

# ESTRATEGIA EMPRESARIAL EN LA PROTECCIÓN DE LA INFORMACIÓN DE LA BANCA DE NEGOCIO EN EL BANCO POPULAR DE AHORRO EN MATANZAS.

**Dr. C. Roberto Pons García<sup>1</sup>, Lic. Gladys Torres Reyes<sup>2</sup>  
Lic. Miguel A. Morán Hernández<sup>3</sup>**

1. *Universidad de Matanzas – Sede “Camilo Cienfuegos”, Vía Blanca Km.3, Matanzas, Cuba.  
roberto.pons@umcc.cu*

2. *Dirección Provincial Banco Popular de Ahorro Matanzas, Calzada General Calzada Gral.  
Betancourt No. 23618 Playa, Matanzas, Cuba. gladys.torres@a3912.ma.bpa.cu*

3. *Dirección Provincial Banco Popular de Ahorro Matanzas, Calzada General Calzada Gral.  
Betancourt No. 23618 Playa, Matanzas, Cuba. miguel@a3832.ma.bpa.cu*

## Resumen

En la actualidad, resulta innegable el hecho de que las organizaciones se encuentran inmersas en entornos y mercados competitivos y globalizados; entornos en los que toda organización que desee tener éxito (o, al menos, subsistir) tiene la necesidad de alcanzar “buenos resultados” empresariales; por lo que se hace necesario renovar y perfeccionar las medidas a tomar para proteger la información de sus procesos así como los informes de resultados de sus negocios, para que puedan ser una empresa competitiva del mundo empresarial. La presente investigación persigue como objetivo: Elaborar una estrategia para proteger el flujo de la información de la Banca de Negocio en el Banco Popular de Ahorro. Entre las técnicas y métodos utilizados se encuentran: entrevistas a trabajadores y directivos de la empresa, revisión de documentos, observación, criterio de expertos y tormenta de ideas. Además, se emplean herramientas informáticas, que permiten dar un basamento científico a la investigación realizada. El procedimiento empleado posibilita diseñar la estrategia que debe ser desplegada en el proceso, así como la política de operaciones, lo que contribuye a proteger la información que es un bien de la empresa, como base para el mejoramiento competitivo de la entidad y la elevación de la satisfacción de los clientes.

*Palabras claves: estrategia, política, operaciones, procesos.*

---



---

CD Monografías 2019  
(c) 2019, Universidad de Matanzas  
ISBN: 978-959-16-4317-9

## Introducción

Los trascendentales cambios operados en el mundo moderno, caracterizados por su incesante desarrollo, la acelerada globalización de la economía, la acentuada dependencia que incorpora en alto volumen de información y los sistemas que la proveen; el aumento de la vulnerabilidad y el amplio espectro de amenazas, tales como las amenazas cibernéticas; la escala y los costos de las inversiones actuales y futuras en información y en sistemas de información; y el potencial que poseen las tecnologías para cambiar drásticamente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos, han impuesto nuevos retos en el desarrollo de la protección de la información de la empresa, jugando un papel más amplio la Seguridad Informática.

El desarrollo tecnológico, en los últimos siglos, ha sido el más grande de la historia, y en los últimos años la rápida evolución de la informática, las computadoras y la conexión de estas en red han cambiado la forma en que el ser humano percibe el mundo. Es evidente que el sistema digital, debido a su crecimiento experimental, ha cambiado fuertemente la cultura y se podría decir que para casi todo el quehacer humano es necesario el utilizar una computadora.

En el entorno de los negocios en el siglo XXI, la mayor ventaja de una computadora conectada a INTERNET consiste en la enorme cantidad de información equivalente a tener la mejor bibliografía disponible al alcance de la mano. Entre otras ventajas de los ordenadores con conexión a red, Larsen (2002, 62) menciona el acceso a las diferentes variedades de información y la manipulación que de ésta se puede hacer. En este contexto y conscientes de la utilidad que presta la informática a todos los ámbitos del quehacer humano también es muy importante tener presente el cómo almacenar la información y resguardarla de todas las posibles eventualidades que pudieran surgir.

Las características que priman en el entorno de cualquier entidad moderna, que incorpore a su gestión las tecnologías de información, sustentadas sobre una infraestructura tecnológica con amplio grado de integración de redes, comunicaciones y sistemas de información de punta, para maximizar a través de su soporte logístico el control interno, la contabilidad, y consecuentemente sus

Resultados, demanda transformaciones en la práctica de la disciplina orientada a ejercer un control superior mediante la auditoría y en especial en la auditoría interna.

En la actualidad debido a los cambios tecnológicos, y a que estos permiten también efectuar operaciones ilícitas como resultado del enorme aumento de la tecnología de la información para mejorar su desempeño, también se ha desarrollado muy pronto un lado negativo e inseguro para todas las redes de información con las que nos vemos envueltos hoy en día,

por lo que las organizaciones han ido adoptando muy lentamente, la seguridad informática dentro de sus operaciones.

En cuanto a la seguridad informática, las computadoras y la Internet son ahora una parte familiar de nuestras vidas. Quizás no las vemos a menudo, pero ahí están; involucradas de alguna manera en la mayoría de nuestras actividades diarias, en los negocios de cualquier empresa, en las instituciones educativas, en las diferentes áreas de gobierno, sin el apoyo de estas herramientas ninguna de ellas sería capaz de manejar la impresionante cantidad de información que parece caracterizar a nuestra sociedad. Pero también existe una problemática en ellas, la seguridad; para ello se han desarrollado firewalls dispositivos de software que protegen la integridad de las mismas. Cada vez más personas necesitarán conocer el manejo de las computadoras así como las protecciones que día a día se van ofreciendo para garantizarnos la seguridad en el manejo de la información.

Los inconvenientes en cuestión de seguridad no son conocidos por todos los usuarios de la red y por ello no saben cómo protegerse de dicha vulnerabilidad que tienen cada vez que se conectan a esta red de trabajo.

La generalizada informatización de los procesos y disciplinas que impactan directamente en la sociedad, en especial las relacionadas con la gestión económica, que hace apenas una década se procesaban manualmente, así como los propios cambios que introduce su tratamiento informatizado, introducen transformaciones sustanciales sobre el concepto tradicional del control interno, la estructura del registro y consecuentemente la práctica de las auditorías. Convendría hablar un poco de qué se entiende por Seguridad. En esta investigación se entenderá por seguridad en redes, a la protección frente ataques e intrusiones en recursos corporativos por parte de intrusos a los que no se permite acceso a dichos recursos. La seguridad siempre será relativa al tipo de servicios que queremos ofrecer a los usuarios autorizados, según se establece en la política de seguridad de la empresa en bien de asegurar y proteger informaciones en el ámbito de los negocios.

Creo conveniente definir primeramente las partes elementales que se relacionan con la seguridad en informática. En primer lugar tenemos la WAN (World Área Network) es una gran red de cómputo de cobertura mundial y una de las más comunes es Internet. En segundo lugar, está LAN (Local Área Network) que es una red mediana denominada local ya que está limitada a una pequeña área geográfica y normalmente es utilizada por empresas privadas, públicas, educativas, etc. Estas dos redes llegan a interactuar utilizando un conjunto de protocolos de comunicación de datos.

Al hablar sobre la seguridad de redes, nos referimos al gran índice de inseguridad interna de la infraestructura informática de las instituciones, así como la falta de una cultura informática, necesaria para enfrentar estos problemas.

Para la mejor comprensión del tema de investigación se definen los siguientes conceptos:

Seguridad Informática: Sistema de medidas administrativas, organizativas, físicas, técnicas, legales y educativas, dirigidas a prevenir, evitar, detectar y responder a acciones que pongan en riesgo la información que se procese, intercambie, reproduzca y conserve a través de las tecnologías de información.

Sistema de Seguridad Informática: Conjunto de medios administrativos, medios técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados.

En consulta a diversos especialistas y organizaciones, coinciden en que el 80% de la violación a la información se da por parte del personal que labora dentro de las mismas organizaciones.

A medida que el comercio de las instituciones vía electrónica, la inseguridad en la transacciones comerciales se vuelve un problema crucial y en constante crecimiento, que debe ser contemplado por la alta dirección en la toma de decisiones y en la implementación de soluciones.

El alto grado de vulnerabilidad de la información transferida por la red y la facilidad de ataques externos e internos, se traducen en pérdidas que ascienden hasta miles de dólares en términos de información alterada, robada o perdidas.

Desde que incorporamos la informática y la tecnología a los procesos de nuestras empresas, esto ha implicado que las actividades que se realicen sean sistemáticas, sean más ágiles y sencillas. Sin embargo, toda facilitación debe ir de la mano con la Seguridad y Protección.

La seguridad informática (en adelante S.I) consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

## **Materiales y Métodos**

Para realización de la investigación se desarrolló el procedimiento “Despliegue de las estrategias de operaciones” para proyectar la estrategia y sus políticas operacionales en el proceso seleccionado como objeto de estudio. Entre las técnicas y métodos utilizados se encuentran: entrevistas a trabajadores y directivos de la empresa, revisión de documentos, observación, criterio de expertos y tormenta de ideas.

## **Resultados**

### CARACTERIZACIÓN DE LA ENTIDAD.

El BPA, fue creado mediante el Decreto-Ley No. 69 de fecha 18 de mayo de 1983, con carácter de banco estatal integrante del sistema bancario nacional, con autonomía orgánica, personalidad jurídica y patrimonio propio, estableciéndose en dicho cuerpo legal su razón social. Su capital fue aportado por el Estado cubano y bajo el precepto de un funcionamiento independiente lo ha ido incrementando, mediante la capitalización de las reservas y ajustes por concepto de corrección monetaria.

La dirección provincial del BPA en la provincia de Matanzas pertenece al Banco Central de Cuba (BCC) y se encuentra ubicada en la calzada General Betancourt, No.26318; cuenta con una amplia red de oficinas que incluye 22 sucursales, 28 cajas de ahorro, un centro provincial distribuidor de efectivo, dos centros de negocios y el centro de formación bancaria, donde se capacitan nuestros cuadros y especialistas de acuerdo a las necesidades de aprendizaje.

El BPA, institución financiera especializada del Estado, se creó con el objetivo de impulsar el desarrollo del ahorro monetario de la población en su conjunto, cuenta entre sus principales productos y servicios con una variedad de actividades lucrativas relacionadas con el negocio de la banca, tanto en moneda nacional como en divisa.

Estrategia organizacional: La entidad tiene establecida su estrategia organizacional desde el año 1997 y anualmente se reciben de la Oficina Central los escenarios para el próximo año que se pretende planificar, informando sobre las proyecciones en los negocios, ingresos, gastos y utilidades del banco en ambas monedas, así como otros indicadores que deben tenerse en cuenta a partir de las indicaciones del Ministerio de Economía y Planificación o el Banco Central de Cuba, es decir, se define y/o actualiza su razón de ser y la meta que se propone la institución, así como los objetivos y criterios de medida que se deben ejecutar para alcanzarla; los cuales son adecuados por cada Dirección Provincial y éstos a su vez en las 22 sucursales. Trimestralmente, se evalúa el cumplimiento de cada criterio de medida, que sirve como punto de referencia para desarrollar el trabajo comercial y de control de los gastos e ingresos, así como para medir el nivel de ejecución.

Como parte de la estrategia organizacional la empresa define como:

Misión: El BPA es una institución financiera, destinada a captar y colocar recursos financieros a través de productos y servicios, con una orientación de banca universal, líder en el segmento de personas naturales.

Con el uso racional y efectivo del capital humano, el fortalecimiento y desarrollo del mismo y de los recursos tecnológicos con que cuenta, garantiza brindar al cliente una atención integral y de calidad en función de satisfacer sus necesidades.

Visión: El BPA es la institución financiera líder en la atención a las personas naturales, con un control interno razonable y en fortalecimiento constante, mantiene la mayor Red de Sucursales en el país, dotadas de un sistema informático único. Posee un capital humano

profesional, que avanza hacia un desarrollo que le permita alcanzar niveles de competencia superior, comprometido con la prestación de un servicio de calidad, dotado de valores sólidos y principios éticos que garanticen las características que lo distinguen.

Objetivos:

- Captar los recursos monetarios temporalmente libres de la población.
- Conceder créditos personales a corto mediano y largo plazo.
- Realizar operaciones de cobros y pagos a personas naturales y jurídicas por cuenta propia y por cuenta de terceros.
- Fijar y cobrar las tasas por los servicios que presta
- Evaluar proyectos de inversiones tanto constructivas como financieras
- Emitir y operar tarjetas de crédito, débito y cualesquiera otros medios avanzados de pago.

#### SELECCIONAR UN PROCESO.

El éxito de toda organización depende, cada vez más, de que sus procesos empresariales estén alineados con su estrategia, misión y objetivos. Detrás del cumplimiento de un objetivo, se encuentra la realización de un conjunto de actividades que, a su vez, forman parte de un proceso. Es por ello que el principal punto de análisis lo constituye, precisamente, la gestión de la empresa basada en los procesos que la integran. De ahí, que el enfoque de procesos, después de muchos años de haberse aplicado, sea hoy una herramienta tan poderosa por su capacidad de contribuir de forma sostenida a los resultados, siempre que la empresa diseñe y estructure sus procesos pensando en sus clientes (Zariategui, 1999).

Los procesos de la organización se pueden dividir en distintos tipos en función de la repercusión directa que tienen sobre el producto o servicio ofrecido. Existe diversidad en cuanto a la clasificación de los procesos, no obstante, es común en las bibliografías consultadas, (Gil Ojeda & Vallejo García, 2008) y ("Empresa Excelente," Mayo 2016), el análisis basado en tres criterios: procesos estratégicos; procesos operativos, claves, de línea o misionales y procesos de soporte, apoyo o complementarios, lo que va a estar en dependencia de su intervención en el cumplimiento de la misión de la organización:

- Procesos estratégicos: se encuentran directamente vinculados al ámbito de las responsabilidades de la dirección y, generalmente, al largo plazo. Ofrecen salidas que regulan, proporcionan directrices y límites de actuación para los otros procesos de la

organización. Mantienen y despliegan las políticas y estrategias, con vistas a garantizar la toma de decisiones acertada, fortalecer la operatividad del negocio y contribuir a mejorar la perspectiva del cliente.

- **Procesos claves:** son el núcleo del negocio, están directamente ligados a los servicios que se prestan y aportan valor a la relación de la compañía con sus clientes, persiguen como fin principal la satisfacción de sus necesidades. Incluyen todos los procesos que proporcionan el resultado previsto por la entidad en el cumplimiento de su objeto social o razón de ser. Suelen intervenir varias áreas funcionales en su ejecución y son los que pueden conllevar los mayores recursos.

- **Procesos de apoyo:** pese a ser procesos menores desde un punto de vista estratégico y corporativo, complementan enormemente el desempeño de procesos superiores y determinan en muchos casos el éxito o el fracaso de los mismos. Incluyen todos aquellos procesos para la provisión de los recursos que son necesarios en los procesos estratégicos y operativos. Pueden ser fácilmente subcontratables, es decir, la empresa no se resiente en el momento en que opta por externalizar alguna de las tareas o actividades que se llevan a cabo en estos procesos.

En la figura 1 se presenta el mapa de procesos de la institución el cual está integrado 11 procesos fundamentales

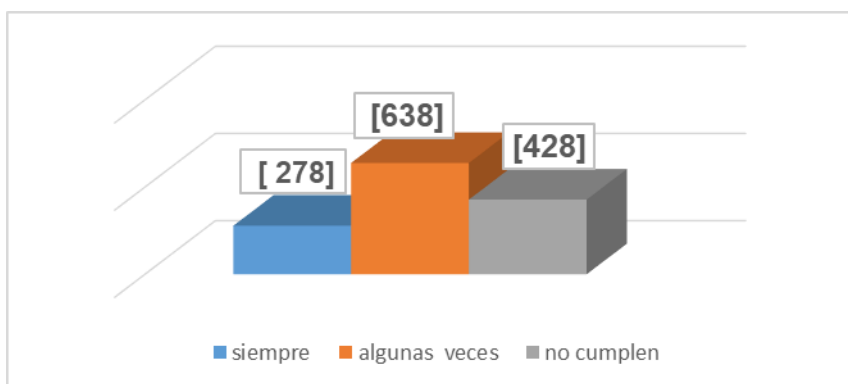


**Figura 1: Mapa de procesos. Fuentes: Manual de Instrucciones y Procedimientos.**

Los sistemas de hardware y software al ser creados por seres humanos y más aún los usuario en sí por su naturaleza, le imprimen a la Informática un sentimiento de inseguridad que debe estar controlado; y nadie mejor que los dueños de cada proceso en conjunto con algún especialista en esta materia, para orientarnos hacia qué medidas efectivas adoptar para estar protegidos.

Actualmente, leyes como Sarbanes-Oxley, la norma ISO 27000, y la norma BASC proporcionan marcos sugeridos de acción para que las empresas implementen e inviertan de manera razonable y a la medida un sistema de S.I.

Para argumentar la investigación se realizó una encuesta a los trabajadores del área de negocio para demostrar el conocimiento de las medidas preventivas para la protección de la información sobre la gestión de los negocios en una empresa, ya que este es un bien de una organización.



**Figura 2: Cantidad de servicios. Fuente: Elaboración propia.**

Según en investigaciones realizadas en más de 1500 organizaciones, de ellas, más de 100 instituciones bancarias, el 75% de estas ha tenido algunos problemas de seguridad informática. De ellas, el 40% ha enfrentado problemas de seguridad, debido a la falta de apoyo de la alta dirección para invertir en medidas y herramientas de seguridad, y solo el 38% se debió a la falta de herramientas adecuadas.

El eslabón más débil de esta cadena en la seguridad lo constituye el factor humano, y no el tecnológico, lo cual destaca la importancia de tener una cultura de seguridad, porque no existe en muchas empresas un responsable de la seguridad informática calificado.

A través del Sistema Bancario y Financiero Cubano (SBFC) transitan anualmente miles de millones de pesos e informaciones financieras que reportan altos negocios nacionales e internacionales, circunstancia que lo convierte en un objetivo apetecido por los que se deciden a delinquir. De esta forma, la prevención y detección de ilegalidades juega un papel significativo. Durante los últimos diez años las nuevas tecnologías de la información modernizaron el funcionamiento de la banca, integrado en sistemas automatizados los procesos de ejecución de las operaciones de las instituciones por lo que hay que continuar trabajando en proteger de forma segura la información.

La elevación de los niveles de seguridad informática se consigue implantando un conjunto de controles, que incluyan políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software, los que deben ser establecidos, implementados,



supervisados y mejorados cuando sea necesario para cumplir los objetivos específicos de seguridad de la organización.

Es por ello que deben ser de amplio dominio de los usuarios de las tecnologías en el BPA, los procedimientos y controles establecidos en el Manual de Instrucción y Procedimiento, pero aún es insuficiente la metodología para proceder con el tema de la protección del flujo de la información por los portadores de datos acerca del tema.

### **Propuesta de acciones para la mejora de la protección de la información:**

No.	Propuesta de Acciones
1	Aprobar en los consejos de dirección del BPA a cada nivel la estrategia empresarial institucional para la protección a la información.
2	Elaborar documento normativo que permita la consulta sistemática de los trabajadores para su buen desempeño en la protección eficiente de la información en las áreas de negocio del BPA.
3	Utilizar la página Web Biblioteca Virtual con una publicación sobre el tema: Medidas de protección a la información de la banca de negocio.
4	Elaborar un plegable con frecuencia mensual como temas de protección a la información de negocio.
5	Realizar intercambio con los trabajadores del área de negocio para precisar los temas sobre la protección a información.

### **Conclusiones**

El estudio del flujo del proceso seleccionado permitió la identificación de los principales problemas que afectan su ejecución.

Los resultados obtenidos en esta investigación, pudieran convertirse en aportes para las entidades bancarias, en busca de la mejora continua de los procesos y poderlas implementar todas las oficinas.

La implementación de las soluciones propuestas, tiene un impacto positivo y determinante en la eficiencia económica y social que se alcanza con el perfeccionamiento de los procesos.

Se realizó un plan de actividades para dotar a la dirección de las herramientas necesarias para la toma de decisiones, el ahorro de tiempo en las operaciones lo que trae implícito la mejora de la calidad del servicio, permitiendo además incrementar la eficiencia y la eficacia de la organización.

## Bibliografía

ÁLVAREZ BASALDÚA, DANIEL Tesis Seguridad en Informática (Auditoría de sistema), Universidad Iberoamericana, México, 2005. (consulta enero 25 de 2017). 2005.

BPA .Manual instrucción y Procedimiento Grupo 00-160 subgrupo 40 Seguridad Informática, título Generalidades. 2019.

BUGARINIS HERNÁNDEZ, FERNANDO. Tesis para obtener grado de maestría en ciencias en administración de negocios, Instituto Politécnico Nacional de México, 2007. (consulta enero 27 de 2017).

GONZÁLEZ ALFONSO BÁRBARO ADRIEL, RIVERO PEÑA CLAUDIO RANGEL; Verdades del correo electrónico; 2014/17 No.1 (página 27 a la 29) Revista del Banco Central de Cuba. 2014.

LÓPEZ MARRERO MERCEDES E TORRES TOLEDO IDANIA. Efectividad de medidas de la banca frente a riesgos informáticos Edición 11 No.2 Revista del Banco Central de Cuba, 2008

PÉREZ GONZÁLEZ, MAYLÉN, RIVERO PEÑA, CLAUDIO RANGEL. Realidades de la Seguridad Informática; Edición 14 No.2 Revista del Banco Central de Cuba. 2011.