



## RESUMEN

---

La liberalización y la globalización de los Servicios Financieros, junto con la creciente sofisticación de la tecnología financiera, están haciendo cada vez más diversas y complejas las actividades en las entidades financieras en términos de seguridad.

En otros tiempos la seguridad de la información era fácilmente administrable, solo bastaba con resguardar los documentos mas importantes bajo llave y mantener seguros a los empleados que poseen conocimiento poniendo guardias de seguridad. Hoy en día es más fácil

Los sistemas electrónicos entraron en las oficinas y obligaron a los sistemas de seguridad a evolucionar para mantenerse al día con la tecnología cambiante. Luego hace unos 9 años, los negocios, aun las empresas más pequeñas, se conectaron a Internet (una amplia red publica con pocas reglas y sin guardianes)

De manera similar a otro tipo de crímenes, el cuantificar los gastos y pérdidas en seguridad de la información o crímenes cibernéticos es muy difícil. Se tiende a minimizar los incidentes por motivos muchas veces justificables. Por otro lado el objetivo fundamental de la seguridad no es proteger los sistemas, sino reducir los riesgos y dar soporte a las operaciones del negocio. La computadora más segura en el mundo es aquella que esta desconectada de cualquier red, enterrada profundamente en algún oscuro desierto y rodeada de guardias armados, pero es también la más inútil.

La seguridad es solo uno de los componentes de la administración de riesgos, minimizar la exposición de la organización y dar soporte a su capacidad de lograr su misión. Para ser efectiva, la seguridad debe estar integrada a los procesos del negocio y no delegada a algunas aplicaciones técnicas.

Los incidentes de seguridad devastadores tienden más a ser internos que externos. Muchos de estos incidentes involucran a alguien llevando a cabo una actividad autorizada de un modo no autorizado. Aunque la tecnología tiene cierta ingerencia en limitar esta clase de eventos internos, las verificaciones y balances como parte de los procesos del negocio son mucho más efectivos.

Las computadoras no atacan a las organizaciones, lo hace la gente. Los empleados bien capacitados tienen mayores oportunidades para detectar y prevenir los incidentes de seguridad antes de que la organización sufra algún daño. Pero para que los empleados sean activos, se requiere que entiendan como reconocer, responder e informar los problemas, lo cual constituye la piedra angular de la organización con conciencia de seguridad lo que nosotros llamamos “cultura de la seguridad”

El presente trabajo describe como se define un plan de seguridad para la una entidad financiera, donde se definen las políticas de seguridad, concluyendo con un plan de implementación o adecuación a las políticas anteriormente definidas.

## ABSTRACT

---

The liberalization and globalization of the financial services with the increasing sophistication of the financial technology are facing more complex a financial enterprise activities in terms of security.

Long time ago, security information was easily management, just it was enough guard the more important documents under the keys and places employees; who has the knowledge; safe, just placing bodyguards; nowadays it is harder.

The electronics systems got in the office and made systems security evolved to be update with the technology changes. Then, 9 years ago, the business; even the small companies were connected to internet (a public network with few rules and without security)

In a similar way of ofther kind of crimes, measure security IT expenses and lost or cybernetic crimes are very difficult. People tend to minimize incidents for justifying reasons.

By the order hand, the main objective of IT Security is not to protect the systems; it is to reduce risks and to support the business operations. The most secure computer in the world is which disconnected form the network, placed is deeply in any dark desert and be surrounded by armed bodyguards, but it is also the most useless.

Security is just one of the components o risk management – minimize the exposition of the business and support the capacity of meet his mission. To be effective, security must be integrated through the business process and not delegate to some technical applications.

The more destructive security incidents tend mostly to be internal instead of external. Many of these involve someone taking an authorized activity in a way non-authorized. Although technology has some concern in limit these kinds of internal

events, the verifications and balances as part of the business process are more affective.

Computers does not attack enterprises, people do it. Employees with Knowledge have more opportunities to detect and prevent security incidents before the enterprises suffer damage. But to make employees more concern, we need that they understand, reply and inform security incidents – which are called “security culture”.

The present work describes how you can define a Security Plan for a financial enterprise, where the politicians of security are defined, concluding with an implementation plan or adaptation to the previously defined politicians.