



IMPLEMENTACIÓN DEL SOFTWARE “POWER-RISK”

MÓDULO DE PREVENCIÓN DE FRAUDE INTERNO

1. ANTECEDENTES y OBJETIVOS

Como es bien conocido, en los últimos años **la gestión de riesgos** en las instituciones financieras ha cobrado vital prioridad e importancia, parte de la cual es la implementación de políticas y procedimientos que garanticen la solvencia y estabilidad de las mismas.

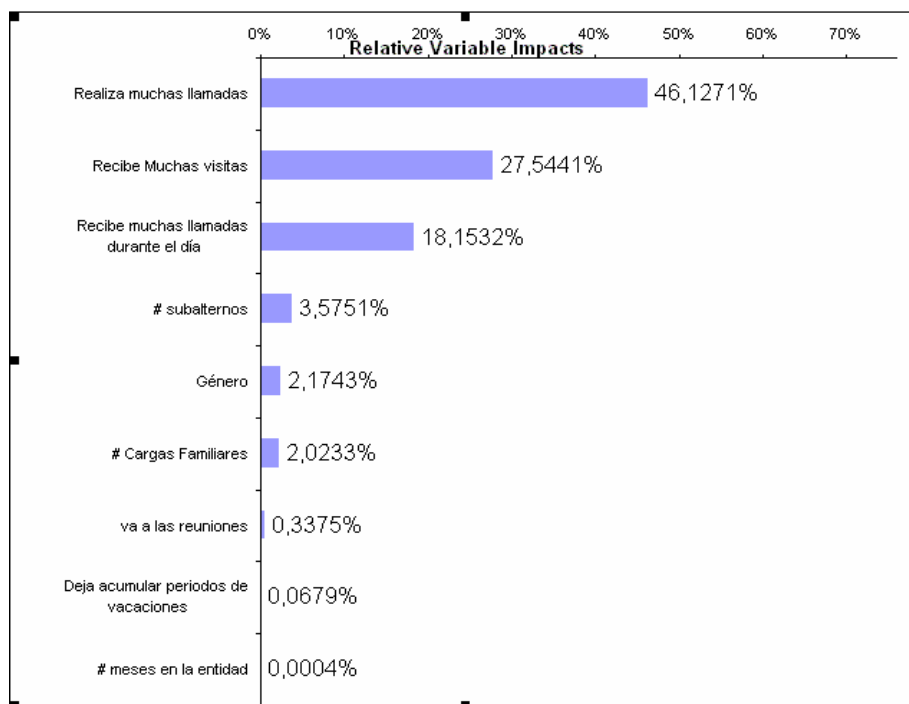
Por ende es necesario el contar con **herramientas cuantitativas** que nos permitan llevar un control sobre dos entes vitales dentro del funcionamiento de las instituciones como son: **los clientes y los funcionarios**.

A continuación se provee una breve descripción del módulo:

Módulo de Prevención de Fraude Interno

Modelo basado en **variables cualitativas y cuantitativas** que nos permite obtener la probabilidad que existe de que **cada uno de los funcionarios cometa fraude interno**, que además nos permite identificar **cuáles son las variables o indicadores clave** que tienen mas impacto en dicha probabilidad.

El módulo es una herramienta indispensable de gestión en el proceso de “**Conozca a su Funcionario**” (KYE), implementado a nivel internacional.



2. PLAN GENERAL

A continuación se listan las **actividades** que forman parte del plan de **implementación del software y capacitación**.

PLAN DE IMPLEMENTACIÓN DE SOFTWARE Y CAPACITACIÓN

FASES:

- ✓ Implementación de herramientas informáticas;
- ✓ Conformación de Base de Datos histórica para alimentar el modelo;
- ✓ Entrenamiento de la Red Neuronal;
- ✓ Capacitación al personal involucrado en la administración del Módulo de Prevención de Fraude Interno.

3. BREVE DESCRIPCIÓN DE LAS ACTIVIDADES A REALIZARSE

FASES:

En esta etapa se realizará la **Implementación del Sistema Informático PowerRisk Módulo de Prevención de Fraude Interno**, herramienta que permite la medición del riesgo y el control los funcionarios que posee una Institución. Dentro de esta etapa de Implementación se considera: **Instalación, Conectividad, Pruebas, Parametrización de la Herramienta, Capacitación, Análisis de indicadores.**

La Parametrización de:

- Sucursales, Oficinas, Agencias;
- Variables Cualitativas;
- Variables Cuantitativas;
- Las Variables Categóricas.

Funcionalidades del Módulo de Prevención de Fraude Interno

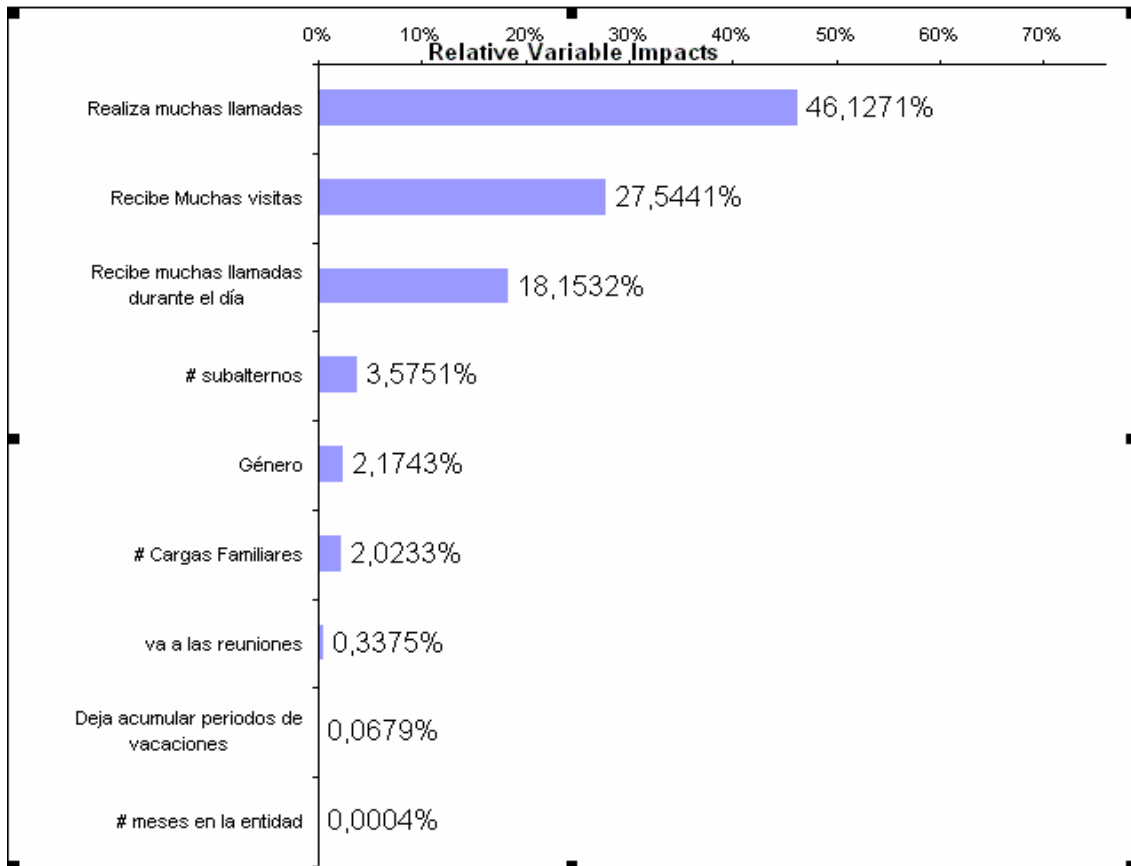
- Facilita la definición de variables Cualitativas, Cuantitativas y Categóricas.
- Permite la conformación de la Base de Datos necesaria para entrenar a la red neuronal.

	J	K	L	M	N	O	P
1			Train-Test Report for "Net Trained on Data Set #1 (2)"				
2	Comete o no Fraude		Tag				
			Used	Prediction	Prediction%	Incorrect%	Good/Bad
3	Comete Fraude		test	Comete Fraude	78,70%	78,70%	Bad
4	No Comete Fraude		test	No Comete Fraude	100,00%	0,00%	Good
5	No Comete Fraude		train				
6	Comete Fraude		train				
7	Comete Fraude		train				
8	No Comete Fraude		train				
9	No Comete Fraude		train				
10	Comete Fraude		train				
11	No Comete Fraude		train				
12	No Comete Fraude		train				
13	No Comete Fraude		test	No Comete Fraude	75,50%	24,50%	Good
14	No Comete Fraude		train				
15	Comete Fraude		train				
16	Comete Fraude		train				
17	No Comete Fraude		train				
18	No Comete Fraude		test	No Comete Fraude	99,65%	0,35%	Good
19	No Comete Fraude		train				
20	No Comete Fraude		train				
21	No Comete Fraude		train				
22	No Comete Fraude		test	No Comete Fraude	81,56%	18,44%	Good
23	Comete Fraude		train				
24	No Comete Fraude		test	No Comete Fraude	100,00%	0,00%	Good
25	No Comete Fraude		train				
26	Comete Fraude		train				
27	No Comete Fraude		train				
28	Comete Fraude		train				
29	No Comete Fraude		test	No Comete Fraude	100,00%	0,00%	Good
30	Comete Fraude		test	Comete Fraude	100,00%	0,00%	Good
31	Comete Fraude		train				
32	No Comete Fraude		train				
33	Comete Fraude		train				
34	Comete Fraude		train				

- Permite el entrenamiento de la red neuronal, a partir de la cual se obtienen:
 - 1) Probabilidades de ocurrencia de un evento de Fraude Interno;
 - 2) Puntajes de riesgo (por funcionario);
 - 3) Predicción de cometimiento de Fraude Interno;
 - 4) Asignación de funcionarios a grupos de Alto Riesgo y Bajo Riesgo;
 - 5) Chequeo interno de la precisión del Modelo.

1	A	B	C	D	E	F	G	H	I	J
SCORING FUNCIONARIOS (CONOZCA A SU FUNCIONARIO)										
2	# meses en la entidad	# Género	# Cargas subalternos	Recibe muchas llamadas durante el día	Realiza muchas llamadas	Recibe Muchas visitas	Deja acumular periodos de vacaciones	va a las reuniones	Comete a no Fraude	
3	100	1	27	6	1	0	1	1	1	1 Comete Fraude
4	63	0	17	2	1	0	1	1	0	0 No Comete Fraude
5	39	0	15	1	1	1	1	0	1	1 No Comete Fraude
6	61	1	6	4	0	1	1	0	0	0 Comete Fraude
7	44	0	4	5	1	0	1	1	1	1 Comete Fraude
8	16	0	23	5	1	0	0	0	0	0 No Comete Fraude
9	60	0	8	2	0	0	0	0	0	1 No Comete Fraude
10	39	1	2	1	1	1	0	0	0	1 Comete Fraude
11	22	0	29	5	0	0	0	0	0	0 No Comete Fraude
12	89	0	25	1	0	0	0	0	0	1 No Comete Fraude
13	85	1	27	6	0	1	0	1	1	1 No Comete Fraude
14	15	1	24	0	1	0	0	0	0	1 No Comete Fraude
15	50	1	2	3	1	1	0	0	0	1 Comete Fraude
16	21	0	5	0	1	1	0	1	1	1 Comete Fraude
17	44	0	13	5	0	1	0	1	0	0 No Comete Fraude
18	48	1	22	6	0	0	0	0	1	1 No Comete Fraude
19	68	0	18	3	1	1	0	1	0	0 No Comete Fraude
20	49	0	30	1	0	1	0	0	1	1 No Comete Fraude
21	95	1	10	5	0	0	0	0	0	0 No Comete Fraude
22	63	1	20	1	0	0	1	0	1	1 No Comete Fraude
23	60	0	18	6	1	1	1	1	1	1 Comete Fraude
24	55	1	11	4	0	1	0	0	0	0 No Comete Fraude
25	17	0	17	1	1	1	0	0	0	0 No Comete Fraude
26	42	1	18	0	1	1	1	1	1	0 Comete Fraude
27	93	1	30	3	1	0	1	0	0	0 No Comete Fraude
28	37	0	15	3	1	1	1	0	0	0 Comete Fraude
29	92	0	20	2	0	0	0	0	0	1 No Comete Fraude
30	66	0	6	5	1	1	1	1	1	1 Comete Fraude
31	47	0	15	3	1	1	1	1	1	1 Comete Fraude
32	18	0	20	5	0	1	0	1	1	0 No Comete Fraude
33	68	1	10	3	1	1	1	1	1	1 Comete Fraude
34	40	1	2	2	1	0	0	0	0	0 Comete Fraude

El Módulo permite además **identificar el impacto** de cada una de las variables que inciden en que el funcionario tienda a cometer Fraude Interno.



Capacitación para la adecuada Administración y Manejo del Aplicativo:

Sesiones de Capacitación para el personal responsable de la Unidad de Riesgos:

- Parametrización del Aplicativo;
- Registro de datos históricos;
- Interpretación de indicadores;
- Generación de Reportes bajo diferentes supuestos y filtros.



Capacitación para personal informático:

- Instalación del Aplicativo;
- Administración de la Base de Datos;
- Parametrizaciones necesarias.

4. ESPECIFICACIONES TÉCNICAS DEL APLICATIVO POWER-RISK, MÓDULO DE PREVENCIÓN DE FRAUDE INTERNO

Características del Software:

- Parametrizable;
- Customizable;
- Cálculo del Impacto de las variables en los indicadores de probabilidad;
- Generación de reportes por filtros múltiples (Ej: sucursal, oficina, agencia, tipo de pérdida, etc.).
- Diseño de tecnología de punta Power Builder V 9;
- Los modelos serán procesados utilizando como núcleo herramientas de Redes Neuronales las cuales determinarán las probabilidades de eventos y el impacto de cada una de las variables; dichas herramientas constituyen modelos informáticos avanzados de punta.
- Adaptable a cualquier base de datos (oracle, sybase, SQL server);

Requerimientos técnicos

- Procesador Pentium IV;
- Sistema operativo Windows 2000, Windows XP;
- 512 MB mínimo (1 GB Recomendado);
- Espacio libre en el disco 5 GB;
- Protocolo de red TCP/IP;
- Cableado de red categoría 5.

Implementación del Sistema

- El sistema se implementará en la base de datos que posee la institución puede ser esta (Oracle, Sybase, SQLserver), en caso contrario se implementará en MySQL que no tiene costos adicionales por licencia.
- La interrelación entre las bases de datos se realizan mediante Triggers (Evento que se ejecuta cuando se cumple una condición establecida), ya sean en las bases de datos de la institución o en la base de datos del sistema.
- Se implementará una carga automática de funcionarios de la institución (si el sistema institucional de control de funcionarios se encuentra en la misma base de datos se implementará a través de triggers); caso contrario se realiza a través de procedimientos, los cuales se trabajarán conjuntamente con el departamento informático de la institución.

Reportes que se generan

La generación de los reportes es por filtros múltiples Ej: (Por sucursal, y tipo de pérdida, agencia, oficial del cliente, etc.)

- Puntajes de riesgo de funcionarios;
- Impacto de las variables más relevantes que tienden a desencadenar en Fraude Interno;
- Reportes de funcionarios y sus probabilidades de realizar Fraude Interno.

Acompañamiento en la implementación

- Se dará soporte y asesoría en la construcción de la base de datos, establecimiento de formatos para recopilación de información.



- Establecimiento de parámetros (Variables Cualitativas y Cuantitativas, Variables Categóricas, etc.)
- Implementación de procedimientos o triggers para carga automática de la información, trabajo conjunto con el departamento de informática de la Institución.
- Pruebas del sistema.
- Manuales de Usuario y de Instalación software Power Risk Módulo Prevención de Fraude Interno.
- Interpretación de resultados.

5. CRONOGRAMA DE TRABAJO

El tiempo estimado Implementación del Software y Capacitación es de 2 meses. Se anexa cronograma de trabajo propuesto.

	MES 1		MES 2	
ACTIVIDADES DE LA IMPLEMENTACIÓN Y CAPACITACIÓN				
FASES:				
Implementación de la herramienta informática				
Conformación real de Base de Datos para alimentar el modelo				
Entrenamiento de Red Neuronal				
Capacitación al personal involucrado en la administración del Sistema				

6. INVERSIÓN

Nota: ESTE MÓDULO PUEDE ADQUIRIRSE ÚNICAMENTE JUNTO CON EL MÓDULO POWER RISK RIESGO OPERATIVO. En ese caso se optimizan costos, por lo que el valor citado incluye el valor de viáticos, hospedaje, traslados y pasajes del personal que realizará la implementación y capacitación de ambos sistemas.

7. VIGENCIA DE LA PROPUESTA

Esta propuesta tiene una vigencia de 15 días a partir de la entrega de la misma.