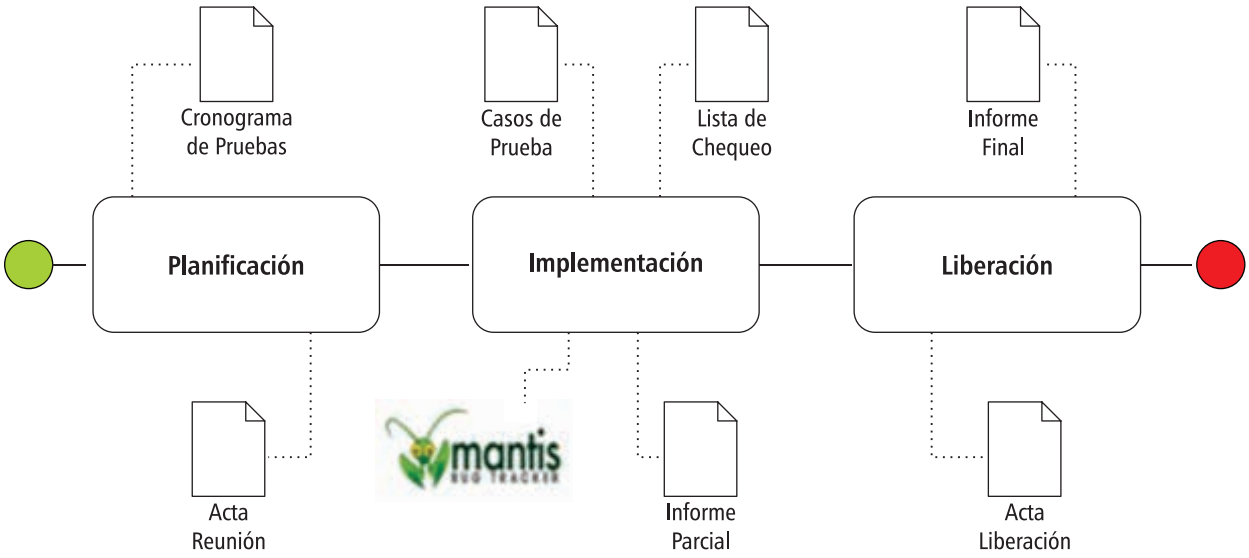
Términos y definiciones

SW – *Software*
HW – *Hardware*
GB – *Gigabyte*
RAM – *Random Access Memory*
NC – No conformidades
EPGD – Especialista Principal del Grupo de Desarrollo
EFC – Especialista en Funciones de Calidad
CP – Caso de Prueba

Etapas del procedimiento

El procedimiento de prueba de *software* integra un conjunto de actividades que describen los pasos que hay que llevar a cabo en este proceso, como son: la planificación, el diseño de casos de prueba, la ejecución y los resultados, tomando en consideración cuántos esfuerzos y recursos se van a requerir para obtener como resultado una correcta construcción del *software*. La siguiente figura describe gráficamente las etapas del procedimiento de pruebas.

FIGURA 1 Etapas del procedimiento.



Planificación

En esta etapa se reúne el Comité de Proyecto, donde se efectúa un intercambio entre todos los roles que intervienen en el proceso de pruebas. En cada reunión se confecciona un acta como evidencia de la misma, con una periodicidad mensual. También se analizan las etapas correspondientes, según los cronogramas de proyectos para decidir cuáles entrarán a revisión en el mes en cuestión. Las tareas a realizar en esta etapa son:

- Realizar Comité de Proyectos.
- Acordar con los desarrolladores cronograma de pruebas.
- Definir cantidad de inspecciones mensuales.
- Preparar ambiente de pruebas.

Implementación

El objetivo fundamental de esta etapa son las revisiones. Para ello, los desarrolladores entregarán al Especialista Principal de Desarrollo los casos de pruebas, que luego serán entregados al Especialista en Funciones de Calidad para procesarlos y proceder a revisar la aplicación, apoyándose en las listas de chequeo. Una vez concluido este proceso, se insertarán las no conformidades detectadas en la herramienta mantis para su posterior análisis y monitoreo. Además, al subdirector de Informatización se le informará sobre el estado del proceso mediante un informe parcial, una vez culminada cada inspección. Las tareas a realizar en esta etapa son las siguientes:

- Entregar los artefactos.
- Realizar las revisiones.
- Ejecutar los tipos de pruebas.
- Elaborar Informe Parcial de Pruebas.
- Monitorear no conformidades.

Liberación

En esta etapa se procede a cerrar las no conformidades resueltas, una vez confirmada a través de las pruebas de regresión por el Especialista en Funciones de Calidad. También se valoran las principales y más urgentes dificultades encontradas durante todo el proceso de pruebas por el subdirector de Informatización, de conjunto con el Especialista Principal de Desarrollo y el Especialista en Función de Calidad. Por último, se procede a liberar el producto. Las tareas a realizar en esta etapa serían:

- Realizar pruebas de regresión.
- Cerrar no conformidades.
- Liberar el módulo.
- Elaborar Informe Final de Pruebas.

Requisitos necesarios para la recepción del producto

Se creará un ambiente de pruebas, donde estará disponible la aplicación a revisar.

Se deberá hacer entrega de clave(s) personalizada(s), según los usuarios del sistema, y el expediente de proyecto, según la metodología de desarrollo en la etapa correspondiente.

Tipos de pruebas a realizar

Para garantizar el éxito de las inspecciones semanales, el Especialista de Calidad se apoyará en algunos tipos de pruebas que se especifican a continuación.

- *Pruebas exploratorias*

No son más que un proceso de exploración del producto, que valida la calidad de la entrega, donde se evaluarán los requisitos necesarios para su

recepción. De no cumplirse, las pruebas serán abortadas automáticamente.

- *Pruebas de integración*

Las pruebas de integración se llevan a cabo durante la construcción del sistema; involucran un número creciente de módulos y terminan probando el sistema como conjunto. Se prueban todos los módulos asociados. Se realizan con el fin de encontrar fallos en las interfaces entre el *software* y otros con los que interacciona.

- *Pruebas funcionales*

Evalúan el conjunto de características y capacidades de los componentes del sistema. Aseguran el trabajo apropiado de los requisitos funcionales, incluyendo la navegación, entrada de datos, procesamiento y obtención de resultados.

Función. Consiste en la revisión de las funcionalidades presentes en la aplicación (según Catálogo de Requisitos), fijando la atención en las validaciones, excepciones y servicios.

Seguridad. Asegurar que tanto los datos como el sistema solamente serán accedidos por los actores deseados, y cada uno con sus permisos específicos.

Se verifica lo siguiente:

- Que se aplique apropiadamente cada regla de negocio.
- Que los resultados esperados ocurran cuando se usen datos válidos.
- Que sean desplegados los mensajes apropiados de error y precaución, cuando se usan datos inválidos.

- *Pruebas de usabilidad*

Prueba enfocada a factores humanos, estéticos, ayuda sensitiva al contexto y en línea. Errores en la interfaz de usuario, como pueden ser: correspondencia entre sí, similitud en el prototipo, mismo tipo de letra, mismos tipos de botones, íconos, formato, visibilidad, navegabilidad, menús, colores, legibilidad, etcétera.

- *Pruebas de fiabilidad*

Recuperación y tolerancia a fallas. Verificar que los procesos de recuperación manual o automática restauran apropiadamente la base de datos, aplicaciones y sistemas, y los llevan a un estado conocido o deseado.

- *Pruebas de rendimiento*

Enfocadas a monitorear el tiempo en flujo de ejecución, acceso a datos, en llamada a funciones y sistema para identificar y direccionar los cuellos de botellas y los procesos ineficientes.

Contención. Enfocada a la validación de las habilidades del elemento a probar para manejar aceptablemente la demanda de múltiples actores sobre un mismo recurso.

- *Pruebas de portabilidad*

Configuración. Enfocada a asegurar que funciona en diferentes configuraciones de *hardware* y *software*. Esta prueba es implementada también como prueba de rendimiento del sistema.

Instalación. Enfocada a asegurar la instalación en diferentes configuraciones de *hardware* y *software* bajo diferentes condiciones, insuficiente espacio en disco, etcétera.

- *Pruebas de regresión*

Prueba enfocada a comprobar que las incidencias detectadas en una iteración previa fueron resueltas correctamente por el equipo de proyecto, para poder pasar a la siguiente iteración, en la que se comprobará que no se introdujeron errores, al corregir los encontrados anteriormente. El propósito de estas pruebas es asegurar que los defectos identificados en la ejecución anterior de la prueba se han corregido, y que los cambios realizados no han introducido nuevos defectos o reintroducido defectos anteriores.

- *Pruebas de sistema*

Asegura la apropiada navegación dentro del sistema, ingreso de datos, procesamiento y recuperación. Comprueba la implementación apropiada de las reglas de negocio.

- *Pruebas de valores límites*

Pruebas diseñadas para evaluar el manejo de error con valores límites o valores extremos. Si una condición de entrada está en un rango de valores entre A y B, se debe diseñar pruebas para los límites A y B, así como para los valores dentro de los límites y por encima de estos.

Herramientas para pruebas

- *Caso de prueba*

Son un conjunto de entradas, condiciones de ejecución y resultados esperados desarrollados para un objetivo particular. Se diseñan aplicando técnicas como las de caja blanca y caja negra. Se ejecutan en el *software*, siguiendo el caso de prueba, o se comparan las salidas obtenidas con los resultados esperados, con el fin de determinar si existe algún error. Cada caso de pruebas debe tener la identificación y el objetivo, la descripción detallada de las entradas, su modo de ejecución y la descripción detallada de las salidas esperadas.

Especifican la forma de probar el sistema, incluyendo las entradas, las precondiciones, la especificación de los actores que realizarán las pruebas y las condiciones bajo las cuales ha de probarse. Es un conjunto de entradas y resultados esperados aplicar, resumir y comparar. Su análisis es rápido, pues consiste en verificar si existe o no un control que es aplicable al objeto analizado.

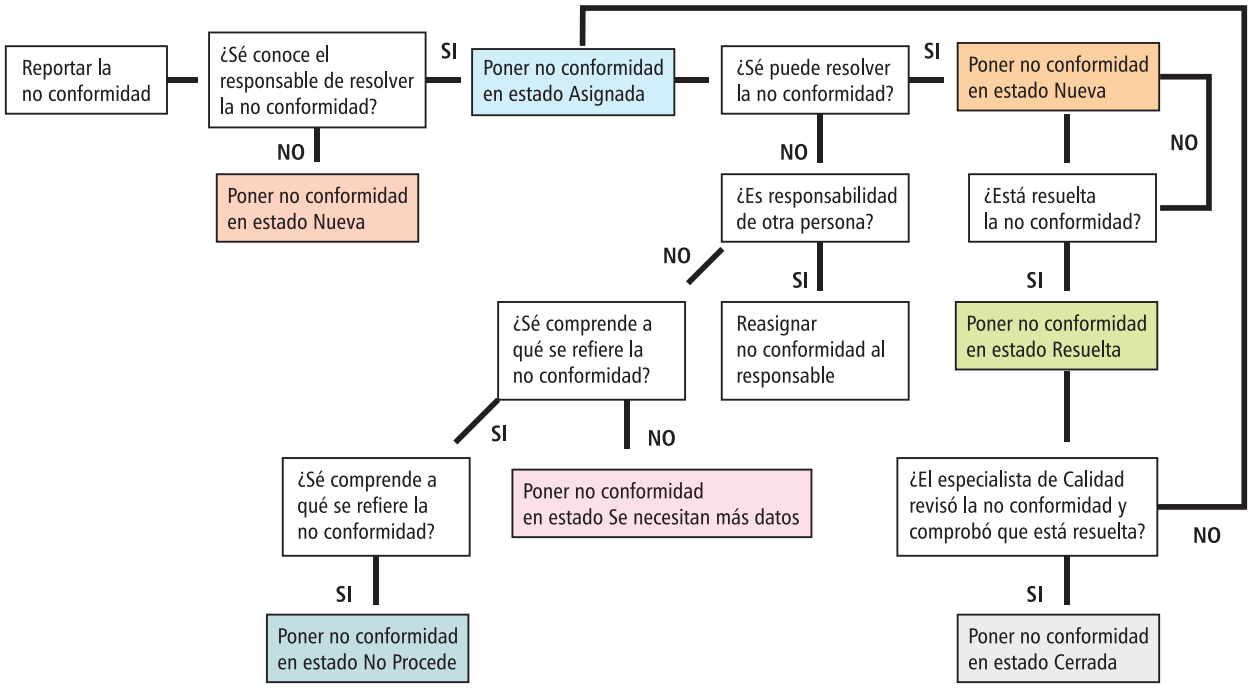
- *Informe de Pruebas*

Contiene la información acerca de la ejecución de las pruebas. Para cada caso de prueba, se debe especificar la salida obtenida, y de ser diferente a la esperada, documentar el error encontrado con el mayor nivel de detalle posible. Se debe entregar todos los viernes al jefe de la unidad administrativa, después de conciliado con el Especialista Principal del Grupo de Desarrollo.

- *Mantis Bug Tracker*

Mantis es un sistema de registro y control de no conformidades. El acceso a la aplicación, al ser de tipo Web, se realiza mediante un navegador. Mantis no tiene ninguna restricción al tipo de navegador que debe usarse para trabajar como cliente. El objetivo de Mantis es crear y mantener un sistema de

FIGURA 2 Flujo de las no conformidades en Mantis



Nota: En cada estado se pueden especificar tipos de resoluciones para argumentar y apoyar la selección del estado correspondiente.

Estado	Estado
Asignada	Abierta, Reabierta
Resuelta	Corregida
Se necesitan más datos	Abierta, Reabierta, No es Reproducible

que ejercitan un componente, con el propósito de causar fallas y detectar defectos.

- *Listas de chequeo*

Se define como un listado de preguntas en forma de cuestionario, que sirven para verificar el grado de cumplimiento de determinadas reglas establecidas *a priori* con un fin determinado. Son fáciles de

control de no conformidades, y está diseñado de manera que sea fácilmente modificable, personalizable y actualizable.

- *GitLab*

Es un servicio web de control de versiones y desarrollo de *software* colaborativo basado en Git. Además de gestor de repositorios, el servicio ofrece

también alojamiento de *wikis* y un sistema de seguimiento de errores, todo ello publicado bajo una licencia de código abierto.

- *Nas Desarrollo*

Herramienta ftp para el repositorio del código fuente y expedientes de proyectos.

Roles y responsabilidades

Especialista Principal de Desarrollo:

- Entregar al Especialista en Informática la documentación de los proyectos que van a ser revisados en cada etapa, previa revisión con los desarrolladores designados.
- Revisar y despachar con los desarrolladores las no conformidades detectadas en las diferentes etapas para cada uno de los proyectos, y tomar las medidas pertinentes.
- Tomar decisiones cuando existan discrepancia entre las partes implicadas en las revisiones.
- Enviar al subdirector de Informatización la relación de proyectos que serán revisados en cada etapa.

Especialista de Calidad:

- Revisar la documentación y aplicaciones recibidas del Especialista Principal.
- Entregar Informe de No Conformidades detectadas en la etapa correspondiente al Especialista Principal y al subdirector de Informatización.
- Subdirector de Informatización.
- Tomar decisiones estratégicas con respecto a los avances de los proyectos.

Estos roles se definieron en la investigación de *Desoft*, pero en su adaptación pueden ejecutarse por los cargos que se correspondan en el sistema bancario.

Flujo de trabajo

1. Acerca de la documentación que debe entregar el Especialista Principal del Grupo de Desarrollo (EPGD) al Especialista en Funciones de Calidad (EFC).
   a) El EPGD debe revisar los artefactos y documentos que le entregan sus especialistas, según sus respectivos avances. El artefacto principal que se necesita es el Caso de Prueba (CP) de cada proyecto a revisar. Además, se necesita acceso a cada módulo integrante de dichos proyectos. En su defecto, puede utilizarse el manual de usuario parcial, si existe.
   b) El EPGD entrega al EFC los artefactos que van a ser revisados a partir del lunes siguiente, y notifica de esta acción al subdirector de Informatización.
2. Acerca de las tareas del EFC.
   a) El EFC debe notificar al subdirector de Informatización que ha recibido o no los artefactos que va a revisar antes de que finalice la jornada laboral correspondiente al lunes.
   b) El EFC debe revisar los documentos de la metodología vigente para los proyectos de desarrollo y elaborar el Informe Parcial (IP), donde reflejará de manera expedita las no conformidades (NC) que encuentre. Las mismas serán introducidas en la herramienta *Mantis* para su posterior análisis y monitoreo.
   c) El EFC debe revisar los módulos que haya recibido y utilizar como base el CP recibido del EPGD, o en su defecto, el manual de usuario parcial correspondiente a dichos módulos.
   d) El EFC deberá elaborar el Informe Parcial (IP), donde, además de reflejar de manera expedita las funcionalidades con problemas, tendrá que incluir las pantallas que serán reflejadas en la herramienta *Mantis* para su posterior análisis y monitoreo.
3. Acerca de la entrega y discusión del Informe Resumen del EFC.
   a) El Informe Parcial (IP) deberá ser enviado por el EFC al EPGD en la tarde del viernes, luego de conciliado con el EPGD. Debe mandar una copia de dicho informe al subdirector de Informatización.
   b) Si al momento de la recepción del informe el EPGD encontrara NC que pudieran ser salvadas en no más de 1 día laborable, debe informarlo al subdirector de Informatización, para que este tome decisiones al respecto, y en caso de aprobarlo, notificarlo de inmediato al EFC.
   c) El EPGD deberá entregar al EFC los artefactos corregidos a más tardar al día siguiente de la decisión del subdirector de Informatización.
   d) Una vez confeccionada la versión definitiva de la revisión de calidad, el EFC deberá enviar por correo electrónico el Informe Final al EPGD y al subdirector de Informatización.
4. Acerca de las NC detectadas y su solución para la siguiente iteración de pruebas.
   a) El EPGD debe elaborar un plan de acción para el tratamiento de las NC y definir cuáles de las NC serán consideradas nuevamente para la revisión de calidad del siguiente periodo.
   b) Estas NC deben ser incluidas en los artefactos que entregará a EFC en el siguiente periodo.

Resultados

Con el propósito de respaldar la solución propuesta, se escogió un proyecto con el cual se validó la aplicabilidad del procedimiento. Cabe destacar que el proyecto nació junto con la idea de la solución. Sus revisiones se han realizado en un periodo de tres años. El procedimiento propuesto se aplica en las pruebas de *software* y tiene posibilidades de extender su uso en otras divisiones.

Conclusiones

En el actual mercado tan competitivo, solo los productos de calidad sobreviven. La calidad, aunque es una percepción subjetiva del cliente, nace en la filosofía de la empresa, que se esfuerza por ofrecer productos y servicios que superen las expectativas del cliente. Para ello, realizar pruebas del producto es un factor fundamental. Además, para aumentar las probabilidades de detectar errores, incluso menores, es importante que las pruebas las realice otra persona. No es secreto para nadie que es difícil que el que construye el *software* identifique los propios errores que comete. Por eso es fundamental utilizar herramientas avanzadas y personalizadas para la automatización y realización de pruebas de *software*, y contar con un equipo de probadores altamente calificados. Seguir un procedimiento ordenado para las pruebas de *software* mejora el proceso de desarrollo, y esta mejora redunda en beneficios para cualquier entidad.

Bibliografía

- ¿Qué son las metodologías agiles? Disponible en:http://blog.leanmonitor.com/es/que-son-las-metodologias-agiles/
- María Clara Choucair. Consultado el 10/2/2016, disponible en: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/XXVII_Salon_Informatica/MariaClaraChoucairPruebasDeSoftware.pdf
- Beneficios de aplicar metodologías agiles en el desarrollo de *software*. Disponible en: http://www.i2btech.com/blog-i2b/tech-deployment/5-beneficios-de-aplicar-metodologias-agiles-en-el-desarrollo-de-software/
- Metodologías agiles de desarrollo de software. Disponible en:http://danielgrifol.es/metodologias-agiles-de-desarrollo-de-software/
- Metodología para procesos de desarrollo de software v3.0.doc
- Jacobson, I. (*et. al*), El proceso unificado de desarrollo de software. Addison Wesley, Madrid, España, 2000.
- Carlos Blanco Bueno. Construcción y Pruebas de Software, 2011.
- Flores, Mariano. Aplicación de una metodología de dirección integrada de proyecto al Sistema Integrado de Gestión Empresarial en la Unión Eléctrica. (SIGEMETODO V1.0). Maestría EOI América-CENSAI. Mayo 2001.
- Moliner, E, Softmétodo V 1.0, Softcal, 2003.
- Rafael, M. Ingeniería del software. Metodologías de desarrollo, 05.02.2008.
- Patricio, L. T., Emilio, A. S. L. Metodologias ágiles en el desarrollo de Software.

* **Gerente de Sistemas del BCC, Ingeniera de la Empresa de Aplicaciones Informáticas Desoft de la División Territorial Guantánamo, e Ingeniera de la Empresa de Aplicaciones Informáticas Desoft de la División Territorial Sancti Spíritus, respectivamente**

Una solución para la seguridad perimetral de SABIC.NEF

Lic. DANIEL RAMOS RODRÍGUEZ e Ing. MARICET ESTÉVEZ FRESNEDO*

(TRABAJO QUE OBTUVO EL TERCER LUGAR EN EL EVENTO CIENTÍFICO DE BPA "RAÚL LEÓN TORRAS" 2018, Y MENCIÓN EN EL EVENTO CIENTÍFICO "RAÚL LEÓN TORRAS" 2018 DEL SISTEMA BANCARIO NACIONAL, CELEBRADO EN LA HABANA)

ANTECEDENTES, OBJETIVOS, HIPÓTESIS Y NUEVA PROYECCIÓN

Problema que resuelve la nueva versión

Todas las versiones del manual "*Una propuesta para la seguridad perimetral de SABIC.NEF*" están enfocadas en brindar una propuesta de solución a la siguiente interrogante: ¿Cómo mejorar la seguridad del sistema informático contable *SABIC.NEF* desde su entorno informático?

El OBJETIVO. Elaborar un manual técnico-metodológico como vía para dar respuesta a la interrogante anterior, que nos lleva a la HIPÓTESIS, donde la propuesta de seguridad perimetral para *SABIC.NEF* podrá mejorar la seguridad del sistema *SABIC.NEF*.

La versión 2.0 surge como una necesidad, a partir de cambiarse el entorno informático de SABIC, pues al migrarse los servidores de SABIC a plataformas de los sistemas operativos superiores a la anterior, el referido manual ya no se ajustaba a la interfaz y estructura lógica de los nuevos sistemas operativos.

La versión 2.0 está dirigida a implementarse en las plataformas *Windows Server* 2012 R2 en servidores de dominio y *Windows Server* 2008 R2 en servidores de Base de Datos. En algunos capítulos fue necesario incluir aspectos relacionados con la seguridad desde los servidores de comunicación, por ser el proveedor de las comunicaciones del SABIC, así como temas relacionados con la seguridad en las redes sociales, los navegadores Web, el espionaje y la recolección oculta de datos en las diferentes versiones de los sistemas operativos *Windows,* y otros temas que de forma directa o indirecta pudieran afectar la seguridad de nuestro Sistema Contable Financiero.

ESTRUCTURA GENERAL DEL MANUAL

La estructura general del manual está concebida como un paquete de 12 manuales independientes, donde cada uno de ellos forma un capítulo con un tema de seguridad diferente, interrelacionándose unos con otros en cuanto a los contenidos que abordan.

Para la aplicación de todos los capítulos que forman el manual, se elaboró una metodología sobre las medidas organizativas y logísticas necesarias para implementar y desplegar el Manual de Seguridad Perimetral en cualquier provincia.

ESTRUCTURA GENERAL DEL MANUAL. OBJETIVOS Y BASE LEGAL

La estructuración del manual en capítulos ha permitido concentrar en cada uno de ellos objetivos específicos de seguridad, en correspondencia con las buenas prácticas de seguridad informática y lo establecido por las normativas de la Base Legal con respecto a los temas que se abordan.

En cada capítulo se hace referencia de manera clara a la Base Legal que se le da cumplimiento, al implementarse el sistema de medidas técnicas que en el mismo se proponen.

ESTRUCTURA GENERAL DEL MANUAL. ESCALABILIDAD A CAMBIOS TECNOLÓGICOS

El formato y la nueva estructura del manual están concebidos para que sean escalables, o sea, que si en un futuro los servidores se migran a versiones de los sistemas operativos superiores, es muy fácil adaptar el contenido del manual a los nuevos requerimientos.

El manual crea las bases y principios de seguridad a tener en cuenta, si algún día el BPA decide migrar el Sistema Informático Contable a la plataforma Linux (Software Libre). Solo tendría que cambiarse el contenido de algunos capítulos, pero manteniendo los objetivos, las políticas, las medidas y la referencia a la Base Legal.

ESTRUCTURA Y CONTENIDO. INTERFAZ CON EL USUARIO

La nueva versión del manual se sustenta en el principio de que, para cada medida técnica que se orienta, se describe paso por paso, y se ilustra con imágenes o fotos la configuración que se propone. Además, se presentan los resultados en forma de imágenes (fotos) para que el administrador de la red pueda comprobar, medir y valorar los resultados obtenidos y los esperados.

ESTRUCTURA Y CONTENIDO. LA CAPACITACIÓN Y AUTOPREPARACIÓN DEL ADMINISTRADOR DE RED

La forma en que se encuentra estructurado el manual, y la profundidad y diversidad de los contenidos que se abordan, permiten a cada administrador de red apropiarse de nuevos conocimientos, profundizar en ellos y realizar propuestas de seguridad en correspondencia con las necesidades propias de seguridad de cada lugar.

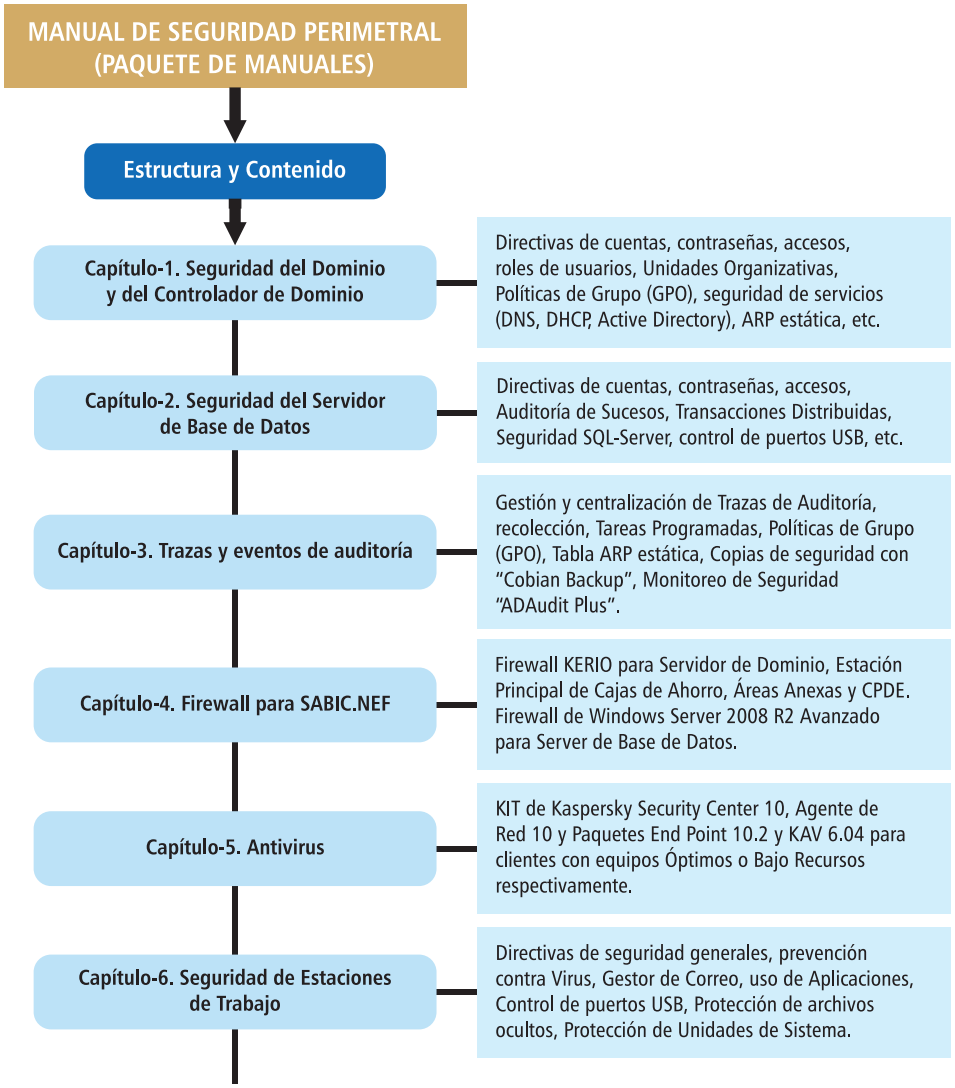
ESTRUCTURA Y CONTENIDO. EL CONTROL INTERNO Y LAS OBLIGACIONES DEL ADMINISTRADOR DE RED

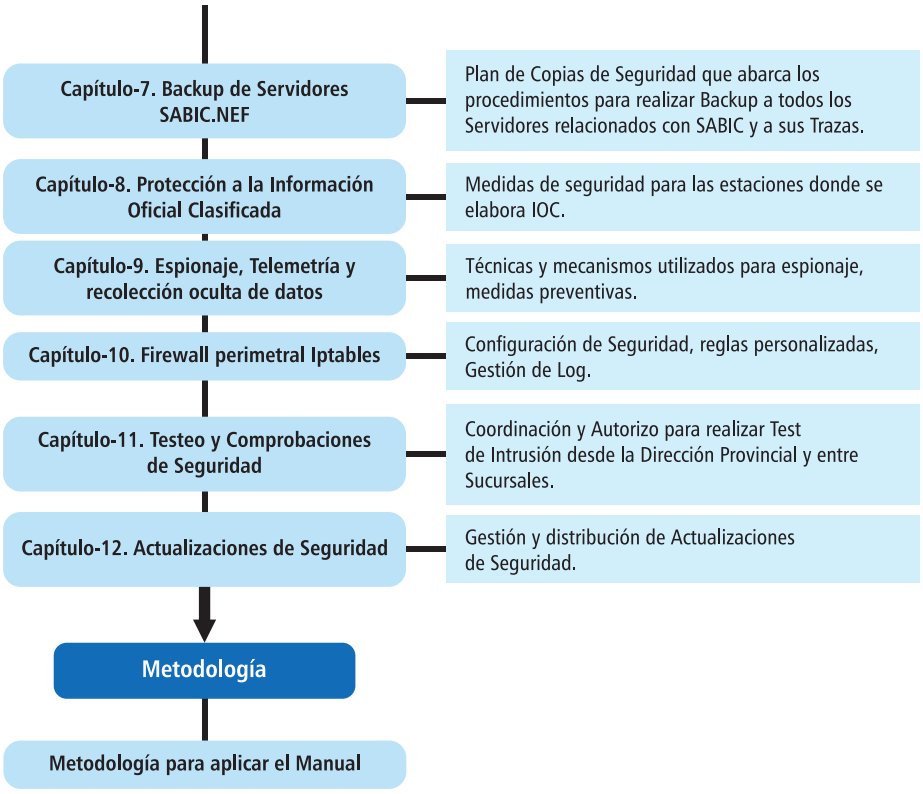
Las versiones anteriores de este manual han sido utilizadas como Guía de Control por especialistas de la seguridad informática, y como Guía de Auditoría en los programas de seguridad informática desarrollados por auditores.

Las medidas técnicas dirigidas a la recolección de trazas crean las condiciones necesarias para que el administrador de red pueda cumplir las obligaciones dispuestas en el Reglamento de Seguridad adjunto a la Resolución Nº 127/07 del MIC, así como muchas de las funciones y responsabilidades dispuestas en el MIP: 00-102-04.

LA NUEVA ESTRUCTURA ORGANIZATIVA

Una propuesta de seguridad para SABIC.NEF y una síntesis del contenido que trata cada capítulo:





ASPECTOS TÉCNICOS Y DE PROCEDIMIENTOS NUEVOS O MODIFICADOS

Capítulo 1. Seguridad del dominio y del controlador de dominio

- Windows Server 2012 R2 Standard.
- Estructura organizativa del directorio activo:
  Se garantiza que el grupo global *„Usuarios_sabic"* contenga a todos los usuarios y equipos de SABIC.
  > Se crea una unidad organizativa (UO) llamada *„SABIC"* la cual contiene a todos los usuarios y equipos de SABIC, excepto al usuario del administrador de la red.
  > Se implementa una GPO (Política de Grupo) a la UO *„SABIC"*, aplicándose políticas para:
  - No permitir cambiar fecha ni hora.
  - Restricción de software.
  - Se quita el menú *Opciones* de carpeta del menú *Herramientas*, garantizándose que los usuarios no puedan activar la opción de mostrar archivos y carpetas ocultos.
  - Se oculta la unidad de sistema (C:\).

  (Estos dos últimos aspectos son indispensables para proteger los eventos que se recolectan localmente en el *Shutdown*; se requieren aseguramientos que son abordados en el Capítulo 6)
  > Se impide a los usuarios compartir archivos y carpetas, quedando como único responsable el administrador de la red.
  > DHCP: reservaciones, exclusiones, máscara de subred ajustada, auditoría del servicio activada, filtro de MAC desde el propio servicio.
  > ARP: Tabla *arp* estática implementada por directiva en el *Startup* (Capítulo 3). *Firewall Kerio* activado. Puertos fijos para RPC y otros servicios (Capítulo 4). Otras modificaciones menos relevantes.

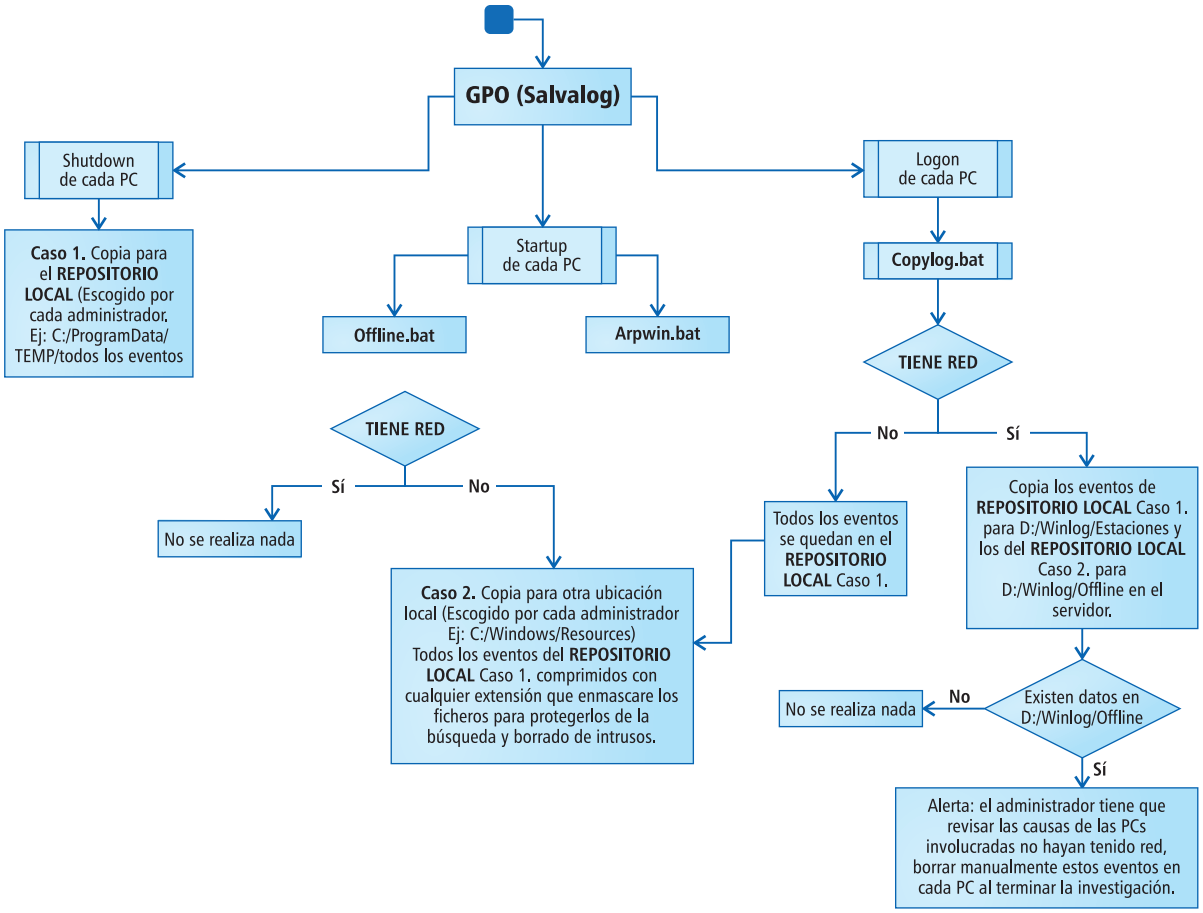
Capítulo 2. Seguridad del Servidor de Base de Datos

- *Firewall de Windows* con seguridad avanzada activada. Reglas personalizadas *Inbound* y *Outbound* (Capítulo 4).
- Otras modificaciones menos relevantes.

Capítulo 3. Trazas y eventos de auditoría

- La concepción de la gestión de recolección de los eventos de auditoría se resume en el siguiente diagrama; se ha revisado la seguridad y protección de los mismos para cuando el equipo se encuentra conectado a la red o desconectado, además de crearse mecanismos que permiten monitorear si algún equipo estuvo en algún momento sin red. Cuando el equipo cliente esté sin red, antes de que el usuario inicie sesión, se ejecutará el *script* *„Offline.bat"*, el cual realizará una copia secreta de los *„.evt"* enmascarando su extensión, los cuales serán copiados al Servidor de Dominio, cuando el equipo tenga red. Las razones de estos procedimientos son obvias.

- Se detalla mucho mejor la estructura de gestión de trazas.



- Se modifican todos los *script* y *batch*, y se incorporan otros necesarios.
- Se especifican las adecuaciones a realizar en cada *script* o *batch* para adecuarlos a cada lugar.
- Se entrega un programa (*Winlog.exe*) para automatizar la creación del directorio *D:\Winlog* con toda su estructura interna.
- Se cambió la estructura del directorio *D:\Winlog*, separándose los eventos de las estaciones de trabajo del resto de las trazas.

***Recolección de los eventos de auditoría*:**

Se implementa una GPO llamada *„Salvalog"* consistente en:

- En el *Shutdown* se ejecuta *„evtbpa.vbs"*, el cual copia todos los eventos de auditoría (evt) para un *„repositorio local temporal"*, el cual preferiblemente debe ser un directorio oculto en cada equipo y de conocimiento solo del administrador de red.
- En el *Startup* se ejecuta *„arpwin.bat"*, garantizándose la misma tabla *arp* estática en todos los equipos que tienen sistema operativo superior a *Windows XP*.
- En el *Logon* se ejecuta *„copylog.bat"* el cual copia los eventos de las Estaciones de Trabajo para „D:\Winlog\Estaciones" del Servidor de Dominio.
- El directorio „D:\Winlog\Estaciones" del Servidor de Dominio se protege con permisos restringidos.
- El repositorio local temporal se protege con medidas establecidas en los capítulos 1 y 6, de igual forma queda protegido el fichero *„access.log"* de *MyUSBOnly*.
- El repositorio local temporal se define como *„File System"* y se le da tratamiento confidencial.
- Se realizan ajustes de permisos sobre el *repositorio local temporal,* que evitan la duplicidad en la copia de los eventos al servidor.
- El camino del *repositorio local temporal* lo decide cada administrador de red, garantizándose que no sea el mismo en cada lugar, anteriormente se utilizaba (C:\Windows\Resources).
- Se protege el directorio *„D:\Winlog\SCRIPT"*, garantizándose la confidencialidad requerida con respecto al origen y destino de la información.
- El *script „arpwin.bat"* renombra todas las interfaces de red con *„Ethernet"*, elimina la caché *arp* y establece entradas *arp* estáticas.

Copia de seguridad diaria de todas las trazas:

Se identifica y se tiene en cuenta que el directorio (*D:\Winlog*) cuenta con una importancia alta en la estimación de riesgos, debido a que se pueden perder todas las trazas en los siguientes casos:

- El HDD del Servidor de Dominio se puede dañar.
- El Servidor de Dominio se lo pueden robar.
- El Servidor de Dominio puede dañarse físicamente, producto de un desastre natural o incendio.

Dado lo anterior, se establece una salva incremental diariamente del directorio anterior para la PC del administrador de la red, la cual se encuentra

fuera del local de los servidores. Para la tarea anterior se utiliza el Software *„Cobian Backup"*.

Revisión de trazas de auditoría:

- Se establece el Software *„ADAudit Plus"* para la auditoría del Servidor de Dominio.
- Se establece el Software *„ADAudit Plus"* en la estación de trabajo del administrador de la red para la auditoría de los eventos de las estaciones de trabajo; se nutre de la salva diaria que *Cobian Backup* realiza.
- Se establece *„Eventlog Explorer"* para la revisión manual de los eventos de *Windows*.

Otras modificaciones menos relevantes.

Capítulo 4. Firewall para SABIC.NEF

Se abordan configuraciones de *Firewall* para los siguientes escenarios:

Escenario	Tipo de Firewall activado
Servidor de Dominio	Kerio 7.4.2
Servidor de Base de Datos	Firewall de Windows con seguridad avanzada
Cajas de ahorro	Kerio 7.4.2
Áreas anexas	Kerio 7.4.2
Centro Provincial de Efectivo	Kerio 7.4.2

Política de tráfico

- En todos los escenarios se eliminan las reglas predeterminadas y se adicionan reglas puntuales personalizadas a cada lugar; al final de cada regla se deniega cualquier otro tráfico.

Servidor de Dominio

- Se establecen puertos fijos para algunos servicios que de forma predeterminada utilizan puertos aleatorios en el rango del 49152 al 65535, el cual abarca 16384 puertos.
- Al establecer los puertos fijos anteriores, se minimiza el riesgo de tener que abrir 16384 en el Servidor de Dominio.
- Se generan las trazas y se recolectan.

Servidor de Base de Datos

- Se eliminan todas las reglas predefinidas.
- Se establecen reglas de entrada (*Inbound*) y de salida (*Outbound*) personalizadas.
- Se incorpora nueva regla que permite realizar las reservaciones de saldo por SABIC.
- Se generan las trazas y se recolectan.

Cajas de ahorro:

Se tiene en cuenta que la primera línea de defensa la constituye el *Modem-router,* pero lo administra ETECSA. Además, no existe un Servidor de Comunicaciones desde donde se pueda filtrar el tráfico y garantizar la seguridad requerida, por lo que se establece el *Firewall Kerio* 7.4.2 en la Estación Principal o Servidor de SABIC local, el cual debe contar con dos interfaces de red.

- Se establece la guía de instalación y configuración.

Áreas anexas:

En este escenario la defensa perimetral se comporta igual que en las cajas de ahorro, con la agravante de que la Base de Datos no se encuentra local, o sea, se encuentra remotamente en la sucursal tutelar; de ahí la necesidad de extremar la seguridad, y para ello se propone el *Firewall Kerio* 7.4.2.

Se establece la guía de instalación y configuración.

CPDE (Centro Provincial Distribuidor de Efectivo)

Algunos CPDE cuentan con el mismo escenario que las áreas anexas, por lo que se establece la misma solución de seguridad.

Se establece la guía de instalación y configuración.

Capítulo 5. Antivirus

- Se describe cómo instalar y configurar el *Kaspersky Security Center* 10.1.249 con agente de red 10.1, paquetes de instalación para equipos administrados con *Kaspersky Endpoint Security Center* 10.2.1.23 y *Kaspersky* 6.0.4.1611.
- Se crean tres subgrupos:
  - Equipos óptimos
  - Equipos bajos recursos
  - Servidores

En el Servidor de Administración se debe instalar:

- *Kaspersky Security Center* 10.1.249 en español
- *Kaspersky Endpoint Security Center* 10.2.1.23.

En equipos clientes se debe instalar:

- En equipos óptimos (de buenas prestaciones -al menos 1 GB de RAM).
- *Kaspersky Endpoint Security Center* 10.2.1.23.

- En equipos de bajos recursos (de bajas prestaciones –menos de 1 GB de RAM).
- Agente de Red 10.1.
- *Kaspersky* 6.0.4.
- El despliegue en equipos clientes se realizará a través de paquetes de instalación generados desde el Servidor de Administración.
- Otras modificaciones menos relevantes.

Capítulo 6. Seguridad de las estaciones de trabajo

- En el Capítulo 1 se establece como política en la Unidad Organizativa *„SABIC"* quitar del *Explorer* el menú *Opciones* de carpetas del menú *Herramientas* y se oculta la unidad de Sistema C:\.
- En el Capítulo 4 se establece utilizar como repositorio local temporal de trazas un directorio preferiblemente oculto por el sistema.
- En el Capítulo 6 se establecen medidas que deben aplicarse en cada estación de trabajo, las cuales están en correspondencia con los capítulos anteriores.
- Otras modificaciones menos relevantes.

Capítulo 7. Backup de servidores y estaciones principales

- Copias de seguridad automáticas de los sistemas operativos, utilizando el Rol *"Windows Server Backup"*, en Servidor de Dominio y en el de Base de Datos.
- *Backup* de particiones de sistema con el *Software ACRONIS*, para servidores físicos y virtualizados con *ESXi*.
- Se propone utilizar el "Plan de Copias de Seguridad" como alternativa para organizar los *Backup* de sistemas operativos, trazas y Base de Datos. Otras modificaciones menos relevantes.

Capítulo 8. Protección a la información oficial

- Se proponen medidas alternativas para aplicar en las PC de los directores.
- Otras modificaciones menos relevantes.

Capítulo 9. Espionaje, telemetría y recolección oculta de datos

- Se realiza un análisis histórico con ejemplos que demuestran la participación y colaboración de la Empresa Microsoft en varios planes de la CIA y la NSA.
- Manipulación de sistemas de encriptamiento por parte de organizaciones de Estados Unidos, con propósito de espionaje.
- Formas y vías que ha utilizado Microsoft para introducir la telemetría embebida en los sistemas operativos, actualizaciones de seguridad y hasta en el *Hardware*.
- Medidas preventivas contra la telemetría y la recolección oculta de datos.
- Otras modificaciones menos relevantes.

Capítulo 10. Firewall perimetral Iptables

- Se encuentra en fase organizativa y en desarrollo.

Capítulo 11. Testeo y comprobaciones de seguridad

- Se encuentra en desarrollo; se cuenta con la parte organizativa por fases o etapas y la parte documentada, donde se exponen los requisitos técnicos (herramientas a utilizar, estado de los *Firewall* y reglas de acceso ACL en los *Modem-Router* y otros), el autorizo formal, la protección de los informes, valoraciones y plan de medidas derivado de los resultados en cada fase o etapa.

Capítulo 12. Actualizaciones de seguridad

- Se encuentra en fase organizativa y en desarrollo.

METODOLOGÍA PARA EL DESPLIEGUE A NIVEL PROVINCIAL

Paso 1. Conformación y preparación de un equipo de trabajo encargado de organizar y controlar la instalación y despliegue a nivel provincial.

Paso 2. Implementación del manual en la sucursal experimental escogida.

Paso 3. Despliegue provincial.

¿En qué consiste cada paso?
En tres pasos:

Paso 1. *Conformación y preparación de un equipo de trabajo encargado de organizar y controlar la instalación y despliegue a nivel provincial.*

- Aprobar en el Comité de Seguridad Informática la aplicación y despliegue del manual (Acuerdo 6058 CECM).
- Selección y conformación del equipo de trabajo. Estudio previo de cada capítulo (autopreparación).
- Seleccionar la sucursal experimental (el administrador de red automáticamente forma parte del equipo de trabajo).
- Adecuación de los *script* y gestión de las herramientas y software a utilizar.
- Indicar a todas las sucursales. Certificar la realización de los *backup* de las particiones de sistema y de buteo de todos los servidores de dominio.

Paso 2. *Implementación del manual en la sucursal experimental.*

- El equipo de trabajo completo aplica progresivamente el manual.
- Se monitorea el correcto funcionamiento de cada capítulo aplicado.
- Tener en cuenta para su aplicación:
  - No aplicar después del día 25 del mes.
  - No aplicar si se ha instalado alguna versión o actualización del SABIC.
  - No aplicar si no se ha realizado el *Backup* de la partición de sistema y de buteo.
  - No aplicar si en la sucursal se encuentran aplicando mantenimiento a todo el *Hardware* de la sucursal.
  - No aplicar si existen servicios como DNS, DHCP u otros con problemas (deben revisarse los eventos de servicios y sistema operativo).
  - No aplicar si se tiene conocimiento de que se estén realizando réplicas desde la Oficina Central.
  - No aplicar si se tiene conocimiento de funcionamiento inestable de algún *Switch* o tarjeta de red.

Paso 3. *Despliegue provincial*
Cuenta con cuatro etapas:

Etapa 1. Preparación de todos los administradores de red

- Organizar y fijar la reunión provincial. Todos deben tener la documentación en sus manos con antelación.
- Se debe tener la seguridad de que todo se aplicó correctamente en la sucursal experimental, y que se cuenta con varios días de funcionamiento sin problemas.
- Se debe determinar el orden en que se aplicarán los capítulos.
- Debe comprenderse la necesidad de reforzar la seguridad de la red, lo cual repercute en la seguridad del Sistema Informático Contable.
- Debe comprenderse la obligación de cumplir con lo legislado en el Reglamento de Seguridad adjunto a la Resolución Nº 127/07 del MIC, así como lo instruido por el BPA en sus manuales de procedimientos.
- Debe quedar clara la responsabilidad del administrador de red en todo lo anterior.
- Debe comprenderse que la aplicación del Manual Técnico que se propone constituye una variante por donde es posible organizar y controlar la seguridad de cada red LAN con SABIC, así como cumplir con las obligaciones del personal.
- Debe quedar claro que en cada *script*, medida o procedimiento que se propone, se han analizado los posibles puntos vulnerables, corrigiéndose o minimizándose, por lo que modificar a criterio e iniciativa de una persona puede motivar brechas y comprometer el Sistema de Seguridad.

Etapa 2. Fecha de cumplimiento

- La tarea debe tener un comienzo y un final planificado, de lo contrario, la operatividad diaria de los responsables de la misma dilataría o comprometería su cumplimiento.
- La fecha de cumplimiento debe pactarse o acordarse en el Comité de Seguridad Informática, teniendo en cuenta la experiencia de su aplicación en la sucursal experimental (Paso 2).

Etapa 3. Seguimiento y control

- Orientar la utilización del modelo *"Revisión del Manual de Seguridad Perimetral de SABIC.NEF"* para el envío de los criterios, sugerencias o modificaciones a realizar en cada capítulo (Anexo I).

Etapa 4: Certificación

- Se deberá certificar inmediatamente al Departamento de Seguridad y Protección el estado de aplicación y cumplimiento de cada capítulo (Anexo II).
- El proceso de certificación constituye una etapa de autocontrol, en que se podrá detectar si algún aspecto se quedó sin aplicar y, por tanto, es el momento de corregirlo.

CONCLUSIONES

Como se ha podido apreciar en el desarrollo de este trabajo, estamos en presencia de un proyecto muy abarcador y de extrema importancia para la seguridad informática del BPA. Aún quedan capítulos por concluir, los cuales se encuentran en desarrollo, pero en su gran mayoría se encuentran aplicados a nivel provincial, y otros indistintamente en algunas sucursales de otras provincias.

RECOMENDACIONES

Considerando el aporte de este trabajo a la seguridad informática de las redes del BPA, particularmente a la seguridad perimetral del Sistema Informático Contable SABIC, recomendamos a las direcciones de Seguridad y Protección e Informática de nuestra Oficina Central continuar brindando apoyo a este proyecto y, de esta forma, lograr mejores niveles de organización y seguridad en las redes informáticas del BPA.

Anexo 1. "Revisión del Manual de Seguridad Perimetral de SABIC.NEF"

REVISIÓN DEL MANUAL DE SEGURIDAD PERIMETRAL DE SABIC.NEF
Sucursal: _____

Capítulo	Nombre del capítulo	Sección	Sugerencia agregar (A), modificar (M) eliminar (E)			Aspectos a modificar, agregar o eliminar	Otras observaciones
			A	M	E		

Anexo 2. "Certificación de la aplicación del Manual de Seguridad Perimetral de SABIC.NEF"

CERTIFICACIÓN DE CUMPLIMIENTO
MEDIDAS DE SEGURIDAD PERIMETRAL PARA SABIC.NEF

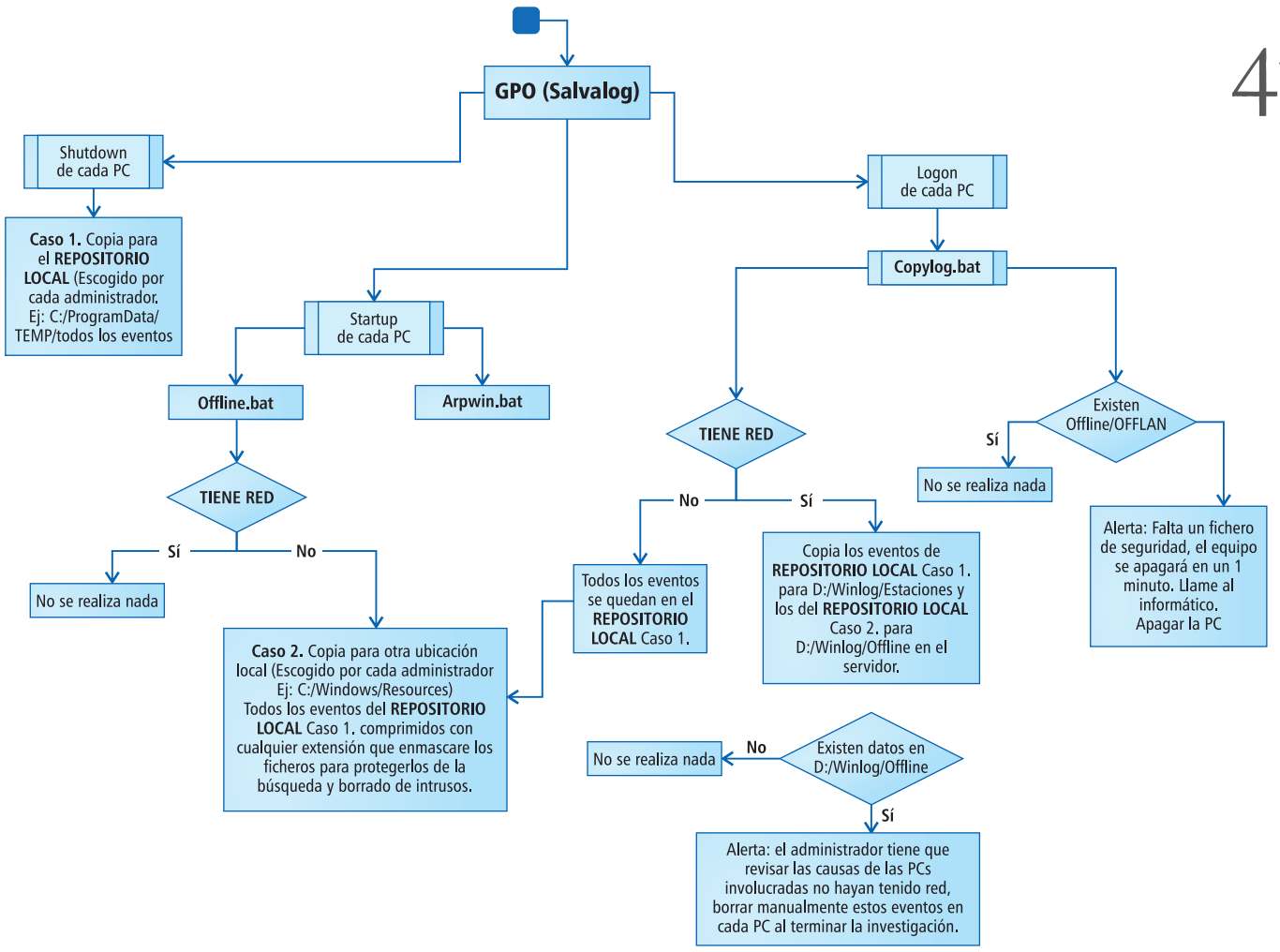
SUCURSAL:_____ **FECHA:**_____

Certificamos el cumplimiento e implementación del Capítulo Nº_____
Título:_____, comprobándose los siguientes resultados:

(Marque con "x" en la columna si se ejecutó (S), no se ejecutó (N) o se ejecutó parcialmente (P), agregue comentarios, problemas observados, causas de no aplicarse algún punto específico).

Ejemplo:

No.	Medidas, políticas o procedimientos	Ejecución S	Ejecución N	Ejecución P	Comentarios (causas)
1.2_Directivas generales para el Servidor de Dominio					
	Se aplicó del punto 1 al 21.				
	Quedaron puntos pendientes.				
1.2.1_Procedimiento para las contraseñas combinadas					
	Se aplicó todo su contenido.				
1.2.2_Política para recursos compartidos en el servidor					
	Se aplicó todo su contenido.				
1.2.3_Eliminar *AutoPlay* desde el sistema operativo					
	Se aplicó todo su contenido.				
1.2.3_Eliminar *AutoPlay* desde el sistema operativo					
	Se aplicó todo su contenido.				
1.x					
1.xx					
1.xxx					



* Especialista en Seguridad y Protección, y Especialista en Seguridad Técnica de la Información en Soportes Informáticos de la Dirección Provincial de BPA de Camagüey, respectivamente

La sede "The Royal Bank of Canada" en La Habana

Lic. INDIRA ÁLVAREZ NIEVES*

The Royal Bank of Canada se fundó en 1864 en Halifax, Nueva Escocia, pero fue en 1901 que asumió el nombre con que se le conoce actualmente. En sus inicios, era *Merchants Bank* o *Merchants Bank of Halifax,* como lo denominaron en 1869. Sus creadores fueron comerciantes de la ciudad, que tenían el propósito de organizar la industria pesquera y maderera, y de implementar su comercio en Europa. En 1901 su sede se estableció en Montreal hasta los años sesenta del pasado siglo, cuando se trasladó a Toronto, donde hoy se encuentra.

A finales del siglo XIX, comenzó su expansión en otros países. En 1898 el administrador general del banco, Mr. E. L. Pease, visitó La Habana para explorar la posibilidad de inaugurar una sucursal en una ciudad que reconocía por sus importantes valores arquitectónicos y patrimoniales, acción que consideraba una gran oportunidad desde el punto de vista económico. En marzo de 1899 se concretó la idea con la inauguración de la primera filial extranjera en la isla por la dirección del banco, tras el fin del dominio colonial, la cual sirvió de escuela para una gran parte de los ejecutivos bancarios cubanos.

En breve tiempo, la sucursal *The Royal Bank of Canada* en la capital cubana se convirtió en una de las más solventes, con un depósito de $127 000 000. En las primeras cinco décadas del siglo XX, esta institución llegó a tener en Cuba 24 sucursales. Su preeminencia en el mundo bancario de la isla crecía en la medida que se estrechaban los nexos con sus similares nacionales; fue miembro de *La Habana Clearing House* y accionista del Banco Nacional. Además, en 1950 operaba como entidad centralizadora de toda la actividad bancaria del país.

En la década de los cincuenta del pasado siglo, sus utilidades siempre fueron superiores al millón de dólares, en lo cual influyó la riqueza proveniente de las propiedades que adquirió y del caudal acumulado por sus servicios. A finales de los años treinta, llegó a poseer nueve centrales que eran operados por *Sugar Plantation Operation Company*. Los primeros destinatarios de sus préstamos fueron firmas de financiamientos de autos con el 14% del total, y la industria azucarera con el 11%. Entre sus principales clientes, estaban empresas extranjeras como *la Compañía Nacional de Alimentos*, "Créditos y Descuentos Mercantiles", *Esso Standard Oil*, *General Motor Acceptance Corporation*, *Petrolera Shell de Cuba* S. A., *Cuban Telephone Compa* y *General Electric Cubana* S. A.

Después del triunfo de la Revolución cubana, en 1960 y 1961 se dictaron las resoluciones sobre la intervención de los bancos, proceso liderado por Ernesto Che Guevara y Raúl Cepero Bonilla. El 5 de abril de 1961, mediante la Instrucción Administrativa Nº 44 se dispuso consolidar todas las oficinas bancarias, con excepción de algunas agencias. Con la nacionalización de estas entidades, su dirección fue asumida por un administrador delegado designado por el Gobierno revolucionario, en tanto las instituciones pasaron a formar parte de otras empresas, como ocurrió con *The Royal Bank of Canada*, que fue adquirido por el Banco Nacional de Cuba.

Pero la historia de *The Royal Bank of Canada* en Cuba no puede ser contada sin hacer referencia a los inmuebles que le sirvieron de sede en cada etapa, especialmente el ubicado en Aguiar #367.

Enlazar la buena fortuna en los negocios con la imagen que transmitía la institución bancaria, y particularmente disponer de una edificación confortable, sólida y atractiva, constituían una premisa de la actividad empresarial que desarrolló en territorio cubano durante seis décadas.

En busca de la sede apropiada

La inauguración de la primera sucursal tuvo como escenario un modesto edificio de alquiler, ubicado en la calle Obrapía #25. Apenas transcurridos tres años, se decidió tener una edificación propia. Con este propósito, en 1902 se compró un solar en Obrapía #257, que ocupaba la antigua droguería de Lobo y Torralbas que fue necesario demoler. El diseño del inmueble lo asumió el arquitecto cardenense José Toraya Sicre. Su construcción, realizada por la compañía *Purdy & Herdenson*, concluyó en 1904.

La propiedad era de dos pisos, el primero destinado al banco, y el segundo a oficinas. La fachada era de sillería, con un arco monumental en la puerta. Toda la obra fue realizada con estructura de acero. En la remodelación de 1911 se añadieron algunas habitaciones en la segunda planta. Años más tarde, en este inmueble radicó la Bolsa de La Habana comprada en 1919.

El crecimiento de las operaciones demandó más espacio, por lo que en 1917 se decidió construir otro edificio. El lugar escogido fue Aguiar #367, esquina a Obrapía, circuito conocido como *Wall Street Habanero* por la cantidad de oficinas bancarias y servicios públicos instalados en la zona. El proyecto fue realizado por el arquitecto Luis García Nattes, y repitió como contratista la conocida compañía *Purdy & Henderson*.

La *Purdy & Henderson*, establecida en el país en 1901, fue encargada de la construcción de numerosas e importantes obras como el Banco Nacional de Cuba (Obispo y Cuba), la Droguería Johnson, el Centro Gallego, el Centro Asturiano, el Capitolio Nacional, entre otras, incluyendo un conjunto de residencias privadas en el Vedado. Además, se involucró en otros sectores de la economía nacional.

La licencia para la nueva sede solicitada por la dirección del banco, consistió en un inmueble de seis pisos. La planta baja sería destinada a las operaciones bancarias, y el resto de los pisos se rentaría para oficinas. Entre las empresas que arrendaron locales, estuvieron:

- Compañía de seguros "El sol del Canadá" (seguros sobre la vida), Despacho 512.
- *Sugar Sales Corporation* (compra y venta de azúcares y de sacos para sus envases), Despacho 212.
- Sres. Vilela y Mayorbe (corredores, fincas rústicas y urbanas), Despacho 205.
- Sucursal de los Sres. Topping Brothers de Nueva York (exportadores de ferretería gruesa, efectos navales y herramientas), Despacho 217.

Fachada principal.

- Sr. Rogelio C. Novo, representante de las "Canteras de Toledo" (contratista de carretera), departamentos 318 y 319.
- Cía. Forestal Agrícola y Ganadera, V. Hermosa, S. en C. (venta de maderas del país, traviesa, carbón vegetal y otros productos agrícolas y ganaderos), departamentos 209 y 210.
- Sr. J. A. Cabasa y Cía., representantes exclusivos de varias fábricas.
- Bufete del abogado Eduardo Delgado y del notario Adolfo Delgado, departamentos 207 y 208.
- *Havana Importation Co.* (importadores y exportadores), Departamento 216.
- Barbería del Sr. Matías Bernardo (salón elegante con variados servicios), departamentos 201 y 202.

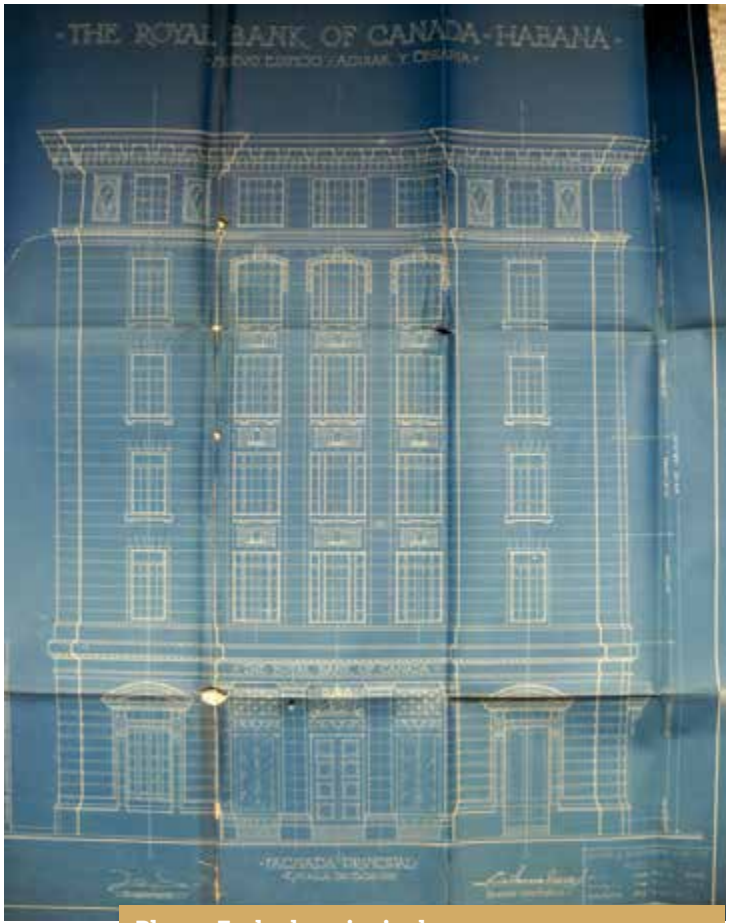
En el ámbito constructivo en Cuba, desde los primeros años del siglo XX, se desarrollaron técnicas que permitieron atender las necesidades surgidas por el crecimiento de la población urbana, y se generalizó la utilización del hormigón. El empleo de estructuras de acero y la invención de los ascensores facilitaron la construcción de edificios altos.

En los inmuebles se extendía el uso de columnas colosales, que en la mayoría de los casos iban

del basamento a la cornisa. Por lo general, en el primer piso se concentraba la ornamentación, en tanto el resto de las plantas era tratado como un elemento unitario, aunque con gran limpieza decorativa. Además, se utilizaban amplios ventanales sin balcones, y a modo de cornisa un gran ático que remataba la edificación.

La memoria descriptiva de la sede cubana *The Royal Bank of Canada* toma en cuenta los adelantos técnicos de la época en materia de construcción:

- Para acceder a los seis pisos del edificio, se instalaron dos ascensores, se construyó una escalera principal, y en el patio del fondo se ubicó una escalera de escape para casos de incendio. Para la ventilación de las diferentes áreas, se previeron dos patios laterales al fondo y otro central abierto desde el segundo piso, que solamente se cerraba en la porción de la planta baja por un lucernario de vidrios alambrados y emplomados.
- Las cimentaciones del inmueble, al igual que los pilares, columnas, arquitrabes, escaleras, bóvedas de valores y placas de pisos, eran de cemento armado (hormigón), y de ladrillos los muros y tabiques. En la fachada de la planta baja se utilizó cantería de Jaimanita. En el resto del inmueble, incluidas las decoraciones y cornisas, se empleó piedra artificial de cemento, a la que se le añadió un tinte amarillo con el propósito de acentuar su magnificencia.
- Las decoraciones interiores se hicieron con yeso. Los pisos de la primera planta se cubrieron con mármol blanco; los de la segunda, con losas hidráulicas que imitaban mosaicos; los de los patios, de cemento. En la soladura de cubierta se utilizó el ladrillo catalán. La carpintería se realizó con armadura metálica y cristal, pero las puertas de calles e interiores se construyeron de cedro, y de bronce las lucetas giratorias. Los huecos de las ventanas y las barandas de las escaleras eran de hierro forjado.



Plano: Fachada principal.

En 1918, durante la construcción del inmueble, se decidió agregar un séptimo piso destinado a restaurante y club. Este *Lunch Club,* como se le conoció, fue organizado por representantes, banqueros y comerciantes de La Habana, hasta que en 1928 el espacio fue utilizado para oficinas.

Después de terminado el edificio, en 1921 se solicitó una licencia para hacer reformas en el segundo piso, las que consistieron en el cierre y apertura de nuevos vanos, demolición de tabiques, construcción de una bóveda para libros y una escalera que conducía al entresuelo. La bóveda se levantó con ladrillos, y la escalera se hizo de cemento armado, revestida con mármol blanco con la baranda de hierro forjado.

La edificación se mostraba como un gran bloque dividido en tres secciones: la primera coincidía con la primera planta, la segunda incluía el resto de los pisos, y la tercera comprendía una gran cornisa, a modo de remate. La fachada se ubicó retirada de la acera, según las ordenanzas oficiales. Este detalle, unido a la escalinata y a las voluminosas columnas, proporcionó un aire de distinción a la entrada del banco.

El edificio *"The Royal Bank of Canada"* es un ejemplo significativo de la arquitectura moderna. En una descripción de la época, se hace referencia a importantes detalles sobre los materiales de construcción, la fachada y el interior del edificio:

- La planta baja, ocupada por las oficinas del banco, tiene su entrada por la calle Aguiar, donde se abre un amplio pórtico fabricado de piedra y mármol blanco, con cuatro columnas toscanas que sostienen el arquitrabe, y a cada lado una puerta más con bellos ornamentos en sus remates. Una de estas puertas da acceso a los elevadores eléctricos para los pisos altos.
- El gran salón donde se hallan las oficinas de contabilidad y caja, así como el mostrador con numerosas ventanillas para atender al público, están construidos siguiendo el estilo general, habiéndose empleado profusamente el bronce y el mármol de Tavernell. En el centro del salón se colocaron varias mesas también de mármol con cubierta de cristal para uso del público, y a su alrededor algunos bancos de caoba oscura barnizada. Esta parte del local está cubierta a la altura del segundo piso por una gran claraboya de cristal cuajado en colores, que matiza suavemente la luz (...).

Oficinas del séptimo piso (1928).

- Todo el interior del edificio está provisto de esos modernos detalles de utilidad, comodidad e higiene, como elevadores conductores mecánicos, teléfonos intercomunicables, armarios guardarropas, filtros para aguas, extinguidores de incendios, etcétera. Por la necesidad de atender cuidadosamente la libre circulación del aire, se construyó este edificio separado de los colindantes por un pasillo de dos metros, de modo que el aire y la luz penetran con abundancia, no solamente por el patio central abierto en los pisos superiores, sino también por el aludido callejón (La Habana, 1919, p.84).

En el momento que se interviene esta institución bancaria, sus oficinas se encontraban en la primera planta, y el resto de los pisos estaba arrendado por otras compañías. En el inmueble se continuó realizando funciones públicas y, a pesar de las modificaciones efectuadas, se conserva su integridad como un valioso ejemplo del patrimonio moderno cubano.

En la segunda década del presente siglo, comenzó el proceso de restauración del inmueble por la Oficina del Historiador de la Ciudad de La Habana. Actualmente, el edificio es la sede del Tribunal Supremo Nacional.

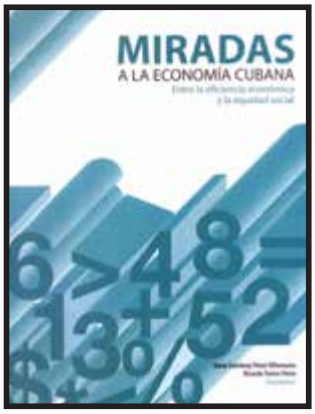
Bibliografía

- Documento sobre The Royal Bank of Canada. La Habana, 1917, Legajo 59-A, Fondo Urbanismo, Archivo Nacional de Cuba.
- Fondo: Banco Nacional de Cuba, Legajo 317 N° 19, ANC.
- La Habana y sus grandes edificios modernos, 1919.
- Rodríguez Marcano, Yamira (2004). *The Royal Bank of Canada.* La Habana

* Especialista en Museografía de la Dirección de Patrimonio de la OHC de La Habana

MIRADAS A LA ECONOMÍA CUBANA: ENTRE LA EFICIENCIA ECONÓMICA Y LA EQUIDAD SOCIAL

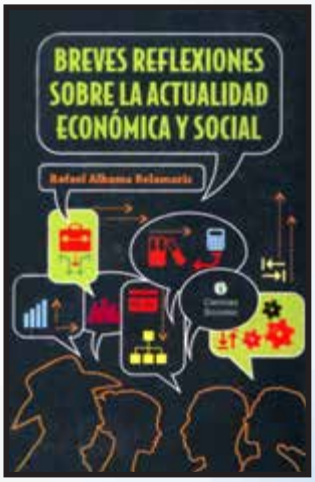
Omar Everleny Pérez Villanueva y Ricardo Torres Pérez



El texto enfatiza en las transformaciones en curso del modelo económico y social, observando las relaciones y tensiones entre la búsqueda de la eficiencia económica y la equidad social.

BREVES REFLEXIONES SOBRE LA ACTUALIDAD ECONÓMICA Y SOCIAL

Rafael Alhama Belamaric



Aborda los cambios políticos, sociales y económicos que tienen amplia repercusión en la nación. Mediante estas reflexiones, el autor llama a la socialización del pensamiento colectivo e individual.

TRABAJAR EN Y CON GRUPOS. EXPERIENCIAS Y REFLEXIONES BÁSICAS

Manuel A. Calviño

El presente volumen expone el destino de los hombres y está relacionado inexorablemente con los grupos. La emergencia de las actuaciones grupales responde a una necesidad y a un condicionamiento histórico.

COMUNICACIÓN DIALÓGICA Y TRANSFORMACIÓN SOCIAL EN LA WEB. ACERCAMIENTO A EXPERIENCIAS CUBANAS

Miriela Fernández Lozano y Yohana Lezcano Lavandera

Este cuaderno permite formar a quienes en Cuba llevan sus posicionamientos y propuestas al mundo digital, y se manifiestan y debaten allí. Asimismo, resulta un acercamiento a una zona de la realidad cubana que ha apostado también por la transformación "conectándose".

BANCO CENTRAL DE CUBA